ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.

«Ελληνικό Πλαίσιο Παροχής Υπηρεσιών
Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας»

Πλαίσιο Ψηφιακής Αυθεντικοποίησης

Έκδοση 3.00

Νοέμβριος 2008

PLANET
ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ

ΠΑΡΟΧΗΣ ΣΥΜΒΟΥΛΕΥΤΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

ΕΡΕΥΝΗΤΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΙΝΣΤΙΤΟΥΤΟ ΣΥΣΤΗΜΑΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΕΡΕΥΝΗΤΙΚΗ ΜΟΝΑΔΑ eGovernment

ATHENS TECHNOLOGY CENTER A.B.E.T.E.

ΕΛΕΓΧΟΣ ΕΓΓΡΑΦΟΥ – ΙΣΤΟΡΙΚΟ ΕΚΔΟΣΕΩΝ

Ημερομηνία	Έκδοση	Συγγραφείς	Αλλαγές
15/10/2007	1.00	PLANET – ΕΠΙΣΕΥ – ATC Πανεπιστήμιο Αιγαίου	Έκδοση 1.00
25/05/2008	2.00	PLANET – ΕΠΙΣΕΥ – ATC Πανεπιστήμιο Αιγαίου	Έκδοση 2.00
10/11/2008	3.00	PLANET – ΕΠΙΣΕΥ – ATC Πανεπιστήμιο Αιγαίου	Έκδοση 3.00

ΑΚΡΩΝΥΜΙΑ – ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Όρος/ Ακρωνύμιο	Επεξήγηση
A.G.A.F.	Australian Government e-Authentication Framework
e-GIF	E-government Interoperability Framework
E-ID	Μοναδικό Ηλεκτρονικό Αναγνωριστικό
G2G	Government to Government
P.I.N.	Προσωπικός Κωδικός Πρόσβασης
P.K.I.	Public Key Infrastructure
SSL	Secure Socket Layer
V.I.E.S.	Ανακεφαλαιωτικός Πίνακας Ενδοκοινοτικών Αποκτήσεων / Παραδόσεων
V.P.N.	Virtual Private Network
Α.Δ.	Αριθμός Διαβατηρίου
Α.Δ.Α.Ε.	Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
Α.Δ.Τ.	Αριθμός Δελτίου Ταυτότητας
Α.Μ.Ε.	Αριθμός Μητρώου Εργαζομένου
Α.Μ.Κ.Α.	Αριθμός Μητρώου Κοινωνικής Ασφάλισης
Α.Π.Δ.	Αναλυτική Περιοδική Δήλωση
Α.Σ.Ε.Π	Ανώτατο Συμβούλιο Επιλογής Προσωπικού
Α.Φ.Ε	Αποδεικτικό Φορολογικής Ενημερότητας
Α.Φ.Μ.	Αριθμός Φορολογικού Μητρώου
Δ.Δ.	Δημόσια Διοίκηση
Δ.Ο.Υ.	Δημόσια Οικονομική Υπηρεσία
Ε.Κ.Α.Μ	Ενιαίος Κωδικός Αριθμός Μητρώου
Η.Δ.Υ.	Ηλεκτρονικά Διαθέσιμη Υπηρεσία
Ι.Κ.Α.	Ίδρυμα Κοινωνικών Ασφαλίσεων

Όρος/ Ακρωνύμιο	Επεξήγηση
ΚΔΠ	Κεντρική Διαδικτυακή Πύλη
Ν.Π.Δ.Δ	Νομικό Πρόσωπο Δημόσιου Δικαίου
Ν.Π.Ι.Δ	Νομικό Πρόσωπο Ιδιωτικού Δικαίου
Ο.Τ.Α.	Οργανισμός Τοπικής Αυτοδιοίκησης
Π.Δ.	Προεδρικό Διάταγμα
ΠΨΑ	Πλαίσιο Ψηφιακής Αυθεντικοποίησης
Υ.Δ.Κ.	Υποδομή Δημόσιου Κλειδιού
ΥΑ	Υπουργική Απόφαση
ΥΠΕΣ	Υπουργείο Εσωτερικών
Φ.Δ.Π.	Φορέας Διαχείρισης Πλαισίου
Φ.Ε.Κ.	Φύλλο Εφημερίδας της Κυβερνήσεως
Φ.Π.Α.	Φόρος Προστιθέμενης Αξίας

ΟΡΟΛΟΓΙΑ

Όρος	Επεξήγηση
Audit Service	Υπηρεσία Εποπτείας
Authorization	Εξουσιοδότηση
Back-office	Υποστηρικτικά πληροφοριακά συστήματα
Brute Force Attack	Επίθεση Εξαντλητικής Αναζήτησης
Buffer Overflow	Υπερχείλιση Προσωρινών Χώρων Αποθήκευσης
Clear Text	Καθαρή Μορφή
Confidentiality	Εμπιστευτικότητα
Credential	Διαπιστευτήριο
Digital Certificate	Ψηφιακό Πιστοποιητικό
Eavesdropping	Υποκλοπή επικοινωνίας-δεδομένων
Flooding Attack	Επίθεση Πλημμύρας
Front-Office	Πληροφοριακά Συστήματα Λειτουργίας
Impact	Αρνητική Συνέπεια
Impersonation Attack	Επίθεση πλαστοπροσωπίας
Injection Attack	Επίθεση με προσθήκη κακόβουλου κώδικα
Intranet	Ιδιωτικό Δίκτυο
Man-in-the-Middle Attack	Επίθεση Ενδιάμεσου
One-Time Password	Συνθηματικό Μιας Χρήσης
On-the-fly	Σε πραγματικό χρόνο
Owner	Ιδιοκτήτης
Outsourcing	Εξωτερική ανάθεση
Password	Συνθηματικό
Patch	Πακέτο Αναβάθμισης Λογισμικού
Privacy	Ιδιωτικότητα

Όρος	**Επεξήγηση**
Public Key Infrastructure	Υποδομή Δημόσιου Κλειδιού
Registration Repudiation	Αποποίηση Εγγραφής
Replay attack	Επίθεση Επανάληψης
Risk Assessment	Αποτίμηση Επικινδυνότητας
Secure Channel	Ασφαλές Κανάλι Επικοινωνίας
Session hijacking	Υποκλοπή Συνόδου
Spoofing	Απόκρυψη Ταυτότητας
Threat	Δυνητική Απειλή
Virtual Private Network	Εικονικό Ιδιωτικό Δίκτυο
Vulnerability	Σημείο Ευπάθειας
Worm	Σκουλήκι

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

1. ΕΠΙΤΕΛΙΚΗ ΣΥΝΟΨΗ

1.1 Ποιος είναι ο σκοπός του παρόντος εγγράφου

Το παρόν έγγραφο περιλαμβάνει το **Πλαίσιο Ψηφιακής Αυθεντικοποίησης** (Έκδοση 3.00) και αποτελεί μέρος της Γ' έκδοσης του Πλαισίου Ηλεκτρονικής Διακυβέρνησης. Σκοπός του Πλαισίου Ψηφιακής Αυθεντικοποίησης (ΠΨΑ) είναι να υποστηρίξει τους φορείς της Δημόσιας Διοίκησης που προσφέρουν υπηρεσίες ηλεκτρονικής διακυβέρνησης, στην επιλογή των κατάλληλων μηχανισμών αυθεντικοποίησης και στον καθορισμό των διαδικασιών εγγραφής και ταυτοποίησης των χρηστών.

1.2 Ποιοι πρέπει να διαβάσουν το παρόν έγγραφο

Το Πλαίσιο Ψηφιακής Αυθεντικοποίησης απευθύνεται σε όλους όσοι εμπλέκονται στη διαδικασία σχεδιασμού και ανάπτυξης νέων ηλεκτρονικών υπηρεσιών, καθώς και σε πολίτες, επιχειρήσεις και φορείς που αξιοποιούν τις προσφερόμενες ηλεκτρονικές υπηρεσίες. Ειδικότερα απευθύνεται σε:

- Ανώτερα στελέχη του δημόσιου και ιδιωτικού τομέα με αρμοδιότητες λήψης αποφάσεων, το ενδιαφέρον των οποίων εστιάζεται, χωρίς όμως να περιορίζεται, σε κανόνες και οδηγίες που διατυπώνονται σχετικά με τη στρατηγική, τις βασικές αρχές και τις πολιτικές για την αυθεντικοποίηση των πολιτών και επιχειρήσεων στις ηλεκτρονικές υπηρεσίες των φορέων του Δημοσίου.
- Επιχειρησιακά στελέχη των φορέων της Δημόσιας Διοίκησης και μονάδων τους που ασχολούνται με θέματα οργάνωσης και βελτίωσης διαδικασιών, το ενδιαφέρον των οποίων εστιάζεται, χωρίς όμως να περιορίζεται, σε κανόνες και οδηγίες που διατυπώνονται για οργανωτικά και επιχειρησιακά θέματα των φορέων αναφορικά με τους ρόλους, τις αρμοδιότητες και τις διαδικασίες που απαιτούνται για την υποστήριξη της λειτουργίας και τη συνεχή βελτίωση των παρεχόμενων ηλεκτρονικών υπηρεσιών.
- Στελέχη των διευθύνσεων πληροφορικής των φορέων της Δημόσιας Διοίκησης, αναδόχους έργων ανάπτυξης πληροφοριακών συστημάτων και διαδικτυακών τόπων, κατασκευαστές λογισμικού ανάπτυξης διαδικτυακών τόπων και παρόχους συναφών υπηρεσιών, το ενδιαφέρον των οποίων εστιάζεται, χωρίς όμως να περιορίζεται, σε κανόνες και οδηγίες που διατυπώνονται για τεχνικά θέματα που αφορούν στο σχεδιασμό και την ανάπτυξη ηλεκτρονικών υπηρεσιών.

1.3 Γιατί το ΠΨΑ είναι χρήσιμο

Όλες οι ηλεκτρονικές υπηρεσίες που σήμερα προσφέρονται από την Ελληνική Δημόσια Διοίκηση, αξιοποιούν ως μέθοδο ταυτοποίησης και αυθεντικοποίησης τη χρήση ονομάτων χρηστών και συνθηματικών (user name και password) για την επιβεβαίωση της ηλεκτρονικής ταυτότητας των χρηστών. Το γεγονός ότι η επιλογή της συγκεκριμένης μεθόδου αυθεντικοποίησης δε λαμβάνει υπόψη της την κρισιμότητα των υπηρεσιών, σε ότι αφορά τις

επιπτώσεις που είναι δυνατόν να προκληθούν στο φορέα και στο χρήστη σε περίπτωση εκδήλωσης κάποιου περιστατικού ασφάλειας, εγείρει μείζονα ερωτήματα αναφορικά με την καταλληλότητα του συγκεκριμένου μηχανισμού αυθεντικοποίησης, όπως επίσης και για την καταλληλότητα και αξιοπιστία των αντίστοιχων διαδικασιών εγγραφής και ταυτοποίησης.

Το ΠΨΑ αποσκοπεί στη θέσπιση κανόνων και οδηγιών για την ιεράρχηση της κρισιμότητας κάθε ηλεκτρονικής υπηρεσίας και συνεπώς την επιλογή των μηχανισμών αυθεντικοποίησης με τρόπο σαφή, απλό, μεθοδικό και καλά τεκμηριωμένο. Οι κανόνες και οδηγίες του ΠΨΑ βασίζονται, κατά κύριο λόγο, στο ισχύον νομικό και κανονιστικό πλαίσιο για την προστασία των προσωπικών και ευαίσθητων προσωπικών δεδομένων, καθώς και στην προστασία της ιδιωτικότητας του πολίτη.

Η υιοθέτηση του ΠΨΑ από τους φορείς της Δημόσιας Διοίκησης, ακολουθώντας ουσιαστικά τις επιταγές του εθνικού και ευρωπαϊκού νομοθέτη, αναμένεται να βελτιώσει σημαντικά την ασφάλεια των ηλεκτρονικών συναλλαγών, εφαρμόζοντας την «*αρχή της αναλογικότητας*» κατά τη διαδικασία επιλογής των μηχανισμών αυθεντικοποίησης: όσο πιο σοβαρές είναι οι επιπτώσεις που μπορεί να προκύψουν από τη μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση των δεδομένων που αξιοποιεί μια υπηρεσία, τόσο πιο ισχυροί πρέπει να είναι οι μηχανισμοί αυθεντικοποίησης. Επιπλέον, η εφαρμογή των οδηγιών του ΠΨΑ εξασφαλίζει τη συμμόρφωση του φορέα με τις διατάξεις του νομικού και κανονιστικού πλαισίου για την προστασία των προσωπικών, ευαίσθητων προσωπικών και οικονομικών δεδομένων που ανταλλάσσονται στις ηλεκτρονικές συναλλαγές.

Για τους αναδόχους έργων ανάπτυξης ηλεκτρονικών υπηρεσιών για δημόσιους φορείς και τους κατασκευαστές σχετικού λογισμικού, η εφαρμογή του ΠΨΑ θα τους δώσει τη δυνατότητα να δημιουργήσουν προϊόντα και εφαρμογές που θα ανταποκρίνονται σε ένα σύνολο κοινών προδιαγραφών αυθεντικοποίησης, οι οποίες θα είναι γνωστές εκ των προτέρων και δε θα διαφοροποιούνται σημαντικά από έργο σε έργο.

1.4 Βασικές αρχές και περιεχόμενα του ΠΨΑ

Η κύρια συνεισφορά του ΠΨΑ είναι η παροχή συγκεκριμένων κατευθυντηρίων κανόνων και οδηγιών, βασισμένων στο ισχύον νομικό – κανονιστικό πλαίσιο, για:

- Την κατηγοριοποίηση των δεδομένων που επεξεργάζονται οι ηλεκτρονικές υπηρεσίες σε «Απλά», «Οικονομικά» ή «Ευαίσθητα» (βλέπε και ενότητα 9.1.1) Ο ν. 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως ισχύει, ορίζει τα δεδομένα προσωπικού χαρακτήρα (άρθρο 2α) καθώς και τα ευαίσθητα δεδομένα (άρθρο 2β). Τα λεγόμενα «οικονομικά δεδομένα» εμπίπτουν στην κατηγορία των «απλών δεδομένων» με την επιφύλαξη δεδομένων που σχετίζονται με τη λήψη παροχών κοινωνικής πρόνοιας, τα οποία ο νόμος κατατάσσει στα ευαίσθητα. Τα οικονομικά δεδομένα δεν ορίζονται νομοθετικά. Ωστόσο εκτιμάται ότι παρόλο που τα οικονομικά δεδομένα εντάσσονται στα «απλά δεδομένα» η χρήση τους ενέχει ορισμένους πρόσθετους κινδύνους για τα υποκείμενα και ως εκ τούτου υπάρχουν περιπτώσεις οικονομικών συναλλαγών που εντάσσονται στα ευαίσθητα δεδομένα (βλέπε ενότητα 9.1.1). Ελλείψει νομοθετικού ορισμού, ως «οικονομικά δεδομένα» νοούνται οι πληροφορίες που

καλύπτονται από το φορολογικό απόρρητο, δηλ. «οι φορολογικές δηλώσεις, τα φορολογικά στοιχεία, οι εκθέσεις και κάθε άλλο στοιχείο του φακέλου που έχει σχέση με τη φορολογία ή άπτεται αυτής» (άρθρο 85 Κώδικα Φορολογικών Στοιχείων).

- Τον καθορισμό **«επιπέδων εμπιστοσύνης»** για τις ηλεκτρονικές υπηρεσίες, με βάση την κατηγορία των δεδομένων που αξιοποιούν, αλλά και λαμβάνοντας υπόψη τις πιθανές επιπτώσεις που μπορεί να προκληθούν σε περίπτωση μη ορθής λειτουργίας ή διαχείρισής τους.
- Τη συσχέτιση κάθε επιπέδου εμπιστοσύνης με κατάλληλα **«επίπεδα αυθεντικοποίησης»**, όπου για κάθε επίπεδο αυθεντικοποίησης έχουν οριστεί συγκεκριμένοι μηχανισμοί αυθεντικοποίησης.
- Τη συσχέτιση κάθε επιπέδου εμπιστοσύνης με τις κατάλληλες **«διαδικασίες εγγραφής»** των χρηστών στην υπηρεσία.

Οι φορείς της Δημόσιας Διοίκησης που σχεδιάζουν και αναπτύσσουν ηλεκτρονικές υπηρεσίες θα πρέπει να ακολουθήσουν τα παρακάτω βασικά βήματα, όπως αυτά προβλέπονται στο παρόν ΠΨΑ:

- Να προσδιορίσουν το **επίπεδο εμπιστοσύνης** στο οποίο εντάσσεται η υπηρεσία, αφού πρώτα προσδιορίσουν επακριβώς τις κατηγορίες δεδομένων που αξιοποιούνται.
- Ανάλογα με το επίπεδο εμπιστοσύνης και ακολουθώντας τις συστάσεις του παρόντος ΠΨΑ, να επιλέξουν τον κατάλληλο **μηχανισμό αυθεντικοποίησης**.
- Ανάλογα με το επίπεδο εμπιστοσύνης και ακολουθώντας τις συστάσεις του παρόντος ΠΨΑ, να υιοθετήσουν τις απαραίτητες **διαδικασίες εγγραφής** των χρηστών.

1.5 Ποιος διαχειρίζεται το ΠΨΑ

Η διαχείριση του ΠΨΑ γίνεται για όλο το δημόσιο τομέα σε κεντρικό επίπεδο από το Φορέα Διαχείρισης του Πλαισίου (ΦΔΠ). Οι αρμοδιότητες του ΦΔΠ περιλαμβάνουν τον καθορισμό της στρατηγικής για τις διαδικασίες εγγραφής, ταυτοποίησης και αυθεντικοποίησης των χρηστών ηλεκτρονικών υπηρεσιών, τον καθορισμό των οδηγιών και προτύπων του ΠΨΑ, τη διάδοση του ΠΨΑ, την παρακολούθηση της εφαρμογής του Πλαισίου, την αξιολόγηση των προτάσεων ανανέωσης και τη συντήρηση του Πλαισίου. Μέχρι τον προσδιορισμό ή τη σύσταση του φορέα που θα αναλάβει το ρόλο του ΦΔΠ και μέχρι το τέλος του έργου «**Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και Πρότυπα Διαλειτουργικότητας**» (τέλος 2008), οι αρμοδιότητες του ΦΔΠ για τη συντήρηση του Πλαισίου θα ασκούνται από τον ανάδοχο του παραπάνω έργου, δηλαδή την ένωση νομικών προσώπων «**PLANET Α.Ε. – ΕΠΙΣΕΥ/ΕΜΠ – ATC ABETE**», σε συνεργασία με τα στελέχη της Αναθέτουσας Αρχής (**Κοινωνία της Πληροφορίας Α.Ε.**) και του φορέα για τον οποίο προορίζεται το έργο (**Υπουργείο Εσωτερικών**) και ιδιαίτερα τα στελέχη της Επιτροπής Παρακολούθησης και Παραλαβής του Έργου.

1.6 Πώς μπορεί κάποιος να προτείνει αλλαγές στο ΠΨΑ

Το ΠΨΑ, το οποίο είναι διαθέσιμο στην ηλεκτρονική διεύθυνση www.e-gif.gov.gr, δεν αποτελεί ένα στατικό σύνολο κανόνων, οδηγιών, προτύπων και προδιαγραφών σχετικά με τους μηχανισμούς ψηφιακής αυθεντικοποίησης, αντίθετα υπόκειται σε διαρκή αυστηρή και λεπτομερή διαδικασία επανεξέτασης και αναθεώρησης. Καθ' όλη τη διάρκεια ισχύος μιας έκδοσης του Πλαισίου, όλοι οι εμπλεκόμενοι έχουν δικαίωμα υποβολής προτάσεων και σχολίων για το περιεχόμενο του Πλαισίου. Οι προτάσεις μπορεί να αφορούν αλλαγές ή διορθώσεις σε υφιστάμενους κανόνες και πρότυπα ή προσθήκες που πρέπει να γίνουν στο Πλαίσιο ώστε να οριοθετηθούν καλύτερα ορισμένα θέματα ή να καλυφθούν νέοι τομείς. Οι προτάσεις μπορούν να υποβάλλονται μέσω ηλεκτρονικού ταχυδρομείου στη διεύθυνση plaisio@ypesdda.gov.gr, καθώς και στο διαδικτυακό τόπο www.e-gif.gov.gr. Οι προτάσεις αξιολογούνται από το ΦΔΠ και όσες γίνουν αποδεκτές ενσωματώνονται στην επόμενη έκδοση του Πλαισίου. Είναι επίσης δυνατή η επικοινωνία με το ΦΔΠ στο τηλέφωνο 213-1300866.

1.7 Αλλαγές από την προηγούμενη έκδοση

Το παρόν έγγραφο αποτελεί την τρίτη έκδοση του Πλαισίου Ψηφιακής Αυθεντικοποίησης. Η τρίτη έκδοση του Πλαισίου δεν διαφέρει από τη δεύτερη έκδοσή του όσον αφορά στη δομή και το περιεχόμενό της, καθώς δεν υποβλήθηκαν σχόλια και παρατηρήσεις από επιχειρήσεις, αναδόχους έργων ηλεκτρονικής διακυβέρνησης, την Αναθέτουσα Αρχή και το φορέα για τον οποίο προορίζεται το έργο (Υπουργείο Εσωτερικών) κατά τη διαβούλευση του Πλαισίου (Ιούνιος-Οκτώβριος 2008). Βασική διαφοροποίηση της παρούσας έκδοσης του Πλαισίου από την προηγούμενη αποτελεί η προσθήκη του Κεφαλαίου 15 «ΠΑΡΑΡΤΗΜΑ Δ: ΟΜΟΣΠΟΝΔΕΣ ΤΑΥΤΟΤΗΤΕΣ (FEDERATED IDENTITIES)».

2. ΕΙΣΑΓΩΓΗ

Σκοπός του **Πλαισίου Ψηφιακής Αυθεντικοποίησης** είναι η υποστήριξη των φορέων Δημόσιας Διοίκησης που παρέχουν ή σχεδιάζουν να παρέχουν ηλεκτρονικές υπηρεσίες προς τους συναλλασσόμενους με αυτούς φορείς, επιχειρήσεις και πολίτες, αναφορικά με την επιλογή των κατάλληλων μηχανισμών αυθεντικοποίησης και εγγραφής των χρηστών.

Η υιοθέτηση των οδηγιών και κατευθύνσεων του ΠΨΑ θα επιτρέψει τη βελτίωση του επιπέδου ασφάλειας των παρεχόμενων υπηρεσιών από φορείς της Δημόσιας Διοίκησης, επιτρέποντας τη βελτίωση της συνολικής λειτουργίας της ελληνικής Δημόσιας Διοίκησης.

Το ΠΨΑ αποτελεί σημαντική παράμετρο της στρατηγικής της Ελληνικής Δημόσιας Διοίκησης για τη μετάβαση και προσαρμογή των υπηρεσιών της στις απαιτήσεις της σύγχρονης εποχής και την εναρμόνισή τους με την ευρωπαϊκή πολιτική και κατευθύνσεις.

2.1 Αρχιτεκτονική του Πλαισίου Ηλεκτρονικής Διακυβέρνησης

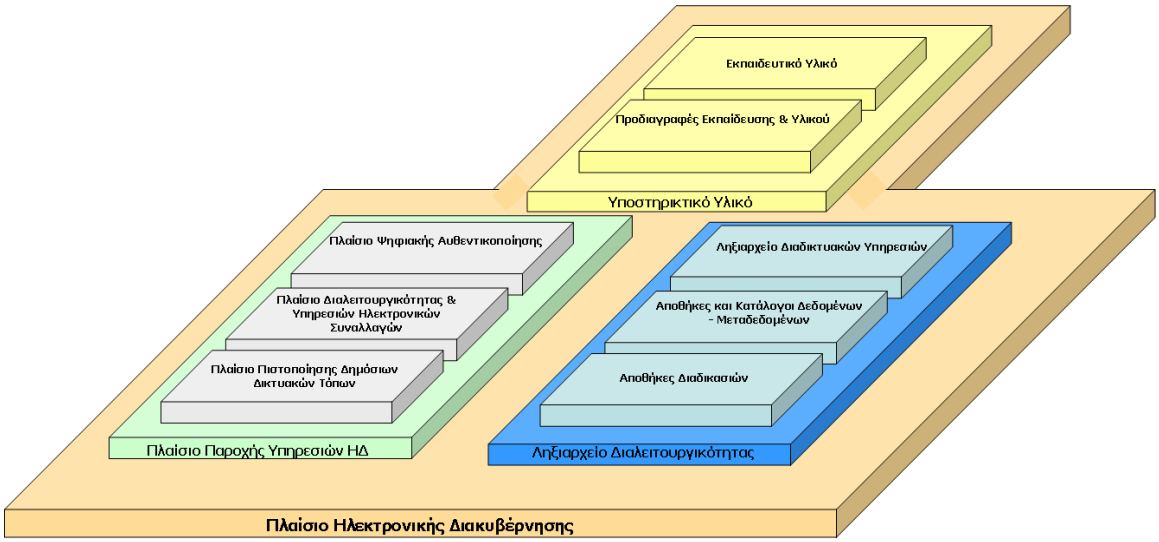
Το Πλαίσιο Ηλεκτρονικής Διακυβέρνησης περιλαμβάνει τρία επιμέρους πλαίσια, καθένα από τα οποία ρυθμίζει συγκεκριμένες πτυχές της Ηλεκτρονικής Διακυβέρνησης:

- Το Πλαίσιο Πιστοποίησης Δημόσιων Διαδικτυακών Τόπων (ΠΠ-ΔΔΤ)
- Το Πλαίσιο Διαλειτουργικότητας & Υπηρεσιών Ηλεκτρονικών Συναλλαγών (ΠΔ&ΥΗΣ)
- Το Πλαίσιο Ψηφιακής Αυθεντικοποίησης (ΠΨΑ)

Σε αντιστοιχία με τις καλυπτόμενες υπηρεσίες του ΠΔ&ΥΗΣ, το Πλαίσιο παρέχει επίσης έναν ταμιευτήρα (Ληξιαρχείο Διαλειτουργικότητας), ο οποίος περιέχει:

- Τυποποιημένες, πρότυπες περιγραφές διαδικασιών
- Τυποποιημένα σχήματα δεδομένων και μεταδεδομένων
- Τις καλυπτόμενες ηλεκτρονικές υπηρεσίες ανά φορέα, σε διαφορετικά επίπεδα ηλεκτρονικής ολοκλήρωσης

Επιπλέον, το Πλαίσιο συμπληρώνεται από ενέργειες εκπαίδευσης, εκπαιδευτικό υλικό και υλικό διάδοσης.



Σχήμα 1: Αρχιτεκτονική του Πλαισίου Ηλεκτρονικής Διακυβέρνησης

2.2 Πλαίσιο Ψηφιακής Αυθεντικοποίησης

Το παρόν έγγραφο αποτελεί το τρίτο μέρος του Πλαισίου Ηλεκτρονικής Διακυβέρνησης, το **Πλαίσιο Ψηφιακής Αυθεντικοποίησης (ΠΨΑ)**. Σκοπός του Πλαισίου Ψηφιακής Αυθεντικοποίησης είναι να υποστηρίξει τους φορείς της Δημόσιας Διοίκησης που προσφέρουν υπηρεσίες ηλεκτρονικής διακυβέρνησης, στην επιλογή των κατάλληλων μηχανισμών αυθεντικοποίησης και στον καθορισμό των διαδικασιών εγγραφής και ταυτοποίησης των χρηστών.

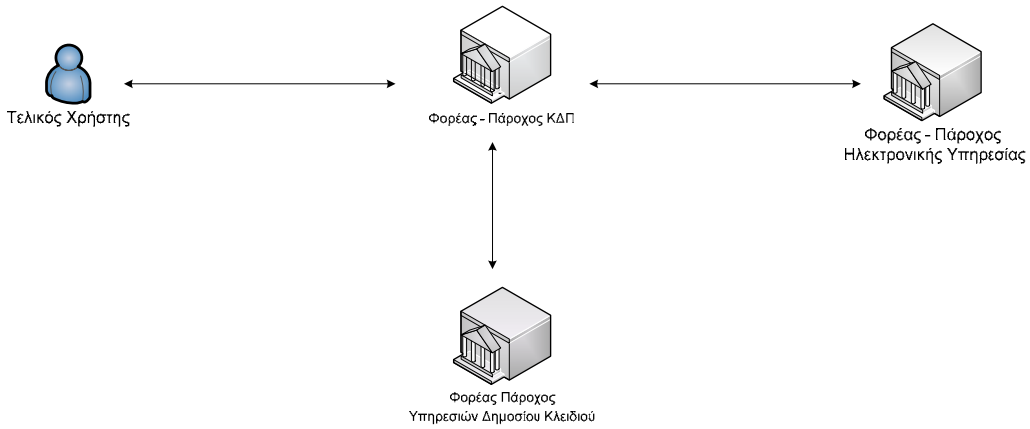
Το Πλαίσιο Ψηφιακής Αυθεντικοποίησης απαιτεί τη συμμόρφωση όλων των οντοτήτων που εμπλέκονται στις υπηρεσίες ηλεκτρονικής διακυβέρνησης με στόχο την επίτευξη ενός ασφαλούς και έμπιστου περιβάλλοντος για την ορθή διεκπεραίωση αυτών μέσω του Διαδικτύου. Συγκεκριμένα οι εμπλεκόμενες οντότητες και οι οδηγίες / κανόνες του ΠΨΑ που αφορούν την κάθε συγκεκριμένη οντότητα παρουσιάζονται στον πίνακα που ακολουθεί:

Εμπλεκόμενες Οντότητες	Κανόνες του ΠΨΑ που πρέπει να εφαρμόζονται
Ο Φορέας πάροχος της ηλεκτρονικής υπηρεσίας	Ο πάροχος της ηλεκτρονικής υπηρεσίας πρέπει να καθορίζει τα δεδομένα που εμπλέκονται στην προσφερόμενη υπηρεσία με στόχο να τα κατατάσσει σε μια από τις κατηγορίες της ενότητας 9.1.1 και στη συνέχεια να αποφασίζει για τα επίπεδα εμπιστοσύνης (ενότητες 4, 9.1.2 και 9.1.3), εγγραφής (ενότητες 8, 9.1.2 και 9.1.3) και αυθεντικοποίησης (ενότητες 7, 9.1.2 και 9.1.3) στα οποία θα ενταχθεί η υπηρεσία. Για να εξασφαλιστεί η συμμόρφωση με το ισχύον θεσμικό κανονιστικό πλαίσιο και τα προβλεπόμενα από το ΠΨΑ, οι φορείς του δημοσίου που προσφέρουν ηλεκτρονικές υπηρεσίες θα πρέπει να ικανοποιούν τους κανόνες της ενότητας 10.1. Επίσης ο φορέας είναι υπεύθυνος για τη διασφάλιση της συμμόρφωσης της προσφερόμενης ηλεκτρονικής υπηρεσίας, αναφορικά με τις διαδικασίες εγγραφής και αυθεντικοποίησης που υιοθετούνται, με τους κανόνες που ορίζει το ΠΨΑ στην ενότητα 10.2.

Εμπλεκόμενες Οντότητες	Κανόνες του ΠΨΑ που πρέπει να εφαρμόζονται
Ο Φορέας πάροχος της Κεντρικής Διαδικτυακής Πύλης (ΚΔΠ)	Η συνολική αρχιτεκτονική της ΚΔΠ, οι μηχανισμοί ταυτοποίησης που υιοθετούνται και τα γενικότερα μέτρα ασφάλειας που υλοποιεί για την προστασία των ηλεκτρονικών υπηρεσιών, θα πρέπει να ικανοποιούν τους κανόνες που καθορίζει το ΠΨΑ στην ενότητα 10.3.
Ο Φορέας πάροχος Υπηρεσιών Δημοσίου Κλειδιού	Όλοι οι Πάροχοι Υπηρεσιών Δημοσίου Κλειδιού θα πρέπει να συμμορφώνονται με τους κανόνες που καθορίζει το ΠΨΑ στην ενότητα 10.4.
Ο Τελικός Χρήστης	Οι τελικοί χρήστες θα πρέπει να είναι ενήμεροι για τα προβλεπόμενα στην ενότητα 9.2 του ΠΨΑ.

Πίνακας 1: Κανόνες ΠΨΑ

Η γενική αρχιτεκτονική του ΠΨΑ παρουσιάζεται στο σχήμα που ακολουθεί.



Σχήμα 2: Γενική Αρχιτεκτονική του ΠΨΑ

Συνοπτικά, οι φορείς προσφέρουν τις υπηρεσίες τους μέσω της ΚΔΠ, αφού πρώτα δηλώσουν τις απαιτήσεις τους για κάθε υπηρεσία (επίπεδο εμπιστοσύνης, αυθεντικοποίησης, εγγραφής), καθώς επίσης και τα απαιτούμενα δικαιολογητικά που πρέπει οι χρήστες να υποβάλλουν κατά τη διαδικασία εγγραφής. Οι τελικοί χρήστες, αφού αρχικά εγγραφούν στην ηλεκτρονική υπηρεσία μέσω της ΚΔΠ, μπορούν να αξιοποιήσουν τις προσφερόμενες ηλεκτρονικές υπηρεσίες αφού πρώτα ελεγχθεί και διαπιστωθεί η ορθότητα της ηλεκτρονικής τους ταυτότητας.

2.3 Βασικές Έννοιες του ΠΨΑ

Βασική έννοια	Περιγραφή
Πλαίσιο Ψηφιακής Αυθεντικοποίησης	Ως Πλαίσιο Ψηφιακής Αυθεντικοποίησης, υπό το πρίσμα του Πλαισίου Ηλεκτρονικής Διακυβέρνησης, θεωρείται το σύνολο των απαιτουμένων διαδικασιών αναφορικά με (α) την εγγραφή (β) την ταυτοποίηση και (γ) την αυθεντικοποίηση που πρέπει να ακολουθούνται από τις εμπλεκόμενες οντότητες για την επίτευξη του επιθυμητού επιπέδου ασφάλειας και εμπιστοσύνης μεταξύ των συναλλασσομένων οντοτήτων.
Απαιτήσεις Ασφάλειας	Ως απαιτήσεις ασφάλειας θεωρούνται οι ιδιότητες-χαρακτηριστικά ασφάλειας (Ιδιωτικότητα, Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση), οι οποίες απαιτείται να διασφαλίζονται κατά την παροχή μιας ηλεκτρονικής υπηρεσίας.
Ιδιωτικότητα	Ως ιδιωτικότητα νοείται η μη αποκάλυψη προσωπικών πληροφοριών σε μη εξουσιοδοτημένες οντότητες.
Εμπιστευτικότητα	Ως Εμπιστευτικότητα θεωρείται η διαδικασία διασφάλισης μη εξουσιοδοτημένης αποκάλυψης των δεδομένων που αξιοποιούνται κατά τη διεκπεραίωση μιας συναλλαγής.
Ακεραιότητα Δεδομένων	Ως ακεραιότητα των δεδομένων θεωρείται η διαδικασία διασφάλισης μη εξουσιοδοτημένης τροποποίησης των δεδομένων που αξιοποιούνται κατά τη διεκπεραίωση μιας συναλλαγής.
Αυθεντικοποίηση	Ως αυθεντικοποίηση θεωρείται η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Συγκεκριμένα, κατά τη διαδικασία αυθεντικοποίησης αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός χρήστη ή κάποιων χαρακτηριστικών της.
Διαπιστευτήρια-Μηχανισμός Αυθεντικοποίησης	Ως διαπιστευτήρια νοούνται τα εχέγγυα που παρουσιάζει μια οντότητα προκειμένου να αποδείξει τη γνησιότητα ενός ισχυρισμού και συγκεκριμένα της ταυτότητας ή του ρόλου της.
Επίπεδο Εμπιστοσύνης	Η «εμπιστοσύνη» ερμηνεύεται ως «η πίστη στην αξιοπιστία, εντιμότητα, αξία ή ικανότητα κάποιας οντότητας». Υπό το πρίσμα του ΠΨΑ, ως επίπεδο εμπιστοσύνης θεωρείται ο βαθμός βεβαιότητας που έχει μια υπηρεσία για την ορθότητα τόσο της ταυτότητας της ηλεκτρονικής οντότητας που επιθυμεί να διεκπεραιώσει μια συναλλαγή στο πλαίσιο μιας ηλεκτρονικής υπηρεσίας, όσο και των δεδομένων που απαιτούνται για την επιτυχή ολοκλήρωση της συναλλαγής λαμβάνοντας υπόψη και την κρισιμότητα των δεδομένων αυτών (απλά, προσωπικά, ευαίσθητα).
Εγγραφή Οντότητας	Με τον όρο «εγγραφή μιας οντότητας» σε μια υπηρεσία ορίζεται το σύνολο των διαδικασιών δια των οποίων η οντότητα εκδηλώνει ενδιαφέρον χρήσης μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας και παρέχει τα απαιτούμενα στοιχεία για τη λήψη του δικαιώματος αυτού.
Επίπεδο Εγγραφής	Ως επίπεδο εγγραφής θεωρείται η ένταξη σε συγκεκριμένο σύνολο διαδικασιών που ακολουθούνται για τη συλλογή των απαιτούμενων στοιχείων και την πιστοποίηση της ορθότητας, έχοντας ως πεδίο αναφοράς το επίπεδο εμπιστοσύνης που απαιτείται για την παροχή μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας.

Βασική έννοια	Περιγραφή
Επίπεδο Αυθεντικοποίησης	Ως επίπεδο αυθεντικοποίησης θεωρείται η ένταξη μιας οντότητας σε συγκεκριμένου τύπου διαπιστευτήρια για την τεκμηρίωση της εγκυρότητας της ταυτότητάς της, με βάση το επίπεδο εμπιστοσύνης που απαιτείται να διασφαλιστεί για την παροχή μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας.
Ηλεκτρονική Ταυτότητα	Με τον όρο «ηλεκτρονική ταυτότητα» νοείται η ταυτότητα που αξιοποιεί ο χρήστης για την αναγνώρισή του σε μια ηλεκτρονική υπηρεσία.
Ταυτοποίηση	Με τον όρο ταυτοποίηση, υπό το πρίσμα του ΠΨΑ, νοείται η διαδικασία δήλωσης ταυτότητας από το χρήστη στις υπηρεσίες ηλεκτρονικής διακυβέρνησης.
Απλά Δεδομένα	Ως απλά δεδομένα, υπό το πρίσμα του ΠΨΑ, θεωρούνται πληροφορίες που είναι δημοσίως προσπελάσιμες και δεν περιέχονται σε αυτές προσωπικά δεδομένα.
Προσωπικά Δεδομένα	Ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα, υπό το πρίσμα του ΠΨΑ, θεωρούνται πληροφορίες που αναφέρονται στο υποκείμενο των δεδομένων, δηλαδή στο φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική (άρθρο 2α σε συνδυασμό με άρθρο 2γ του ν. 2472/97). Δε λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.
Ευαίσθητα Δεδομένα	Ως ευαίσθητα προσωπικά δεδομένα, προσδιορίζονται στο νόμο (άρθρο 2β του ν. 2472/97, όπως ισχύει) τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.
Αρχή Εγγραφής	Η Αρχή Εγγραφής ή καταχώρισης αποτελεί την οντότητα που είναι υπεύθυνη για τη συλλογή των απαιτούμενων στοιχείων και την πιστοποίηση της ταυτότητας μιας οντότητας που αιτείται εγγραφής σε κάποια ηλεκτρονική υπηρεσία.
Αρχή Πιστοποίησης	Η Αρχή Πιστοποίησης αποτελεί την οντότητα εκείνη που αναλαμβάνει την τεχνική διαχείριση των ψηφιακών πιστοποιητικών για ολόκληρο τον κύκλο ζωή τους.

Πίνακας 2: Βασικές Έννοιες ΠΨΑ

2.4 Πεδίο εφαρμογής του Πλαισίου

Το Πλαίσιο Ψηφιακής Αυθεντικοποίησης απευθύνεται σε όλους τους φορείς της Δημόσιας Διοίκησης, οι οποίοι διαθέτουν, αναπτύσσουν ή σχεδιάζουν να αναπτύξουν διαδικτυακό τόπο με σκοπό να παρέχουν πληροφορίες και υπηρεσίες σε πολίτες, επιχειρήσεις και άλλους φορείς. Αναλυτικότερα, το Πλαίσιο απευθύνεται σε:

- Υπουργεία και Γενικές Γραμματείες
- Περιφέρειες
- Νομαρχιακές Αυτοδιοικήσεις
- Οργανισμούς Τοπικής Αυτοδιοίκησης
- Εποπτευόμενους φορείς του Δημόσιου Τομέα
- Ανεξάρτητες Αρχές

και τους υπόλοιπους φορείς του Δημόσιου Τομέα όπως αυτός ορίζεται βάσει του Ν. 2527/97, άρθρο 1.

Επιπρόσθετα, απευθύνεται σε οργανισμούς του ευρύτερου Δημόσιου και του Ιδιωτικού Τομέα, οι οποίοι διαδραματίζουν σημαντικό ρόλο στην ανάπτυξη και παροχή ηλεκτρονικών υπηρεσιών μέσω δημόσιων διαδικτυακών τόπων προς πολίτες, επιχειρήσεις και άλλους φορείς, και αναλυτικότερα:

- Δημόσιες Επιχειρήσεις Κοινής Ωφέλειας
- Τραπεζικούς και Χρηματοπιστωτικούς Οργανισμούς
- Επιχειρήσεις Πληροφορικής και Υπηρεσιών που δραστηριοποιούνται στην ανάπτυξη λογισμικού και την παροχή συναφών υπηρεσιών για φορείς της Δημόσιας Διοίκησης (π.χ. ανάπτυξη δικτυακών πυλών, υλοποίηση πληροφοριακών συστημάτων).

Επιπλέον, το Πλαίσιο απευθύνεται σε οποιονδήποτε ενδιαφερόμενο πολίτη.

2.5 Επίπεδα Κατάταξης Κανόνων & Προτύπων

Το Πλαίσιο Ψηφιακής Αυθεντικοποίησης έχει υιοθετήσει τρία επίπεδα κατάταξης κανόνων & προτύπων ως προς τις απαιτήσεις συμμόρφωσης.

- **Κανόνες Υποχρεωτικοί (ΚΥ)**. Σε αυτή την περίπτωση η συμμόρφωση με την προδιαγραφή που τίθεται είναι επιβεβλημένη.
- **Κανόνες Προαιρετικοί (ΚΠ)**. Οι προαιρετικοί κανόνες προτείνεται να ακολουθούνται. Η μη συμμόρφωση με έναν προαιρετικό κανόνα επιτρέπεται σε εξαιρετικές περιπτώσεις και εφόσον τεκμηριώνεται επαρκώς.

- **Κανόνες υπό Διαμόρφωση / Μελέτη (ΚΜ)**. Η κατηγορία αυτή περιλαμβάνει κανόνες, πρότυπα, προδιαγραφές, τις οποίες το Πλαίσιο επεξεργάζεται και ενδέχεται να υιοθετήσει σε επόμενη έκδοσή του.

Επίσης, οι λέξεις-κλειδιά: ΠΡΕΠΕΙ ΝΑ, ΔΕΝ ΠΡΕΠΕΙ ΝΑ, ΑΠΑΙΤΕΙΤΑΙ ΝΑ, ΘΑ ΠΡΕΠΕΙ ΝΑ, ΔΕΝ ΘΑ ΠΡΕΠΕΙ ΝΑ, ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ, ΔΕΝ ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ, ΣΥΝΙΣΤΑΤΑΙ ΝΑ, ΔΥΝΑΤΑΙ ΝΑ, ΠΡΟΑΙΡΕΤΙΚΑ και ΜΕΛΕΤΑΤΑΙ ΝΑ, σύμφωνα με την ερμηνεία που έχει δοθεί από το Internet Engineering Task Force (IETF) Request For Comments (RFC) 2119[1] για αντίστοιχες λειτουργίες, συμπληρώνουν τα επίπεδα συμμόρφωσης. Αναλυτικά:

- Οι φράσεις-κλειδιά ΠΡΕΠΕΙ ΝΑ, ΑΠΑΙΤΕΙΤΑΙ ΝΑ και ΘΑ ΠΡΕΠΕΙ ΝΑ εμφανίζονται σε Κανόνες Υποχρεωτικούς και σημαίνουν ότι η προδιαγραφή αποτελεί απόλυτη απαίτηση του Πλαισίου. Όταν η φράση-κλειδί ΠΡΕΠΕΙ ΝΑ συνοδεύεται από τη λέξη «αποφεύγεται», ερμηνεύεται ότι επιτρέπεται περιορισμένος αριθμός ή εύρος παρεκκλίσεων από την εφαρμογή του Κανόνα, χωρίς να συνεπάγεται τη μη συμμόρφωση με τον Κανόνα. Σε αυτή την περίπτωση, πρέπει να τεκμηριώνονται επαρκώς οι λόγοι των παρεκκλίσεων και να γίνουν κατανοητές οι συνέπειες από τη μη συμμόρφωση στην προδιαγραφή.
- Οι φράσεις-κλειδιά ΔΕΝ ΠΡΕΠΕΙ ΝΑ και ΔΕΝ ΘΑ ΠΡΕΠΕΙ ΝΑ εμφανίζονται σε Κανόνες Υποχρεωτικούς και ερμηνεύονται ως αυστηρή απαγόρευση της προδιαγραφής.
- Οι φράσεις-κλειδιά ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ, ΣΥΝΙΣΤΑΤΑΙ ΝΑ, ΔΥΝΑΤΑΙ ΝΑ και ΠΡΟΑΙΡΕΤΙΚΑ εμφανίζονται σε Κανόνες Προαιρετικούς και αφήνουν το ενδεχόμενο της παράληψης – αθέτησης μιας προδιαγραφής, εάν συντρέχουν τεκμηριωμένοι λόγοι. Ωστόσο, θα πρέπει να ληφθούν σοβαρά υπόψη και να γίνουν κατανοητές οι συνέπειες από τη μη συμμόρφωση στην προδιαγραφή.
- Η φράση-κλειδί ΔΕΝ ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ εμφανίζεται σε Κανόνες Προαιρετικούς και αφήνει ανοικτό το ενδεχόμενο της υιοθέτησης μιας συμπεριφοράς που δεν συνιστάται, αρκεί να ληφθούν σοβαρά υπόψη και να γίνουν κατανοητές οι συνέπειες από την υιοθέτηση της συγκεκριμένης συμπεριφοράς.
- Η φράση-κλειδί ΜΕΛΕΤΑΤΑΙ ΝΑ εμφανίζεται σε Κανόνες υπό Μελέτη/ Διαμόρφωση και ορίζει προδιαγραφές, των οποίων η ενσωμάτωση στο Πλαίσιο εξετάζεται. Ωστόσο, μία υπό μελέτη προδιαγραφή μπορεί, σε επόμενη έκδοση του Πλαισίου, να αποτελεί υποχρεωτική προδιαγραφή, οπότε μια υλοποίηση που δεν υπακούει σήμερα στην προδιαγραφή ΠΡΕΠΕΙ ΝΑ λαμβάνει υπόψη της ότι μελλοντικά ενδεχομένως να πρέπει να συμμορφωθεί ως προς αυτή.

[1] IETF Network Working Group, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997, http://www.ietf.org/rfc/rfc2119.txt

3. ΘΕΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Η αξιοποίηση υπηρεσιών ηλεκτρονικής διακυβέρνησης απαιτεί συλλογή και επεξεργασία διαφορετικού είδους πληροφοριών, όπως προσωπικών δεδομένων, των οποίων η προστασία, επεξεργασία και μη αποκάλυψη και δημοσιοποίηση αποτελεί βασική κανονιστική απαίτηση, σύμφωνα με τις ειδικότερες προϋποθέσεις και εγγυήσεις της σχετικής νομοθεσίας (ν. 2472/97), που πρέπει να εκπληρώνεται από τις υπηρεσίες ηλεκτρονικής διακυβέρνησης.

Η συνταγματική και έννομη τάξη αναγνωρίζει την πληροφοριακή ιδιωτικότητα (informational privacy) ως το δικαίωμα και τη δυνατότητα του ατόμου να γνωρίζει, να ελέγχει και καταρχήν να προσδιορίζει τη χρήση των προσωπικών πληροφοριών του από άλλες οντότητες, ιδιώτες και κράτος. Ως ιδιωτικότητα ορίζεται η μη αποκάλυψη προσωπικών πληροφοριών σε μη εξουσιοδοτημένες οντότητες η οποία αποτελεί βασική παράμετρο της σχετικής νομοθεσίας που αναγνωρίζεται ρητά (άρθρο 10 ν.2472/97), ενώ η παραβίασή της τιμωρείται και με ποινικές κυρώσεις (άρθρο 22 § 4 ν. 2472/97). Το δικαίωμα στην ιδιωτικότητα αναφέρεται στη δυνατότητα ελέγχου της χρήσης των προσωπικών πληροφοριών.

Ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα νοείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων, δηλαδή στο φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική (άρθρο 2α σε συνδυασμό με άρθρο 2γ του ν. 2472/97). Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων. Στον όρο "προσωπικά δεδομένα" περιλαμβάνονται και αυτά τα οποία χρησιμοποιούνται συνήθως για τον προσδιορισμό της ταυτότητας του προσώπου. Με το σύνηθες προσδιοριστικό της ταυτότητας ενός προσώπου, το όνομα, μπορούν να εξομοιωθούν ο αριθμός της κοινωνικής ασφάλισης, ο αριθμός του δελτίου ταυτότητας, ο αριθμός πελάτη και άλλα παρόμοια στοιχεία. Ως στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου έχουν γίνει αποδεκτά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (π.χ. κωδικός αναγνώρισης ή πρόσβασης, αριθμός PIN κ.α.).

Οι προσωπικές πληροφορίες μπορεί να αφορούν τις σχέσεις ενός προσώπου προς πρόσωπα ή τις σχέσεις προς πράγματα. Σε αυτές τις σχέσεις αντιστοιχούν πληροφορίες τόσο για τα εξωτερικά στοιχεία όσο και για ψυχικές καταστάσεις (απόψεις, κίνητρα, επιθυμίες), ενέργειες, αντιδράσεις, τρόπους συμπεριφοράς, ανεξάρτητα από το αν αφορούν το παρόν ή το παρελθόν και πόσο ανατρέχουν σε αυτό. Είναι αναμφισβήτητο ότι στις πληροφορίες προσωπικού χαρακτήρα εντάσσονται και οι σχέσεις προς το περιβάλλον. Ως τέτοιες νοούνται, για παράδειγμα, στοιχεία για την περιουσιακή κατάσταση, για την επαγγελματική και οικονομική δραστηριότητα, την οικογενειακή κατάσταση, τις προσωπικές δραστηριότητες και σχέσεις

(συνήθειες του ελεύθερου χρόνου, συμμετοχή και δραστηριοποίηση σε ενώσεις, καταναλωτική συμπεριφορά) καθώς και για τις σχέσεις και καταστάσεις ιδιωτικού και δημοσίου δικαίου (ιδιοκτησία, συμβατικές σχέσεις, διοικητικές άδειες κλπ.).

Ως ευαίσθητα προσδιορίζονται σαφώς στο νόμο (άρθρο 2β του ν. 2472/97, όπως ισχύει) τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Οι βασικές υποχρεώσεις της Διοίκησης σχετικά με τη διασφάλιση της Ιδιωτικότητας όταν παρέχονται υπηρεσίες ηλεκτρονικής διακυβέρνησης με χρήση δεδομένων προσωπικού χαρακτήρα, είναι:

1. Κατά τη συλλογή και επεξεργασία δεδομένων θα πρέπει να λαμβάνεται πρόνοια ώστε να υπάρχει σαφής προσδιορισμός και διαχωρισμός των δεδομένων προσωπικού και στατιστικού χαρακτήρα.
2. Θα πρέπει να διασφαλίζεται, με διαδικασίες ανωνυμοποίησης/ πολλαπλής κωδικοποίησης, ότι από τα δεδομένα στατιστικού χαρακτήρα δεν είναι δυνατός ο προσδιορισμός της ταυτότητας των φυσικών προσώπων.
3. Με εγκυκλίους και άλλα μέσα ενημέρωσης-εκπαίδευσης θα πρέπει να καταστούν γνωστές και σαφείς στους δημόσιους υπαλλήλους οι κατηγορίες των ευαίσθητων δεδομένων για να αποφευχθεί σχετική σύγχυση (π.χ. παρατηρείται σχετική σύγχυση μεταξύ των δεδομένων που αφορούν φυλετική ή εθνική προέλευση (φυλετική ή εθνική μειονότητα) που συνιστούν ευαίσθητα δεδομένα και αυτών που αφορούν την ιθαγένεια που συνιστούν απλά δεδομένα).

Σε περίπτωση προσφυγής σε εξωτερικούς ιδιωτικούς φορείς για την αποθήκευση και πρόσβαση σε προσωπικά δεδομένα χρήστη:

1. Θα πρέπει να περιλαμβάνονται στη σχετική σύμβαση όροι για τη συλλογή και επεξεργασία δεδομένων.
2. Θα ήταν χρήσιμο ένα ενιαίο πρότυπο συμβατικών όρων που θα προσδιορίζουν τις υποχρεώσεις των τρίτων ως προς τη συλλογή και χρήση προσωπικών δεδομένων. Οι πρότυποι όροι θα μπορούσαν να χρησιμοποιηθούν από τις υπηρεσίες με τις αναγκαίες κατά περίπτωση προσαρμογές.
3. Σε περίπτωση ανάθεσης της παροχής υπηρεσιών ηλεκτρονικής διακυβέρνησης σε τρίτους, εφόσον οι υπηρεσίες αυτές προϋποθέτουν ή/και συνεπάγονται συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, η αναλυτική περιγραφή και ποιότητα των πολιτικών εφαρμογής των κανόνων προστασίας και των πολιτικών/ μέτρων ασφάλειας θα έπρεπε να αναχθεί σε κριτήριο επιλογής αναδόχου ή/και όρο ανάθεσης.

4. ΕΠΙΠΕΔΑ ΕΜΠΙΣΤΟΣΥΝΗΣ

4.1 Γενική Προσέγγιση

Τα δεδομένα που αξιοποιούνται από τις υπηρεσίες ηλεκτρονικής διακυβέρνησης μπορούν να κατηγοριοποιηθούν, ως προς το βαθμό κρισιμότητάς τους, με βάση τα παρακάτω κριτήρια:

- Δεδομένα Προσωπικού Χαρακτήρα ή Προσωπικά δεδομένα: κάθε πληροφορία που αφορά ένα φυσικό πρόσωπο.
- Ευαίσθητα δεδομένα προσωπικού χαρακτήρα, δηλαδή τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.
- Οικονομικά δεδομένα: τα οικονομικά δεδομένα εφόσον συνδέονται με φυσικά πρόσωπα αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα, ενώ εάν σχετίζονται με αίτηση ή λήψη παροχών που εμπίπτουν στην κοινωνική πρόνοια, τότε μπορεί να θεωρηθούν ευαίσθητα δεδομένα.

Ο καθορισμός του βαθμού κρισιμότητας των δεδομένων εξαρτάται κατά κύριο λόγο από τις επιπτώσεις που μπορεί να προκύψουν:

- για το χρήστη ή / και το φορέα που προσφέρει την υπηρεσία, λόγω της αποκάλυψης ή «παράνομης και αθέμιτης» χρήσης των δεδομένων,
- στην ιδιωτικότητα του ατόμου.

Κατά την ανάλυση και τον προσδιορισμό των επιπέδων εμπιστοσύνης λαμβάνονται υπόψη τα παραπάνω κριτήρια που αναφέρονται τόσο στο χαρακτηρισμό των δεδομένων, όσο και στην εκτίμηση της πιθανότητας επέλευσης βλάβης (Αποκάλυψη Εμπιστευτικών Δεδομένων, Μη εξουσιοδοτημένη τροποποίηση, Μη διαθεσιμότητα Δεδομένων, Αποποίηση) είτε αυτή οφείλεται σε παράνομη ή αθέμιτη χρήση είτε όχι.

Συνεπώς, όσο πιο κρίσιμη θεωρείται μια υπηρεσία, τόσο μεγαλύτερο επίπεδο εμπιστοσύνης απαιτείται για την ορθότητα και εγκυρότητα των στοιχείων που επιδεικνύει ή προσκομίζει ο χρήστης για τη χρήση των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Σε κάθε περίπτωση, το επίπεδο εμπιστοσύνης που επιλέγεται για μια υπηρεσία θα πρέπει να στοχεύει στα ακόλουθα:

- Στην ελευθερία της πληροφόρησης και ενημέρωσης των πολιτών για θέματα δημόσιας διαβούλευσης
- Στην εκπλήρωση του δικαιώματος συμμετοχής στην κοινωνία της πληροφορίας
- Στη διαφύλαξη του δικαιώματος κάθε πολίτη για αποτελεσματική και ασφαλή διεκπεραίωση των συναλλαγών του με τους δημόσιους φορείς
- Στη διαφύλαξη και ορθή διαχείριση των προσωπικών δεδομένων κάθε πολίτη

4.2 Προσδιορισμός Επιπέδων Εμπιστοσύνης

Προϋπόθεση για την παροχή μιας υπηρεσίας ηλεκτρονικής διακυβέρνησης από κάποιο δημόσιο φορέα είναι να προσδιοριστεί το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η ηλεκτρονική υπηρεσία. Η «εμπιστοσύνη», ερμηνεύεται ως «η πίστη στην αξιοπιστία, εντιμότητα, αξία ή ικανότητα κάποιας οντότητας». Υπό το πρίσμα του ΠΨΑ, ως επίπεδο εμπιστοσύνης μπορεί να θεωρηθεί ο βαθμός βεβαιότητας που έχει μια υπηρεσία για την ορθότητα τόσο της ηλεκτρονικής οντότητας ενός πολίτη που επιθυμεί να διεκπεραιώσει ηλεκτρονικά μια συναλλαγή, όσο και των δεδομένων που απαιτούνται για την επιτυχή ολοκλήρωση της συναλλαγής λαμβάνοντας υπόψη και την κρισιμότητα των δεδομένων αυτών (απλά, προσωπικά, ευαίσθητα).

Συνεπώς, το κάθε επίπεδο εμπιστοσύνης προσδιορίζει όχι μόνο το βαθμό βεβαιότητας ότι ο πολίτης που επιδεικνύει συγκεκριμένου τύπου διαπιστευτήρια είναι πράγματι αυτός που ισχυρίζεται ότι είναι, με κύριο στόχο να εξασφαλιστεί η δημιουργία εμπιστοσύνης μεταξύ της υπηρεσίας και του χρήστη για τη διεκπεραίωση της συναλλαγής, αλλά και ότι αξιοποιούνται οι κατάλληλοι μηχανισμοί ασφάλειας για την προστασία των δεδομένων που απαιτούνται με βάση την κρισιμότητά τους.

Το επίπεδο εμπιστοσύνης για κάθε ηλεκτρονική υπηρεσία που προσφέρεται στους πολίτες, όπως έχει ήδη αναφερθεί, διαμορφώνεται ανάλογα με την αξία των συναλλαγών, την κρισιμότητα των δεδομένων που χρησιμοποιούνται, των άμεσων ή έμμεσων επιπτώσεων που μπορεί να προκύψουν από την εκδήλωση επιθέσεων, καθώς επίσης και από την αντίστοιχη επιρροή του θεσμικού πλαισίου. Τα επίπεδα εμπιστοσύνης για τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, σύμφωνα με τα προαναφερόμενα κριτήρια, περιγράφονται στις επόμενες υποενότητες.

4.2.1 Επίπεδο 0

Στο επίπεδο εμπιστοσύνης 0 εντάσσονται υπηρεσίες που αξιοποιούν δημόσια προσπελάσιμες πληροφορίες και έχουν ως κύριο στόχο την πληροφόρηση των πολιτών γύρω από συγκεκριμένα θέματα. Οι υπηρεσίες αυτές δεν απαιτούν:

1. τη χρήση ή ανταλλαγή οποιουδήποτε τύπου προσωπικών ή οικονομικών δεδομένων
2. κάποιο βαθμό βεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας ενός πολίτη.

Οι επιπτώσεις που μπορούν να προκύψουν για τις υπηρεσίες αυτού του επιπέδου θεωρούνται ασήμαντες. Η μοναδική απαίτηση είναι η διαθεσιμότητα των υπηρεσιών.

4.2.2 Επίπεδο 1

Στο επίπεδο εμπιστοσύνης 1 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή δεδομένων μικρής ή ελάχιστης κρισιμότητας, όπως για παράδειγμα του ονοματεπώνυμου ή της διεύθυνσης του ηλεκτρονικού ταχυδρομείου, για τη διεκπεραίωση μιας συναλλαγής. Σε αντίθεση με το επίπεδο εμπιστοσύνης 0, στο συγκεκριμένο επίπεδο η ηλεκτρονική υπηρεσία απαιτεί κάποιο

μικρό βαθμό βεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας του πολίτη ώστε να αποδεικνύεται η ορθότητα την στοιχείων που υποβάλλονται.

Οι επιπτώσεις, οι οποίες είναι δυνατό να προκληθούν από την εκδήλωση κάποιων επιθέσεων και απειλών, είναι δευτερεύουσας σημασίας. Παρόλα αυτά προτείνονται κάποια μέτρα ασφάλειας που έχουν ως στόχο την προστασία των δεδομένων που ανταλλάσσονται και την ελαχιστοποίηση της πιθανότητας εμφάνισης κάποιας απειλής.

4.2.3 Επίπεδο 2

Στο επίπεδο εμπιστοσύνης 2 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή προσωπικών δεδομένων τα οποία δεν είναι χαρακτηρισμένα ως ευαίσθητα, όπως για παράδειγμα στοιχεία που αφορούν την οικογενειακή κατάσταση του χρήστη, ημερομηνία γέννησης, φύλο κ.λπ. Θα πρέπει να σημειωθεί, με βάση την κείμενη νομοθεσία, ότι τα οικονομικά δεδομένα που δεν καλύπτονται από το φορολογικό απόρρητο εντάσσονται στα προσωπικά δεδομένα.

Στο συγκεκριμένο επίπεδο ο βαθμός βεβαιότητας για την ορθότητα της ηλεκτρονικής οντότητας που αξιοποιεί την υπηρεσία χαρακτηρίζεται ως μέτριος, καθώς πρέπει να εξασφαλίζεται ότι οι υπηρεσίες προσφέρονται μόνο σε εξουσιοδοτημένα άτομα.

Οι επιπτώσεις που είναι δυνατό να προκληθούν από την εμφάνιση κάποιων επιθέσεων και απειλών αφορούν κυρίως στη δημοσιοποίηση προσωπικών στοιχείων, χωρίς τη γνώση ή έγκριση του χρήστη, είτε σε μη εξουσιοδοτημένα άτομα είτε στο ευρύ κοινό.

4.2.4 Επίπεδο 3

Στο επίπεδο εμπιστοσύνης 3 εντάσσονται υπηρεσίες που απαιτούν ανταλλαγή είτε ευαίσθητων προσωπικών δεδομένων (όπως για παράδειγμα στοιχεία που αφορούν το ποινικό μητρώο ενός χρήστη) είτε υπηρεσίες ηλεκτρονικής ολοκλήρωσης επιπέδου 4, όπου ο χρήστης πραγματοποιεί και τις οικονομικές συναλλαγές που απαιτούνται με ηλεκτρονικό τρόπο. Συνεπώς, οι επιπτώσεις που μπορεί να προκληθούν από κάποιο περιστατικό ασφάλειας είναι ιδιαίτερα σημαντικές και ως εκ τούτου είναι απαραίτητο να διασφαλιστεί υψηλός βαθμός εμπιστοσύνης για την ηλεκτρονική ταυτότητα ενός χρήστη.

5. ΘΕΣΜΙΚΟ-ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΨΗΦΙΑΚΗΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Η Εγγραφή, Ταυτοποίηση και Αυθεντικοποίηση των χρηστών προϋποθέτει τη συλλογή και διαχείριση δεδομένων που αναφέρονται στην ταυτότητα των χρηστών.

Εφόσον πρόκειται για Εγγραφή, Ταυτοποίηση και Αυθεντικοποίηση νομικών προσώπων που συναλλάσσονται ηλεκτρονικά με τη Δημόσια Διοίκηση, εφαρμόζονται οι κανόνες που αφορούν την επωνυμία και τη νόμιμη εκπροσώπηση των νομικών προσώπων. Η εφαρμογή των κανόνων αυτών είναι κρίσιμη, κυρίως κατά το στάδιο της Εγγραφής και του προσδιορισμού και εξέτασης της νομιμοποίησης των φυσικών προσώπων που νομιμοποιούνται να συναλλάσσονται με τη διοίκηση δεσμεύοντας το νομικό πρόσωπο. Εν προκειμένω εφαρμόζονται αναλόγως οι γενικές διατάξεις που αφορούν την αντιπροσώπευση των νομικών προσώπων.

Στην περίπτωση που ο χρήστης είναι φυσικό πρόσωπο, η Εγγραφή, Ταυτοποίηση και Αυθεντικοποίηση προϋποθέτουν και ταυτόχρονα συνεπάγονται περαιτέρω συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα, δηλαδή πληροφοριών που αναφέρονται σε φυσικά πρόσωπα. Η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα ρυθμίζεται από το Ν. 2472/97, οι ρυθμίσεις του οποίου αφορούν χωρίς διάκριση και την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο δημόσιο τομέα.

Το κύριο ζήτημα που τίθεται και εξετάζεται αφορά ειδικότερα τη νομική βάση της επεξεργασίας, την εφαρμογή των γενικών αρχών επεξεργασίας, τις τυχόν διαδικαστικές προϋποθέσεις νομιμότητας της επεξεργασίας, καθώς και τα δικαιώματα των προσώπων στο είδος και την έκταση των δεδομένων προσωπικού χαρακτήρα που επιτρέπεται να υφίστανται επεξεργασία για τις υπό εξέταση διαδικασίες. Έστω και ως εκ περισσού, κρίνουμε σκόπιμο να υπενθυμίσουμε ότι, όπως προκύπτει και από τις αναφορές στον ορισμό και την έννοια των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται σε άλλα κεφάλαια του παρόντος, η νομοθεσία για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα βρίσκει εφαρμογή αποκλειστικά στην επεξεργασία δεδομένων φυσικών προσώπων.

Ως προς τη νόμιμη βάση της επεξεργασίας προκαταρκτικά επισημαίνεται ότι με βάση το συνταγματικό-νομοθετικό πλαίσιο η επεξεργασία προσωπικών δεδομένων καταρχήν απαγορεύεται και επιτρέπεται κατ' εξαίρεση μόνο εφόσον συντρέχουν οι βάσεις νομιμότητας της επεξεργασίας που ορίζονται στα άρθρα 5-8 του ν. 2472/97, όπως ισχύει. Τόσο οι ουσιαστικές όσο και οι διαδικαστικές προϋποθέσεις νομιμότητας της επεξεργασίας διαφοροποιούνται καταρχήν με κριτήριο το είδος και την κατηγορία των δεδομένων («απλά» και ευαίσθητα και ειδικότερες κατηγορίες ευαίσθητων δεδομένων) ενώ ο νόμος περιέχει ειδικές ρυθμίσεις για τη «διασύνδεση» ως μορφή επεξεργασίας δεδομένων.

5.1 Νομική/ Νόμιμη βάση επεξεργασίας

Στο βαθμό που αναφερόμαστε στις διαδικασίες Εγγραφής, Αυθεντικοποίησης και Ταυτοποίησης φυσικών προσώπων και συγκεκριμένων συναλλασσομένων με τη Δημόσια Διοίκηση οι νόμιμες βάσεις επεξεργασίας μπορεί να συνίστανται διαζευκτικά: α) στη συγκατάθεση του προσώπου, β) στην εκπλήρωση νόμιμης υποχρέωσης του υπεύθυνου επεξεργασίας και γ) στην εκπλήρωση έργου δημοσίου συμφέροντος ή στην άσκηση δημόσιας εξουσίας.

Στη συγκεκριμένη περίπτωση, η συγκατάθεση του προσώπου τίθεται στο άρθρο 5 παρ. 1 του ν. 2472/97 ως κανόνας για τη σύννομη επεξεργασία προσωπικών δεδομένων, προβλέπονται ωστόσο εξαιρέσεις στην παράγραφο 2. Μία από αυτές τις εξαιρέσεις προβλέπει τα ακόλουθα: «Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν: β) Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο (Σημείωση: εννοεί το νόμο εν γένει και όχι το συγκεκριμένο νόμο)».

Από τους συντάκτες του παρόντος παραδοτέου κειμένου για το ΠΨΑ δεν προτείνεται η εισαγωγή ειδικής νομοθετικής ρύθμισης, καθώς το γενικό πνεύμα της νομοθεσίας και η σχετική συνταγματική ρύθμιση προτάσσει τη συγκατάθεση ως εκδήλωση του δικαιώματος προστασίας προσωπικών δεδομένων. Εξάλλου, στο βαθμό που η χρήση υπηρεσιών ηλεκτρονικής διακυβέρνησης δεν είναι υποχρεωτική για τους πολίτες, η παροχή συγκατάθεσης είναι ένας τρόπος για να γνωρίζουν οι πολίτες τις συνέπειες της ηλεκτρονικής αίτησης και παροχής υπηρεσιών. Υπενθυμίζεται ότι η συγκατάθεση, σύμφωνα με την οικεία νομοθεσία (άρθρο 2 ι του ν. 2472/97), είναι ρητή, ειδική και «κατόπιν πληροφόρησης». Δεν προτείνεται συνεπώς ουδεμία απόκλιση από τον κανόνα της συγκατάθεσης.

Ο ν. 2472/97 προκρίνει τη συγκατάθεση του προσώπου ως κανόνα. Κατ' εξαίρεση ή ελλείψει αυτής της συγκατάθεσης ισχύουν οι άλλες, προαναφερόμενες νόμιμες βάσεις επεξεργασίας. Εφόσον νομοθετική διάταξη, ειδική και μεταγενέστερη του ν. 2472/97, προβλέπει την εγγραφή/ ταυτοποίηση/ αυθεντικοποίηση ως υποχρέωση των συναλλασσομένων και αντίστοιχα ως αρμοδιότητα της Δημόσιας Διοίκησης τότε ενδέχεται να μην απαιτείται η ύπαρξη συναίνεσης του προσώπου, στο βαθμό που από το σύνολο της ρύθμισης δεν τίθεται θέμα προσβολής του συνταγματικού δικαιώματος προστασίας των προσωπικών δεδομένων (άρθρο 9Α του Συντάγματος).

Η συγκατάθεση σύμφωνα με το ν. 2472/97, όπως ισχύει, πρέπει να είναι ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή, και εν πλήρη επίγνωση, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για το σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπεύθυνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.

Η συγκατάθεση προσδιορίζεται από το νόμο ως ρητή, συνεπώς απορρίπτεται η εικαζόμενη ή σιωπηρή συγκατάθεση: η αίτηση για ηλεκτρονική παροχή μιας υπηρεσίας ή συναλλαγής ή η

αποδοχή μιας τέτοιας υπηρεσίας ή συναλλαγής δεν επέχει θέση συγκατάθεσης, τουλάχιστον όταν πρόκειται για δηλώσεις/ υπηρεσίες/ συναλλαγές που παράγουν έννομα αποτελέσματα (*Βλ. Rechtliche Rahmenbedingungen für E-Government, 67*).

Ένα περαιτέρω ζήτημα αναφέρεται στην εγκυρότητα της «ηλεκτρονικής συγκατάθεσης»: οι διατάξεις του ν. 3471/06 που αφορούν την προστασία των προσωπικών δεδομένων στο πεδίο των ηλεκτρονικών επικοινωνιών προβλέπουν και την παροχή συγκατάθεσης με ηλεκτρονικά μέσα. Στην περίπτωση αυτή ο νόμος απαιτεί να εξασφαλίζει ο υπεύθυνος επεξεργασίας ότι ο συνδρομητής ή χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωσή του η οποία καταγράφεται με ασφαλή τρόπο και είναι ανά πάσα στιγμή προσβάσιμη στο χρήστη ή συνδρομητή και μπορεί οποτεδήποτε να ανακληθεί. Το άρθρο 5 του ν. 3471/06 [που αντικατάστησε τον ν. 2774/99 (πρώτο μέρος) και τροποποίησε εν μέρει τον γενικό ν. 2472/97 για την επεξεργασία και προστασία προσωπικών δεδομένων] αφορά την προστασία απορρήτου και ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες. Δεν τροποποιεί τον ορισμό της συγκατάθεσης, όπως αυτός περιλαμβάνεται στο άρθρο 2 ι του ν. 2472/97. Η τελευταία ρύθμιση μπορεί, βέβαια, να ερμηνευτεί κατά τρόπο ώστε να καταλαμβάνει και την ηλεκτρονική συγκατάθεση. Είναι όμως θέμα ερμηνείας και όχι συγκεκριμένης ρύθμισης. Ακριβώς λόγω της ειδικότητάς της αυτή η ρύθμιση, το πεδίο εφαρμογής της οποίας αφορά τα δημόσια δίκτυα επικοινωνιών, δεν είναι δυνατόν να χρησιμεύσει αυτοτελώς για τη θεμελίωση της δυνατότητας της ηλεκτρονικής συγκατάθεσης.

Όπως προκύπτει από την πρόσφατη από 18.07.2007 γνωμοδότηση (48/07) της Αρχής Προστασίας Προσωπικών Δεδομένων, η Αρχή αποδέχεται ως νομική βάση της επεξεργασίας την ελεύθερη, ρητή και ειδική συγκατάθεση των υποκειμένων των δεδομένων όπως την ορίζει ο ν. 2472/1997 **σε συνδυασμό και με το ν. 3471/2006** για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.

Εάν πρόκειται για την επεξεργασία ευαίσθητων δεδομένων, η συγκατάθεση πρέπει αναγκαστικά να περιβληθεί έγγραφο τύπο. Η ειδικότερη διαμόρφωση της διαδικασίας για την παροχή συγκατάθεσης εξαρτάται από το μοντέλο παροχής ηλεκτρονικής υπηρεσίας που θα επιλεγεί. Το ενδεχόμενο να παρέχεται μία γενική συγκατάθεση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προσκρούει στην απαίτηση της «ειδικής δήλωσης βούλησης», ώστε να είναι έγκυρη η συγκατάθεση. Οπωσδήποτε και σε κάθε περίπτωση όπου απαιτείται έγγραφη συγκατάθεση, όπως στην περίπτωση της επεξεργασίας ευαίσθητων δεδομένων, η ηλεκτρονική παροχή της μπορεί να γίνει δεκτή - με βάση τις γενικές διατάξεις - μόνον εφόσον πρόκειται για «προηγμένη ηλεκτρονική υπογραφή» (άρθρο 3 Π.Δ. 150/2001).

5.2 Εφαρμογή γενικών αρχών επεξεργασίας

Οι γενικές αρχές επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως κατοχυρώνονται στο άρθρο 4 του ν. 2472/97 και έχουν ερμηνευτεί από την Αρχή Προστασίας Προσωπικών Δεδομένων, ισχύουν και στον προσδιορισμό των όρων επεξεργασίας στο πλαίσιο των διαδικασιών αυθεντικοποίησης και ταυτοποίησης.

Συγκεκριμένα η επεξεργασία πρέπει να συνάδει προς τις αρχές της αναλογικότητας και του σκοπού. Από την αρχή της αναλογικότητας απορρέει καταρχήν η αρχή της φειδούς ως προς

την επεξεργασία δεδομένων: θα πρέπει να συλλέγονται τα ελάχιστα απαιτούμενα προσωπικά δεδομένα για την εκπλήρωση του σκοπού, δηλ. της παροχής συγκεκριμένης υπηρεσίας ή κατηγορίας υπηρεσιών. Θα πρέπει να συλλέγονται εκείνα και μόνο όσα είναι αναγκαία και κατάλληλα για την εκπλήρωση του σκοπού αυτού (αναγκαιότητα, προσφορότητα, υπό στενή έννοια αναλογικότητα των δεδομένων). Όσον αφορά την αρχή του σκοπού, αυτή επιτάσσει να μη χρησιμοποιούνται τα δεδομένα για σκοπούς μη συμβατούς με αυτούς για τους οποίους έχουν συλλεχθεί.

Οι αρχές αυτές ισχύουν για την ταυτοποίηση και τα διάφορα στάδια αυτής. Είναι προφανές ότι το είδος της υπηρεσίας που προσφέρεται και το αντίστοιχο επίπεδο εμπιστοσύνης προσδιορίζει και εάν και ποια προσωπικά δεδομένα πρέπει να συλλέγονται και να υπόκεινται σε επεξεργασία. Εξ αυτού απορρέουν ειδικότερα οι ακόλουθες αρχές:

- Στην περίπτωση υπηρεσιών (πληροφόρησης και αναζήτησης προτύπων και φορμών κλπ.) για τις οποίες δεν είναι αναγκαίος ο προσδιορισμός της ταυτότητας του συναλλασσόμενου, αυτές θα πρέπει να προσφέρονται χωρίς να λαμβάνει χώρα καμία συλλογή δεδομένων προσωπικού χαρακτήρα.
- Στην περίπτωση υπηρεσιών πληροφόρησης, αυτές μπορούν να παρέχονται χωρίς να είναι αναγκαία η καταχώριση του συνόλου της IP διεύθυνσης του αποδέκτη της υπηρεσίας, εφόσον δεν είναι αναγκαίο για την παροχή της υπηρεσίας ή την τυχόν χρέωσή της.
- Στην περίπτωση υπηρεσιών απλών (π.χ. Newsletter), αυτές μπορούν να παρέχονται με αναγκαία μόνη την καταχώριση της ηλεκτρονικής διεύθυνσης του παραλήπτη χωρίς να είναι αναγκαία η συλλογή και επεξεργασία ονοματεπώνυμου και ταχυδρομικής διεύθυνσης.

Η αυθεντικοποίηση και η ταυτοποίηση του συναλλασσόμενου θα πρέπει να παραλείπεται εφόσον αυτή δεν απαιτείται εν γένει από το νόμο για την παροχή της ίδιας υπηρεσίας off-line (υπό την ουσιαστική έννοια της νομικά δεσμευτικής ρύθμισης, δηλ. μπορεί να πρόκειται και για υπουργική απόφαση που εκδίδεται κατ' εξουσιοδότηση νόμου). Αντίθετα, εάν στην «κλασική» παροχή της υπηρεσίας είναι αναγκαία η ταυτοποίηση, κατά μείζονα λόγο πρέπει αυτή να απαιτείται στο πλαίσιο της ηλεκτρονικής διεκπεραίωσης. Μία παράμετρος που καθιστά αναγκαία τη μονοσήμαντη ταυτοποίηση του συναλλασσόμενου είναι η πρόσβαση σε προσωπικά δεδομένα αυτού, ανεξαρτήτως εάν πρόκειται για «απλά» ή ευαίσθητα, προκειμένου να καταστεί δυνατή η παροχή της υπηρεσίας.

Στην περίπτωση υπηρεσιών για την παροχή των οποίων κρίνεται αναγκαία η αυθεντικοποίηση και ταυτοποίηση του χρήστη – λήπτη μιας υπηρεσίας, τα δεδομένα που συλλέγονται θα πρέπει να περιορίζονται στα αναγκαία για την ταυτοποίηση που απαιτούνται για την παροχή της συγκεκριμένης υπηρεσίας. Εφόσον ζητούνται περαιτέρω μη αναγκαία στοιχεία, θα πρέπει να επισημαίνεται στο συναλλασσόμενο με τη διοίκηση η μη υποχρεωτικότητα της παροχής των συγκεκριμένων στοιχείων. Σε κάθε περίπτωση, όμως, υφίσταται η γενικότερη δέσμευση από τη νομοθετικά απαιτούμενη συνάφεια και προσφορότητα των δεδομένων με και για το σκοπό που επιδιώκεται.

Από τις ίδιες αρχές απορρέει η αναγκαιότητα τεχνικού και οργανωτικού διαχωρισμού των δεδομένων που είναι απαραίτητα για την ταυτοποίηση και αυθεντικοποίηση του συναλλασσόμενου με τη διοίκηση και των δεδομένων που αφορούν το περιεχόμενο της αιτηθείσας ή παρεχόμενης πληροφορίας και υπηρεσίας, καθώς ενδέχεται να μην ταυτίζονται οι χειριστές των δύο σταδίων.

Στοιχείο της ποιότητας των δεδομένων, στενά συνδεδεμένο και με την αρχή της αναλογικότητας, είναι η επιταγή για ακρίβεια των δεδομένων. Τα προσωπικά δεδομένα πρέπει να είναι αληθή, ακριβή και συνεπώς να υπόκεινται σε επικαιροποίηση, ώστε να εξακολουθούν να ανταποκρίνονται στην πραγματικότητα. Η ανακρίβεια, η διατήρηση αναληθών ή μη επικαιροποιημένων δεδομένων ενδέχεται να εκθέσει τα άτομα σε ιδιαίτερους κινδύνους και διακρίσεις.

Σύμφωνα με το άρθρο 4 δ του ν. 2472/97 τα δεδομένα πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Η κρίση για την εκπλήρωση του σκοπού και την καταστροφή των δεδομένων δεν επαφίεται στον υπεύθυνο επεξεργασίας αλλά ελέγχεται από την Αρχή Προστασίας Προσωπικών Δεδομένων. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων.

Σύμφωνα με τη δεύτερη παράγραφο του άρθρου 4 του ν. 2472/97, όπως τροποποιήθηκε ως άνω σύμφωνα με το άρθρο 20 παρ. 2 Ν. 3471/2006, η τήρηση των διατάξεων της προηγούμενης παραγράφου βαρύνει τον υπεύθυνο επεξεργασίας. Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί ή υφίστανται επεξεργασία κατά παράβαση της προηγούμενης παραγράφου καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας. Η Αρχή, εάν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επιβάλλει τη διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένων προσωπικού χαρακτήρα που έχουν ήδη συλλεγεί ή τύχει επεξεργασίας.

5.3 Τα δικαιώματα των προσώπων

Η νομοθεσία για την προστασία προσωπικών δεδομένων (ν. 2427/97) περιέχει ειδικούς κανόνες για τα δικαιώματα των προσώπων (άρθρα 11-14).

Ανεξάρτητα από τη νόμιμη βάση της συλλογής και επεξεργασίας δεδομένων (για ταυτοποίηση κλπ.) είναι αναγκαία η ενημέρωση των προσώπων για τη συλλογή και παραγωγή δεδομένων που συνεπάγονται οι διαδικασίες της ταυτοποίησης και αυθεντικοποίησης. Ο υπεύθυνος επεξεργασίας οφείλει (άρθρο 11), κατά το στάδιο της συλλογής των σχετικών δεδομένων προσωπικού χαρακτήρα, να ενημερώνει με τρόπο πρόσφορο και σαφή το συναλλασσόμενο-αιτούντα που είναι το υποκείμενο των δεδομένων για τα εξής τουλάχιστον στοιχεία:

- την ταυτότητά του και την ταυτότητα του τυχόν εκπροσώπου του,

- το σκοπό της επεξεργασίας,
- τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων,
- την ύπαρξη του δικαιώματος πρόσβασης.

Είναι επίσης, όπως προαναφέρθηκε, αναγκαίο να ενημερώνεται ο συναλλασσόμενος για την υποχρεωτικότητα ή μη παροχής των στοιχείων, καθώς και για τις συνέπειες μη παροχής υποχρεωτικών στοιχείων.

Ο νόμος δεν προσδιορίζει τους ειδικότερους τρόπους της ενημέρωσης. Η ενημέρωση μπορεί να γίνει και ηλεκτρονικά, είτε με γενική αναγραφή των σχετικών όρων στο δικτυακό τόπο, είτε εξειδικευμένα προς το συναλλασσόμενο με τη διοίκηση. Ακόμη και εάν επιλέγεται η πρώτη εναλλακτική λύση, σε κάθε περίπτωση είναι σκόπιμο να επισημαίνεται στον ηλεκτρονικά συναλλασσόμενο ειδικά και συγκεκριμένα η ύπαρξη και ο «τόπος» της ενημέρωσης.

Κατ' εφαρμογή των γενικών κανόνων, το υποκείμενο των δεδομένων, εν προκειμένω ο συναλλασσόμενος με τη διοίκηση, έχει τα δικαιώματα της πρόσβασης, διόρθωσης και αντίρρησης ως προς τα δεδομένα που τον αφορούν, όπως αυτά προσδιορίζονται στα άρθρα 12 και 13 του ν. 2472/97, όπως ισχύει.

5.4 Συμμόρφωση με διαδικαστικές προϋποθέσεις

Ο ν. 2472/97 έχει εισαγάγει σύστημα γνωστοποίησης των αρχείων και επεξεργασίας δεδομένων προσωπικού χαρακτήρα (άρθρο 6). Η συλλογή και επεξεργασία δεδομένων αναγκαίων για την ταυτοποίηση και την αυθεντικοποίηση θα πρέπει να γνωστοποιείται στην Αρχή Προστασίας Προσωπικών Δεδομένων.

Με τη γνωστοποίηση ο υπεύθυνος επεξεργασίας πρέπει απαραιτήτως να δηλώνει:

1. Το ονοματεπώνυμο ή την επωνυμία ή τον τίτλο του και τη διεύθυνσή του.
2. Τη διεύθυνση όπου είναι εγκατεστημένο το αρχείο ή ο κύριος εξοπλισμός που υποστηρίζει την επεξεργασία.
3. Την περιγραφή του σκοπού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.
4. Το είδος των δεδομένων προσωπικού χαρακτήρα που υφίστανται ή πρόκειται να υποστούν επεξεργασία ή περιέχονται ή πρόκειται να περιληφθούν στο αρχείο.
5. Το χρονικό διάστημα για το οποίο προτίθεται να εκτελεί την επεξεργασία ή να διατηρήσει το αρχείο.
6. Τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους ανακοινώνει ή ενδέχεται να ανακοινώνει τα δεδομένα προσωπικού χαρακτήρα.
7. Τις ενδεχόμενες διαβιβάσεις και το σκοπό της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες.
8. Τα βασικά χαρακτηριστικά του συστήματος και των μέτρων ασφαλείας του αρχείου ή της επεξεργασίας.

Η γνωστοποίηση της συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της ταυτοποίησης και αυθεντικοποίησης μπορεί να αποτελούν και μέρος γενικότερης γνωστοποίησης της συλλογής και επεξεργασίας προσωπικών δεδομένων για την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης.

Στην περίπτωση που είναι γνωστό ή πιθανολογείται ότι θα λάβει χώρα συλλογή και επεξεργασία «ευαίσθητων δεδομένων», όπως ορίζονται στο ν. 2472/97 τότε είναι αναγκαία η προηγούμενη γνωστοποίηση και η αίτηση προς την Αρχή Προστασίας Προσωπικών Δεδομένων για παροχή σχετικής άδειας (άρθρο 7 ν. 2472/97).

Στη διαδικασία της προηγούμενης γνωστοποίησης / άδειας υπόκειται και η διασύνδεση αρχείων (όπως ορίζεται στο άρθρο 2 στ του ν. 2472/97, δηλ. στη δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα άλλου αρχείου ή αρχείων). Συγκεκριμένα, εάν για την ταυτοποίηση και αυθεντικοποίηση πρόκειται να γίνει διασύνδεση, απαιτείται προηγούμενη άδεια της Αρχής («άδεια διασύνδεσης»), εάν α) ένα τουλάχιστον από τα αρχεία που πρόκειται να διασυνδεθούν περιέχει ευαίσθητα δεδομένα, β) με τη διασύνδεση πρόκειται να αποκαλυφθούν ευαίσθητα δεδομένα ή γ) εάν για την πραγματοποίηση της διασύνδεσης πρόκειται να γίνει χρήση ίδιου (ενιαίου) κωδικού αριθμού. Η άδεια διασύνδεσης της προηγούμενης παραγράφου χορηγείται ύστερα από ακρόαση των υπεύθυνων επεξεργασίας των αρχείων και αναφέρει απαραιτήτως το σκοπό για τον οποίο η διασύνδεση θεωρείται αναγκαία, το είδος των δεδομένων προσωπικού χαρακτήρα που αφορά η διασύνδεση, το χρονικό διάστημα για το οποίο επιτρέπεται η διασύνδεση, καθώς και τυχόν όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία των δικαιωμάτων και ελευθεριών και ιδίως του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων.

Εν γένει κρίνεται ότι το κανονιστικό πλαίσιο που αφορά την επεξεργασία προσωπικών δεδομένων, όπως αυτή περιγράφεται παραπάνω, είναι επαρκές. Τυχόν ειδικά ζητήματα μπορούν να αντιμετωπιστούν με την εξειδίκευση γενικών κανόνων κατά την εφαρμογή της νομοθεσίας και κυρίως κατά την εφαρμογή των αρχών της αναλογικότητας και του σκοπού. Τα όρια της νόμιμης δράσης συμπροσδιορίζονται εξάλλου και από τυχόν όρους και προϋποθέσεις που θα θέσει η Αρχή Προστασίας Προσωπικών Δεδομένων, αποφαινόμενη επί των αιτήσεων για άδειες επεξεργασίας ευαίσθητων δεδομένων και άδειες διασύνδεσης.

5.5 Υποχρεώσεις και ενέργειες της Διοίκησης

Οι ενέργειες που θα πρέπει να εκτελέσει η Διοίκηση σχετικά με την αυθεντικοποίηση πολιτών, επιχειρήσεων και φορέων σε υπηρεσίες ηλεκτρονικής διακυβέρνησης περιλαμβάνουν τα εξής:

1. Θα πρέπει να συνταχθούν έντυπα για την παροχή και λήψη συγκατάθεσης, τα οποία θα δίδονται στους αιτούμενους την εγγραφή. Υπενθυμίζεται ότι ο νόμος 2472/97 δεν απαιτεί έγγραφο τύπο παρά μόνο για την επεξεργασία ευαίσθητων δεδομένων. Ωστόσο καθώς η συγκατάθεση θα πρέπει να είναι σαφής, ρητή, ειδική και «ενημερωμένη» συνιστάται να ακολουθείται ο έγγραφος τύπος ακόμη και για την περίπτωση αυτή.
2. Κατά την αίτηση για εγγραφή σε διάφορες υπηρεσίες θα πρέπει να καθίσταται σαφές στους αιτούντες, εάν και ποια δεδομένα είναι αναγκαία για την εγγραφή.

3. Κατά την αίτηση για λήψη υπηρεσιών θα πρέπει να καθίσταται σαφές στους αιτούντες ποια και τι είδους δεδομένα είναι αναγκαία για την επεξεργασία και τη διεκπεραίωση της αίτησής τους.
4. Κατά την αίτηση θα πρέπει να γίνεται σαφής διαχωρισμός, τόσο στους αιτούντες όσο και στους χειριστές, μεταξύ των απαραίτητων δεδομένων και των δεδομένων των οποίων η παροχή είναι προαιρετική.
5. Θα πρέπει να γίνεται διαχωρισμός των δεδομένων ταυτοποίησης και των δεδομένων που αφορούν το περιεχόμενο της αιτηθείσας ή παρεχόμενης πληροφορίας και υπηρεσίας.
6. Ανεξάρτητα από τη συγκατάθεση, δηλ. ακόμη και εάν η παροχή δεδομένων προβλέπεται ρητά από διάταξη νόμου ως υποχρεωτική (όπως π.χ. στις φορολογικές δηλώσεις), θα πρέπει κατά την εγγραφή σε υπηρεσίες να ενημερώνονται οι αιτούντες, σύμφωνα με το άρθρο 11 του ν. 2472/97, τουλάχιστον για την ταυτότητά του υπεύθυνου επεξεργασίας των δεδομένων και την ταυτότητα του τυχόν εκπροσώπου του, το σκοπό της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων και την ύπαρξη του δικαιώματος πρόσβασης.
7. Η ενημέρωση μπορεί να γίνει και ηλεκτρονικά, με γενική αναγραφή των σχετικών όρων στο δικτυακό τόπο. Στην περίπτωση αυτή θα πρέπει ο «τόπος» της ενημέρωσης να είναι εμφανής και να επισημαίνεται στον εγγραφόμενο - ηλεκτρονικά συναλλασσόμενο.
8. Θα πρέπει να γίνουν όλες οι απαραίτητες διαδικαστικές ενέργειες έναντι της Αρχής Προστασίας Προσωπικών Δεδομένων που απαιτούνται κατά περίπτωση από το νόμο: α) γνωστοποίηση για τη συλλογή και επεξεργασία απλών δεδομένων (συμπεριλαμβάνονται τα οικονομικά δεδομένα, αυτά δηλ. που καλύπτονται από το φορολογικό απόρρητο), β) αίτηση για άδεια στην περίπτωση της επεξεργασίας ευαίσθητων δεδομένων γ) αίτηση για άδεια διασύνδεσης εφόσον γίνεται διασύνδεση αρχείων, εκ των οποίων έστω το ένα περιλαμβάνει ευαίσθητα ή γίνεται χρήση ενιαίου κωδικού αριθμού. Οι ενέργειες αυτές είναι απαραίτητες εφόσον η παροχή υπηρεσιών δεν καλύπτεται από προηγούμενες γνωστοποιήσεις/ αιτήσεις προς την Αρχή. Στην περίπτωση αυτή, δηλαδή όταν έχουν κατατεθεί γνωστοποιήσεις/ αιτήσεις που δεν καλύπτουν την ταυτοποίηση/ ηλεκτρονική παροχή υπηρεσιών, πρέπει να κατατεθούν συμπληρωματικές γνωστοποιήσεις/ αιτήσεις ή τροποποίηση των κατατεθειμένων σύμφωνα με το άρθρο 6 § 4 του ν. 2472/97.
9. Θα πρέπει να επισημαίνεται στους χειριστές των αιτήσεων εγγραφής ή των αιτήσεων για ηλεκτρονική παροχή υπηρεσιών ότι τα προσωπικά δεδομένα θα πρέπει να είναι ακριβή και επικαιροποιημένα. Θα ήταν ίσως σκόπιμο να εισαχθούν συγκεκριμένες προθεσμίες (π.χ. ανά έτος) στο πλαίσιο των οποίων θα ελέγχεται η επικαιροποίηση των δεδομένων.
10. Θα πρέπει να επισημαίνεται στους χειριστές των αιτήσεων εγγραφής ή των αιτήσεων για ηλεκτρονική παροχή υπηρεσιών η υποχρέωση διαγραφής/ καταστροφής δεδομένων που δεν είναι πλέον αναγκαία για την εκπλήρωση ενός σκοπού. Λόγω της πολλαπλότητας

των σκοπών δεν είναι δυνατόν να γίνει περαιτέρω εξειδίκευση της συγκεκριμένης υποχρέωσης.

11. Τα αρχεία-δεδομένα θα πρέπει να καταστρέφονται μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού. Για την καταστροφή θα πρέπει να ακολουθούνται οι οδηγίες της Αρχής Προστασίας Προσωπικών Δεδομένων που περιέχονται στη σχετική Οδηγία 1/2005 (http://www.dpa.gr/secure).

6. ΤΑΥΤΟΠΟΙΗΣΗ ΚΑΤΑ ΤΗ ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

Με τον όρο ταυτοποίηση, υπό το πρίσμα του ΠΨΑ, νοείται η διαδικασία δήλωσης ταυτότητας από το χρήστη στις υπηρεσίες ηλεκτρονικής διακυβέρνησης. Καθώς οι χρήστες-πολίτες αξιοποιούν διαφορετικού είδους «*ταυτότητες*» στις συναλλαγές τους με τη Δημόσια Διοίκηση, η διαδικασία-μέθοδος ταυτοποίησης που θα αξιοποιηθεί στις αντίστοιχες υπηρεσίες ηλεκτρονικής διακυβέρνησης θα επηρεάσει σε μεγάλο βαθμό το ΠΨΑ, καθώς οι διαφορετικοί τρόποι και μέθοδοι ταυτοποίησης δημιουργούν διαφορετικού είδους νομικούς, θεσμικούς ή ακόμα και «τεχνικούς» περιορισμούς.

Λαμβάνοντας υπόψη την Ελληνική συνταγματική και έννομη τάξη και τις υπάρχουσες μεθόδους ταυτοποίησης για συναλλαγές με το Ελληνικό Δημόσιο προτείνεται η ταυτοποίηση των χρηστών σε ηλεκτρονικές υπηρεσίες της δημόσιας διοίκησης μέσω της Κεντρικής Διαδικτυακής Πύλης (ΚΔΠ) με αξιοποίηση ξεχωριστών αναγνωριστικών των χρηστών ανά υπηρεσία.

Με τη συγκεκριμένη προτεινόμενη τεχνική ταυτοποίησης, με χρήση διαφορετικού αναγνωριστικού για κάθε υπηρεσία, οι διαδικασίες της εγγραφής και της αυθεντικοποίησης πραγματοποιούνται στην ΚΔΠ, χωρίς να απαιτείται να έχουν οι χρήστες προηγουμένως εγγραφεί στις ανεξάρτητες ηλεκτρονικές υπηρεσίες, αλλά και ενδεχόμενη εγγραφή τους σε αυτές να μη σχετίζεται με τη διαδικασία αυθεντικοποίησης στην ΚΔΠ και να μην προκύπτει καμία απολύτως συσχέτιση ή πρόβλημα από το γεγονός αυτό για την ολοκλήρωση των παρεχόμενων υπηρεσιών. Κατά τη διάρκεια της εγγραφής του χρήστη στην ΚΔΠ, ο χρήστης πρέπει να εισάγει τα διαφορετικά αναγνωριστικά που απαιτεί ο κάθε φορέας προκειμένου να τον ταυτοποιήσει. Τα αναγνωριστικά αυτά (π.χ. ΑΦΜ, ΑΔΤ, ΑΜΚΑ κλπ.), αν επιθυμεί ο χρήστης, είναι δυνατόν να αποθηκεύονται στην ΚΔΠ και να συνθέτουν τον ψηφιακό φάκελο αναγνωριστικών για το συγκεκριμένο χρήστη. Όταν ο χρήστης επιθυμεί να χρησιμοποιήσει μία ηλεκτρονική υπηρεσία, η ΚΔΠ αναζητά στον ψηφιακό φάκελο αναγνωριστικών του χρήστη το αναγνωριστικό που απαιτείται για την ταυτοποίησή του στη συγκεκριμένη υπηρεσία. Εάν η αναζήτηση είναι επιτυχής, το αναγνωριστικό αποστέλλεται στον εξυπηρετητή της αντίστοιχης υπηρεσίας προκειμένου ο χρήστης να ταυτοποιηθεί και να ξεκινήσει η διαδικασία της αυθεντικοποίησής του. Σε περίπτωση που η αναζήτηση δεν είναι επιτυχής ο χρήστης ενημερώνεται από την ΚΔΠ ότι δεν μπορεί να χρησιμοποιήσει τη συγκεκριμένη ηλεκτρονική υπηρεσία.

Η αποθήκευση του κάθε αναγνωριστικού του χρήστη στην ΚΔΠ δεν είναι νόμιμο να είναι υποχρεωτική. Θα πρέπει να παρέχεται η δυνατότητα, σε κάθε επικοινωνία ο χρήστης να εισάγει εκ νέου τα αναγνωριστικά του ώστε να αποφεύγεται η τήρησή τους από την ΚΔΠ. Η επιλογή, περί τήρησης ή μη των αναγνωριστικών από την ΚΔΠ, θα πρέπει να είναι του χρήστη και να δηλώνεται στη φάση της αρχικής εγγραφής, με τις προϋποθέσεις που ορίζει ο Ν. 2472/97.

Για κάθε νέα ηλεκτρονική υπηρεσία που θα προσφέρεται μέσω της ΚΔΠ είναι απαραίτητο η ΚΔΠ να ενημερώνεται από το δημόσιο φορέα (ιδιοκτήτη της υπηρεσίας) για τα ακόλουθα:

α) Το Αναγνωριστικό που αξιοποιεί η συγκεκριμένη υπηρεσία για ταυτοποίηση (π.χ. Α.Φ.Μ., Α.Δ.Τ.)

β) Το Επίπεδο Εμπιστοσύνης στο οποίο εντάσσεται η υπηρεσία

γ) Το Επίπεδο Αυθεντικοποίησης που απαιτείται, το οποίο προκύπτει από το Επίπεδο Εμπιστοσύνης, καθώς και το συγκεκριμένο μηχανισμό αυθεντικοποίησης στις περιπτώσεις ύπαρξης εναλλακτικών επιλογών που επιθυμεί να υιοθετήσει ο φορέας για τη συγκεκριμένη υπηρεσία

δ) Το Επίπεδο Εγγραφής, το οποίο προκύπτει από το Επίπεδο Εμπιστοσύνης, και το οποίο θα υιοθετηθεί από το φορέα για τη συγκεκριμένη υπηρεσία

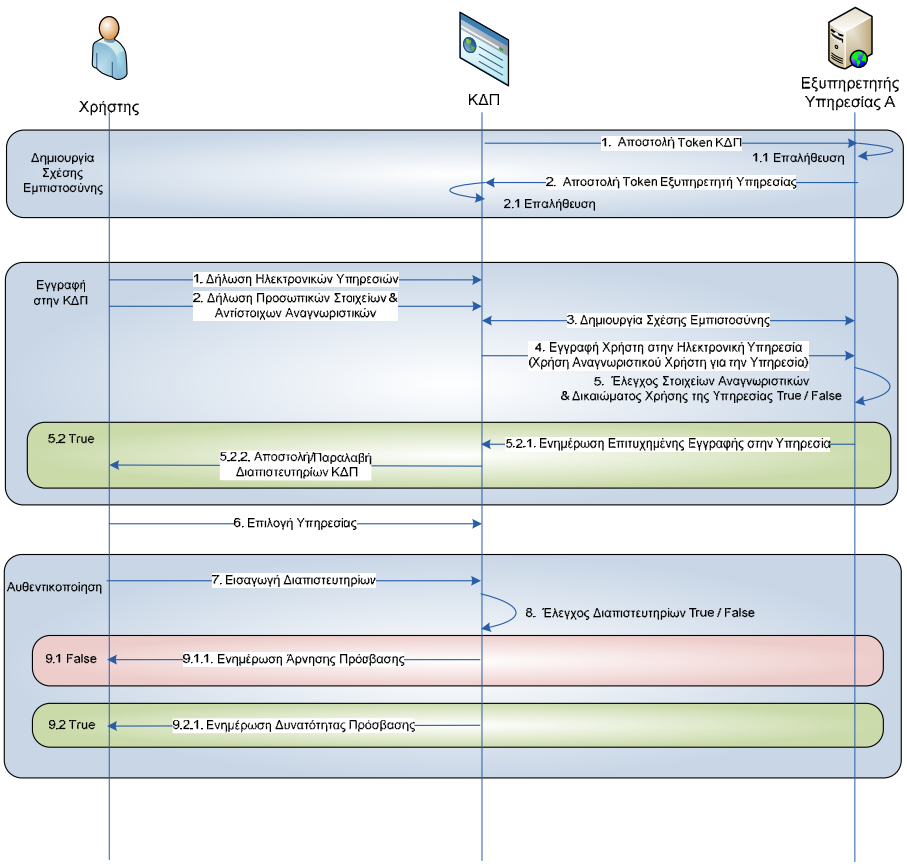
ε) Το Διακριτικό (token) που θα αξιοποιηθεί για τη δημιουργία αμοιβαίας σχέσης εμπιστοσύνης μεταξύ ΚΔΠ και φορέα.

6.1 Περιγραφή λειτουργίας

Δεδομένης της ύπαρξης της ΚΔΠ ως διαμεσολαβητή μεταξύ χρήστη και εξυπηρετητή κάθε ηλεκτρονικής υπηρεσίας κάθε δημόσιας υπηρεσίας, είναι επιτακτική η ανάγκη για την οικοδόμηση μιας σχέσης εμπιστοσύνης μεταξύ της ΚΔΠ και του αντίστοιχου εξυπηρετητή, έτσι ώστε να επιτυγχάνεται η απαιτούμενη βεβαιότητα για τις "ταυτότητες" των οντοτήτων αυτών. Η δημιουργία της σχέσης αυτής βασίζεται στην ανταλλαγή ενός διακριτικού (token) που αξιοποιείται για την ταυτοποίηση και αυθεντικοποίησή τους. Επίσης, η δημιουργία ενός Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network) μεταξύ τους μπορεί να διασφαλίσει, μεταξύ άλλων, και την εμπιστευτικότητα και ακεραιότητα των δεδομένων που ανταλλάσσονται μέσω του ασφαλούς καναλιού (secure channel) που δημιουργείται. Επιπλέον ενδέχεται να απαιτούνται και υπηρεσίες μη αποποίησης αποστολής και λήψης μηνύματος, καθώς και υπηρεσίες χρονοσήμανσης.

Για να μπορέσει ένας πολίτης να χρησιμοποιήσει μία ηλεκτρονική υπηρεσία θα πρέπει πρώτα να εγγραφεί στην ΚΔΠ. Συγκεκριμένα, ο αιτών χρήστης συμπληρώνει την αίτηση εγγραφής δηλώνοντας τα στοιχεία του, επιλέγει μία προς μία τις ηλεκτρονικές υπηρεσίες που επιθυμεί να χρησιμοποιήσει, δηλώνει τα μοναδικά αναγνωριστικά που αντιστοιχούν στις υπηρεσίες που επέλεξε (π.χ. ΑΦΜ για την περίπτωση οικονομικών υπηρεσιών) και δηλώνει αν επιθυμεί, ανά παρεχόμενη υπηρεσία, να αποθηκευθεί στην ΚΔΠ το ανά περίπτωση απαιτούμενο αναγνωριστικό. Η ΚΔΠ δημιουργεί μία σχέση εμπιστοσύνης με τον εξυπηρετητή της κάθε υπηρεσίας που επιθυμεί να εγγραφεί ο αιτών χρήστης, ελέγχει τα στοιχεία του και κατά πόσο έχει δικαίωμα χρήσης της ηλεκτρονικής υπηρεσίας. Εφόσον τα αποτελέσματα των παραπάνω ελέγχων είναι θετικά, ο χρήστης ενημερώνεται για την επιτυχημένη εγγραφή του στην ΚΔΠ και τις ηλεκτρονικές υπηρεσίες και ακολούθως παραλαμβάνει τα διαπιστευτήριά του, σύμφωνα με το πλαίσιο που ορίζει ρητά η ΚΔΠ και ανάλογα με το επίπεδο εμπιστοσύνης της κάθε παρεχόμενης ηλεκτρονικής υπηρεσίας.

Ακολούθως, προκειμένου να χρησιμοποιήσει κάποια ηλεκτρονική υπηρεσία, ο χρήστης επισκέπτεται την ΚΔΠ και επιλέγει την υπηρεσία αυτή. Η ΚΔΠ, γνωρίζοντας το επίπεδο εμπιστοσύνης της συγκεκριμένης υπηρεσίας, άρα και το επίπεδο αυθεντικοποίησης που απαιτείται για τους αιτούντες προσπέλασης στην υπηρεσία αυτή, ενημερώνει το χρήστη για τα διαπιστευτήρια που απαιτείται να παρουσιάσει προκειμένου να του επιτραπεί η πρόσβαση. Ο χρήστης εισάγει τα διαπιστευτήριά του και εφόσον το αποτέλεσμα του σχετικού ελέγχου είναι θετικό, μπορεί να κάνει πλέον χρήση της αιτούμενης υπηρεσίας. Για την υποστήριξη παροχής επιπρόσθετων υπηρεσιών μη-αποποίησης, η ΚΔΠ διατηρεί αρχείο καταγραφής (log file) κάθε προσπάθειας αυθεντικοποίησης. Σε περίπτωση που η προσπάθεια είναι επιτυχημένη, το αρχείο περιλαμβάνει την ώρα, την ημερομηνία, το όνομα του χρήστη (username) και τα διαπιστευτήρια που αντιστοιχούν στη συγκεκριμένη σύνοδο. Σε περίπτωση που αυτή είναι αποτυχημένη, το αρχείο περιλαμβάνει μόνον την ώρα, την ημερομηνία και το όνομα του χρήστη (username). Η παραπάνω διαδικασία παρουσιάζεται στην ακόλουθη εικόνα:

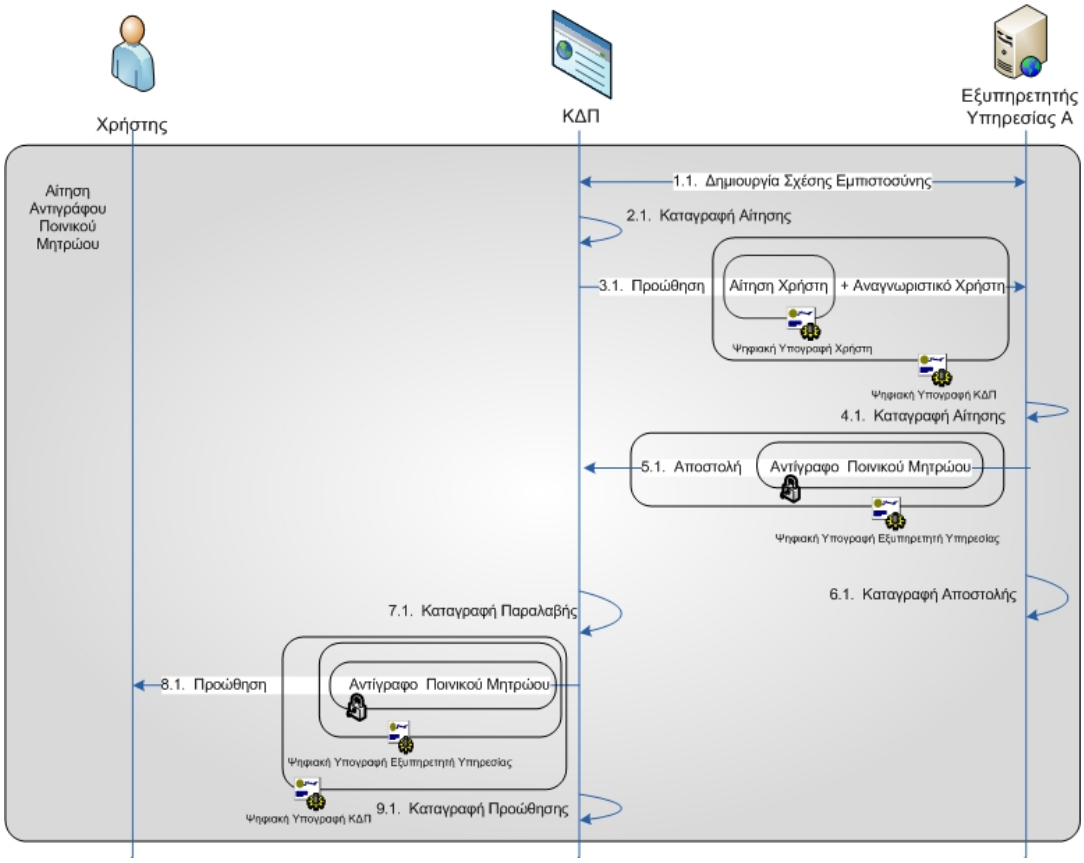


Εικόνα 1: Αρχικοποίηση - Εγγραφή – Αυθεντικοποίηση (με ταυτοποίηση στην ΚΔΠ και δι' αυτής στην Υπηρεσία)

6.1.1 Αξιοποίηση υπηρεσιών επιπέδου εμπιστοσύνης 3

Οι ενέργειες που πραγματοποιούνται στη περίπτωση που ο χρήστης ενεργοποιεί υπηρεσία επιπέδου εμπιστοσύνης 3 (π.χ. αίτηση χορήγησης αντιγράφου πιστοποιητικού ποινικού μητρώου) παρουσιάζονται στην Εικόνα 2. Συγκεκριμένα μετά την επιτυχή ολοκλήρωση της διαδικασίας αυθεντικοποίησης, δημιουργείται η αμοιβαία σχέση εμπιστοσύνης μεταξύ της ΚΔΠ και του εξυπηρετητή της υπηρεσίας. Στη συνέχεια η ΚΔΠ καταγράφει την αίτηση του χρήστη και την προωθεί στον εξυπηρετητή της υπηρεσίας μαζί με το αναγνωριστικό του χρήστη. Η αίτηση η οποία προωθείται στον εξυπηρετητή είναι υπογεγραμμένη ψηφιακά από το χρήστη, ούτως ώστε να αποδεικνύεται ότι ο χρήστης είναι ο εντολέας της ενέργειας αυτής. Η ΚΔΠ με τη σειρά της υπογράφει την αίτηση του χρήστη και την αποστέλλει στον εξυπηρετητή της υπηρεσίας. Ο εξυπηρετητής της υπηρεσίας καταγράφει την αίτηση που παρέλαβε και στη συνέχεια αποστέλλει στην ΚΔΠ τα δεδομένα που ζητήθηκαν. Δεδομένης της κρισιμότητας των δεδομένων, αφού η υπηρεσία ανήκει στο υψηλότερο Επίπεδο Εμπιστοσύνης, ο εξυπηρετητής κρυπτογραφεί τα δεδομένα με το δημόσιο κλειδί του χρήστη, τα υπογράφει ψηφιακά και τα προωθεί στην ΚΔΠ, καταγράφοντας παράλληλα την αποστολή. Η ΚΔΠ, με τη σειρά της, καταγράφει την παραλαβή, ελέγχει την εγκυρότητα της ψηφιακής υπογραφής του εξυπηρετητή της υπηρεσίας, η οποία συνοδεύει τα δεδομένα και τα προωθεί στο χρήστη καταγράφοντας ταυτόχρονα την αποστολή τους. Ο χρήστης αποκρυπτογραφεί τα δεδομένα που παραλαμβάνει κάνοντας χρήση του ιδιωτικού του κλειδιού[2] και επαληθεύει την προέλευση και την ακεραιότητά τους μέσω της ψηφιακής υπογραφής της ΚΔΠ και του εξυπηρετητή που τα συνοδεύουν.

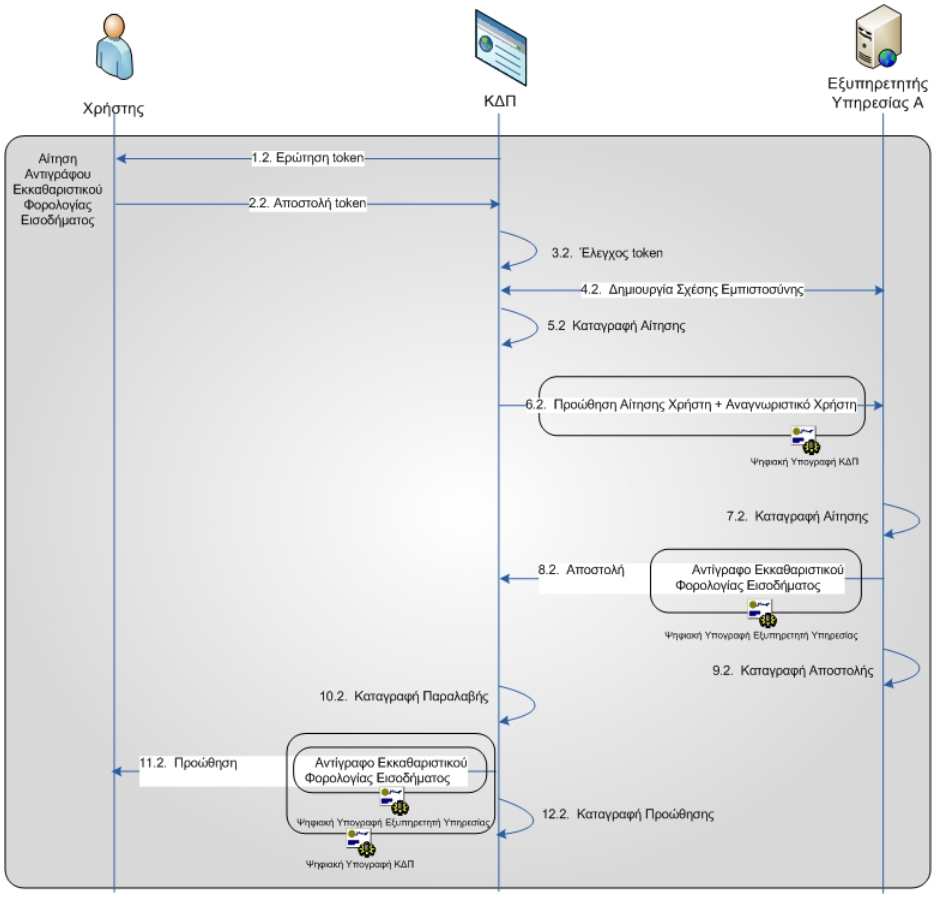
[2] Με το δημόσιο κλειδί του χρήστη κρυπτογραφείται κλειδί συμμετρικής κρυπτογράφησης, το οποίο με τη σειρά του χρησιμοποιείται δευτερογενώς για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων (ψηφιακός φάκελος – digital envelope)



Εικόνα 2: Χρήση Υπηρεσίας Επιπέδου Εμπιστοσύνης 3 (με ταυτοποίηση στην ΚΔΠ και δι' αυτής στην Υπηρεσία)

6.1.2 Αξιοποίηση υπηρεσιών επιπέδου εμπιστοσύνης 2

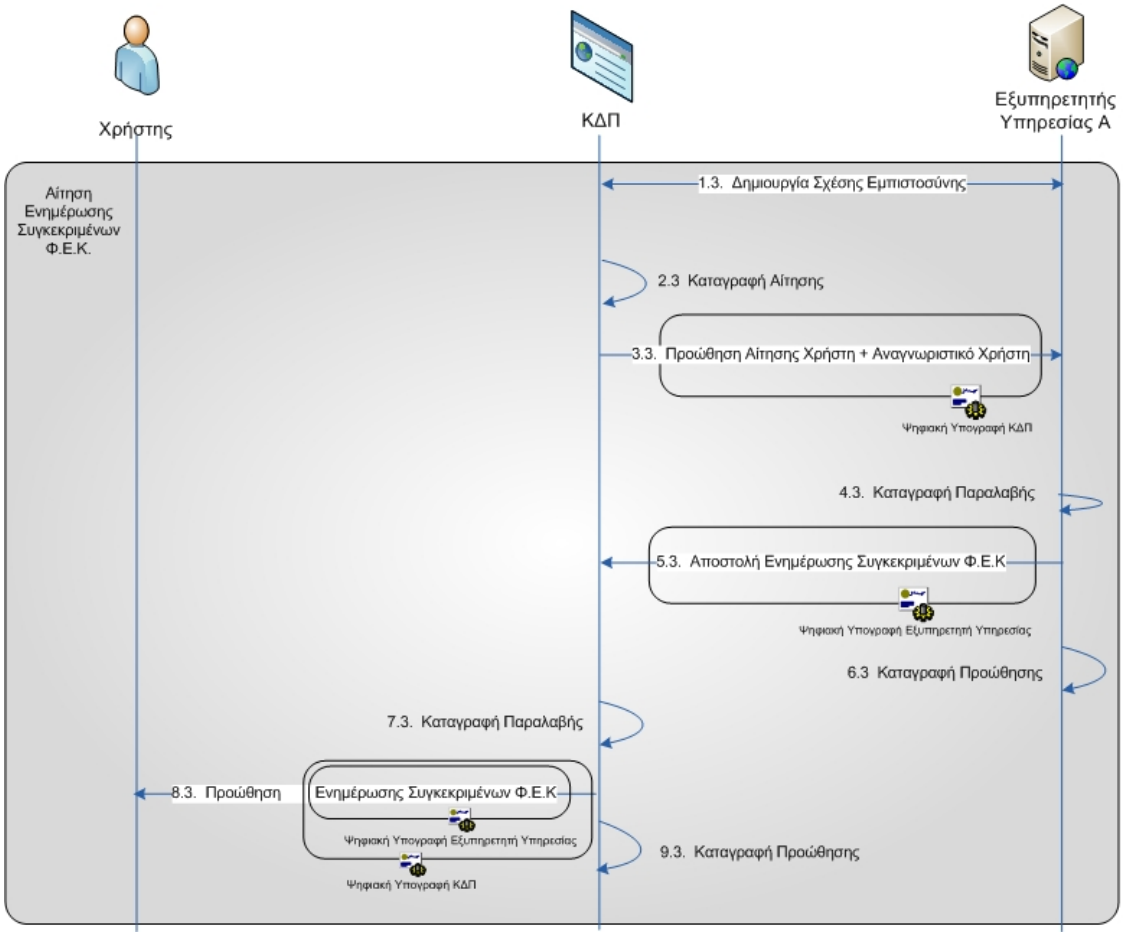
Οι ενέργειες που πραγματοποιούνται για υπηρεσίες επιπέδου εμπιστοσύνης 2 (π.χ. αίτηση χορήγησης αντιγράφου εκκαθαριστικού σημειώματος φορολογίας εισοδήματος) αποτυπώνονται στην Εικόνα 3. Η ΚΔΠ ζητά από το χρήστη να παρουσιάσει τα διαπιστευτήρια που έχει στην κατοχή του, διαπιστευτήρια τα οποία έχουν παραληφθεί από το χρήστη κατά τη διαδικασία της εγγραφής του. Εφόσον η αυθεντικοποίηση ολοκληρωθεί με επιτυχία, δημιουργείται η αμοιβαία σχέση εμπιστοσύνης μεταξύ της ΚΔΠ και του εξυπηρετητή της υπηρεσίας. Σε περίπτωση που δεν αξιοποιούνται συνθηματικά μιας χρήσης, οι διαδικασίες 1.2, 2.2 & 3.2 της Εικόνα 3 παραλείπονται. Στη συνέχεια η ΚΔΠ καταγράφει την αίτηση του χρήστη και την προωθεί στον εξυπηρετητή της υπηρεσίας. Η αίτηση, μαζί με το αναγνωριστικό του χρήστη για την υπηρεσία αυτή, προωθούνται στον εξυπηρετητή ψηφιακά υπογεγραμμένα από την ΚΔΠ. Ο εξυπηρετητής της υπηρεσίας καταγράφει την αίτηση που παρέλαβε και αποστέλλει στην ΚΔΠ τα δεδομένα που ζητήθηκαν. Δεδομένης της απαίτησης για μη-αποποίηση αποστολής των δεδομένων, ο εξυπηρετητής υπογράφει ψηφιακά τα δεδομένα με το ψηφιακό πιστοποιητικό του, καταγράφοντας παράλληλα την αποστολή αυτή. Η ΚΔΠ, με τη σειρά της, καταγράφει την παραλαβή και επαληθεύει την ψηφιακή υπογραφή που τα συνοδεύει. Τέλος, προωθεί στο χρήστη τα δεδομένα με την ψηφιακή υπογραφή του εξυπηρετητή, αφού επιπλέον τα έχει υπογράψει ψηφιακά και αυτή και καταγράφει την αποστολή τους.



Εικόνα 3: Χρήση Υπηρεσίας Επιπέδου Εμπιστοσύνης 2 (με ταυτοποίηση στην ΚΔΠ και δι' αυτής στην Υπηρεσία)

6.1.3 Αξιοποίηση υπηρεσιών επιπέδου εμπιστοσύνης 1

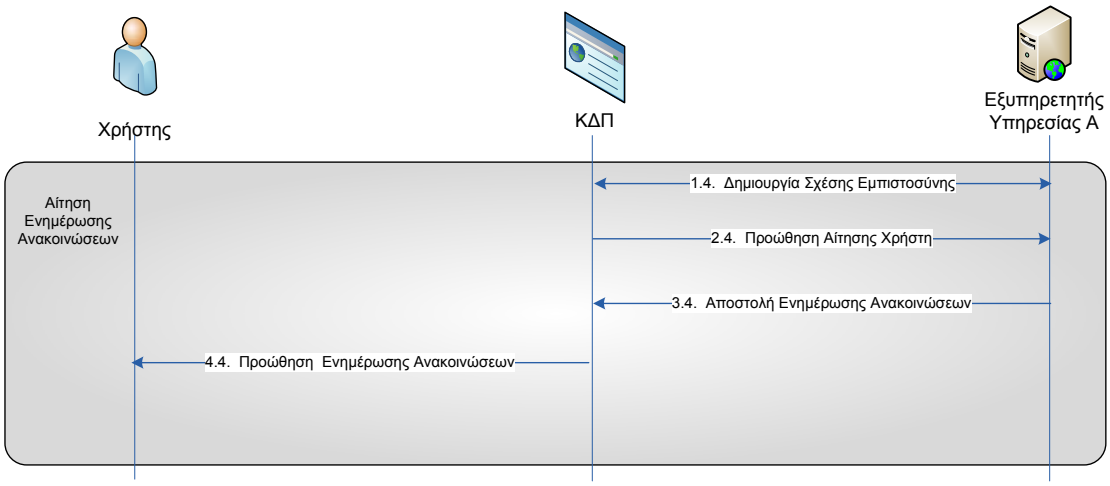
Για υπηρεσίες που εντάσσονται στο επίπεδο εμπιστοσύνης 1, οι αντίστοιχες ενέργειες παρουσιάζονται στην Εικόνα 4. Η ΚΔΠ καταγράφει την αίτηση του χρήστη και την προωθεί στον εξυπηρετητή της υπηρεσίας μαζί με το μοναδικό αναγνωριστικό του χρήστη, αφού πρώτα τα υπογράψει ψηφιακά. Ο εξυπηρετητής της υπηρεσίας καταγράφει την αίτηση που παρέλαβε και στη συνέχεια αποστέλλει στην ΚΔΠ τα δεδομένα που ζητήθηκαν. Προκειμένου να διαφυλαχθεί η μη αποποίηση αποστολής των δεδομένων, ο εξυπηρετητής υπογράφει ψηφιακά τα δεδομένα καταγράφοντας παράλληλα την αποστολή αυτή. Η ΚΔΠ, με τη σειρά της, καταγράφει την παραλαβή, ελέγχει την εγκυρότητα της ψηφιακής υπογραφής που συνοδεύει τα δεδομένα και τα προωθεί στο χρήστη μαζί με την ψηφιακή υπογραφή του εξυπηρετητή, υπογράφοντάς τα ψηφιακά και αυτή.



Εικόνα 4: Χρήση Υπηρεσίας Επιπέδου Εμπιστοσύνης 1 (με ταυτοποίηση στην ΚΔΠ και δι' αυτής στην Υπηρεσία)

6.1.4 Αξιοποίηση υπηρεσιών επιπέδου εμπιστοσύνης 0

Για τις περιπτώσεις υπηρεσιών επιπέδου εμπιστοσύνης 0, η ΚΔΠ μεταφέρει την αίτηση του χρήστη στον αντίστοιχο εξυπηρετητή έχοντας προηγουμένως δημιουργήσει τη σχέση εμπιστοσύνης με αυτόν. Στη συνέχεια ο εξυπηρετητής της υπηρεσίας αποστέλλει τα δεδομένα στην ΚΔΠ, η οποία με τη σειρά της τα προωθεί στο χρήστη. Η διαδικασία αυτή αποτυπώνεται στην Εικόνα 5.



Εικόνα 5: Χρήση Υπηρεσίας Επιπέδου Εμπιστοσύνης 0 (με ταυτοποίηση στην ΚΔΠ και δι' αυτής στην Υπηρεσία)

6.2 Πλεονεκτήματα & Μειονεκτήματα

Τα πλεονεκτήματα της συγκεκριμένης υλοποίησης είναι πολλαπλά: συμμορφώνεται πλήρως με το ισχύον νομοθετικό πλαίσιο, αναιρεί την οποιαδήποτε απαίτηση περί ύπαρξης πολλαπλών σημείων αυθεντικοποίησης του χρήστη, όπως κυρίως και την ανάγκη έκδοσης πολλαπλών διαπιστευτηρίων ή τήρησής τους στην ΚΔΠ. Επιπρόσθετα, η λύση αυτή επιτρέπει την υποστήριξη υπηρεσιών διαλειτουργικότητας, μέσω της ΚΔΠ, μεταξύ διαφορετικών υπηρεσιών, όπου αυτό είναι επιθυμητό.

Τα «μειονεκτήματα» της συγκεκριμένης υλοποίησης αφορούν στις τεχνολογικές απαιτήσεις αναφορικά με τη δημιουργία συνόδων μεταξύ της ΚΔΠ και του εξυπηρετητή της υπηρεσίας κάθε φορέα, με απολύτως ικανοποιητικό επίπεδο εμπιστοσύνης (trust) και υψηλής διαθεσιμότητας. Επίσης απαιτείται η ανάπτυξη συγκεκριμένου λεπτομερούς πλαισίου για τον έλεγχο (auditing) των παρεχόμενων υπηρεσιών από την ΚΔΠ.

7. ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΟΝΤΟΤΗΤΩΝ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Με τον όρο αυθεντικοποίηση νοείται η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Συγκεκριμένα, κατά τη διαδικασία αυθεντικοποίησης αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός χρήστη ή κάποιων χαρακτηριστικών της. Σε καμία περίπτωση δε θα πρέπει η αυθεντικοποίηση ενός χρήστη να συγχέεται με την παροχή εξουσιοδότησης (authorization) στους προσφερόμενους πληροφοριακούς πόρους.

Στην ενότητα αυτή παρουσιάζονται οι εναλλακτικοί μηχανισμοί και μέθοδοι αυθεντικοποίησης που είναι ρεαλιστικά εφικτό να αξιοποιηθούν στις υπηρεσίες ηλεκτρονικής διακυβέρνησης. Θα πρέπει να σημειωθεί ότι η επιλογή κάποιας συγκεκριμένης μεθόδου αυθεντικοποίησης δεν αποτελεί αντικείμενο της παρούσας ενότητας, καθώς εξαρτάται από το επίπεδο εμπιστοσύνης στο οποίο έχει ενταχθεί η υπηρεσία (για περισσότερες λεπτομέρειες βλέπε ενότητα 9). Επισημαίνεται, όμως, ότι όσο μεγαλύτερο είναι το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται μία υπηρεσία, τόσο ισχυρότερος μηχανισμός αυθεντικοποίησης απαιτείται.

7.1 Μηχανισμοί Αυθεντικοποίησης

Τα συστήματα αυθεντικοποίησης είναι δυνατό να κατηγοριοποιηθούν με βάση τη μέθοδο η οποία αξιοποιείται για την πιστοποίηση της ταυτότητας ενός χρήστη. Οι μέθοδοι αυτοί διαχωρίζονται [24] με βάση τα εξής χαρακτηριστικά:

- Κάτι που γνωρίζει (something known) ο χρήστης, για παράδειγμα ένα συνθηματικό
- Κάτι που κατέχει (something possessed) ο χρήστης, για παράδειγμα μία έξυπνη κάρτα
- Κάποιο χαρακτηριστικό γνώρισμα (something inherent), για παράδειγμα βιομετρικές μέθοδοι
- Συνδυασμός κάποιων εκ των ανωτέρω χαρακτηριστικών γνωρισμάτων

Οι μηχανισμοί αυθεντικοποίησης, ανεξάρτητα από τα χαρακτηριστικά που υιοθετούν, αξιοποιούν δύο τύπους κλειδιών:

- Μυστικά κλειδιά: Σε αυτά συμπεριλαμβάνονται τα συνθηματικά, οι κωδικοί και τα συμμετρικά κλειδιά.
- Ασύμμετρα κλειδιά: Σε αυτά συμπεριλαμβάνονται ζεύγη κλειδιών, από τα οποία το ένα είναι δημόσια γνωστό (δημόσιο κλειδί), ενώ το άλλο παραμένει μυστικό (ιδιωτικό κλειδί).

Συνεπώς τα συστήματα αυθεντικοποίησης μπορούν να χαρακτηριστούν ως μονοδιάστατα ή πολυδιάστατα, ανάλογα με τα διαφορετικά χαρακτηριστικά που αξιοποιούν, ώστε να εξασφαλίσουν το επιθυμητό επίπεδο βεβαιότητας για την ταυτότητα κάποιας ηλεκτρονικής οντότητας. Για παράδειγμα, η χρήση ενός ιδιωτικού κλειδιού ως διακριτικού αυθεντικοποίησης

που προστατεύεται από το συνθηματικό του χρήστη αντιπροσωπεύει ένα χαρακτηριστικό παράδειγμα διδιάστατου συστήματος αυθεντικοποίησης.

7.2 Διακριτικά Αυθεντικοποίησης

Τα διακριτικά αυθεντικοποίησης αξιοποιούνται για τον έλεγχο της ορθότητας της ηλεκτρονικής ταυτότητας των χρηστών ενός συστήματος. Ανάλογα με το επιθυμητό επίπεδο ασφάλειας υιοθετείται και ο αντίστοιχος συνδυασμός χαρακτηριστικών και κλειδιών αυθεντικοποίησης [20] όπως προαναφέρθηκε στην ενότητα 7.1.

7.2.1 Συνθηματικά

Τα συνθηματικά αποτελούν τον ευρύτερα αποδεκτό τρόπο αυθεντικοποίησης, όπου ο χρήστης πιστοποιεί την ορθότητα της ταυτότητάς του κάνοντας χρήση ενός μυστικού που είναι γνωστό μόνο σε αυτόν. Ο χρήστης πρέπει να απομνημονεύσει το μυστικό κωδικό (something known) και να μην τον αποκαλύπτει σε άλλους χρήστες ή οντότητες. Συνήθως τα συνθηματικά δεν αποθηκεύονται καθώς επιλέγονται με τρόπο ώστε να είναι ευκολομνημόνευτα.

7.2.2 Διακριτικά συνθηματικών μιας χρήσης (one time password tokens)

Τα διακριτικά συνθηματικών μιας χρήσης είναι συσκευές υλικού οι οποίες αξιοποιούνται για τη δημιουργία συνθηματικών, τα οποία δεν απαιτείται να απομνημονεύει ο χρήστης και τα οποία χρησιμοποιούνται μόνο μια φορά. Η παραγωγή των συνθηματικών στηρίζεται σε συγκεκριμένους αλγόριθμους κρυπτογράφησης. Η επαναχρησιμοποίηση ενός κωδικού για μελλοντική αυθεντικοποίηση του χρήστη δεν είναι δυνατή.

7.2.3 Διακριτικά Χαλαρής Αποθήκευσης (soft tokens)

Τα διακριτικά χαλαρής αποθήκευσης αναφέρονται σε μυστικά κλειδιά, τα οποία αποθηκεύονται σε κάποιο μέσο αποθήκευσης όπως σκληρός δίσκος, CD, USB token κ.λπ. Τα κλειδιά είναι αποθηκευμένα σε κρυπτογραφημένη μορφή, ενώ η προσπέλασή τους είναι δυνατή μόνο με τη χρήση του κατάλληλου συνθηματικού.

7.2.4 Διακριτικά Υλικού – Σκληρής Αποθήκευσης (hard tokens)

Τα διακριτικά υλικού σκληρής αποθήκευσης αναφέρονται σε συσκευές υλικού οι οποίες αποθηκεύουν τα απαιτούμενα μυστικά κλειδιά και προσφέρουν tamper proof προστασία. Όλες οι κρυπτογραφικές διαδικασίες πραγματοποιούνται εσωτερικά στη συσκευή και συνεπώς δεν υπάρχει καμία δυνατότητα ανάγνωσης των κλειδιών από εξωτερικές οντότητες. Για την ενεργοποίηση των κλειδιών συνηθίζεται η χρήση κάποιου συνθηματικού.

7.3 Απαιτήσεις Αυθεντικοποίησης

Στις υπηρεσίες ηλεκτρονικής διακυβέρνησης θα πρέπει να υποστηρίζονται εναλλακτικοί τρόποι αυθεντικοποίησης, με βάση τη βεβαιότητα που απαιτείται για την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας. Για το λόγο αυτό, πριν αποφασιστεί ο συγκεκριμένος μηχανισμός αυθεντικοποίησης για κάποια υπηρεσία, είναι απαραίτητο να προσδιοριστεί το επίπεδο εμπιστοσύνης, και συνεπώς το επίπεδο αυθεντικοποίησης, στο οποίο εντάσσεται η υπηρεσία αυτή. Επιπλέον θα πρέπει να παρέχεται στους χρήστες η δυνατότητα πρόσβασης σε υπηρεσίες χαμηλότερου επιπέδου όταν αυθεντικοποιούνται με την αξιοποίηση ισχυρότερων διακριτικών, σε σχέση με αυτό που απαιτεί η υπηρεσία με βάση το επίπεδο εμπιστοσύνης που εντάσσεται. Για παράδειγμα, ένας χρήστης που αυθεντικοποιείται με την αξιοποίηση του ψηφιακού του πιστοποιητικού θα πρέπει να μπορεί να έχει πρόσβαση και στις υπηρεσίες που αυθεντικοποιείται με το συνθηματικό του.

Λαμβάνοντας υπόψη τους υπάρχοντες μηχανισμούς αυθεντικοποίησης και τα αντίστοιχα διακριτικά αυθεντικοποίησης, προκύπτουν τα ακόλουθα επίπεδα αυθεντικοποίησης:

7.3.1 Επίπεδο Αυθεντικοποίησης 0 (ΕΑ0)

Σε αυτό το επίπεδο δεν απαιτείται αυθεντικοποίηση του χρήστη καθώς οποιαδήποτε οντότητα είναι δυνατόν να έχει πρόσβαση στις πληροφορίες που θεωρούνται δημόσιες. Συνήθως, τέτοιου τύπου υπηρεσίες είναι όσες παρέχουν πληροφοριακό υλικό.

7.3.1.1 Απαιτήσεις ασφάλειας

Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον, τα ακόλουθα:

- Ακεραιότητα του παρεχόμενου πληροφοριακού υλικού
- Αυθεντικότητα υπηρεσίας

7.3.1.2 Συσχετισμός με επίπεδο εμπιστοσύνης

Το επίπεδο αυθεντικοποίησης 0 σχετίζεται με το επίπεδο εμπιστοσύνης 0, καθώς δεν απαιτείται η επιβεβαίωση της ορθότητας της ηλεκτρονικής ταυτότητας του χρήστη.

7.3.1.3 Προτεινόμενος μηχανισμός αυθεντικοποίησης

Δεν απαιτείται μηχανισμός αυθεντικοποίησης.

7.3.2 Επίπεδο Αυθεντικοποίησης 1 (ΕΑ1)

Σε αυτό το επίπεδο αυθεντικοποίησης απαιτείται μικρή έως μέτρια βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας, καθώς αφορούν υπηρεσίες στις οποίες δικαίωμα πρόσβασης έχουν μόνον εξουσιοδοτημένες οντότητες. Τέτοιου είδους υπηρεσίες θεωρούνται αυτές που υποστηρίζουν τη δυνατότητα παροχής αιτήσεων στους χρήστες για

περαιτέρω (off-line) επεξεργασία και την πραγματοποίηση της συναλλαγής με το φορέα σε φυσικό επίπεδο.

7.3.2.1 Απαιτήσεις ασφάλειας

Σε αυτό το επίπεδο αυθεντικοποίησης θα πρέπει να διασφαλίζονται, κατ' ελάχιστον, τα ακόλουθα:

- Εμπιστευτικότητα των
    - δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη (τήρηση κανόνων προστασίας προσωπικών δεδομένων)
    - διαπιστευτηρίων του χρήστη
- Ακεραιότητα των
    - δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη
    - διαπιστευτηρίων του χρήστη
    - δεδομένων που λαμβάνονται από την ηλεκτρονική υπηρεσία
- Αυθεντικότητα υπηρεσίας

7.3.2.2 Συσχετισμός με επίπεδο εμπιστοσύνης

Το επίπεδο αυθεντικοποίησης 1 σχετίζεται με τα επίπεδα εμπιστοσύνης 1 και 2, καθώς απαιτείται έως και μέτρια βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας του χρήστη.

7.3.2.3 Προτεινόμενος μηχανισμός αυθεντικοποίησης

Οι μηχανισμοί αυθεντικοποίησης που προτείνονται για το συγκεκριμένο επίπεδο συμπεριλαμβάνουν: συνθηματικά και συνθηματικά μιας χρήσης (για περισσότερες λεπτομέρειες βλέπε ενότητες 7.2.1 & 7.2.2).

7.3.3 Επίπεδο Αυθεντικοποίησης 2 (ΕΑ2)

Σε αυτό το επίπεδο αυθεντικοποίησης απαιτείται υψηλή βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας μιας οντότητας, καθώς είναι εξαιρετικά κρίσιμο να εξασφαλιστεί ότι μόνο εξουσιοδοτημένα πρόσωπα έχουν τη δυνατότητα πρόσβασης στις προσφερόμενες υπηρεσίες. Εδώ εντάσσονται οι ηλεκτρονικές υπηρεσίες που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα ή υποστηρίζουν τη διενέργεια οικονομικών συναλλαγών.

7.3.3.1 Απαιτήσεις ασφάλειας

Στο ΕΑ2 θα πρέπει να διασφαλίζονται κατ' ελάχιστον τα ακόλουθα:

- Εμπιστευτικότητα των
    - δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη (ιδιωτικότητα)

- διαπιστευτηρίων του χρήστη
- δεδομένων που αποστέλλονται από το χρήστη στην ηλεκτρονική υπηρεσία
- δεδομένων που ο χρήστης λαμβάνει από την ηλεκτρονική υπηρεσία

- Ακεραιότητα των
  - δεδομένων ταυτοποίησης (αναγνωριστικά) του χρήστη
  - διαπιστευτηρίων του χρήστη
  - δεδομένων που αποστέλλονται από το χρήστη στην ηλεκτρονική υπηρεσία
  - δεδομένων που ο χρήστης λαμβάνει από την ηλεκτρονική υπηρεσία
- Αυθεντικότητα υπηρεσίας
- Μη αποποίηση
  - αποστολής δεδομένων
  - λήψης δεδομένων
- Υπηρεσίες εποπτείας (auditing)
- Χρονοσήμανση των ενεργειών

7.3.3.2 Προτεινόμενος μηχανισμός αυθεντικοποίησης

Ο μηχανισμός αυθεντικοποίησης που προτείνεται για το συγκεκριμένο επίπεδο αξιοποιεί ψηφιακά πιστοποιητικά (digital certificates) που θα εκδίδονται από την κατάλληλη Υποδομή Δημόσιου Κλειδιού (PKI) και την Αρχή Χρονοσήμανσης (Time Stamping Authority - TSA), υπό την αίρεση βεβαίως ότι η TSA επιτελεί και έργο CA. Επιπρόσθετα προτείνεται η αξιοποίηση διακριτικών χαλαρής ή σκληρής αποθήκευσης. Ο διαχωρισμός αυτός πραγματοποιείται δεδομένου ότι θεωρείται ότι δεν προάγει στην παρούσα φάση την ευρεία διάδοση υπηρεσιών ηλεκτρονικής διακυβέρνησης η απαίτηση όλοι οι πολίτες να προμηθευτούν άμεσα αναγνώστες έξυπνων καρτών για να δύνανται να έχουν πρόσβαση στις ηλεκτρονικές υπηρεσίες υψηλού επιπέδου εμπιστοσύνης. Ουσιαστικά στόχος είναι να μη δημιουργηθούν έμμεσα προϋποθέσεις αποκλεισμού της συντριπτικής πλειονότητας των πολιτών από τις παρεχόμενες και υπό ανάπτυξη ηλεκτρονικές υπηρεσίες. Παράλληλα βεβαίως τονίζεται η ανάγκη προσεχτικής μελέτης όσων προβλέπει το Π.Δ. 150/2001 σε σχέση με τις «ψηφιακές υπογραφές» και τις ενδεχόμενες απαιτήσεις μη αποποίησης στο πλαίσιο μιας ηλεκτρονικής υπηρεσίας, κυρίως όσον αφορά τα διακριτικά χαλαρής αποθήκευσης. Σε κάθε περίπτωση, αποκλειστικά υπεύθυνος για την τελική επιλογή του τύπου διακριτικών αποθήκευσης είναι πάντοτε ο φορέας παροχής της ηλεκτρονικής υπηρεσίας. Όποια επιλογή και αν τελικά υιοθετηθεί, τα διακριτικά αποθήκευσης θα πρέπει να προστατεύονται από τους αντίστοιχους προσωπικούς κωδικούς του χρήστη.

7.3.3.3 Συσχετισμός με επίπεδο εμπιστοσύνης

Το επίπεδο αυθεντικοποίησης 2 σχετίζεται με το επίπεδο εμπιστοσύνης 3 καθώς απαιτείται υψηλή βεβαιότητα για την ορθότητα της ηλεκτρονικής ταυτότητας του χρήστη.

7.3.4 Σύνοψη Συσχετισμού Επιπέδων Εμπιστοσύνης & Αυθεντικοποίησης

Στον παρακάτω πίνακα συνοψίζεται η συσχέτιση μεταξύ Επιπέδων Εμπιστοσύνης και Επιπέδων Αυθεντικοποίησης. Όπως είναι φανερό, η συσχέτιση αυτή δεν αποτελεί ένα προς ένα αντιστοιχία.

Επίπεδο Εμπιστοσύνης	Επίπεδο Αυθεντικοποίησης
0	0
1,2	1
3	2

Πίνακας 3. Συσχέτιση Επιπέδου Εμπιστοσύνης & Επιπέδου Αυθεντικοποίησης

8. ΔΙΑΔΙΚΑΣΙΕΣ ΕΓΓΡΑΦΗΣ ΟΝΤΟΤΗΤΩΝ

Με τον όρο *εγγραφή μιας οντότητας σε μια υπηρεσία* ορίζεται το σύνολο των διαδικασιών μέσω των οποίων η οντότητα εκδηλώνει ενδιαφέρον χρήσης μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας και παρέχει όλα τα στοιχεία που απαιτούνται για την έγκριση του δικαιώματος αυτού.

Για τον προσδιορισμό του κατάλληλου επιπέδου εγγραφής, οι δημόσιες υπηρεσίες θα πρέπει να λάβουν υπόψη το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η παρεχόμενη υπηρεσία. Όπως έχει ήδη προαναφερθεί όσο υψηλότερο είναι το επίπεδο εμπιστοσύνης, τόσο υψηλό θα πρέπει να είναι και το επίπεδο εγγραφής, λαμβάνοντας επιπλέον υπόψη και το διακριτικό αυθεντικοποίησης που θα απαιτηθεί για τη διαδικασία αυθεντικοποίησης.

Ενδεικτικά, για υπηρεσίες που υποστηρίζουν οικονομικές συναλλαγές δεν θα πρέπει να επιτρέπεται η εγγραφή να πραγματοποιείται μόνο με τη συμπλήρωση μιας ηλεκτρονικής φόρμας (όπως πραγματοποιείται στις υπάρχουσες υπηρεσίες ηλεκτρονικής διακυβέρνησης), αλλά θα πρέπει να υπάρχει η κατάλληλη διαδικασία κατά την οποία ο χρήστης αφού αρχικά επιβεβαιώσει τη γνησιότητα της ταυτότητάς του, θα μπορεί να παραλάβει το κατάλληλο διακριτικό αυθεντικοποίησης και περαιτέρω να αξιοποιήσει την υπηρεσία.

Στην ενότητα αυτή αποτυπώνονται τα πρότυπα, οι προδιαγραφές και οι διαδικασίες που απαιτούνται για την εγγραφή μιας οντότητας σε μία υπηρεσία ηλεκτρονικής διακυβέρνησης, προκειμένου να ελεγχθεί η πληρότητα, η ορθότητα και η εγκυρότητα των δεδομένων που υποβάλλονται από τον αιτούντα και να εκδοθεί το κατάλληλο διακριτικό αυθεντικοποίησης για την παροχή πρόσβασης στις παρεχόμενες υπηρεσίες. Σε κάθε περίπτωση θα πρέπει να σημειωθεί ότι το επίπεδο εγγραφής δεν είναι απαραίτητο να ταυτίζεται με τα επίπεδα εμπιστοσύνης ή αυθεντικοποίησης.

Αξίζει να σημειωθεί ότι η επιτυχημένη ολοκλήρωση ενός συγκεκριμένου Επίπεδου Εγγραφής δεν αποκλείει την ανάγκη ολοκλήρωσης των υπολοίπων επιπέδων εγγραφής σε περίπτωση που ο χρήστης επιθυμεί να κάνει χρήση υπηρεσιών που ανήκουν σε αυτά.

8.1 Τύποι Οντοτήτων

Οι οντότητες που μπορούν να αιτηθούν πρόσβασης στις υπηρεσίες ηλεκτρονικής διακυβέρνησης είναι:

- Φυσικά Πρόσωπα
- Νομικά Πρόσωπα Ιδιωτικού Δικαίου (ΝΠΙΔ)
- Νομικά Πρόσωπα Δημοσίου Δικαίου (ΝΠΔΔ)

8.2 Επίπεδα και Τρόποι Εγγραφής Φυσικών Προσώπων

Για την εγγραφή ενός φυσικού προσώπου σε κάποια ηλεκτρονική υπηρεσία είναι πιθανόν να απαιτείται η προσκόμιση συγκεκριμένων εγγράφων ή πιστοποιητικών τα οποία θα λειτουργούν

ως αποδεικτικά της ορθότητας και εγκυρότητας των στοιχείων που δηλώνει το προς εγγραφή φυσικό πρόσωπο. Η επικοινωνία μεταξύ αιτούντος και παρόχου της υπηρεσίας θα διεξάγεται μέσω της «Αρχής Εγγραφής» (βλέπε και ενότητα 13.1.5.2.2), η οποία ουσιαστικά θα παρέχει τη λειτουργική διεπαφή και επικοινωνία μεταξύ των δύο οντοτήτων και θα είναι υπεύθυνη για τον έλεγχο και πιστοποίηση των στοιχείων του προς εγγραφή φυσικού προσώπου.

Ο τρόπος με τον οποίο απαιτείται να προσκομιστούν τα έγγραφα αυτά καθώς και το πλήθος τους και τα στοιχεία που καλούνται να πιστοποιήσουν, προσδιορίζονται με διαφορετικό τρόπο σε κάθε Επίπεδο Εγγραφής. Προκειμένου τα έγγραφα να θεωρούνται έγκυρα θα πρέπει να χαρακτηρίζονται ως δημόσια, δηλαδή να προέρχονται ή να έχουν εκδοθεί από:

- Τις αρχές της νομοθετικής, εκτελεστικής και δικαστικής εξουσίας του κράτους
- Τις δημόσιες υπηρεσίες, νομικά πρόσωπα δημόσιου δικαίου και οργανισμούς τοπικής αυτοδιοίκησης
- Τους οργανισμούς και τις επιχειρήσεις κοινής ωφέλειας
- Τα νομικά πρόσωπα ιδιωτικού δικαίου, που τελούν υπό την εποπτεία του κράτους και ανήκουν στο δημόσιο τομέα
- Συμβολαιογράφους και υποθηκοφυλακεία
- Ληξιαρχεία
- Τις ελληνικές κοινότητες και τα ιδρύματα του εξωτερικού, όπως εκπαιδευτικά, φιλανθρωπικά, εκκλησιαστικά, πολιτιστικά
- Τα δημόσια εκπαιδευτικά ιδρύματα της χώρας, όλων των βαθμίδων εκπαίδευσης
- Τους διεθνείς οργανισμούς
- Υπηρεσίες ξένων κρατών εγκατεστημένες στην ελληνική επικράτεια

Θα πρέπει να σημειωθεί ότι στα επίπεδα εγγραφής που ακολουθούν προδιαγράφονται οι γενικές απαιτήσεις που διέπουν τη διαδικασία εγγραφής. Οίκοθεν νοείται ότι όσο πιο κρίσιμη είναι η παρεχόμενη υπηρεσία τόσο αυστηρότεροι έλεγχοι θα πρέπει να επιβάλλονται κατά τη διαδικασία της εγγραφής με στόχο την ελαχιστοποίηση μη επιθυμητών ενεργειών. Επιπροσθέτως, οι φορείς θα πρέπει να καθορίζουν επακριβώς τα έγγραφα που απαιτούνται για την επιτυχή ολοκλήρωση της διαδικασίας εγγραφής στα διαφορετικά επίπεδα.

8.2.1 Επίπεδο Εγγραφής 0

Ως Επίπεδο Εγγραφής 0 ορίζεται το σύνολο των διαδικασιών που πρέπει να ακολουθήσει ένας χρήστης προκειμένου να εξασφαλίσει πρόσβαση σε υπηρεσίες που κυρίως παρέχουν πληροφοριακό υλικό.

8.2.1.1 Διαδικασία Εγγραφής

Δεν απαιτείται κάποια συγκεκριμένη διαδικασία εγγραφής.

8.2.1.2 Απαιτήσεις ασφάλειας

Για το συγκεκριμένο επίπεδο εγγραφής δεν υπάρχουν απαιτήσεις ασφάλειας. Η επικοινωνία με τα αρμόδια γραφεία εγγραφής είναι ανώνυμη.

8.2.1.3 Συσχετισμός με Επίπεδο Αυθεντικοποίησης

Οι διαδικασίες του Επιπέδου Εγγραφής 0 θα πρέπει να ακολουθηθούν για τις ηλεκτρονικές υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 0.

8.2.2 Επίπεδο Εγγραφής 1

Στο Επίπεδο Εγγραφής 1 εντάσσεται το σύνολο των διαδικασιών που πρέπει να ακολουθήσει ένας χρήστης για να αποκτήσει πρόσβαση σε υπηρεσίες που επεξεργάζονται προσωπικά δεδομένα (π.χ. δυνατότητα συμπλήρωσης ηλεκτρονικών αιτήσεων και φορμών για την έκδοση κάποιου δημοσίου εγγράφου).

8.2.2.1 Διαδικασία Εγγραφής

Η διαδικασία εγγραφής που προβλέπεται στο επίπεδο 1 έχει ως εξής: Ο χρήστης θα πρέπει να συμπληρώσει ηλεκτρονικά κάποια αίτηση, η οποία και θα περιλαμβάνει πεδία στα οποία θα πρέπει να συμπληρώσει τα προσωπικά του στοιχεία (Όνομα, Επίθετο, Ημερομηνία Γέννησης), τα αναγνωριστικά του για τις ηλεκτρονικές υπηρεσίες στις οποίες επιθυμεί να εγγραφεί π.χ. Αριθμός Δελτίου Ταυτότητας, Αριθμός Φορολογικού Μητρώου, τη διεύθυνση αλληλογραφίας και την ηλεκτρονική διεύθυνση αλληλογραφίας του. Μετά την υποβολή της ηλεκτρονικής αίτησης, ο χρήστης λαμβάνει ένα αντίγραφο στη διεύθυνση του ηλεκτρονικού του ταχυδρομείου, το οποίο λειτουργεί ως αποδεικτικό των στοιχείων της αίτησης που έχει υποβάλλει. Επίσης, η συμπληρωμένη αίτηση αποστέλλεται ηλεκτρονικά στην Αρχή Εγγραφής η οποία αποστέλλει σχετικό αίτημα στον εξυπηρετητή της αντίστοιχης υπηρεσίας προκειμένου ο φορέας να πραγματοποιήσει έλεγχο αναφορικά με:

1. την εγκυρότητα των στοιχείων της υποβληθείσας αίτησης,
2. τη μη ύπαρξη άλλου λογαριασμού για τον αιτούντα χρήστη για το συγκεκριμένο επίπεδο εγγραφής,
3. την εγκυρότητα των αναγνωριστικών,
4. αν ο αιτών δικαιούται να χρησιμοποιήσει την ηλεκτρονική υπηρεσία που δήλωσε.

Ανεξάρτητα του επιπέδου εγγραφής, η Αρχή Εγγραφής καταγράφει την αίτηση του χρήστη, χωρίς όμως να αποθηκεύει κάποιο από τα στοιχεία ή αναγνωριστικό του χρήστη. Μετά την ολοκλήρωση του ελέγχου ο οποίος διεξάγεται από την πλευρά του φορέα, ο εξυπηρετητής της υπηρεσίας αποστέλλει απάντηση στο σχετικό αίτημα ενημερώνοντας την Αρχή Εγγραφής για το αποτέλεσμα του ελέγχου. Η επικοινωνία μεταξύ της Αρχής Εγγραφής και του εκάστοτε εξυπηρετητή υπηρεσίας πραγματοποιείται υπό το καθεστώς ύπαρξης αμοιβαίας σχέσης εμπιστοσύνης.

Σε περίπτωση που οι απαντήσεις που λάβει η Αρχή Εγγραφής αναφορικά με τους παραπάνω ελέγχους είναι θετικές, δημιουργείται ένας λογαριασμός για το χρήστη που υπέβαλε αίτηση. Στη συνέχεια ο χρήστης ενημερώνεται, στη διεύθυνση αλληλογραφίας του με συστημένη επιστολή, για το όνομα χρήστη και το συνθηματικό που θα πρέπει να χρησιμοποιεί προκειμένου να αυθεντικοποιείται και να κάνει χρήση των ηλεκτρονικών υπηρεσιών που δήλωσε.

Σε περίπτωση που η Αρχή Εγγραφής διαπιστώσει ότι ο φορέας, για κάποιο συγκεκριμένο λόγο, δεν έκανε δεκτή την αίτηση, ενημερώνει σχετικά το χρήστη στη διεύθυνση αλληλογραφίας του ότι η αίτησή του απορρίφθηκε, εξηγώντας ταυτόχρονα την ακριβή αιτία.

8.2.2.2 Απαιτήσεις ασφάλειας

Οι απαιτήσεις ασφάλειας στο συγκεκριμένο επίπεδο εγγραφής είναι η

- Εμπιστευτικότητα των
    - δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
    - δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
    - διαπιστευτηρίων του χρήστη
- Ακεραιότητα των
    - δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
    - δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
    - διαπιστευτηρίων του χρήστη

Ενδεικτικά, πρωτόκολλο που διασφαλίζει τις προαναφερθείσες απαιτήσεις ασφάλειας είναι το SSL.

- Μη – Αποποίηση
    - αποστολής και Λήψης Δεδομένων

Η μη αποποίηση διασφαλίζεται με την υποβολή της αίτησης (συμπεριλαμβανομένων και των δικαιολογητικών) και την έκδοση των απαιτούμενων διαπιστευτηρίων.

8.2.2.3 Συσχετισμός με Επίπεδο Αυθεντικοποίησης

Οι διαδικασίες του Επιπέδου Εγγραφής 1 θα πρέπει να ακολουθηθούν για τις ηλεκτρονικές υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 1.

8.2.3 Επίπεδο Εγγραφής 2

Το Επίπεδο Εγγραφής 2 ορίζει τις διαδικασίες που απαιτούνται για την εγγραφή σε υπηρεσίες αντίστοιχες με αυτές που επιπέδου 1, με τη διαφορά ότι τώρα το έγγραφο / πιστοποιητικό που αιτείται ο χρήστης μπορεί να του αποσταλεί ηλεκτρονικά.

8.2.3.1 Διαδικασία Εγγραφής

Και σε αυτό το επίπεδο ο χρήστης πρέπει να συμπληρώσει μια αίτηση με τα προσωπικά στοιχεία του, αντίστοιχη με αυτή του επιπέδου 1, η οποία αποστέλλεται στην Αρχή Εγγραφής με στόχο τη διενέργεια των ίδιων ελέγχων που γίνονται στο επίπεδο 1. Αντίγραφο της ηλεκτρονικής αίτησης αποστέλλεται και στον αιτούντα ως αποδεικτικό των στοιχείων που δηλώθηκαν.

Θεωρώντας ότι οι έλεγχοι που αναφέρονται στην ενότητα 8.2.2.1 ολοκληρώθηκαν επιτυχώς, δημιουργείται ο λογαριασμός του χρήστη και εκδίδεται το διακριτικό συνθηματικών μιας χρήσης εφόσον δεν έχει ήδη εκδοθεί άλλο και ο χρήστης δεν έχει αναφέρει κλοπή ή δυσλειτουργία του. Πέντε εργάσιμες ημέρες (βλέπε υποσημείωση 3) από την υποβολή της αίτησης, ο χρήστης μπορεί να παραλάβει από την αρμόδια υπηρεσία το κατάλληλο διακριτικό αυθεντικοποίησης αφού πρώτα ταυτοποιηθεί - αυθεντικοποιηθεί στον αρμόδιο υπάλληλο επιδεικνύοντας δημόσια έγγραφα που αναγράφουν τα αναγνωριστικά του, το δελτίο της αστυνομικής του ταυτότητας, το αντίγραφο της ηλεκτρονικής αίτησης που υπέβαλλε, καθώς και ένα δημόσιο έγγραφο που να αποδεικνύει τη διεύθυνση μόνιμης κατοικίας του. Σε περίπτωση που ο φορέας κάποιας υπηρεσίας επιθυμεί την προσκόμιση κάποιου ακόμα εγγράφου, ο χρήστης θα ενημερώνεται σχετικά κατά τη διάρκεια της εγγραφής και θα πρέπει να το προσκομίσει μαζί με τα υπόλοιπα ώστε να παραλάβει το διακριτικό αυθεντικοποίησης που έχει εκδοθεί γι' αυτόν.

Σε περίπτωση που η Αρχή Εγγραφής διαπιστώσει την ύπαρξη μη-έγκυρων στοιχείων στην ηλεκτρονική αίτηση, προβαίνει σε ενέργειες αντίστοιχες με αυτές του επιπέδου 1.

8.2.3.2 Απαιτήσεις ασφάλειας

Οι απαιτήσεις ασφάλειας στο συγκεκριμένο επίπεδο εγγραφής είναι η

- Εμπιστευτικότητα των
  - δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
  - δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
  - διαπιστευτηρίων του χρήστη
- Ακεραιότητα των
  - δεδομένων που αποστέλλει ο χρήστης στην Αρχή Εγγραφής
  - δεδομένων που αποστέλλονται στο χρήστη από την Αρχή Εγγραφής
  - διαπιστευτηρίων του χρήστη
- Μη – Αποποίηση
  - αποστολής και λήψης δεδομένων
  - συμμετοχής σε ηλεκτρονικές συναλλαγές

Ενδεικτικά, ένα πρωτόκολλο που διασφαλίζει τις περισσότερες από τις προαναφερθείσες απαιτήσεις ασφάλειας είναι το SSL.

8.2.3.3 Συσχετισμός με Επίπεδο Αυθεντικοποίησης

Οι διαδικασίες του Επιπέδου Εγγραφής 2 θα πρέπει να ακολουθηθούν για τις ηλεκτρονικές υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 1.

8.2.4 Επίπεδο Εγγραφής 3

Το Επίπεδο Εγγραφής 3 ορίζει τις διαδικασίες που απαιτούνται για την εγγραφή σε υπηρεσίες που επεξεργάζονται ευαίσθητα προσωπικά δεδομένα ή οικονομικά δεδομένα.

8.2.4.1 Διαδικασία Εγγραφής

Σε αντιστοιχία με τα προηγούμενα επίπεδα, ο χρήστης συμπληρώνει την ηλεκτρονική αίτηση η οποία θα πρέπει να εγκριθεί από την Αρχή Εγγραφής. Μετά την έγκριση δημιουργείται ο λογαριασμός του χρήστη, ενώ η αίτηση προωθείται στην Αρχή Πιστοποίησης η οποία είναι υπεύθυνη για την έκδοση των ψηφιακών πιστοποιητικών. Δεκαπέντε εργάσιμες ημέρες[3] μετά από την υποβολή της αίτησης, ο χρήστης θα μπορεί να παραλαμβάνει το αντίστοιχο διακριτικό αυθεντικοποίησης από την αρμόδια υπηρεσία αφού πρώτα ταυτοποιηθεί στον αρμόδιο υπάλληλο επιδεικνύοντας δημόσια έγγραφα αντίστοιχα με αυτά του επιπέδου 2. Μετά την παραλαβή του διακριτικού αυθεντικοποίησης, και σε διάστημα δέκα εργάσιμων ημερών (βλέπε υποσημείωση 3) ο προσωπικός κωδικός πρόσβασης (PIN – Personal Identification Number) του διακριτικού αποστέλλεται με συστημένη επιστολή στη διεύθυνση αλληλογραφίας του χρήστη.

Σε περίπτωση που η Αρχή Εγγραφής διαπιστώσει με βάση τα στοιχεία που θα λάβει από τον εξυπηρετητή την ύπαρξη μη-έγκυρων στοιχείων στην ηλεκτρονική αίτηση, προβαίνει σε ενέργειες αντίστοιχες με αυτές του επιπέδου 1.

8.2.4.2 Απαιτήσεις ασφάλειας

Οι απαιτήσεις ασφάλειας στο συγκεκριμένο επίπεδο εγγραφής είναι αντίστοιχες με αυτές του επιπέδου 2.

8.2.4.3 Συσχετισμός με Επίπεδο Αυθεντικοποίησης

Οι διαδικασίες του Επιπέδου Εγγραφής 3 θα πρέπει να ακολουθηθούν για τις ηλεκτρονικές υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 2.

8.2.5 Διαδικασία Εγγραφής σε πολυεισοδικές υπηρεσίες

Πέραν των συνήθων μονοεισοδικών ηλεκτρονικών υπηρεσιών, οι οποίες μελετώνται διεξοδικά και οι οποίες εκτιμάται ότι αντιστοιχούν σε σημαντικό ποσοστό των σήμερα αιτουμένων από τους πολίτες στο μη ψηφιακό περιβάλλον, οι δημόσιοι φορείς παρέχουν πληθώρα και άλλων υψηλότερης πολυπλοκότητας υπηρεσιών. Οι υπηρεσίες αυτές, οι οποίες εφεξής θα

[3] ο χρόνος παραλαβής είναι ενδεικτικός και θα πρέπει να καθοριστεί από την Αρχή Πιστοποίησης

αποκαλούνται *πολυεισοδικές υπηρεσίες*, δεν μπορούν να αντιμετωπιστούν ενιαία και χρήζουν ξεχωριστής αντιμετώπισης εκάστη.

Για την ολοκληρωμένη μελέτη κάθε πολυεισοδικής υπηρεσίας απαιτείται λεπτομερής μελέτη, ανάλυση και καταγραφή της ροής εργασίας της (workflow), καταγραφή της διαδοχής των απαιτουμένων ενεργειών, αποτύπωση της αναγκαιότητας και του τρόπου συνεργασίας υπηρεσιών ενδεχομένως και διαφορετικών φορέων, καθώς και προσδιορισμός κρίσιμων σημείων και ενδεχομένων σημείων αναμονής και αποθήκευσης προσωρινά παραγόμενων ενδιάμεσων δεδομένων.

Σε γενική προσέγγιση και σε πρώτο επίπεδο ανάλυσης, για να ολοκληρωθεί μία συνήθης πολυεισοδική υπηρεσία απαιτείται σωρευτικά να ικανοποιηθούν δύο ή περισσότερες μονοεισοδικές υπηρεσίες, ενδεχομένως και διαφορετικών επιπέδων εμπιστοσύνης. Στην περίπτωση αυτή, το επίπεδο εμπιστοσύνης στο οποίο τελικά θα ενταχθεί η πολυεισοδική υπηρεσία θα πρέπει να μην υπολείπεται του υψηλότερου επιπέδου εμπιστοσύνης των επιμέρους μονοεισοδικών υπηρεσιών.

Η πρωτοβουλία ενός πολίτη να εγγραφεί σε μία πολυεισοδική υπηρεσία θα μπορούσε, ανάλογα με το σχεδιασμό που τελικά θα υιοθετούνταν, να απαιτούσε:

a. είτε να προηγηθεί τη στιγμή εκείνη η ρητή εγγραφή του πολίτη στις ξεχωριστές μονοεισοδικές υπηρεσίες, όπως ακριβώς έχει προβλεφθεί για την καθεμία από αυτές

b. είτε να διεξαχθεί η εγγραφή του πολίτη απευθείας στην πολυεισοδική υπηρεσία, με όφελος για αυτόν διαφανώς (transparently) να επιτευχθεί επιπλέον η έμμεση εγγραφή του και στις επιμέρους μονοεισοδικές υπηρεσίες. Η εγγραφή του πολίτη στην πολυεισοδική υπηρεσία προφανώς θα περιλαμβάνει την αναγκαιότητα παροχής από αυτόν σωρευτικά των αναγνωριστικών που απαιτούνται από καθεμία από τις μονοεισοδικές υπηρεσίες, λαμβάνοντας υπόψη το γεγονός ότι ενδέχεται κάποιο αναγνωριστικό που απαιτείται από μία μονοεισοδική υπηρεσία είτε να ταυτίζεται, είτε να υπερκαλύπτει το αναγνωριστικό άλλης επιμέρους μονοεισοδικής υπηρεσίας.

Μελετώντας τα υπόλοιπα θέματα ανάπτυξης των πολυεισοδικών υπηρεσιών, επιπλέον της εγγραφής, τα οποία εκτιμώνται και ως τα περισσότερο πολύπλοκα, κατά το σχεδιασμό θα πρέπει να έχει προβλεφθεί η επίλυση του προβλήματος της αναγκαιότητας προσωρινής αποθήκευσης των παραγομένων αποτελεσμάτων των επιμέρους μονοεισοδικών υπηρεσιών, μέχρι την ολοκληρωμένη παραλαβή όλων και τη συνολική απάντηση-παροχή υπηρεσίας προς τον πολίτη.

Θα πρέπει, παράλληλα, να έχει ληφθεί μέριμνα ώστε, αν μετά το στάδιο εγγραφής και κατά το στάδιο παροχής της πολυεισοδικής υπηρεσίας, προκύψει, για κάποιο λόγο, άρνηση παροχής μιας από τις επιμέρους μονοεισοδικές υπηρεσίες για τον πολίτη, αυτή να καταγραφεί ρητά, ώστε στην τελική ολοκληρωμένη απάντηση που θα αποσταλεί στον πολίτη να του καταστεί σαφής και με απλές εκφράσεις η αιτία άρνησης παροχής της πολυεισοδικής υπηρεσίας, ουσιαστικά δηλαδή να ενημερωθεί για το ποια επιμέρους ενέργεια - μονοεισοδική υπηρεσία δεν τελεσφόρησε και ποιες προχώρησαν χωρίς προβλήματα.

Όσον αφορά ενδεχόμενες περιπτώσεις πολυεισοδικών υπηρεσιών, σύμφωνα με τη ροή εργασίας των οποίων σε συγκεκριμένο στάδιο εξέλιξής τους απαιτείται προσκόμιση από τον πολίτη συγκεκριμένων επιπλέον στοιχείων για την ολοκλήρωση, θα πρέπει κατά το σχεδιασμό του συστήματος να έχει ληφθεί μέριμνα για την ενημέρωση του πολίτη στο σωστό χρόνο για τις εκ μέρους του απαιτούμενες ενέργειες.

Ως ενδεικτικό παράδειγμα περιγράφεται ακολούθως η διαδικασία εγγραφής στην πολυεισοδική υπηρεσία με τίτλο *«Έκδοση Διαβατηρίου ανηλίκου ηλικίας 12 ετών».* Για την έκδοση διαβατηρίου ανηλίκου ηλικίας 12 ετών, σύμφωνα με τα ισχύοντα, απαιτούνται οι ακόλουθες ενέργειες:

1. Συμπλήρωση αίτησης έκδοσης διαβατηρίου
2. Πληρωμή παραβόλου για έκδοση διαβατηρίου ισχύος δύο ετών
3. Έκδοση πιστοποιητικού εγγραφής στα δημοτολόγια του Δήμου ή Κοινότητας που είναι εγγεγραμμένος ο αιτών
4. Πρόσφατη έγχρωμη ψηφιακή φωτογραφία

Στα ανωτέρω απαιτούμενα βήματα-ενέργειες, μπορούμε να θεωρήσουμε ότι τα [1+2] και [3] αποτελούν συνήθεις μονοεισοδικές υπηρεσίες. Κατά συνέπεια ένας πολίτης, μπορεί να αιτηθεί αξιοποίησης της πολυεισοδικής ηλεκτρονικής υπηρεσίας *«Έκδοση Διαβατηρίου ανηλίκου ηλικίας 12 ετών».* Το σύστημα ανταποκρινόμενο στη σχετική αίτησή του, θεωρώντας ότι κατά τη σχεδίαση ισχύει η υπόθεση περί αποδοχής της προαναφερόμενης επιλογής [b], ζητά από το αιτούντα να δηλώσει σωρευτικά τα απαιτούμενα αναγνωριστικά των μεμονωμένων μονοεισοδικών υπηρεσιών *«Συμπλήρωση αίτησης και Πληρωμή παραβόλου για έκδοση διαβατηρίου ισχύος δύο ετών»* και *«Έκδοση πιστοποιητικού εγγραφής στα δημοτολόγια»*. Όταν ολοκληρωθούν οι δύο αυτές επιμέρους μονοεισοδικές υπηρεσίες, τότε απαιτείται να ενημερωθεί ο πολίτης από το σύστημα με πρόσφορο τρόπο ότι η υπηρεσία ολοκληρώθηκε και είναι πλέον σε θέση ο πολίτης, αν έχει διαθέσιμες τις απαιτούμενες φωτογραφίες στο πλαίσιο της ενέργειας [4], να μεταβεί στο αντίστοιχο Γραφείο Υποδοχής Αιτήσεων της Διεύθυνσης Διαβατηρίων της Ελληνικής Αστυνομίας για τα περαιτέρω.

8.3 Επίπεδα και Τρόποι Εγγραφής Νομικών Προσώπων Ιδιωτικού και Δημόσιου Δικαίου

Η ιδιαιτερότητα των Νομικών Προσώπων Δημόσιου και Ιδιωτικού Δικαίου έγκειται στο γεγονός ότι δεν έχουν φυσική υπόσταση και όλες τους οι συναλλαγές πραγματοποιούνται μέσω νομίμως εξουσιοδοτημένων εκπροσώπων.

Ως προς την εκπροσώπηση των νομικών προσώπων σημειώνεται ότι σύμφωνα με τους γενικούς κανόνες «όποιος έχει τη διοίκηση νομικού προσώπου φροντίζει τις υποθέσεις του και το αντιπροσωπεύει δικαστικά και εξώδικα». Υποκατάσταση απαγορεύεται, εφόσον η συστατική πράξη ή το καταστατικό δεν ορίζει διαφορετικά (Άρθρο 66 Αστικού Κώδικα), Η έκταση της εξουσίας εκείνου που έχει τη διοίκηση προσδιορίζεται από τη συστατική πράξη ή το καταστατικό του νομικού προσώπου. Ο προσδιορισμός αυτός ισχύει και για τους τρίτους

(άρθρο 68 ΑΚ). Δικαιοπραξίες και πράξεις που πραγματοποίησε μέσα στα όρια της εξουσίας του το όργανο που διοικεί το νομικό πρόσωπο υποχρεώνουν το νομικό πρόσωπο (άρθρο 70 ΑΚ). Περαιτέρω εφαρμόζονται οι διατάξεις περί εντολής (άρθρα 713 επ. ΑΚ) και αντιπροσώπευσης (άρθρα 211 επ. ΑΚ) όπως προβλέπονται στον Αστικό Κώδικα ή/και εξειδικεύονται ενδεχομένως από τη συστατική πράξη ή το καταστατικό του νομικού προσώπου.

Αντίστοιχα, και στις ηλεκτρονικά προσφερόμενες υπηρεσίες η εγγραφή των Νομικών αυτών Προσώπων γίνεται μέσω νομίμως εξουσιοδοτημένων εκπροσώπων, οι οποίοι θα πρέπει να αποδεικνύουν ότι ενεργούν για λογαριασμό του φορέα, καθώς και ότι είναι εξουσιοδοτημένοι όχι μόνο για την εγγραφή αλλά και για την περαιτέρω χρήση των ηλεκτρονικών υπηρεσιών που επιθυμούν να εγγραφούν. Ενδέχεται να εξουσιοδοτηθούν περισσότερα του ενός όργανα ή φυσικά πρόσωπα και να υπάρχει διαφοροποίηση ανά υπηρεσία ή ομάδα υπηρεσιών ή ανά επίπεδο εμπιστοσύνης.

Τα νομικά πρόσωπα χρησιμοποιούν διάφορα αναγνωριστικά, όπως Αριθμό Μητρώου Ανωνύμων Εταιρειών, Αριθμό Μητρώου Εργοδότη κλπ., καθώς πρέπει να εξυπηρετηθούν διαφορετικές ανάγκες της έννομης τάξης, όπως π.χ. η επιταγή της διαφάνειας ως προς τη σύσταση και λειτουργία των νομικών προσώπων, οι ανάγκες της ασφαλιστικής νομοθεσίας κλπ. Ομοίως, το ζήτημα των πολλαπλών αναγνωριστικών αφορά και τα φυσικά πρόσωπα, καθώς και σε αυτά μπορεί να έχουν αποδοθεί διαφορετικά αναγνωριστικά, όπως ο Αριθμός Δελτίου Ταυτότητας, ο Αριθμός Φορολογικού Μητρώου, ο Αριθμός Μητρώου Ασφαλισμένου κλπ. Σε κάθε περίπτωση, όμως, τα διαφορετικά αυτά αυτοτελή αναγνωριστικά έχουν συγκεκριμένο πεδίο αξιοποίησης και βεβαίως δεν σχετίζονται με τη διαδικασία της ταυτοποίησης του νομικού προσώπου για την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης, αφού οι διαδικασίες για την εκπροσώπηση ενός νομικού προσώπου προσδιορίζονται από τον Αστικό Κώδικα ή εξειδικεύονται από τη συστατική πράξη ή το καταστατικό του. Ουσιαστικά η ταυτοποίηση του νομικού προσώπου, για την εγγραφή και χρήση ηλεκτρονικών υπηρεσιών, γίνεται δια του εκπροσώπου ή των εκπροσώπων του, όπως και στα λοιπά φυσικά πρόσωπα.

Σε περίπτωση αλλαγής του εκπροσώπου ενός νομικού προσώπου, θα πρέπει να ακυρωθούν τα διαπιστευτήρια που είχαν εκδοθεί και να επαναληφθεί η διαδικασία εγγραφής στην υπηρεσία για το νέο εκπρόσωπο. Βεβαίως θα απαιτηθεί να προσκομιστούν έγγραφα από τα οποία να προκύπτει η νόμιμη νέα εκπροσώπηση του φορέα από το συγκεκριμένο φυσικό πρόσωπο.

Κατά τα λοιπά, τα επίπεδα εγγραφής είναι αντίστοιχα με αυτά των φυσικών προσώπων όπως και οι διαδικασίες εγγραφής που προβλέπονται σε κάθε επίπεδο.

8.4 Διαδικαστικά Ζητήματα Εγγραφής Οντοτήτων

Η επιτυχής ολοκλήρωση της εγγραφής προφανώς δε διασφαλίζει ότι ο χρήστης αποκτά αυτομάτως πρόσβαση σε όλες ανεξαιρέτως τις υπηρεσίες που ανήκουν στο συγκεκριμένο επίπεδο εμπιστοσύνης, καθώς θα πρέπει να έχει αιτηθεί σχετικά για την καθεμία, δηλώνοντας τα αντίστοιχα αναγνωριστικά κατά την υποβολή της αίτησης εγγραφής. Έτσι για παράδειγμα, ένας χρήστης μπορεί να έχει εγγραφεί σε Χ αριθμό υπηρεσιών επιπέδου εμπιστοσύνης 2 και να έχει παραλάβει το διακριτικό αυθεντικοποίησής του. Προκειμένου, όμως, να εγγραφεί σε μία ακόμα υπηρεσία επιπέδου εμπιστοσύνης 2 θα πρέπει να απευθυνθεί εκ νέου στην Αρχή

Εγγραφής, υποβάλλοντας αντίστοιχη αίτηση. Επί θετικής απάντησης της Αρχής Εγγραφής σε σχετικό αίτημα, προφανώς δεν θα απαιτηθεί παραλαβή νέου διακριτικού αυθεντικοποίησης.

8.5 Ακύρωση Εγγραφής - Διαπιστευτηρίων

Πιθανοί λόγοι ανάκλησης του δικαιώματος χρήσης μια ηλεκτρονικής υπηρεσίας, μέσω της ακύρωσης των διαπιστευτηρίων που έχουν εκδοθεί, είναι:

- Σχετικό αίτημα του χρήστη (βλέπε και σχετική ενότητα 9.2.3)
- Απόφαση του φορέα για συγκεκριμένους χρήστες (λόγω μη συμμόρφωσης / αποδοχής των όρων χρήσης της υπηρεσίας)
- Λήξη ισχύος των διαπιστευτηρίων που είχαν εκδοθεί

Η περίοδος ισχύος ενός διαπιστευτηρίου εξαρτάται από τα χαρακτηριστικά της υπηρεσίας και καθορίζεται από το φορέα παροχής της υπηρεσίας. Σε κάθε περίπτωση, όταν αυτό λήξει, θα πρέπει να εκδοθεί νέο το οποίο ο χρήστης θα παραλάβει με διαδικασία αντίστοιχη με αυτή που είχε παραλάβει και το αρχικό (ανάλογα με το Επίπεδο Εγγραφής στο οποίο έχει ενταχθεί η υπηρεσία). Σε όλες τις περιπτώσεις ακύρωσης εγγραφής – διαπιστευτηρίων, ισχύουν οι γενικές διατάξεις που αφορούν την επεξεργασία των δεδομένων του χρήστη. Συγκεκριμένα:

α) σύμφωνα με το άρθρο 4 παρ. 1 εδαφ. β του ν. 2472/97, τα δεδομένα προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία πρέπει να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.

β) σύμφωνα με το άρθρο 4 παρ. 1 εδαφ. δ του ίδιου νόμου, τα δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους.

Εφόσον ακυρώνεται η εγγραφή / χορήγηση διαπιστευτηρίων θα πρέπει καταρχήν να διαγράφονται τα σχετικά δεδομένα, εφόσον δεν συντρέχει πλέον ο νόμιμος λόγος συλλογής και επεξεργασίας. Με επιφυλάξεις θα μπορούσε να προταθεί η περαιτέρω τήρηση εφόσον:

- κρίνεται σκόπιμο από το φορέα εγγραφής για πιθανή μελλοντική χρήση (π.χ. νέα αίτηση ενδιαφερόμενου χρήστη) και ο ενδιαφερόμενος χρήστης, αφού ενημερωθεί, δώσει τη συγκατάθεσή του για την περαιτέρω τήρηση. Συνιστάται το σχετικό ερώτημα να τίθεται ήδη κατά την πρώτη εγγραφή.
- κρίνεται αναγκαίο να τηρηθούν από το φορέα εγγραφής για ένα διάστημα εφόσον τίθενται ζητήματα τήρησης και διατήρησης διοικητικών αρχείων. Στην περίπτωση αυτή θα πρέπει να τηρηθούν μόνο οι αναγκαίες και πρόσφορες προς τούτο εγγραφές.
- κρίνεται αναγκαίο να τηρηθούν από το φορέα εγγραφής, προκειμένου να χρησιμοποιηθούν σε περίπτωση διοικητικής διαφοράς μεταξύ διοίκησης και χρήστη, εφόσον είτε η διαφορά αφορά την ανάκληση-λήξη διαπιστευτηρίων είτε τα σχετικά δεδομένα είναι αναγκαία ως αποδεικτικά στοιχεία.

9. ΟΔΗΓΙΕΣ ΕΦΑΡΜΟΓΗΣ ΠΛΑΙΣΙΟΥ ΨΗΦΙΑΚΗΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

9.1 Οδηγίες για τους Δημόσιους Φορείς

Στην ενότητα αυτή περιλαμβάνονται οδηγίες για την εφαρμογή του Πλαισίου Ψηφιακής Αυθεντικοποίησης από τους δημόσιους φορείς και οργανισμούς. Είναι σκόπιμο οι οδηγίες αυτές να ακολουθούνται τόσο στα πρώτα στάδια ανάπτυξης μιας ηλεκτρονικής υπηρεσίας, όσο και κατά τη διάρκεια της παραγωγικής λειτουργίας της.

9.1.1 Κατηγοριοποίηση Δεδομένων

Η προτεινόμενη κατηγοριοποίηση των δεδομένων που δυνητικά μπορούν να αξιοποιηθούν σε μια ηλεκτρονική υπηρεσία (βλέπε τον πίνακα που ακολουθεί) έχει βασιστεί στις αντίστοιχες κατηγοριοποιήσεις που έχουν υιοθετήσει:

1. η εθνική νομοθεσία (ν. 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα),
2. η κοινοτική νομοθεσία (Οδηγία 95/46/ΕΚ για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών) και
3. η διεθνής νομοθεσία (Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία ισχύει ως εσωτερικό δίκαιο).

Επιπλέον έχουν ληφθεί υπόψη απόρρητα τα οποία κατοχυρώνονται νομοθετικά, όπως το φορολογικό και ιατρικό απόρρητο.

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΑΠΛΑ ΔΕΔΟΜΕΝΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το επίπεδο εμπιστοσύνης**
Κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί να διαπιστωθεί. *Λόγω της ευρύτητας του ορισμού δεν είναι δυνατός ο ακριβής προσδιορισμός των δεδομένων που εντάσσονται στα «απλά»*	Άρθρο 2α ν. 2472/97 Ορισμός δεδομένων	Με την επιφύλαξη α) της ένταξης ορισμένων από τα αναφερόμενα στον πίνακα 1) στο προστατευτικό πεδίο απορρήτων, όπως το φορολογικό απόρρητο και
	Άρθρο 5 ν. 2690/99 (ΚΔΔ - Εξαιρέσεις από πρόσβαση σε διοικητικά έγγραφα για την προστασία της ιδιωτικής ή οικογενειακής ζωής)	β) του ενδεχόμενου να εντάσσονται ορισμένα απλά δεδομένα στο πεδίο της ιδιωτικής ή οικογενειακής ζωής σύμφωνα με τον ΚΔΔ
Ενδεικτικά πρόκειται για **Στοιχεία για τον προσδιορισμό της ταυτότητας του προσώπου**. Με το σύνηθες προσδιοριστικό της ταυτότητας ενός προσώπου, το όνομα, μπορούν να εξομοιωθούν ο αριθμός της κοινωνικής ασφάλισης, ο αριθμός δελτίου ταυτότητας, ο αριθμός πελάτη και άλλα παρόμοια στοιχεία. Ως στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου έχουν γίνει αποδεκτά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (κωδικός αναγνώρισης ή πρόσβασης, PIN κ.α.).	Ν. 2472/97	Τηρουμένων των προϋποθέσεων και εγγυήσεων επεξεργασίας που εισάγει ο νόμος 2472/97 και ιδίως τα άρθρα 4, 5 και 6 τα **απλά δεδομένα** μπορούν καταρχήν να ενταχθούν στα επίπεδα εμπιστοσύνης 1, 2
Πληροφορίες που αφορούν – **προσωπική ή/και οικογενειακή κατάσταση**		Τα δεδομένα που αφορούν την **προσωπική ή οικογενειακή κατάσταση** μπορεί να ενταχθούν σε υψηλότερο επίπεδο εμπιστοσύνης, καθώς νομολογιακά έχει κριθεί ότι εμπίπτουν στην κατηγορία του ιδιωτικού βίου
Επάγγελμα - Επαγγελματικές ιδιότητες**- Επαγγελματικές** σχέσεις **Οικονομικές σχέσεις** **Οικονομικά στοιχεία – περιουσιακή κατάσταση**		Για τα **οικονομικά στοιχεία** βλ. και στην ειδική κατηγορία του πίνακα

Έννομες σχέσεις και καταστάσεις δημοσίου και ιδιωτικού δικαίου, όπως - σχέσεις προς πράγματα (κινητά και ακίνητα) - συμβατικές σχέσεις - εκπλήρωση υποχρεώσεων έναντι του δημοσίου/τρίτων (φορολογική και ασφαλιστική ενημερότητα) - διοικητικές άδειες κ.λπ.		
ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΕΥΑΙΣΘΗΤΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το επίπεδο εμπιστοσύνης**
Πρόκειται για δεδομένα που αφορούν	Άρθρο 2β ν. 2472/97 Ορισμός ευαίσθητων δεδομένων	
Φυλετική ή Εθνική προέλευση (όχι ιθαγένεια) Τα πολιτικά φρονήματα Θρησκευτικές ή φιλοσοφικές πεποιθήσεις Συμμετοχή σε συνδικαλιστική οργάνωση Την κοινωνική πρόνοια (θα μπορούσαν να θεωρηθούν δεδομένα οικονομικού χαρακτήρα – αφορούν κυρίως την ιδιότητα «πτωχού» - χρήζοντος κοινωνικής υποστήριξης και συνακόλουθα του λήπτη παροχών κοινωνικής πρόνοιας) Ερωτική ζωή Ποινικές διώξεις ή καταδίκες Συμμετοχή σε ενώσεις προσώπων που μπορεί να σχετίζεται με ή να αποκαλύπτει ευαίσθητα δεδομένα		Η ρητή ένταξη των δεδομένων αυτών σε κατηγορία αναβαθμισμένης προστασίας επιτάσσει την ένταξή τους στο ανώτερο επίπεδο εμπιστοσύνης
Υγείας (ή ιατρικά δεδομένα - medical data) νοούνται όλα τα δεδομένα όσα έχουν μία σαφή και στενή σχέση με την υγεία (παρελθούσα, παρούσα και μέλλουσα κατάσταση) Ως δεδομένα υγείας νοούνται και όσα παρέχουν μία εκτίμηση για την κατάσταση της υγείας ενός προσώπου (όπως π.χ. η κατανάλωση αλκοόλ, νικοτίνης κλπ.)		Η ένταξη των δεδομένων αυτών στο ανώτερο επίπεδο εμπιστοσύνης απορρέει και από τις ρυθμίσεις για το ιατρικό απόρρητο που περιέχονται στον Κώδικα Ιατρικής Δεοντολογίας (άρθρο 13 ν. 3418/2005)

ΚΑΤΗΓΟΡΙΑ ΔΕΔΟΜΕΝΩΝ: «ΟΙΚΟΝΟΜΙΚΑ ΔΕΔΟΜΕΝΑ»		
Περιγραφή Δεδομένων	**Νομική Βάση**	**Αντιμετώπιση ως προς το επίπεδο εμπιστοσύνης**
Τα οικονομικά δεδομένα, σύμφωνα με την τυπολογία και κατηγοριοποίηση της νομοθεσίας για την προστασία προσωπικών δεδομένων, εντάσσονται στα απλά δεδομένα. Στα δεδομένα της κατηγορίας αυτής εντάσσονται και οι περιπτώσεις οικονομικών συναλλαγών, που διενεργούνται στα πλαίσια κάποιων ηλεκτρονικών υπηρεσιών, με προκαθορισμένο ύψος συναλλαγής (π.χ. αγορά παραβόλου για έκδοση διαβατηρίου)	Άρθρο 2 α ν. 2472/97	Ένταξη σε συνήθη επίπεδα εμπιστοσύνης (βλέπε την αντίστοιχη κατηγορία του παρόντος πίνακα)
Οικονομικές συναλλαγές για τις οποίες το ύψος της συναλλαγής δεν είναι προκαθορισμένο.	-	Δεδομένου ότι η επίπτωση από κάποιο περιστατικό ασφάλειας στη συγκεκριμένη κατηγορία οικονομικών συναλλαγών μπορεί να έχει πολύ σημαντική επίπτωση (σε επίπεδο οικονομικής και άλλης ζημίας) στο υποκείμενο, τα δεδομένα αυτά θα πρέπει να εντάσσονται στο ανώτερο επίπεδο εμπιστοσύνης
Οικονομικά δεδομένα που καλύπτονται από το φορολογικό απόρρητο	Άρθρο 85 Κώδικα Φορολογίας Εισοδήματος	Τα καλυπτόμενα από το φορολογικό απόρρητο στοιχεία, δηλ. «οι φορολογικές δηλώσεις, τα φορολογικά στοιχεία, οι εκθέσεις και κάθε άλλο στοιχείο του φακέλου που έχει σχέση με τη φορολογία ή άπτεται αυτής» θα πρέπει να εντάσσονται στο ανώτερο επίπεδο εμπιστοσύνης

Πίνακας 4: Αντιστοίχηση Κατηγοριών Δεδομένων με Επίπεδα Εμπιστοσύνης

9.1.2 Οδηγίες Προσδιορισμού Επιπέδου εμπιστοσύνης

Για τον προσδιορισμό του επιπέδου εμπιστοσύνης, ο φορέας θα πρέπει:

1. Να προσδιορίσει τα δεδομένα που επεξεργάζεται η υπηρεσία και να τα κατατάξει (με βάση τα στοιχεία του πίνακα που προηγήθηκε) σε μια από τις παρακάτω κατηγορίες:
    a. **Απλά** – (στην κατηγορία αυτή συμπεριλαμβάνονται και τα «**Δημόσια**» προσπελάσιμα δεδομένα)
    b. Οικονομικά
    c. Ευαίσθητα
2. Να προσδιορίσει το επίπεδο εμπιστοσύνης στο οποίο θα ενταχθεί η προσφερόμενη υπηρεσία, λαμβάνοντας υπόψη ότι:
    a. Όσες υπηρεσίες αξιοποιούν **απλά δεδομένα** εντάσσονται στο:
        i. **Επίπεδο εμπιστοσύνης 0,** εφόσον τα δεδομένα αφορούν δημόσια προσπελάσιμες πληροφορίες (ανακοινώσεις, αιτήσεις) και γενικώς δεδομένα που είναι αδύνατον να συσχετισθούν με κάποιο άτομο-πολίτη.
        ii. **Επίπεδο εμπιστοσύνης 1,** εφόσον αφορούν δεδομένα που αναφέρονται σε φυσικό πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί να διαπιστωθεί, και δεν γίνεται επεξεργασία αναγνωριστικών του χρήστη (όπως Αριθμός Δελτίου Ταυτότητας, Αριθμός Φορολογικού Μητρώου κτλ) για την παροχή της υπηρεσίας.
        iii. Επίπεδο εμπιστοσύνης 2, εφόσον αφορούν δεδομένα που αναφέρονται σε φυσικό πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί να διαπιστωθεί, και γίνεται επεξεργασία αναγνωριστικών του χρήστη (όπως Αριθμός Δελτίου Ταυτότητας, Αριθμός Φορολογικού Μητρώου κτλ) για την παροχή της υπηρεσίας. Επίσης στο επίπεδο εμπιστοσύνης 2 εντάσσονται όλες οι υπηρεσίες που αξιοποιούν οικονομικά δεδομένα που δεν εντάσσονται στο φορολογικό απόρρητο και αφορούν οικονομικές συναλλαγές προκαθορισμένου ύψους, καθώς και υπηρεσίες που αξιοποιούν απλά δεδομένα και δεν μπορούν (σύμφωνα με τα παραπάνω) να ενταχθούν στα επίπεδα εμπιστοσύνης 0 ή 1 (για παράδειγμα πληροφορίες που θεωρείται ότι αφορούν τον ιδιωτικό ή/και οικογενειακό βίο του ατόμου).
    b. Όσες υπηρεσίες αξιοποιούν **οικονομικά δεδομένα**:
        i. Αν τα δεδομένα δεν υπάγονται στο φορολογικά απόρρητο (βλέπε και πίνακα) και αφορούν οικονομικές συναλλαγές προκαθορισμένου ύψους

τότε θεωρούνται «Απλά Δεδομένα» και εντάσσονται στο **επίπεδο εμπιστοσύνης 2** (βλέπε περίπτωση a(iii) παραπάνω).

ii. Αν τα δεδομένα αφορούν οικονομικές συναλλαγές μη προκαθορισμένου ύψους εντάσσονται στο **επίπεδο εμπιστοσύνης 3**.

iii. Αν τα δεδομένα υπάγονται στο φορολογικό απόρρητο εντάσσονται **στο επίπεδο εμπιστοσύνης 3.**

c. Όσες υπηρεσίες αξιοποιούν **ευαίσθητα δεδομένα** εντάσσονται στο:

i. **Επίπεδο εμπιστοσύνης 3.**

9.1.3 Συσχετισμός Επιπέδων Εμπιστοσύνης, Αυθεντικοποίησης και Εγγραφής

Στον Πίνακας 5 παρουσιάζεται ο συσχετισμός μεταξύ επιπέδων εμπιστοσύνης–αυθεντικοποίησης και εγγραφής. Ο συσχετισμός αυτός θα πρέπει να λαμβάνεται υπόψη από τους φορείς που παρέχουν υπηρεσίες ηλεκτρονικής διακυβέρνησης κατά την επιλογή των επιπέδων αυθεντικοποίησης-εγγραφής, αφού αρχικά έχουν προσδιορίσει το αντίστοιχο επίπεδο εμπιστοσύνης.

Συνεπώς, μετά την ένταξη της υπηρεσίας σε κάποιο επίπεδο εμπιστοσύνης, ο φορέας θα υιοθετεί επίπεδο αυθεντικοποίησης και εγγραφής σύμφωνα με τα αναγραφόμενα στον πίνακα που ακολουθεί.

Επίπεδο Εμπιστοσύνης	Επίπεδο Εγγραφής	Επίπεδο Αυθεντικοποίησης	Μηχανισμός Αυθεντικοποίησης
0	0	0	-
1	1	1	Συνθηματικά
2	2		Συνθηματικά μιας Χρήσης
3	3	2	Πιστοποιητικά (Διακριτικό Χαλαρής Αποθήκευσης)
			Πιστοποιητικά (Διακριτικό Σκληρής Αποθήκευσης)

Πίνακας 5. Αντιστοίχηση Επιπέδων Εγγραφής, Επιπέδων Αυθεντικοποίησης και Επιπέδων Εμπιστοσύνης

Συγκεκριμένα:

- για υπηρεσίες επιπέδου εμπιστοσύνης 0, δεν απαιτούνται διαδικασίες εγγραφής και αυθεντικοποίησης.

- για τις υπηρεσίες επιπέδου εμπιστοσύνης 1 και 2, μπορούν να αξιοποιηθούν είτε συνθηματικά, είτε συνθηματικά μιας χρήσης σε περιπτώσεις που ο φορέας κρίνει ότι απαιτείται μεγαλύτερος βαθμός βεβαιότητας αναφορικά με την ορθότητα της ηλεκτρονικής ταυτότητας του χρήστη. Σε αυτή την περίπτωση το επίπεδο εγγραφής που θα υιοθετεί η υπηρεσία θα είναι το 2, έτσι ώστε και η διαδικασία εγγραφής να ελαχιστοποιεί τις πιθανότητες μια οντότητα να υποδυθεί μια άλλη.
- όσες υπηρεσίες εντάσσονται στο επίπεδο εμπιστοσύνης 3 ακολουθούν διαδικασίες εγγραφής επιπέδου 3 αποκλειστικά, ενώ η αυθεντικοποίηση των χρηστών πραγματοποιείται με την αξιοποίηση των αντίστοιχων ψηφιακών πιστοποιητικών. Τα πιστοποιητικά των χρηστών είναι δυνατόν να διανέμονται είτε σε διακριτικά χαλαρής αποθήκευσης είτε σε σκληρής αποθήκευσης. Η επιλογή γίνεται από το φορέα, ο οποίος εφόσον επιθυμεί να πληρούνται οι προϋποθέσεις της νομικά κατοχυρωμένης ισοδυναμίας της ιδιόχειρης υπογραφής με την ψηφιακή, δηλαδή να καλύπτονται οι απαιτήσεις του Π.Δ. 150/2001, θα πρέπει να επιλέξει διακριτικά σκληρής αποθήκευσης.

9.2 Οδηγίες προς Φυσικά και Νομικά Πρόσωπα

9.2.1 Εγγραφή σε Υπηρεσία

9.2.1.1 Αρχική Εγγραφή

Προκειμένου ο χρήστης, φυσικό η νομικό πρόσωπο, να μπορέσει να κάνει χρήση μιας ή περισσότερων ηλεκτρονικών υπηρεσιών θα πρέπει να ολοκληρώσει ένα σύνολο διαδικασιών, ανάλογα με το επίπεδο εμπιστοσύνης που εντάσσεται η κάθε υπηρεσία και συνεπώς με το αντίστοιχο επίπεδο εγγραφής, προκειμένου να είναι σε θέση να ταυτοποιείται και να αυθεντικοποιείται επιτυχώς από την ΚΔΠ.

Ο χρήστης για να αξιοποιήσει μία ηλεκτρονική υπηρεσία αρχικά θα πρέπει να εγγραφεί σε αυτήν. Οι ενέργειες που θα πρέπει να πραγματοποιηθούν για την επιτυχή εγγραφή ενός χρήστη είναι οι ακόλουθες:

1. Επιλογή της υπηρεσίας στην οποία επιθυμεί να εγγραφεί, από σύνολο διαθέσιμων επιλογών στο Διαδικτυακό τόπο της ΚΔΠ
2. Υποβολή ηλεκτρονικής αίτησης στο Διαδικτυακό τόπο της ΚΔΠ, για την ηλεκτρονική υπηρεσία στην οποία επιθυμεί να εγγραφεί. Στην αίτηση συμπεριλαμβάνεται η συμπλήρωση της κατά περίπτωση προβλεπόμενης αντίστοιχης ηλεκτρονικής φόρμας.
3. Κατά περίπτωση ηλεκτρονική υποβολή ή απευθείας κατάθεση των απαιτουμένων δικαιολογητικών για την ολοκλήρωση της εγγραφής στην υπηρεσία, όπως αυτά θα έχουν προσδιοριστεί από το φορέα με βάση το επίπεδο εμπιστοσύνης που θα έχει αποφασίσει να εντάξει τη συγκεκριμένη ηλεκτρονική υπηρεσία.

Με την ολοκλήρωση των ενεργειών αυτών, η ΚΔΠ μεριμνά για τη λήψη των υποβληθέντων στοιχείων και τον έλεγχο της ορθότητας και της πληρότητάς τους, ενώ ακολούθως ενημερώνει τον ενδιαφερόμενο για την επιτυχή ή μη εγγραφή του στην υπηρεσία. Επί θετικής εκβάσεως, με βάση το επίπεδο εμπιστοσύνης της ηλεκτρονικής υπηρεσίας, του αποστέλλει ή τον καλεί να παραλάβει τα αντίστοιχα διακριτικά αυθεντικοποίησης, τα οποία απαιτούνται για την προσπέλαση στην υπηρεσία.

Θα πρέπει να σημειωθεί ότι κατά την αρχική εγγραφή του χρήστη θα προσφέρεται η δυνατότητα για ταυτόχρονη εγγραφή σε περισσότερες από μία υπηρεσίες. Στην περίπτωση αυτή μπορεί να παρέχεται η δυνατότητα στον αιτούντα της επιλογής έκδοσης [α] είτε μόνο του «ισχυρότερου» διαπιστευτηρίου αυθεντικοποίησης, με βάση το υψηλότερο επίπεδο εμπιστοσύνης στο οποίο εντάσσεται κάποια από τις υπηρεσίες που αιτήθηκε, [β] είτε, εναλλακτικά, διαφορετικών διαπιστευτηρίων αυθεντικοποίησης, ισάριθμων με τα διαφορετικά επίπεδα εμπιστοσύνης στα οποία εντάσσονται οι υπηρεσίες τις οποίες αιτήθηκε (ένα διακριτικό αυθεντικοποίησης, ανά επίπεδο εμπιστοσύνης).

9.2.1.2 Αίτηση χρήστη για αξιοποίηση νέας υπηρεσίας

Σε περίπτωση που ο χρήστης επιθυμεί να εγγραφεί σε κάποια νέα ηλεκτρονική υπηρεσία, θα πρέπει να πραγματοποιήσει τα ακόλουθα:

1. Επιλογή της νέας υπηρεσίας στην οποία επιθυμεί να εγγραφεί, από σύνολο διαθέσιμων επιλογών στο Διαδικτυακό τόπο της ΚΔΠ
2. Υποβολή ηλεκτρονικής αίτησης στο Διαδικτυακό τόπο της ΚΔΠ, για τη νέα ηλεκτρονική υπηρεσία στην οποία επιθυμεί να εγγραφεί. Στην αίτηση συμπεριλαμβάνεται η συμπλήρωση της κατά περίπτωση προβλεπόμενης αντίστοιχης ηλεκτρονικής φόρμας.
3. Κατά περίπτωση ηλεκτρονική υποβολή ή απευθείας κατάθεση των απαιτουμένων δικαιολογητικών για την ολοκλήρωση της εγγραφής στη νέα υπηρεσία, όπως αυτά θα έχουν προσδιοριστεί από το φορέα με βάση το επίπεδο εμπιστοσύνης που θα έχει αποφασίσει να εντάξει τη συγκεκριμένη ηλεκτρονική υπηρεσία.

Όπως αναφέρεται στην ενότητα 8 «Διαδικασίες Εγγραφής», το τμήμα της ΚΔΠ που είναι υπεύθυνο για την Εγγραφή των χρηστών, σε κάθε αίτηση εγγραφής που δέχεται, ελέγχει εάν έχουν εκδοθεί διακριτικά αυθεντικοποίησης για τον αιτούντα για το επίπεδο στο οποίο ανήκει η νέα υπηρεσία που επιθυμεί να εγγραφεί. Σε περίπτωση που δεν έχουν εκδοθεί διακριτικά αυθεντικοποίησης για το συγκεκριμένο επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η νέα υπηρεσία, η αρμόδια αρχή της ΚΔΠ εκδίδει τα αντίστοιχα διακριτικά και τα αποστέλλει στο χρήστη, με τρόπο παράδοσης ο οποίος διαφοροποιείται ανάλογα με τον τύπο των διακριτικών βλέπε ενότητα 8.2). Σε διαφορετική περίπτωση, αν ο χρήστης έχει παραλάβει από προηγούμενη διαδικασία εγγραφής διακριτικά αυθεντικοποίησης για το συγκεκριμένο επίπεδο εμπιστοσύνης που είναι ενταγμένη η νέα υπηρεσία, δεν παραλαμβάνει νέα διαπιστευτήρια αλλά αξιοποιεί τα υπάρχοντα για τη χρήση της νέας αυτής υπηρεσίας, αμέσως μόλις η ΚΔΠ ενεργοποιήσει τη σχετική δυνατότητα για αυτόν.

Και στην περίπτωση αυτή, μπορεί να παρέχεται η δυνατότητα στον αιτούντα της επιλογής έκδοσης [α] είτε μόνο του «ισχυρότερου» διαπιστευτηρίου αυθεντικοποίησης, με βάση το υψηλότερο επίπεδο εμπιστοσύνης στο οποίο εντάσσεται κάποια από τις υπηρεσίες που αξιοποιεί, [β] είτε, εναλλακτικά, με τη λήψη όλων των διαπιστευτηρίων, ισάριθμων με τα διαφορετικά επίπεδα εμπιστοσύνης στα οποία εντάσσονται οι υπηρεσίες τις οποίες αιτήθηκε ο αιτών (ένα διακριτικό αυθεντικοποίησης, ανά επίπεδο εμπιστοσύνης).

9.2.2 Χρήση Υπηρεσίας

Χρήση κάποιας ηλεκτρονικής υπηρεσίας μπορεί να επιτευχθεί μόνον εφόσον ο αιτών έχει ολοκληρώσει επιτυχώς τη διαδικασία εγγραφής και αφού πραγματοποιήσει τα ακόλουθα βήματα:

1. Επίσκεψη στο Διαδικτυακό τόπο της ΚΔΠ
2. Επιλογή της ηλεκτρονικής υπηρεσίας την οποία επιθυμεί να χρησιμοποιήσει και στην οποία προφανώς έχει ήδη εγγραφεί κατά το παρελθόν
3. Εισαγωγή του απαιτούμενου για την ταυτοποίηση αναγνωριστικού και για την αυθεντικοποίηση διακριτικού

9.2.3 Ανάκληση Εγγραφής Υπηρεσίας

Προκειμένου κάποιος πολίτης να αιτηθεί ανάκλησης εγγραφής σε μία ηλεκτρονική υπηρεσία θα πρέπει να προβεί στις ακόλουθες ενέργειες:

1. Επίσκεψη στο Διαδικτυακό τόπο της ΚΔΠ
2. Εισαγωγή του απαιτούμενου για την ταυτοποίηση αναγνωριστικού και για την αυθεντικοποίηση διακριτικού, ανάλογα με το επίπεδο εμπιστοσύνης της προς ανάκληση ηλεκτρονικής υπηρεσίας
3. Επιλογή της συγκεκριμένης υπηρεσίας για την οποία επιθυμεί να ανακαλέσει την εγγραφή του (ενδεχομένως να παρέχεται η δυνατότητα στον αιτούντα να ανακαλέσει τη δυνατότητά του χρήσης μίας ηλεκτρονικής υπηρεσίας, ακόμη και αν αυθεντικοποιηθεί με διακριτικό που αντιστοιχεί σε υψηλότερο επίπεδο εμπιστοσύνης από την προς ανάκληση υπηρεσία)
4. Επιβεβαίωση της πρόθεσής του να ανακαλέσει τη χρήση της συγκεκριμένης ηλεκτρονικής υπηρεσίας

10. ΣΥΜΜΟΡΦΩΣΗ ΩΣ ΠΡΟΣ ΤΟ ΠΨΑ

10.1 Συμμόρφωση του Φορέα Παροχής Υπηρεσιών ως προς το ΠΨΑ

Οι φορείς του δημοσίου που προσφέρουν ηλεκτρονικές υπηρεσίες θα πρέπει να συμμορφώνονται πλήρως με το ισχύον θεσμικό κανονιστικό πλαίσιο για ψηφιακή αυθεντικοποίηση και να λαμβάνουν όλα τα απαραίτητα μέτρα για την προστασία της ιδιωτικότητας του πολίτη. Ο έλεγχος συμμόρφωσης με τα παραπάνω διενεργείται με την επιβεβαίωση / έλεγχο εφαρμογής των γενικών ενεργειών / κανόνων που ακολουθούν και αναφέρονται στη συμμόρφωση του φορέα που προσφέρει την ηλεκτρονική υπηρεσία με το ισχύον θεσμικό-κανονιστικό πλαίσιο για Ψηφιακή Αυθεντικοποίηση και την προστασία της ιδιωτικότητας του πολίτη.

[ΚΥ.1] Ο φορέας που προσφέρει την υπηρεσία ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με το ισχύον θεσμικό-κανονιστικό πλαίσιο Ψηφιακής Αυθεντικοποίησης. Συγκεκριμένα:

Α) ΠΡΕΠΕΙ ΝΑ συνταχθούν έντυπα για την παροχή και λήψη συγκατάθεσης, τα οποία θα δίδονται στους αιτούμενους της εγγραφής.

Β) Κατά την αίτηση για εγγραφή σε διάφορες υπηρεσίες ΘΑ ΠΡΕΠΕΙ ΝΑ καθίσταται σαφές στους αιτούντες, ποια δεδομένα είναι αναγκαία για την εγγραφή.

Γ) Κατά την αίτηση για λήψη υπηρεσιών ΘΑ ΠΡΕΠΕΙ ΝΑ καθίσταται σαφές στους αιτούντες ποια και τι είδους δεδομένα είναι αναγκαία για την επεξεργασία και τη διεκπεραίωση της αίτησής τους.

Δ) Κατά την αίτηση ΘΑ ΠΡΕΠΕΙ ΝΑ γίνεται σαφής διαχωρισμός μεταξύ των απαραίτητων και των προαιρετικών δεδομένων.

Ε) ΘΑ ΠΡΕΠΕΙ ΝΑ γίνεται διαχωρισμός των δεδομένων ταυτοποίησης και των δεδομένων που αφορούν το περιεχόμενο της αιτηθείσας ή παρεχόμενης πληροφορίας στο πλαίσιο της υπηρεσίας.

ΣΤ) Ανεξάρτητα από τη συγκατάθεση, ΘΑ ΠΡΕΠΕΙ κατά την εγγραφή σε υπηρεσίες να ενημερώνονται οι αιτούντες, σύμφωνα με το άρθρο 11 του ν. 2472/97, για το σκοπό της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων και την ύπαρξη του δικαιώματος πρόσβασης.

Ζ) ΘΑ ΠΡΕΠΕΙ ΝΑ γίνουν όλες οι απαραίτητες διαδικαστικές ενέργειες έναντι της Αρχής Προστασίας Προσωπικών Δεδομένων που απαιτούνται, κατά περίπτωση, όπως προβλέπει ο νόμος (βλέπε Ενότητα 5.4).

Η) Τα δεδομένα που δεν είναι πλέον αναγκαία για την εκπλήρωση ενός σκοπού επεξεργασίας ΠΡΕΠΕΙ ΝΑ διαγράφονται/ καταστρέφονται. Για την καταστροφή ΘΑ ΠΡΕΠΕΙ ΝΑ ακολουθούνται οι οδηγίες της Αρχής Προστασίας Προσωπικών

	Δεδομένων που περιέχονται στη σχετική Οδηγία 1/2005 (http://www.dpa.gr/secure)

[ΚΠ.1]	Καθώς η συγκατάθεση των αιτουμένων εγγραφής σε μια υπηρεσία ([ΚΥ.1]-Α) πρέπει να είναι σαφής, ρητή, ειδική και «ενημερωμένη» ΣΥΝΙΣΤΑΤΑΙ ΝΑ ακολουθείται ο έγγραφος τύπος συγκατάθεσης.

[ΚΠ.2]	Η ενημέρωση των αιτούντων για το σκοπό της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων και την ύπαρξη του δικαιώματος πρόσβασης ([ΚΥ.1]-ΣΤ), ΔΥΝΑΤΑΙ ΝΑ γίνει και ηλεκτρονικά, με γενική αναγραφή των σχετικών όρων στο δικτυακό τόπο. Στην περίπτωση αυτή θα πρέπει ο συγκεκριμένος «τόπος» της ενημέρωσης να είναι εμφανής και να επισημαίνεται στον εγγραφόμενο - ηλεκτρονικά συναλλασσόμενο.

[ΚΠ.3]	Δεδομένου ότι τα προσωπικά δεδομένα πρέπει να είναι ακριβή και επικαιροποιημένα ΣΥΝΙΣΤΑΤΑΙ ΝΑ εισαχθούν συγκεκριμένες προθεσμίες (π.χ. ανά έτος) στο πλαίσιο των οποίων θα ελέγχεται η επικαιροποίηση των δεδομένων.

[ΚΥ.2]	Ο φορέας που προσφέρει μια ηλεκτρονική υπηρεσία ΠΡΕΠΕΙ ΝΑ διασφαλίζει την ιδιωτικότητα των χρηστών της. Συγκεκριμένα: Α) Κατά τη συλλογή και επεξεργασία δεδομένων ΘΑ ΠΡΕΠΕΙ ΝΑ λαμβάνεται πρόνοια ώστε να υπάρχει σαφής προσδιορισμός και διαχωρισμός των δεδομένων προσωπικού χαρακτήρα από τα δεδομένα στατιστικού χαρακτήρα. Β) ΘΑ ΠΡΕΠΕΙ ΝΑ διασφαλίζεται ότι από τα δεδομένα στατιστικού χαρακτήρα δεν είναι δυνατός ο προσδιορισμός της ταυτότητας των φυσικών προσώπων

[ΚΥ.3]	Σε περίπτωση προσφυγής σε εξωτερικούς ιδιωτικούς φορείς για την αποθήκευση και πρόσβαση σε προσωπικά δεδομένα χρηστών ΘΑ ΠΡΕΠΕΙ ΝΑ περιλαμβάνονται στη σχετική σύμβαση όροι για τη συλλογή και επεξεργασία δεδομένων.

10.2 Συμμόρφωση των Ηλεκτρονικών Υπηρεσιών ως προς το ΠΨΑ

Η διαδικασία ελέγχου συμμόρφωσης μιας ηλεκτρονικής υπηρεσίας με το ΠΨΑ, αναφορικά με τις διαδικασίες εγγραφής και το μηχανισμό αυθεντικοποίησης που υιοθετεί, περιλαμβάνει τα ακόλουθα βήματα:

- Επιβεβαιώνεται ότι η κατηγοριοποίηση των δεδομένων που αξιοποιεί η υπηρεσία ακολουθεί τις οδηγίες που ορίζονται στο ΠΨΑ.
- Επιβεβαιώνεται η ορθότητα του Επιπέδου Εμπιστοσύνης στο οποίο εντάχθηκε η υπηρεσία.
- Ελέγχεται η ορθότητα του Επιπέδου Εγγραφής και του Επιπέδου Αυθεντικοποίησης, καθώς και των Μηχανισμών Αυθεντικοποίησης που υιοθετήθηκαν από το φορέα, δηλαδή ότι είναι σύμφωνα με τα προβλεπόμενα σε σχέση με το Επίπεδο Εμπιστοσύνης.
- Ελέγχεται αν ο φορέας παροχής της υπηρεσίας έχει δημοσιοποιήσει τα απαραίτητα στοιχεία και έγγραφα για την εγγραφή των χρηστών.

Ουσιαστικά ο έλεγχος συμμόρφωσης των ηλεκτρονικών υπηρεσιών ως προς το ΠΨΑ, αφορά την επιβεβαίωση / έλεγχο εφαρμογής των ειδικών ενεργειών / κανόνων που ακολουθούν.

Ο «ειδικοί» κανόνες της παρούσας ενότητας αφορούν τη συμμόρφωση μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας αναφορικά με τις διαδικασίες εγγραφής και το μηχανισμό αυθεντικοποίησης που υιοθετεί, σύμφωνα με τα οριζόμενα στο ΠΨΑ.

[ΚΥ.4]	Ο φορέας που προσφέρει μια ηλεκτρονική υπηρεσία ΠΡΕΠΕΙ ΝΑ προσδιορίσει την κατηγορία των δεδομένων που αξιοποιεί / επεξεργάζεται η συγκεκριμένη υπηρεσία. Ο προσδιορισμός της κατηγορίας ΠΡΕΠΕΙ ΝΑ γίνει σύμφωνα με τα οριζόμενα στην Ενότητα 9.1.1.

[ΚΥ.5]	Ο φορέας που προσφέρει μία ηλεκτρονική υπηρεσία ΠΡΕΠΕΙ ΝΑ προσδιορίσει το Επίπεδο Εμπιστοσύνης στο οποίο εντάσσεται η συγκεκριμένη υπηρεσία. Ο προσδιορισμός του Επιπέδου Εμπιστοσύνης προκύπτει από την κατηγορία των δεδομένων που προσδιορίστηκε στον [ΚΥ.4] και σύμφωνα με τα οριζόμενα στην Ενότητα 9.1.2 του ΠΨΑ.

[ΚΥ.6]	Υπηρεσίες που έχουν ενταχθεί στο Επίπεδο Εμπιστοσύνης 0 ΘΑ ΠΡΕΠΕΙ ΝΑ υιοθετήσουν: • Επίπεδο Εγγραφής 0 και • Επίπεδο Αυθεντικοποίησης 0

[ΚΥ.7]	Υπηρεσίες που έχουν ενταχθεί στο Επίπεδο Εμπιστοσύνης 1 ΘΑ ΠΡΕΠΕΙ ΝΑ υιοθετήσουν: • Επίπεδο Εγγραφής 1 και • Επίπεδο Αυθεντικοποίησης 1

[ΚΥ.8]	Υπηρεσίες που έχουν ενταχθεί στο Επίπεδο Εμπιστοσύνης 2 ΘΑ ΠΡΕΠΕΙ ΝΑ υιοθετήσουν: • Επίπεδο Εγγραφής 2 και • Επίπεδο Αυθεντικοποίησης 1

[ΚΥ.9]	Υπηρεσίες που έχουν ενταχθεί στο Επίπεδο Εμπιστοσύνης 3 ΘΑ ΠΡΕΠΕΙ ΝΑ υιοθετήσουν: • Επίπεδο Εγγραφής 3 και • Επίπεδο Αυθεντικοποίησης 2

[ΚΠ.4]	Για τις υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 0, ΔΕΝ ΠΡΟΤΕΙΝΕΤΑΙ η αξιοποίηση κάποιου μηχανισμού αυθεντικοποίησης.

[ΚΠ.5]	Για τις υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Εγγραφής 0, ΔΕΝ ΠΡΟΤΕΙΝΕΤΑΙ κάποια συγκεκριμένη διαδικασία εγγραφής.

[ΚΥ.10]	Υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 1 ΘΑ ΠΡΕΠΕΙ ΝΑ αξιοποιήσουν ως Μηχανισμό Αυθεντικοποίησης τα «ΣΥΝΘΗΜΑΤΙΚΑ»

[ΚΠ.6]	Για Υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 1, ο φορέας ΔΥΝΑΤΑΙ ΝΑ αξιοποιήσει ως μηχανισμό Αυθεντικοποίησης τα «ΣΥΝΘΗΜΑΤΙΚΑ ΜΙΑΣ ΧΡΗΣΗΣ»

[ΚΥ.11] Υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Εγγραφής 1 ΘΑ ΠΡΕΠΕΙ ΝΑ μεριμνούν να αποστέλλεται, δια της Αρχής Εγγραφής, η συμπληρωμένη ηλεκτρονική αίτηση του ενδιαφερόμενου στον εξυπηρετητή της υπηρεσίας, προκειμένου ο φορέας να πραγματοποιήσει έλεγχο σχετικά: με την εγκυρότητα των στοιχείων της αίτησης, την εγκυρότητα των αναγνωριστικών, το δικαίωμα του αιτούντος να χρησιμοποιήσει την υπηρεσία και την επιβεβαίωση ότι δεν υπάρχει άλλος λογαριασμός για τον αιτούντα αυτό για το συγκεκριμένο επίπεδο εγγραφής. Αν η απάντηση που λάβει η Αρχή Εγγραφής από τον εξυπηρετητή της υπηρεσίας είναι αρνητική, τότε ΠΡΕΠΕΙ ΝΑ ενημερώσει σχετικά τον αιτούντα, διαφορετικά ΠΡΕΠΕΙ ΝΑ αποστείλει στο χρήστη με συστημένη επιστολή τα διαπιστευτήρια για τη χρήση της υπηρεσίας.

[ΚΥ.12] Υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Εγγραφής 2 ΘΑ ΠΡΕΠΕΙ ΝΑ αποστέλλουν, δια της Αρχής Εγγραφής, τη συμπληρωμένη ηλεκτρονική αίτηση του ενδιαφερόμενου στον εξυπηρετητή της υπηρεσίας, προκειμένου ο φορέας να πραγματοποιήσει έλεγχο σχετικά: με την εγκυρότητα των στοιχείων της αίτησης, την εγκυρότητα των αναγνωριστικών, το δικαίωμα του αιτούντος να χρησιμοποιήσει την υπηρεσία και την επιβεβαίωση ότι δεν υπάρχει άλλος λογαριασμός για τον αιτούντα αυτό για το συγκεκριμένο επίπεδο εγγραφής. Αν η απάντηση που λάβει η Αρχή Εγγραφής από τον εξυπηρετητή της υπηρεσίας είναι αρνητική, τότε ΠΡΕΠΕΙ ΝΑ ενημερώσει σχετικά τον αιτούντα, διαφορετικά ΠΡΕΠΕΙ ΝΑ εκδώσει το διακριτικό αυθεντικοποίησης, το οποίο ο ενδιαφερόμενος ΘΑ ΠΡΕΠΕΙ να ενημερωθεί ότι μπορεί να παραλάβει από την αρμόδια υπηρεσία, αφού βεβαίως εκεί ΠΡΕΠΕΙ πρώτα ΝΑ ταυτοποιηθεί επιδεικνύοντας τα απαιτούμενα από το φορέα δημόσια έγγραφα.

[ΚΥ.13] Υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Αυθεντικοποίησης 2 ΘΑ ΠΡΕΠΕΙ ΝΑ αξιοποιήσουν ως Μηχανισμό Αυθεντικοποίησης τα «ΠΙΣΤΟΠΟΙΗΤΙΚΑ (Διακριτικό Σκληρής Αποθήκευσης)» (εκτός περιπτώσεων που ο φορέας επιλέξει τη χρήση διακριτικών χαλαρής αποθήκευσης).

[ΚΥ.14] Υπηρεσίες που έχουν υιοθετήσει το Επίπεδο Εγγραφής 3 ΘΑ ΠΡΕΠΕΙ ΝΑ αποστέλλουν, δια της Αρχής Εγγραφής, τη συμπληρωμένη ηλεκτρονική αίτηση του ενδιαφερόμενου στον εξυπηρετητή της υπηρεσίας, προκειμένου ο φορέας να πραγματοποιήσει έλεγχο σχετικά: με την εγκυρότητα των στοιχείων της αίτησης, την εγκυρότητα των αναγνωριστικών, το δικαίωμα του αιτούντος να χρησιμοποιήσει την υπηρεσία και την επιβεβαίωση ότι δεν υπάρχει άλλος λογαριασμός για τον αιτούντα αυτό στο συγκεκριμένο επίπεδο εγγραφής. Αν η απάντηση που λάβει η Αρχή Εγγραφής από τον εξυπηρετητή της υπηρεσίας είναι αρνητική ΠΡΕΠΕΙ ΝΑ

ενημερώσει σχετικά τον αιτούντα, διαφορετικά ΠΡΕΠΕΙ ΝΑ προωθήσει την αίτηση στην Αρχή Πιστοποίησης για την έκδοση των απαραίτητων ψηφιακών πιστοποιητικών. Ο ενδιαφερόμενος ΠΡΕΠΕΙ ΝΑ ενημερωθεί ότι μπορεί να παραλάβει το διακριτικό αυθεντικοποίησης από την αρμόδια υπηρεσία αφού βεβαίως εκεί ΠΡΕΠΕΙ πρώτα ΝΑ ταυτοποιηθεί επιδεικνύοντας τα απαιτούμενα από το φορέα δημόσια έγγραφα. Μετά την παραλαβή του διακριτικού αυθεντικοποίησης, ο προσωπικός κωδικός πρόσβασης (PIN – Personal Identification Number) του διακριτικού ΠΡΕΠΕΙ ΝΑ αποσταλεί με συστημένη επιστολή στη διεύθυνση αλληλογραφίας του αιτούντος.

[ΚΥ.15] Ο φορέας ΠΡΕΠΕΙ ΝΑ δημοσιοποιήσει τα απαραίτητα στοιχεία και έγγραφα που απαιτούνται για την εγγραφή των ενδιαφερομένων στην υπηρεσία.

10.3 Συμμόρφωση της ΚΔΠ ως προς το ΠΨΑ

Επιπλέον των ανωτέρω ελέγχων συμμόρφωσης του Φορέα και των προσφερόμενων Ηλεκτρονικών Υπηρεσιών, απαιτείται και ο έλεγχος συμμόρφωσης της συνολικής αρχιτεκτονικής και μηχανισμού ταυτοποίησης της ΚΔΠ με τα οριζόμενα στο ΠΨΑ. Επίσης πρέπει να ελέγχεται η ικανοποίηση των απαιτήσεων ασφάλειας που τίθενται από το επίπεδο εμπιστοσύνης στο οποίο έχει ενταχθεί η υπηρεσία. Οι σχετικοί κανόνες περιλαμβάνουν:

[ΚΜ.1] Ο μηχανισμός ταυτοποίησης των χρηστών στην ΚΔΠ, και δι' αυτής στην τελική υπηρεσία, ΜΕΛΕΤΑΤΑΙ ΝΑ υλοποιείται χωρίς αποθήκευση διαπιστευτηρίων στην ΚΔΠ και με δυνατότητα του χρήστη να επιλέγει την ενδεχόμενη αποθήκευση στην ΚΔΠ των αναγνωριστικών για κάθε ξεχωριστή υπηρεσία (σύμφωνα με τα οριζόμενα στην ενότητα 6).

[ΚΜ.2] Μεταξύ της ΚΔΠ και του εξυπηρετητή της υπηρεσίας είναι απαραίτητο να έχει εγκαθιδρυθεί και να λειτουργεί αποτελεσματικά μία καλά ορισμένη σχέση εμπιστοσύνης (trust relationship). ΜΕΛΕΤΑΤΑΙ η αξιοποίηση σχετικού διακριτικού (token), το οποίο θα χρησιμοποιείται για την αμοιβαία ταυτοποίηση και αυθεντικοποίησή τους. Επίσης, ΜΕΛΕΤΑΤΑΙ η δημιουργία Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network) μεταξύ τους, ώστε να διασφαλιστεί, μεταξύ άλλων, η εμπιστευτικότητα και ακεραιότητα των δεδομένων που ανταλλάσσονται μέσω του ασφαλούς διαύλου (secure channel) που δημιουργείται.

[ΚΥ.16] Κατά την εκτέλεση της υπηρεσίας, η ΚΔΠ ΠΡΕΠΕΙ ΝΑ αποθηκεύει ασφαλώς στοιχεία που να αφορούν το ιστορικό κάθε επικοινωνίας (λήψη αιτήσεων, αποστολή απαντήσεων, χρόνος διενέργειας της επικοινωνίας κλπ.) με το χρήστη και τον εξυπηρετητή της αντίστοιχης υπηρεσίας, αποκλειστικά και μόνο για σκοπούς διασφάλισης της δυνατότητας ελέγχου (auditing). Η ΚΔΠ ΔΕΝ ΠΡΕΠΕΙ ΝΑ αποθηκεύει κανένα επιπλέον στοιχείο αναφορικά με το χρήστη ή την υπηρεσία. Για την άρτια λειτουργία του μηχανισμού ελέγχου (auditing), η ΚΔΠ ΠΡΕΠΕΙ ΝΑ διασφαλίζει την αποθήκευση των ιχνών ελέγχου όλων των ως άνω επικοινωνιών, σε περιβάλλον διασφάλισης της ακεραιότητας των αποθηκευμένων στοιχείων, δηλαδή αδυναμίας εκ των υστέρων τροποποίησής τους.

[ΚΥ.17] ΠΡΕΠΕΙ ΝΑ λαμβάνονται τα κατάλληλα μέτρα ασφάλειας ώστε να ικανοποιούνται οι απαιτήσεις ασφάλειας που τίθενται από το Επίπεδο Εμπιστοσύνης στο οποίο έχει ενταχθεί η υπηρεσία. Οι απαιτήσεις ασφάλειας ΠΡΕΠΕΙ ΝΑ ικανοποιούνται τόσο στο τμήμα επικοινωνίας μεταξύ ΚΔΠ και εξυπηρετητή υπηρεσίας, όσο και στο τμήμα επικοινωνίας μεταξύ ΚΔΠ και χρήστη.

10.4 Συμμόρφωση Υποκειμένων Αρχών Πιστοποίησης ως προς το Πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου, η οποία ενεργεί ως Πρωτεύουσα Αρχή Πιστοποίησης και έχει την ευθύνη συντονισμού των Υποκειμένων Αρχών σύμφωνα με το άρθρο 20 του Ν. 3448/2006, θα πρέπει να έχει την ευθύνη ελέγχου συμμόρφωσης των Πολιτικών Πιστοποιητικών των Υποκειμένων Αρχών με βάση το Πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών, που παρουσιάζεται στο ΠΑΡΑΡΤΗΜΑ Β: Πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών και τις διατάξεις που δημοσιεύονται στο Φ.Ε.Κ. Τεύχος Β 1654/10-11-2006.

Για να είναι δυνατή η πιστοποίηση, ως προς το Πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών, οποιασδήποτε υποψήφιας Υποκείμενης Αρχής Πιστοποίησης θα πρέπει κατ' αρχάς να συμμορφώνεται με τους ακόλουθους κανόνες.

[ΚΥ.18] Η Υποκείμενη Αρχή Πιστοποίησης ΠΡΕΠΕΙ ΝΑ δημιουργήσει τουλάχιστον τους ρόλους:

- Διαχειριστή Πολιτικής Πιστοποιητικών
- Συγγραφέα Πολιτικής Πιστοποιητικών

Επίσης ΠΡΕΠΕΙ ΝΑ αναθέσει τους παραπάνω ρόλους σε στελέχη της και να αποδώσει αντίστοιχες αρμοδιότητες.

[ΚΥ.19]	Η Υποκείμενη Αρχή Πιστοποίησης ΠΡΕΠΕΙ ΝΑ διαθέτει Πολιτική Ψηφιακών Πιστοποιητικών σύμφωνα με τα οριζόμενα στο Πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών (ΠΑΡΑΡΤΗΜΑ Β: Πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών).

[ΚΥ.20]	Η Υποκείμενη Αρχή Πιστοποίησης ΠΡΕΠΕΙ ΝΑ δημοσιεύσει την Πολιτική Ψηφιακών Πιστοποιητικών στον ιστοχώρο της, σε εμφανές σημείο.

[ΚΥ.21]	Η Υποκείμενη Αρχή Πιστοποίησης ΠΡΕΠΕΙ ΝΑ εναρμονίζεται με το ισχύον νομοθετικό πλαίσιο (Ενότητα 13.1.8).

[ΚΥ.22]	ΠΡΕΠΕΙ ΝΑ διενεργούνται τακτικοί έλεγχοι της πολιτικής ψηφιακών πιστοποιητικών από στελέχη της μονάδας πληροφορικής της Υποκείμενης Αρχής Πιστοποίησης.

[ΚΥ.23]	Τα εκδιδόμενα πιστοποιητικά ΠΡΕΠΕΙ ΝΑ συμμορφώνονται με το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η υπηρεσία για την οποία εκδίδονται.

[ΚΥ.24]	ΠΡΕΠΕΙ ΝΑ πληρούνται οι ελάχιστες προϋποθέσεις του Πλαισίου Πολιτικής Ψηφιακών Πιστοποιητικών, όπως προδιαγράφονται στην ενότητα 13.1.9.

11. ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΠΨΑ

11.1 Εισαγωγή

Τα παραδείγματα που ακολουθούν έχουν ως στόχο να επιδείξουν τη διαδικασία εφαρμογής του ΠΨΑ σε υπηρεσίες που σήμερα προσφέρονται ηλεκτρονικά από Δημόσιους φορείς. Συγκεκριμένα για κάθε ηλεκτρονική υπηρεσία εφαρμόζονται οι οδηγίες εφαρμογής (κανόνες) του ΠΨΑ και στη συνέχεια καταδεικνύονται τυχόν σημαντικές αλλαγές που απαιτούνται αναφορικά με τον μηχανισμό αυθεντικοποίησης ή/και με τις διαδικασίες εγγραφής, σε σχέση με την υφιστάμενη κατάσταση.

11.2 Παράδειγμα Εφαρμογής ΠΨΑ 1 (2 Υπηρεσίες): Υπηρεσίες Δημοτολογίου (μέσω ΚΕΠ)

Στην παρούσα ενότητα εξετάζονται υπηρεσίες του Δημοτολογίου που προσφέρονται ηλεκτρονικά μέσω των Δικτυακών Τόπων των Κέντρων Εξυπηρέτησης Πολιτών (ΚΕΠ). Συγκεκριμένα οι υπηρεσίες αυτές είναι:

- Χορήγηση Αντίγραφου Πιστοποιητικού Γέννησης (ΦΕΚ τ. Β 896/16.07.2002)
- Χορήγηση Πιστοποιητικού Οικογενειακής Κατάστασης

11.2.1 Υπάρχουσα Διαδικασία Εγγραφής

Οι προαναφερόμενες υπηρεσίες παρέχονται ηλεκτρονικά από το δικτυακό τόπο του Κέντρου Εξυπηρέτησης Πολιτών. Προκειμένου λοιπόν κάποιος να κάνει χρήση των υπηρεσιών αυτών, θα πρέπει να εγγραφεί στον ιστότοπο αυτό. Για την επιτυχή ολοκλήρωση της εγγραφής, ο χρήστης επισκέπτεται το δικτυακό τόπο του Κ.Ε.Π. και επιλέγει το σύνδεσμο «Εγγραφή Χρήστη». Ο χρήστης μεταφέρεται στη σχετική ηλεκτρονική σελίδα, συμπληρώνει τη φόρμα εγγραφής και την υποβάλει. Τα υποβληθέντα στοιχεία (βλέπε ενότητα 11.2.2.1.) ελέγχονται και, εφόσον πιστοποιηθεί η ορθότητά τους και η μοναδικότητα του ονόματος χρήστη που εισήγαγε ο χρήστης, δημιουργείται ο λογαριασμός για τον αιτούντα. Προκειμένου να ενεργοποιηθεί ο λογαριασμός του χρήστη, αποστέλλονται στην ηλεκτρονική διεύθυνση που δήλωσε κατά τη διάρκεια της εγγραφής ένας κωδικός ενεργοποίησης και ένα [link]. Ο χρήστης επισκέπτεται το [link], εισάγει τον κωδικό ενεργοποίησης και εφ' όσον ο κωδικός είναι σωστός μπορεί πλέον να κάνει χρήση των ηλεκτρονικών υπηρεσιών που προσφέρονται από τον ιστότοπο του Κέντρου Εξυπηρέτησης Πολιτών.

11.2.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.2.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Τα στοιχεία που καλείται να συμπληρώσει ο χρήστης κατά τη διάρκεια της εγγραφής του στην υπηρεσία είναι:

- Όνομα και Επώνυμο
- Όνομα Πατέρα
- Χώρα, Νομός και Πόλη κατοικίας
- Τηλέφωνο Επικοινωνίας
- Όνομα χρήστη (username) και Συνθηματικό (password) που επιθυμεί να χρησιμοποιεί
- Διεύθυνση ηλεκτρονικού ταχυδρομείου

11.2.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Τα στοιχεία που χρησιμοποιούνται κατά την αξιοποίηση των παραπάνω υπηρεσιών είναι τα ακόλουθα:

- Νομός και Διεύθυνση ΚΕΠ που θα διεκπεραιώσει την αίτηση του χρήστη
- Δημοτολόγιο του δήμου ή της κοινότητας που είναι εγγεγραμμένος ο χρήστης
- Όνομα
- Επώνυμο
- Όνομα Πατέρα
- Αριθμός Δελτίου Ταυτότητας
- Τόπος Γέννησης
- Τηλέφωνο Επικοινωνίας
- Λόγος Έκδοσης Πιστοποιητικού
- Αριθμός Δημοτολογίου (μόνο για την υπηρεσία χορήγησης πιστοποιητικού οικογενειακής κατάστασης)
- Οικογενειακή Κατάσταση (μόνο για την υπηρεσία χορήγησης πιστοποιητικού οικογενειακής κατάστασης)

11.2.3 Επιπτώσεις Απειλών

Οι περισσότερες από τις απειλές που έχουν ως στόχο την υποκλοπή / τροποποίηση των δεδομένων δεν επιφέρουν σημαντικές επιπτώσεις καθώς τα δεδομένα τα οποία αξιοποιούνται είναι «απλά δεδομένα». Οι σημαντικότερες επιπτώσεις που μπορεί να προκύψουν αφορούν περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στην υπηρεσία με στόχο την αίτηση χορήγησης των πιστοποιητικών από μη εξουσιοδοτημένα άτομα.

11.2.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στις παραπάνω υπηρεσίες Δημοτολογίου που προσφέρονται ηλεκτρονικά μέσω του ΚΕΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2.

- *[ΚΥ.4]: Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1, εντάσσονται στην κατηγορία «**Απλά Δεδομένα**».
- *[ΚΥ.5]: Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 2** (γίνεται επεξεργασία αναγνωριστικών του χρήστη – Αριθμός Δελτίου Ταυτότητας).
- Σύμφωνα με τον *[ΚΥ.8]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 2** και **Επίπεδο Αυθεντικοποίησης 1**.
- Σύμφωνα με τους *[ΚΥ.10] και [ΚΠ.6]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΣΥΝΘΗΜΑΤΙΚΑ**», ενώ *προαιρετικά* μπορούν να αξιοποιηθούν και «ΣΥΝΘΗΜΑΤΙΚΑ ΜΙΑΣ ΧΡΗΣΗΣ».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη των υπηρεσιών στο ΠΨΑ.

ΥΠΗΡΕΣΙΕΣ ΔΗΜΟΤΟΛΟΓΙΟΥ (μέσω ΚΕΠ)	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	1)Χορήγηση Αντιγράφου Πιστοποιητικού Γέννησης του ενδιαφερόμενου (ΦΕΚ τ. Β 896/16.07.2002) 2) Χορήγηση Πιστοποιητικού Οικογενειακής Κατάστασης
Αρμόδιος Φορέας	Δήμοι (Δημοτολόγια) / ΚΕΠ
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	ΑΔΤ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 2
Επίπεδο Αυθεντικοποίησης	Επίπεδο 1
Μηχανισμός Αυθεντικοποίησης	Συνθηματικά (Προαιρετικά: Συνθηματικά μιας Χρήσης)
Επίπεδο Εγγραφής	Επίπεδο 2

Πίνακας 6: Ένταξη Υπηρεσιών Δημοτολογίου (μέσω ΚΕΠ) στο ΠΨΑ

11.2.5 Απαιτούμενες Τροποποιήσεις Υπάρχουσας Κατάστασης

Η σημαντικότερη τροποποίηση, σε σχέση με την υφιστάμενη κατάσταση, αφορά τη διαδικασία εγγραφής στις υπηρεσίες (πρέπει να ακολουθηθούν τα προβλεπόμενα από το Επίπεδο Εγγραφής 2) και συγκεκριμένα το γεγονός ότι ο πολίτης πρέπει να παραλάβει ο ίδιος τα συνθηματικά του αφού πρώτα ταυτοποιηθεί μέσω της επίδειξης της Αστυνομικής του Ταυτότητας.

11.3 Παράδειγμα Εφαρμογής ΠΨΑ 2: Αντίγραφο Ποινικού Μητρώου (μέσω ΚΕΠ)

11.3.1 Υπάρχουσα Διαδικασία Εγγραφής

Η χορήγηση αντιγράφου ποινικού μητρώου παρέχεται ηλεκτρονικά από το δικτυακό τόπο του Κέντρου Εξυπηρέτησης Πολιτών. Η διαδικασία εγγραφής στον ιστότοπο του ΚΕΠ, ώστε να είναι δυνατή η αξιοποίηση της υπηρεσίας, έχει ήδη περιγραφεί στην ενότητα 11.2.1.

11.3.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.3.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Τα στοιχεία που καλείται να συμπληρώσει ο χρήστης κατά τη διάρκεια της εγγραφής του στο ΚΕΠ έχουν ήδη περιγραφεί στην ενότητα 11.2.2.1.

11.3.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση της Υπηρεσίας

Τα στοιχεία που χρησιμοποιούνται κατά την αξιοποίηση της υπηρεσίας είναι τα ακόλουθα:

- Κέντρο Εξυπηρέτησης Πολιτών που θα διεκπεραιώσει την αίτηση
- Δήμος ή Κοινότητα τόπου γεννήσεως και η Νομαρχία που ανήκει
- Τύπος Ποινικού Μητρώου
- Όνομα και Επώνυμο
- Όνομα και Επώνυμο Πατέρα
- Όνομα και Επώνυμο Μητέρας
- Ημερομηνία Γέννησης
- Αριθμός Δελτίου Ταυτότητας
- Τόπος γέννησης
- Χώρα Γέννησης
- Τόπος Κατοικίας
- Οδός
- Αριθμός
- Τ.Κ.
- Τηλέφωνο
- Λόγος Έκδοσης Αντιγράφου
- Αποδέκτης Αντιγράφου Ποινικού Μητρώου

Θα πρέπει να τονιστεί ότι στη συγκεκριμένη ηλεκτρονική υπηρεσία είναι απαραίτητο, επιπλέον των στοιχείων που υποβάλλονται από τον ενδιαφερόμενο, να ληφθούν υπόψη και τα παραγόμενα στοιχεία που θα περιλαμβάνονται στο αντίγραφο ποινικού μητρώου, υπό την οπτική του ν.2472/97.

11.3.3 Επιπτώσεις Απειλών

Δεδομένης της υπάρχουσας διαδικασίας εγγραφής στο ΚΕΠ, μπορεί κάποιος να υποδυθεί οποιοδήποτε πολίτη και να αιτηθεί απλώς την έκδοση νόμιμων διακριτικών αυθεντικοποίησης για λογαριασμό του πολίτη χωρίς αυτό να γίνει αντιληπτό, με αποτέλεσμα να έχει τη δυνατότητα αιτήσεων ποινικών μητρώων. Στην περίπτωση, όμως, αυτή ο χρήστης δεν μπορεί να παραλάβει το αντίγραφο ποινικού μητρώου, καθώς απαιτείται η φυσική του παρουσία στο αντίστοιχο ΚΕΠ. Βεβαίως σε περίπτωση που ο υπάλληλος του ΚΕΠ συνεργαζόταν με τον κακόβουλο χρήστη, αυτός θα μπορούσε να αποκτήσει πρόσβαση στο έγγραφο.

11.3.4 Εφαρμογή του ΠΨΑ στην Υπηρεσία

Η εφαρμογή του ΠΨΑ στην υπηρεσία χορήγησης αντίγραφου ποινικού μητρώου που προσφέρεται ηλεκτρονικά μέσω του ΚΕΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2.

- *[ΚΥ.4]: Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στην προαναφερόμενη υπηρεσία, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 (σύμφωνα με το Άρθρο 2β ν. 2472/97 τα δεδομένα που αφορούν ποινικές διώξεις ή καταδίκες χαρακτηρίζονται ως ευαίσθητα), εντάσσονται στην κατηγορία «**Ευαίσθητα Δεδομένα**».
- *[ΚΥ.5]: Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Η υπηρεσία χορήγησης ποινικού μητρώου, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2, εντάσσεται στο **Επίπεδο Εμπιστοσύνης 3**.
- Σύμφωνα με τον *[ΚΥ.9]*, η υπηρεσία θα πρέπει να υιοθετήσει **Επίπεδο Εγγραφής 3** και **Επίπεδο Αυθεντικοποίησης 2**.
- Σύμφωνα με τον *[ΚΥ.13]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΠΙΣΤΟΠΟΙΗΤΙΚΑ** (Διακριτικό Σκληρής Αποθήκευσης)».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΧΟΡΗΓΗΣΗ ΑΝΤΙΓΡΑΦΟΥ ΠΟΙΝΙΚΟΥ ΜΗΤΡΩΟΥ (μέσω ΚΕΠ)	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Χορήγηση Αντιγράφου Ποινικού Μητρώου
Αρμόδιος Φορέας	Αυτοτελές Τμήμα Ποινικού Μητρώου, Υπουργείο Δικαιοσύνης / ΚΕΠ
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	ΑΔΤ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΑΣ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Ευαίσθητα δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 3
Επίπεδο Αυθεντικοποίησης	Επίπεδο 2
Μηχανισμός Αυθεντικοποίησης	Ψηφιακό Πιστοποιητικό αποθηκευμένο σε Διακριτικό Σκληρής Αποθήκευσης
Επίπεδο Εγγραφής	Επίπεδο 3

Πίνακας 7: Ένταξη Υπηρεσίας Χορήγησης Αντιγράφου Ποινικού Μητρώου (μέσω ΚΕΠ) στο ΠΨΑ

11.3.5 Απαιτούμενες Τροποποιήσεις Υπάρχουσας Κατάστασης

Αναφορικά με την αξιοποίηση των διακριτικών αυθεντικοποίησης θα πρέπει να καταργηθεί η αξιοποίηση των συνθηματικών και να αξιοποιηθούν ψηφιακά πιστοποιητικά, εφόσον η απόδοση του τελικού εγγράφου απαιτεί τη φυσική παρουσία του χρήστη. Σε περίπτωση που η παράδοση του εγγράφου γίνεται ηλεκτρονικά θα πρέπει να αξιοποιηθεί διακριτικό σκληρής αποθήκευσης.

Σχετικά με τη διαδικασία της εγγραφής θα πρέπει να ακολουθηθούν οι διαδικασίες εγγραφής επιπέδου 3 και ο χρήστης θα πρέπει να αποδεικνύει την κατοχή του συγκεκριμένου αστυνομικού δελτίου ταυτότητας που δηλώνει.

11.4 Παράδειγμα Εφαρμογής ΠΨΑ 3 (5 Υπηρεσίες): Υπηρεσίες που προσφέρονται από το Ίδρυμα Κοινωνικών Ασφαλίσεων (μέσω ΚΕΠ)

Στην παρούσα ενότητα εξετάζονται ηλεκτρονικές υπηρεσίες που προσφέρονται από το ΙΚΑ μέσω των Δικτυακών Τόπων των Κέντρων Εξυπηρέτησης Πολιτών (ΚΕΠ). Συγκεκριμένα οι υπηρεσίες αυτές είναι:

- Υπεύθυνη Δήλωση Απώλειας Ασφαλιστικού Βιβλιαρίου (ΦΕΚ τ. Β 1171/24.08.2005)
- Δήλωση Διαφωνίας επί των Ασφαλιστικών Στοιχείων - Καταγγελία (ΦΕΚ τ. Β 1171/24.08.2005)
- Έκδοση βεβαίωσης περί μη ασφάλισης ΙΚΑ (ΦΕΚ τ. Β 946/24.07.2002)
- Έκδοση βεβαίωσης περί μη συνταξιοδότησης από το ΙΚΑ (ΦΕΚ τ. Β 946/24.07.2002)
- Έγγραφή - Πιστοποίηση Εργοδότη για χρήση Ηλεκτρονικών Υπηρεσιών προκειμένου να υποβληθεί ηλεκτρονικά μέσω ΚΕΠ η Αναλυτική Περιοδική Δήλωση (ΑΠΔ) (ΦΕΚ τ. Β 777/17.06.2003)

11.4.1 Υπάρχουσα Διαδικασία Εγγραφής

Όλες οι παραπάνω υπηρεσίες του ΙΚΑ παρέχονται ηλεκτρονικά από το δικτυακό τόπο του Κέντρου Εξυπηρέτησης Πολιτών. Η διαδικασία εγγραφής στον ιστότοπο του ΚΕΠ, ώστε να είναι δυνατή η αξιοποίηση της υπηρεσίας, έχει ήδη περιγραφεί στην ενότητα 11.2.1.

11.4.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.4.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Τα στοιχεία που καλείται να συμπληρώσει ο χρήστης κατά τη διάρκεια της εγγραφής του στο ΚΕΠ έχουν ήδη περιγραφεί στην ενότητα 11.2.2.1.

11.4.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση της Υπηρεσίας

Τα στοιχεία που απαιτούνται κατά τη χρήση όλων των παραπάνω ηλεκτρονικών υπηρεσιών είναι τα ακόλουθα:

- Νομός και Διεύθυνση Κ.Ε.Π. που θα διεκπεραιώσει την αίτηση του χρήστη
- Νομός και υποκατάστημα Ασφαλιστικού Φορέα
- Όνομα
- Επώνυμο
- Όνομα Πατέρα
- Τηλέφωνο

- Αριθμός Δελτίου Ταυτότητας

Επιπροσθέτως, για την «Υπεύθυνη Δήλωση Απώλειας Ασφαλιστικού Βιβλιαρίου» απαιτούνται και τα παρακάτω:

- Όνομα Μητέρας
- Έτος Γεννήσεως
- Διεύθυνση Κατοικία -- Οδός, Αριθμός και Τ.Κ. Κατοικίας

Τέλος για τις Υπηρεσίες «Υπεύθυνη Δήλωση Απώλειας Ασφαλιστικού Βιβλιαρίου» και «Δήλωση Διαφωνίας επί των Ασφαλιστικών Στοιχείων - Καταγγελία» αξιοποιείται:

- Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ)

ενώ για τις υπηρεσίες «Έκδοση βεβαίωσης περί μη ασφάλισης ΙΚΑ» και «Έκδοση βεβαίωσης περί μη συνταξιοδότησης από το ΙΚΑ» απαιτείται:

- Αριθμός Μητρώου ΙΚΑ

11.4.3 Επιπτώσεις Απειλών

Οι περισσότερες από τις απειλές που έχουν ως στόχο την υποκλοπή / τροποποίηση των δεδομένων δεν επιφέρουν σημαντικές επιπτώσεις καθώς τα δεδομένα τα οποία αξιοποιούνται είναι «απλά δεδομένα». Οι σημαντικότερες επιπτώσεις που μπορεί να προκύψουν αφορούν περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στην υπηρεσία και υποβολής λανθασμένων δεδομένων (για παράδειγμα κάποιος υποδύεται κάποιον άλλο και καταθέτει ψευδή δήλωση για απώλεια του ασφαλιστικού βιβλιαρίου του).

11.4.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες του ΙΚΑ

Η εφαρμογή του ΠΨΑ στις παραπάνω ηλεκτρονικά προσφερόμενες (μέσω ΚΕΠ) υπηρεσίες του ΙΚΑ θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2.

- *[ΚΥ.4]: Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1, εντάσσονται στην κατηγορία «**Απλά Δεδομένα**»
- *[ΚΥ.5]: Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Όλες οι προαναφερόμενες υπηρεσίες του ΙΚΑ, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 2**.
- Σύμφωνα με τον *[ΚΥ.8]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 2** και **Επίπεδο Αυθεντικοποίησης 1**.
- Σύμφωνα με τους *[ΚΥ.10] και [ΚΠ.6]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΣΥΝΘΗΜΑΤΙΚΑ**», ενώ *προαιρετικά* το ΙΚΑ μπορεί να αξιοποιήσει και «ΣΥΝΘΗΜΑΤΙΚΑ ΜΙΑΣ ΧΡΗΣΗΣ»

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη των υπηρεσιών στο ΠΨΑ.

ΥΠΗΡΕΣΙΕΣ ΙΚΑ (μέσω ΚΕΠ)	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	1) Υπεύθυνη Δήλωση Απώλειας Ασφαλιστικού Βιβλιαρίου (ΦΕΚ τ. Β 1171/24.08.2005) 2) Δήλωση Διαφωνίας επί των Ασφαλιστικών Στοιχείων - Καταγγελία (ΦΕΚ τ. Β 1171/24.08.2005) 3) Έκδοση βεβαίωσης περί μη ασφάλισης ΙΚΑ (ΦΕΚ τ. Β 946/24.07.2002) 4) Έκδοση βεβαίωσης περί μη συνταξιοδότησης από το ΙΚΑ (ΦΕΚ τ. Β 946/24.07.2002) 5) Έγγραφή - Πιστοποίηση Εργοδότη για χρήση Ηλεκτρονικών Υπηρεσιών προκειμένου να υποβληθεί ηλεκτρονικά μέσω ΚΕΠ η Αναλυτική Περιοδική Δήλωση (ΑΠΔ) (ΦΕΚ τ. Β 777/17.06.2003)
Αρμόδιος Φορέας	ΙΚΑ / ΚΕΠ
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	Για Υπηρεσίες (1) και (2) : ΑΜΚΑ / Συνθηματικά Για Υπηρεσίες (3) και (4) : ΑΜ ΙΚΑ / Συνθηματικά Για Υπηρεσία (5) : ΑΔΤ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 2
Επίπεδο Αυθεντικοποίησης	Επίπεδο 1
Μηχανισμός Αυθεντικοποίησης	Συνθηματικά (Προαιρετικά: Συνθηματικά μιας Χρήσης)
Επίπεδο Εγγραφής	Επίπεδο 2

Πίνακας 8: Ένταξη Υπηρεσιών ΙΚΑ (μέσω ΚΕΠ) στο ΠΨΑ

11.4.5 Απαιτούμενες Τροποποιήσεις Υπάρχουσας Κατάστασης

Η σημαντικότερη τροποποίηση, σε σχέση με την υφιστάμενη κατάσταση, αφορά τη διαδικασία εγγραφής στην υπηρεσία (πρέπει να ακολουθηθούν τα προβλεπόμενα από το Επίπεδο Εγγραφής 2) και συγκεκριμένα το γεγονός ότι ο πολίτης πρέπει να παραλάβει ο ίδιος τα συνθηματικά του αφού πρώτα ταυτοποιηθεί μέσω της επίδειξης της Αστυνομικής του Ταυτότητας και - εφόσον το επιλέξει το ΙΚΑ - επίδειξης δημόσιου εγγράφου από το οποίο να προκύπτει ο ΑΜΚΑ ή / και ο Αριθμός Μητρώου ΙΚΑ.

11.5 Παράδειγμα Εφαρμογής ΠΨΑ 4 (5 Υπηρεσίες): Υπηρεσίες που προσφέρονται από τον ΟΑΕΕ (μέσω ΚΕΠ)

Στην παρούσα ενότητα εξετάζονται ηλεκτρονικές υπηρεσίες που προσφέρονται από τον ΟΑΕΕ (πρώην ΤΕΒΕ) μέσω των Δικτυακών Τόπων των Κέντρων Εξυπηρέτησης Πολιτών (ΚΕΠ). Συγκεκριμένα οι υπηρεσίες αυτές είναι:

- Χορήγηση Βεβαίωσης Ποσού Σύνταξης ΟΑΕΕ (ΦΕΚ τ. Β 946/24.07.2002)
- Βεβαίωση περί μη ασφάλισης ΟΑΕΕ (ΦΕΚ τ. Β 946/24.07.2002)
- Βεβαίωση περί μη συνταξιοδότησης ΟΑΕΕ (ΦΕΚ τ. Β 946/24.07.2002)
- Βεβαίωση Ταμειακής ενημερότητας Ν. 2084/92, για θεώρηση βιβλίων και στοιχείων από τη ΔΟΥ (ΦΕΚ τ. Β 1947/30.12.2005)
- Βεβαίωση μη οφειλής για συμμετοχή σε διαγωνισμούς (ΦΕΚ τ. Β 1947/30.12.2005)

11.5.1 Υπάρχουσα Διαδικασία Εγγραφής

Όλες οι παραπάνω υπηρεσίες του ΟΑΕΕ παρέχονται ηλεκτρονικά από το δικτυακό τόπο του Κέντρου Εξυπηρέτησης Πολιτών. Η διαδικασία εγγραφής στον ιστότοπο του ΚΕΠ, ώστε να είναι δυνατή η αξιοποίηση της υπηρεσίας, έχει ήδη περιγραφεί στην ενότητα 11.2.1.

11.5.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.5.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Τα στοιχεία που καλείται να συμπληρώσει ο χρήστης κατά τη διάρκεια της εγγραφής του στο ΚΕΠ έχουν ήδη περιγραφεί στην ενότητα 11.2.2.1.

11.5.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση της Υπηρεσίας

Τα στοιχεία που απαιτούνται κατά τη χρήση όλων των παραπάνω ηλεκτρονικών υπηρεσιών είναι τα ακόλουθα:

- Νομός και Διεύθυνση Κ.Ε.Π. που θα διεκπεραιώσει την αίτηση του χρήστη
- Νομός και υποκατάστημα Ασφαλιστικού Φορέα
- Όνομα
- Επώνυμο
- Όνομα Πατέρα
- Επάγγελμα
- Τηλέφωνο
- Αριθμός Δελτίου Ταυτότητας

Επιπροσθέτως για τις Υπηρεσίες «Βεβαίωση περί μη ασφάλισης ΟΑΕΕ», «Βεβαίωση περί μη συνταξιοδότησης ΟΑΕΕ» και «Βεβαίωση Ταμειακής ενημερότητας Ν. 2084/92, για θεώρηση βιβλίων και στοιχείων από τη ΔΟΥ» αξιοποιείται:

- Αριθμός Μητρώου ΤΕΒΕ

ενώ για τις υπηρεσίες «Βεβαίωση περί μη ασφάλισης ΟΑΕΕ» και «Βεβαίωση μη οφειλής για συμμετοχή σε διαγωνισμούς » απαιτείται και:

- Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ)

11.5.3 Επιπτώσεις Απειλών

Οι περισσότερες από τις απειλές που έχουν ως στόχο την υποκλοπή / τροποποίηση των δεδομένων δεν επιφέρουν σημαντικές επιπτώσεις καθώς τα δεδομένα τα οποία αξιοποιούνται είναι «απλά δεδομένα». Οι σημαντικότερες επιπτώσεις που μπορεί να προκύψουν αφορούν περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στην υπηρεσία και υποβολής λανθασμένων δεδομένων (για παράδειγμα κάποιος υποδύεται κάποιον άλλο και καταθέτει αίτηση για χορήγηση βεβαίωσης περί μη ασφάλισης στον ΟΑΕΕ).

11.5.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες του ΟΑΕΕ

Η εφαρμογή του ΠΨΑ στις παραπάνω ηλεκτρονικά προσφερόμενες (μέσω ΚΕΠ) υπηρεσίες του ΟΑΕΕ θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2.

- *[ΚΥ.4]: Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1, εντάσσονται στην κατηγορία «**Απλά Δεδομένα**»
- *[ΚΥ.5]: Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Όλες οι προαναφερόμενες υπηρεσίες του ΟΑΕΕ, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 2**.
- Σύμφωνα με τον *[ΚΥ.8]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 2** και **Επίπεδο Αυθεντικοποίησης 1**.
- Σύμφωνα με τους *[ΚΥ.10] και [ΚΠ.6]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΣΥΝΘΗΜΑΤΙΚΑ**», ενώ *προαιρετικά* ο ΟΑΕΕ μπορεί να αξιοποιήσει και «ΣΥΝΘΗΜΑΤΙΚΑ ΜΙΑΣ ΧΡΗΣΗΣ».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη των υπηρεσιών στο ΠΨΑ.

ΥΠΗΡΕΣΙΕΣ ΟΑΕΕ (μέσω ΚΕΠ)	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	1) Χορήγηση Βεβαίωσης Ποσού Σύνταξης ΟΑΕΕ (ΦΕΚ τ. Β 946/24.07.2002) 2) Βεβαίωση περί μη ασφάλισης ΟΑΕΕ (ΦΕΚ τ. Β 946/24.07.2002) 3) Βεβαίωση περί μη συνταξιοδότησης ΟΑΕΕ (ΦΕΚ τ. Β 946/24.07.2002) 4) Βεβαίωση Ταμειακής ενημερότητας Ν. 2084/92, για θεώρηση βιβλίων και στοιχείων από τη ΔΟΥ (ΦΕΚ τ. Β 1947/30.12.2005) 5) Βεβαίωση μη οφειλής για συμμετοχή σε διαγωνισμούς (ΦΕΚ τ. Β 1947/30.12.2005)
Αρμόδιος Φορέας	ΟΑΕΕ / ΚΕΠ
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	Για Υπηρεσία (1) : ΑΔΤ / Συνθηματικά Για Υπηρεσίες (2), (3) και (4) : ΑΜ ΤΕΒΕ / Συνθηματικά Για Υπηρεσία (5) : ΑΜΚΑ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 2
Επίπεδο Αυθεντικοποίησης	Επίπεδο 1
Μηχανισμός Αυθεντικοποίησης	Συνθηματικά (Προαιρετικά: Συνθηματικά μιας Χρήσης)
Επίπεδο Εγγραφής	Επίπεδο 2

Πίνακας 9: Ένταξη Υπηρεσιών ΟΑΕΕ (μέσω ΚΕΠ) στο ΠΨΑ

11.5.5 Απαιτούμενες Τροποποιήσεις Υπάρχουσας Κατάστασης

Η σημαντικότερη τροποποίηση, σε σχέση με την υφιστάμενη κατάσταση, αφορά τη διαδικασία εγγραφής στην υπηρεσία (πρέπει να ακολουθηθούν τα προβλεπόμενα από το Επίπεδο Εγγραφής 2) και συγκεκριμένα το γεγονός ότι ο πολίτης πρέπει να παραλάβει ο ίδιος τα συνθηματικά του αφού πρώτα ταυτοποιηθεί μέσω της επίδειξης της Αστυνομικής του Ταυτότητας και εφόσον το επιλέξει ο ΟΑΕΕ, επίδειξης δημόσιου εγγράφου από το οποίο να προκύπτει ο ΑΜΚΑ ή / και ο Αριθμός Μητρώου ΤΕΒΕ.

11.6 Παράδειγμα Εφαρμογής ΠΨΑ 5: Υποβολή Δήλωση Φορολογίας Εισοδήματος

11.6.1 Υπάρχουσα Διαδικασία Εγγραφής

Προκειμένου να εγγραφεί ο χρήστης στην υπηρεσία Δήλωσης Φορολογίας Εισοδήματος πρέπει να επισκεφθεί την ιστοσελίδα της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (www.gsis.gr) και να επιλέξει το σύνδεσμο «Εγγραφή». Ο χρήστης μεταφέρεται στη σχετική ηλεκτρονική σελίδα της Γενικής Γραμματείας Πληροφορικών Συστημάτων, συμπληρώνει τη φόρμα εγγραφής και την υποβάλει. Τα υποβληθέντα στοιχεία (βλέπε ενότητα 11.6.2) ελέγχονται και εφόσον πιστοποιηθεί η ορθότητά τους, εκδίδεται ένας κωδικός χρήστη (user name) και μια συνθηματική λέξη (password) τα οποία και αποστέλλονται στο χρήστη στην ηλεκτρονική διεύθυνση που έχει δηλώσει κατά την εγγραφή του για να είναι δυνατή η μετέπειτα αυθεντικοποίηση του.

11.6.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.6.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Τα στοιχεία που καλείται να συμπληρώσει ο χρήστης κατά της διάρκεια της εγγραφής του στην υπηρεσία είναι:

1. Αριθμός Φορολογικού Μητρώου
2. Επιλογή τύπου προσώπου (Φυσικό ή Νομικό)
3. Α.Φ.Μ. Λογιστή, εάν υπάρχει
4. Στοιχεία ταυτότητας
5. Στοιχεία επικοινωνίας (ηλεκτρονική διεύθυνση)
6. Δ.Ο.Υ. υποβολής δηλώσεων
7. Προσωπικά στοιχεία (ονοματεπώνυμο, πατρώνυμο και διεύθυνση κατοικίας) του φορολογουμένου και της συζύγου του, εφόσον είναι νυμφευμένος.

11.6.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση της Υπηρεσίας

Κατά τη διάρκεια χρήσης της υπηρεσίας, τα στοιχεία που καλείται να συμπληρώσει ο χρήστης είναι το σύνολο των δεδομένων που περιλαμβάνονται στα έντυπα Ε1, Ε2, Ε3 και Ε9.

11.6.3 Επιπτώσεις Απειλών

Δεδομένης της υπάρχουσας διαδικασίας εγγραφής στην υπηρεσία μέσω του ιστοτόπου της ΓΓΠΣ, μπορεί κάποιος να υποδυθεί οποιοδήποτε πολίτη και να αιτηθεί την έκδοση νόμιμων διακριτικών αυθεντικοποίησης για λογαριασμό του πολίτη χωρίς αυτό να γίνει αντιληπτό, με αποτέλεσμα να έχει τη δυνατότητα υποβολής δηλώσεων φορολογίας εισοδήματος με

λανθασμένα στοιχεία για τον πολίτη-θύμα της επίθεσης. Βέβαια, τελικά το πρόβλημα θα εντοπιστεί καθώς θα βρεθούν δύο δηλώσεις φορολογίας εισοδήματος για τον ίδιο Αριθμό Φορολογικού Μητρώου.

Ένα σημαντικό θέμα είναι η διαφύλαξη της εμπιστευτικότητας των (οικονομικών) δεδομένων της φορολογικής δήλωσης. Σε περίπτωση αποκάλυψής τους σε μη εξουσιοδοτημένα πρόσωπα η ΓΓΠΣ (ως φορέας παροχής της ηλεκτρονικής υπηρεσίας) μπορεί να υποστεί νομικές συνέπειες καθώς τα προαναφερόμενα δεδομένα καλύπτονται από το φορολογικό απόρρητο.

11.6.4 Εφαρμογή του ΠΨΑ στην Υπηρεσία

Η εφαρμογή του ΠΨΑ στην υπηρεσία υποβολής δήλωσης φορολογίας εισοδήματος που προσφέρεται ηλεκτρονικά μέσω του ιστοτόπου της ΓΓΠΣ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2.

- *[ΚΥ.4]: Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στην προαναφερόμενη υπηρεσία, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 (με το Άρθρο 85 «Κώδικας Φορολογίας Εισοδήματος» του νόμου Ν. 2238/1994, τα προσωπικά στοιχεία και δεδομένα, που περιέχονται στις φορολογικές δηλώσεις, χαρακτηρίζονται ως απόρρητα και απαγορεύεται η γνωστοποίηση τους σε οποιονδήποτε άλλον εκτός από τα υποκείμενα τους), εντάσσονται στην κατηγορία «**Οικονομικά Δεδομένα (υπαγόμενα στο Φορολογικό Απόρρητο)**».
- *[ΚΥ.5]: Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Η υπηρεσία δήλωσης φορολογίας εισοδήματος, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2, εντάσσεται στο **Επίπεδο Εμπιστοσύνης 3**.
- Σύμφωνα με τον *[ΚΥ.9]*, η υπηρεσία θα πρέπει να υιοθετήσει **Επίπεδο Εγγραφής 3** και **Επίπεδο Αυθεντικοποίησης 2**.
- Σύμφωνα με τον [ΚΥ.13], ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΠΙΣΤΟΠΟΙΗΤΙΚΑ** (Διακριτικό Σκληρής Αποθήκευσης)».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΔΗΛΩΣΗ ΦΟΡΟΛΟΓΙΑΣ ΕΙΣΟΔΗΜΑΤΟΣ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Δήλωση Φορολογίας Εισοδήματος
Αρμόδιος Φορέας	ΓΓΠΣ
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	ΑΦΜ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΑΣ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Οικονομικά δεδομένα υπαγόμενα στο Φορολογικό Απόρρητο
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	4
Επίπεδο Εμπιστοσύνης	Επίπεδο 3
Επίπεδο Αυθεντικοποίησης	Επίπεδο 2
Μηχανισμός Αυθεντικοποίησης	Ψηφιακό Πιστοποιητικό αποθηκευμένο σε Διακριτικό Σκληρής Αποθήκευσης
Επίπεδο Εγγραφής	Επίπεδο 3

Πίνακας 10: Ένταξη Υπηρεσίας Δήλωσης Φορολογίας Εισοδήματος στο ΠΨΑ

11.6.5 Απαιτούμενες Τροποποιήσεις Υπάρχουσας Κατάστασης

Αναφορικά με την αξιοποίηση των διακριτικών αυθεντικοποίησης θα πρέπει να καταργηθεί η αξιοποίηση των συνθηματικών και να αξιοποιηθούν ψηφιακά πιστοποιητικά.

Σχετικά με τη διαδικασία της εγγραφής θα πρέπει να ακολουθηθούν οι διαδικασίες εγγραφής επιπέδου 3 και ο χρήστης να αποδεικνύει, υποβάλλοντας το κατάλληλο δημόσιο έγγραφο, τόσο τον αριθμό του αστυνομικού δελτίου ταυτότητας του όσο και τον Α.Φ.Μ. του.

11.7 Παράδειγμα Εφαρμογής ΠΨΑ 6 (2 Υπηρεσίες): Υπηρεσίες που προσφέρονται από τη ΓΓΠΣ

Στην παρούσα ενότητα εξετάζονται ηλεκτρονικές υπηρεσίες που προσφέρονται από την ΓΓΠΣ μέσω του Δικτυακού τόπου του Taxisnet. Συγκεκριμένα οι υπηρεσίες αυτές είναι:

- Βεβαίωση Φορολογικής Ενημερότητας
- Χορήγηση Αντιγράφου Εκκαθαριστικού Σημειώματος Δήλωσης Φορολογίας Εισοδήματος Φυσικών Προσώπων

11.7.1 Υπάρχουσα Διαδικασία Εγγραφής

Η διαδικασία εγγραφής στις υπηρεσίες γίνεται μέσω της ιστοσελίδας της ΓΓΠΣ όπως έχει ήδη περιγραφεί στην ενότητα 11.6.1.

11.7.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.7.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Τα στοιχεία που καλείται να συμπληρώσει ο χρήστης κατά τη διάρκεια της εγγραφής του έχουν ήδη περιγραφεί στην ενότητα 11.6.2.1.

11.7.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση της Υπηρεσίας

Δεν απαιτούνται επιπρόσθετα στοιχεία από αυτά της εγγραφής.

11.7.3 Επιπτώσεις Απειλών

Αντίστοιχες με αυτές της ενότητας 11.6.3.

11.7.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στις προαναφερόμενες υπηρεσίες που προσφέρεται ηλεκτρονικά μέσω του ιστοτόπου της ΓΓΠΣ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2.

- *[ΚΥ.4]: Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες (παραγόμενα αποτελέσματα), σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 (με το Άρθρο 85 «Κώδικας Φορολογίας Εισοδήματος» του νόμου Ν. 2238/1994, τα προσωπικά στοιχεία και δεδομένα, που περιέχονται στις φορολογικές δηλώσεις, χαρακτηρίζονται ως απόρρητα και απαγορεύεται η γνωστοποίηση τους σε οποιονδήποτε άλλον εκτός από τα υποκείμενα τους), εντάσσονται στην κατηγορία «**Οικονομικά Δεδομένα (υπαγόμενα στο Φορολογικό Απόρρητο)**».
- *[ΚΥ.5]: Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2, εντάσσεται στο **Επίπεδο Εμπιστοσύνης 3**.

- Σύμφωνα με τον *[ΚΥ.9]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 3** και **Επίπεδο Αυθεντικοποίησης 2**.
- Σύμφωνα με τους [ΚΥ.13], ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΠΙΣΤΟΠΟΙΗΤΙΚΑ** (Διακριτικό Σκληρής Αποθήκευσης)».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΥΠΗΡΕΣΙΕΣ ΓΓΠΣ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	1) Βεβαίωση Φορολογικής Ενημερότητας 2) Χορήγηση Αντιγράφου Εκκαθαριστικού Σημειώματος Δήλωσης Φορολογίας Εισοδήματος Φυσικών Προσώπων
Αρμόδιος Φορέας	ΓΓΠΣ
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	ΑΦΜ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Οικονομικά δεδομένα υπαγόμενα στο Φορολογικό Απόρρητο
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	4
Επίπεδο Εμπιστοσύνης	Επίπεδο 3
Επίπεδο Αυθεντικοποίησης	Επίπεδο 2
Μηχανισμός Αυθεντικοποίησης	Ψηφιακό Πιστοποιητικό αποθηκευμένο σε Διακριτικό Σκληρής Αποθήκευσης
Επίπεδο Εγγραφής	Επίπεδο 3

Πίνακας 11: Ένταξη Υπηρεσιών ΓΓΠΣ στο ΠΨΑ

11.7.5 Απαιτούμενες Τροποποιήσεις Υπάρχουσας Κατάστασης

Αναφορικά με την αξιοποίηση των διακριτικών αυθεντικοποίησης θα πρέπει να καταργηθεί η αξιοποίηση των συνθηματικών και να αξιοποιηθούν ψηφιακά πιστοποιητικά.

Σχετικά με τη διαδικασία της εγγραφής θα πρέπει να ακολουθηθούν οι διαδικασίες εγγραφής επιπέδου 3 και ο χρήστης να αποδεικνύει, υποβάλλοντας το κατάλληλο δημόσιο έγγραφο, τόσο τον αριθμό του αστυνομικού δελτίου ταυτότητας του όσο και τον Α.Φ.Μ. του.

11.8 Παράδειγμα Εφαρμογής ΠΨΑ 7: Αιτήματα/ Καταγγελίες Πολιτών μέσω των ΔΔΠ

11.8.1 Προτεινόμενη Διαδικασία Εγγραφής

Η κατάθεση αιτήσεων/ καταγγελιών θα γίνεται ηλεκτρονικά μέσω των Δημοτικών Διαδικτυακών Πυλών (ΔΔΠ). Για τις υπηρεσίες αυτές προτείνεται η εγγραφή των πολιτών με μία αυτόματη διαδικασία. Κατά τη διαδικασία της εγγραφής και εφόσον ο υποψήφιος χρήστης συμπληρώσει την κατάλληλη φόρμα, το σύστημα θα του αποστέλλει κατάλληλο μήνυμα μέσω e-mail όπου θα του ζητάει να ακολουθήσει ένα σύνδεσμο (URL) που θα περιέχει στο σώμα του μηνύματος προκειμένου να ενεργοποιήσει το λογαριασμό του (activation).

11.8.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.8.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Τα στοιχεία που καλείται να συμπληρώσει ο χρήστης κατά τη διάρκεια της εγγραφής του στην υπηρεσία είναι:

- **Υποχρεωτικά Πεδία:**
  a. Ονοματεπώνυμο
  b. Επιθυμητό όνομα χρήστη (username)
  c. Επιθυμητός Κωδικός (password)
  d. Επαλήθευση Κωδικού (password)
  e. E-mail
  f. ΑΦΜ
- **Προαιρετικά Στοιχεία[4]:**
  a. Διεύθυνση Κατοικίας
  b. Στοιχεία Επικοινωνίας

11.8.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Τα στοιχεία που χρησιμοποιούνται κατά την αξιοποίηση της υπηρεσίας είναι τα ακόλουθα:

- Κατηγορία
- Θέμα
- Αναλυτική περιγραφή

[4] Σε κάποια από τα έργα ανάπτυξης ΔΔΠ, τα στοιχεία αυτά ζητούνται υποχρεωτικά ενώ, επιπρόσθετα, ζητούνται και άλλα στοιχεία όπως Αριθμός Δελτίου Ταυτότητας, Αριθμός Δημοτολογίου, ημερομηνία γέννησης, επάγγελμα, πατρώνυμο, μητρώνυμο.

- Συνημμένα έγγραφα
- Στοιχεία προηγούμενης επαφής

11.8.3 Επιπτώσεις Απειλών

Οι περισσότερες από τις απειλές που έχουν ως στόχο την υποκλοπή / τροποποίηση των δεδομένων δεν επιφέρουν σημαντικές επιπτώσεις καθώς θεωρείται (βλέπε παρακάτω ενότητα για κατηγοριοποίηση των δεδομένων) ότι τα δεδομένα τα οποία αξιοποιούνται είναι «απλά δεδομένα». Οι σημαντικότερες επιπτώσεις που μπορεί να προκύψουν αφορούν περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στην υπηρεσία με στόχο την υποβολή αιτημάτων / καταγγελιών από μη εξουσιοδοτημένα άτομα.

11.8.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στην παραπάνω υπηρεσία που θα προσφέρεται ηλεκτρονικά μέσω των ΔΔΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2 του ΠΨΑ.

- *[ΚΥ.4] Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 του ΠΨΑ, εντάσσονται στην κατηγορία «**Απλά Δεδομένα**», εκτός εάν τα συνημμένα έγγραφα ή η αναλυτική περιγραφή περιλαμβάνουν δεδομένα που εντάσσονται στην κατηγορία των ευαίσθητων δεδομένων ή προστατεύονται από το φορολογικό απόρρητο, οπότε θα πρέπει να κατηγοριοποιηθούν σε υψηλότερο επίπεδο.
- *[ΚΥ.5] Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Με την παραδοχή ότι τα δεδομένα των υπηρεσιών εντάσσονται στην κατηγορία «**Απλά**», οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2 του ΠΨΑ, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 2** (εφόσον γίνεται επεξεργασία αναγνωριστικών του χρήστη – ΑΦΜ) ή στο **Επίπεδο Εμπιστοσύνης 1** (εάν δεν γίνεται επεξεργασία αναγνωριστικών του χρήστη – ΑΦΜ). Εάν ισχύει η δεύτερη περίπτωση, ο ΑΦΜ δεν θα έπρεπε να ζητείται κατά την εγγραφή των χρηστών.
- Σύμφωνα με τους *[ΚΥ.8]* και *[ΚΥ.7]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 2 ή 1** (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη) και **Επίπεδο Αυθεντικοποίησης 1**.
- Σύμφωνα με τους *[ΚΥ.10] και [ΚΠ.6]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΣΥΝΘΗΜΑΤΙΚΑ**», ενώ *προαιρετικά* μπορούν να αξιοποιηθούν και «ΣΥΝΘΗΜΑΤΙΚΑ ΜΙΑΣ ΧΡΗΣΗΣ».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΑΙΤΗΜΑΤΑ / ΚΑΤΑΓΓΕΛΙΕΣ ΠΟΛΙΤΩΝ ΜΕΣΩ ΤΩΝ ΔΔΠ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Αιτήματα/ Καταγγελίες Πολιτών
Αρμόδιος Φορέας	Δήμοι, Διεύθυνση ή Υπηρεσία του Δήμου στην επιχειρησιακή ευθύνη της οποίας εμπίπτει το αίτημα / καταγγελία
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	Καμία (εκτός ειδικών περιπτώσεων)[5] / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 2 ή 1 (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη)
Επίπεδο Αυθεντικοποίησης	Επίπεδο 1
Μηχανισμός Αυθεντικοποίησης	Συνθηματικά (Προαιρετικά: Συνθηματικά μιας Χρήσης)
Επίπεδο Εγγραφής	Επίπεδο 2 ή 1 (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη)

Πίνακας 12: Ένταξη Υπηρεσιών Αιτημάτων/Καταγγελιών πολιτών μέσω ΔΔΠ στο ΠΨΑ

11.8.5 Απαιτούμενες Τροποποιήσεις Προτεινόμενης Λύσης

Η σημαντικότερη τροποποίηση, σε σχέση με την προτεινόμενη λύση, αφορά τη διαδικασία εγγραφής στις υπηρεσίες (πρέπει να ακολουθηθούν τα προβλεπόμενα από το Επίπεδο Εγγραφής 1 ή 2) και συγκεκριμένα το γεγονός ότι τα διακριτικά πρέπει να αποσταλούν στον πολίτη με συστημένη επιστολή στη διεύθυνση αλληλογραφίας του (Επίπεδο Εγγραφής 1) ή ο πολίτης πρέπει να παραλάβει ο ίδιος τα συνθηματικά του αφού πρώτα ταυτοποιηθεί μέσω της επίδειξης της Αστυνομικής του Ταυτότητας ή άλλου κατάλληλου αποδεικτικού (Επίπεδο Εγγραφής 2).

Ένα άλλο σημείο που πρέπει να προσεχτεί κατά τη διαδικασία εγγραφής είναι ότι δεν θα πρέπει να ζητούνται στοιχεία, τα οποία δεν απαιτούνται για την αναγνώριση του πολίτη. Τέτοιο στοιχείο φαίνεται να είναι στην προκειμένη περίπτωση ο Αριθμός Φορολογικού Μητρώου, εκτός εάν ο ΑΦΜ χρησιμοποιείται για την αναγνώριση του πολίτη.

[5] Δεν κατονομάζονται

11.9 Παράδειγμα Εφαρμογής ΠΨΑ 8: Αίτηση για Βεβαίωση ΤΑΠ μέσω των ΔΔΠ

Ο πολίτης θα μπορεί επιλέγοντας τη συγκεκριμένη υπηρεσία να κάνει Αίτηση για χορήγηση Βεβαίωσης ΤΑΠ μέσω Διαδικτύου. Πρόκειται για μία απλή αίτηση, η οποία δεν μπορεί ωστόσο να εκδοθεί μέχρι να προσκομίσει ο πολίτης τα απαραίτητα δικαιολογητικά. Το υποσύστημα θα καταγράφει τα στοιχεία της αίτησης και θα επιστρέφει στον πολίτη ένα μοναδικό αριθμό (ή αριθμό πρωτοκόλλου).

11.9.1 Προτεινόμενη Διαδικασία Εγγραφής

Όπως προηγούμενα, Ενότητα 11.8.1.

11.9.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.9.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Όπως προηγούμενα, Ενότητα 11.8.2.1.

11.9.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Τα στοιχεία που χρησιμοποιούνται κατά την αξιοποίηση της υπηρεσίας είναι τα ακόλουθα:

- e-mail
- τηλέφωνο επικοινωνίας
- τόπος παραλαβής

11.9.3 Επιπτώσεις Απειλών

Οι περισσότερες από τις απειλές που έχουν ως στόχο την υποκλοπή / τροποποίηση των δεδομένων δεν επιφέρουν σημαντικές επιπτώσεις καθώς τα δεδομένα τα οποία αξιοποιούνται είναι «απλά δεδομένα». Οι σημαντικότερες επιπτώσεις που μπορεί να προκύψουν αφορούν περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στην υπηρεσία με στόχο την αίτηση χορήγησης της βεβαίωσης από μη εξουσιοδοτημένα άτομα.

11.9.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στην παραπάνω υπηρεσία που θα προσφέρεται ηλεκτρονικά μέσω των ΔΔΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2 του ΠΨΑ.

- *[ΚΥ.4] Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 του ΠΨΑ, εντάσσονται στην κατηγορία «**Απλά Δεδομένα**».
- *[ΚΥ.5] Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2 του ΠΨΑ, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 2**

(εφόσον γίνεται επεξεργασία αναγνωριστικών του χρήστη – ΑΦΜ) ή στο **Επίπεδο Εμπιστοσύνης 1** (εάν δεν γίνεται επεξεργασία αναγνωριστικών του χρήστη – ΑΦΜ).

- Σύμφωνα με τους *[ΚΥ.8]* και *[ΚΥ.7]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 2 ή 1** (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη) και **Επίπεδο Αυθεντικοποίησης 1**.
- Σύμφωνα με *[ΚΥ.10] και [ΚΠ.6]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΣΥΝΘΗΜΑΤΙΚΑ**», ενώ *προαιρετικά* μπορούν να αξιοποιηθούν και «ΣΥΝΘΗΜΑΤΙΚΑ ΜΙΑΣ ΧΡΗΣΗΣ».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΑΙΤΗΣΗ ΓΙΑ ΒΕΒΑΙΩΣΗ ΤΑΠ ΜΕΣΩ ΔΔΠ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Αίτηση για Βεβαίωση ΤΑΠ
Αρμόδιος Φορέας	Δήμοι, Οικονομική υπηρεσία – τμήμα εσόδων του Δήμου
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	Έγγραφο που αποδεικνύει την κυριότητα του ακινήτου (Λογαριασμός ΔΕΗ, Αντίγραφο συμβολαίου) / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 2 ή 1 (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη)
Επίπεδο Αυθεντικοποίησης	Επίπεδο 1
Μηχανισμός Αυθεντικοποίησης	Συνθηματικά (Προαιρετικά: Συνθηματικά μιας Χρήσης)
Επίπεδο Εγγραφής	Επίπεδο 2 ή 1 (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη)

Πίνακας 13: Ένταξη Υπηρεσίας Αίτησης για Βεβαίωση ΤΑΠ μέσω ΔΔΠ στο ΠΨΑ

11.9.5 Απαιτούμενες Τροποποιήσεις Προτεινόμενης Λύσης

Όπως προηγούμενα, Ενότητα 11.8.5.

11.10 Παράδειγμα Εφαρμογής ΠΨΑ 9: Δημοσίευση Αποφάσεων Διοικητικού Συμβουλίου μέσω των ΔΔΠ

Οι υπάλληλοι των δήμων καταχωρούν αποφάσεις στο τοπικό τους σύστημα. Τα δεδομένα αυτά μεταφέρονται στο Data Center του Δήμου, όπου και δημοσιεύονται στη ΔΔΠ. Οι πολίτες έχουν δυνατότητες αναζήτησης, τοπικής αποθήκευσης και εκτύπωσης αποφάσεων του ΔΣ.

11.10.1 Προτεινόμενη Διαδικασία Εγγραφής

Δεν απαιτείται.

11.10.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.10.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Δεν απαιτούνται.

11.10.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Κατά την αξιοποίηση της υπηρεσίας θα υπάρχει η δυνατότητα αναζήτησης αποφάσεων με βάση:

- Αριθμό απόφασης
- Αριθμό πρωτοκόλλου
- Θέμα
- Ημερομηνία (ή διάστημα)
- Λέξεις-Κλειδιά

11.10.3 Επιπτώσεις Απειλών

Καθώς τα δεδομένα τα οποία αξιοποιούνται είναι δημόσια δεδομένα δεν τίθεται θέμα μη εξουσιοδοτημένης πρόσβασης. Μικρές επιπτώσεις μπορεί να υπάρξουν από μη εξουσιοδοτημένη τροποποίηση των δεδομένων ή μη διαθεσιμότητα των.

11.10.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στην παραπάνω υπηρεσία που θα προσφέρεται ηλεκτρονικά μέσω των ΔΔΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2 του ΠΨΑ.

- *[ΚΥ.4] Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 του ΠΨΑ, εντάσσονται στην κατηγορία «**Απλά Δεδομένα**».

- *[ΚΥ.5] Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2 του ΠΨΑ, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 0**, εφόσον τα δεδομένα αφορούν δημόσια προσβάσιμες πληροφορίες.
- Σύμφωνα με τον *[ΚΥ.6]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 0** και **Επίπεδο Αυθεντικοποίησης 0**.
- Σύμφωνα με τον *[ΚΠ.4]*, δεν προτείνεται να χρησιμοποιείται κάποιος μηχανισμός για την αυθεντικοποίηση των χρηστών στη συγκεκριμένη υπηρεσία.

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΔΗΜΟΣΙΕΥΣΗ ΑΠΟΦΑΣΕΩΝ ΔΣ ΜΕΣΩ ΔΔΠ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Δημοσίευση Αποφάσεων Διοικητικού Συμβουλίου
Αρμόδιος Φορέας	Δήμοι, Γραφείο Δημάρχου
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	-
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 0
Επίπεδο Αυθεντικοποίησης	Επίπεδο 0
Μηχανισμός Αυθεντικοποίησης	-
Επίπεδο Εγγραφής	Επίπεδο 0

Πίνακας 14: Ένταξη Υπηρεσίας Δημοσίευσης Αποφάσεων ΔΣ μέσω ΔΔΠ στο ΠΨΑ

11.10.5 Απαιτούμενες Τροποποιήσεις Προτεινόμενης Λύσης

Η προτεινόμενη λύση είναι πλήρως συμβατή με τα προβλεπόμενα στο ΠΨΑ.

11.11 Παράδειγμα Εφαρμογής ΠΨΑ 10: Αιτήσεις Πιστοποιητικών Δημοτολογίου μέσω των ΔΔΠ

Ο πολίτης θα μπορεί, επιλέγοντας τη συγκεκριμένη υπηρεσία, να κάνει Αίτηση για έκδοση πιστοποιητικών Δημοτολογίου.

11.11.1 Προτεινόμενη Διαδικασία Εγγραφής

Όπως προηγούμενα, Ενότητα 11.8.1.

11.11.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.11.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Όπως προηγούμενα, Ενότητα 11.8.2.1.

11.11.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Τα στοιχεία που χρησιμοποιούνται κατά την αξιοποίηση των παραπάνω υπηρεσιών είναι τα ακόλουθα:

- e-mail
- τηλέφωνο επικοινωνίας
- τόπος παραλαβής

11.11.3 Επιπτώσεις Απειλών

Οι περισσότερες από τις απειλές που έχουν ως στόχο την υποκλοπή / τροποποίηση των δεδομένων δεν επιφέρουν σημαντικές επιπτώσεις καθώς τα δεδομένα τα οποία αξιοποιούνται είναι «απλά δεδομένα». Οι σημαντικότερες επιπτώσεις που μπορεί να προκύψουν αφορούν περιπτώσεις μη εξουσιοδοτημένης πρόσβασης στην υπηρεσία με στόχο την αίτηση χορήγησης των πιστοποιητικών από μη εξουσιοδοτημένα άτομα.

11.11.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στην παραπάνω υπηρεσία που θα προσφέρεται ηλεκτρονικά μέσω των ΔΔΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2 του ΠΨΑ.

- *[ΚΥ.4] Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 του ΠΨΑ, εντάσσονται στην κατηγορία «**Απλά Δεδομένα**».
- *[ΚΥ.5] Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2 του ΠΨΑ, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 2** (εφόσον γίνεται επεξεργασία αναγνωριστικών του χρήστη – ΑΦΜ) ή στο **Επίπεδο Εμπιστοσύνης 1** (εάν δεν γίνεται επεξεργασία αναγνωριστικών του χρήστη – ΑΦΜ).

- Σύμφωνα με τους *[ΚΥ.8]* και *[ΚΥ.7]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 2 ή 1** (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη) και **Επίπεδο Αυθεντικοποίησης 1**.
- Σύμφωνα με τους *[ΚΥ.10] και [ΚΠ.6]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΣΥΝΘΗΜΑΤΙΚΑ**», ενώ *προαιρετικά* μπορούν να αξιοποιηθούν και «ΣΥΝΘΗΜΑΤΙΚΑ ΜΙΑΣ ΧΡΗΣΗΣ».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΑΙΤΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΔΗΜΟΤΟΛΟΓΙΟΥ ΜΕΣΩ ΔΔΠ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Αιτήσεις Πιστοποιητικών Δημοτολογίου
Αρμόδιος Φορέας	Δήμοι, Υπηρεσία δημοτολογίων του Δήμου
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	ΑΔΤ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 2 ή 1 (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη)
Επίπεδο Αυθεντικοποίησης	Επίπεδο 1
Μηχανισμός Αυθεντικοποίησης	Συνθηματικά (Προαιρετικά: Συνθηματικά μιας Χρήσης)
Επίπεδο Εγγραφής	Επίπεδο 2 ή 1 (ανάλογα αν γίνεται ή όχι επεξεργασία αναγνωριστικών του χρήστη)

Πίνακας 15: Ένταξη Υπηρεσίας Αίτησης Πιστοποιητικών Δημοτολογίου μέσω ΔΔΠ στο ΠΨΑ

11.11.5 Απαιτούμενες Τροποποιήσεις Προτεινόμενης Λύσης

Όπως προηγούμενα, Ενότητα 11.8.5. Επίσης να σημειωθεί ότι δεν είναι σαφές εάν για την ταυτοποίηση των χρηστών στις υπηρεσίες χρησιμοποιείται ως αναγνωριστικό ο ΑΔΤ ή ο ΑΦΜ που ζητείται κατά την εγγραφή.

11.12 Παράδειγμα Εφαρμογής ΠΨΑ 11: Συμμετοχή πολιτών σε Δημοσκοπήσεις μέσω των ΔΔΠ

Κάθε πολίτης θα μπορεί να συμμετέχει σε μία διαδικασία ηλεκτρονικής δημοσκόπησης. Ο πολίτης επιλέγει τη δημοσκόπηση που τον ενδιαφέρει από αυτές που είναι διαθέσιμες στην ΔΔΠ και απαντά τις αντίστοιχες ερωτήσεις. Στη συνέχεια, το σύστημα αποθηκεύει τις επιλογές του πολίτη και εμφανίζει τα αποτελέσματα των καταχωρήσεων, μέχρι εκείνη τη στιγμή.

11.12.1 Προτεινόμενη Διαδικασία Εγγραφής

Δεν απαιτείται.

11.12.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.12.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Δεν απαιτούνται.

11.12.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Αν και δεν είναι γνωστά τα ακριβή δεδομένα που υποβάλλονται από το χρήστη κατά την αξιοποίηση της υπηρεσίας, εκτιμάται ότι αυτά δεν χρήζουν προστασίας. Όσα αναφέρονται στη συνέχεια για τη συγκεκριμένη υπηρεσία ισχύουν υπό την προϋπόθεση ότι οι απαντήσεις που δίνει ο πολίτης δεν συσχετίζονται με την ταυτότητά του.

11.12.3 Επιπτώσεις Απειλών

Δεδομένου ότι οι δημοσκοπήσεις είναι διαθέσιμες στο σύνολο των πολιτών δεν τίθεται θέμα μη εξουσιοδοτημένης πρόσβασης.

11.12.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στην παραπάνω υπηρεσία που θα προσφέρεται ηλεκτρονικά μέσω των ΔΔΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2 του ΠΨΑ.

- *[ΚΥ.4] Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 του ΠΨΑ, εντάσσονται στην κατηγορία «**Απλά Δεδομένα**».
- *[ΚΥ.5] Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2 του ΠΨΑ, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 0**, εφόσον τα δεδομένα αφορούν δημόσια προσβάσιμες πληροφορίες.
- Σύμφωνα με τον *[ΚΥ.6]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 0** και **Επίπεδο Αυθεντικοποίησης 0**.

- Σύμφωνα με τον *[ΚΠ.4]*, δεν προτείνεται να χρησιμοποιείται κάποιος μηχανισμός για την αυθεντικοποίηση των χρηστών στη συγκεκριμένη υπηρεσία.

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΣΥΜΜΕΤΟΧΗ ΠΟΛΙΤΩΝ ΣΕ ΔΗΜΟΣΚΟΠΗΣΕΙΣ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Συμμετοχή πολιτών σε Δημοσκοπήσεις
Αρμόδιος Φορέας	Δήμοι
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	-
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	3
Επίπεδο Εμπιστοσύνης	Επίπεδο 0
Επίπεδο Αυθεντικοποίησης	Επίπεδο 0
Μηχανισμός Αυθεντικοποίησης	-
Επίπεδο Εγγραφής	Επίπεδο 0

Πίνακας 16: Ένταξη Υπηρεσίας Συμμετοχής Πολιτών σε Δημοσκοπήσεις στο ΠΨΑ

11.12.5 Απαιτούμενες Τροποποιήσεις Προτεινόμενης Λύσης

Η προτεινόμενη λύση είναι πλήρως συμβατή με τα προβλεπόμενα στο ΠΨΑ.

11.13 Παράδειγμα Εφαρμογής ΠΨΑ 12: Πληρωμή Δημοτικού Φόρου μέσω των ΔΔΠ

Ο πολίτης θα μπορεί μέσω του συστήματος να πραγματοποιεί τη δήλωση εισοδήματος που απαιτείται για τον υπολογισμό του τέλους 2%. Το σύστημα υπολογίζει το τέλος και ο πολίτης μπορεί να πληρώσει ηλεκτρονικά τις οφειλές του.

11.13.1 Προτεινόμενη Διαδικασία Εγγραφής

Για την εγγραφή στη συγκεκριμένη υπηρεσία, ο πολίτης θα πρέπει να περάσει από το Δήμο. Ταυτόχρονα, φαίνεται να απασχολεί τους αναδόχους η δυνατότητα (έστω και πιλοτικής) χρήσης ψηφιακών πιστοποιητικών ή άλλων μηχανισμών αυθεντικοποίησης πέραν των συνθηματικών.

11.13.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.13.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Όπως προηγούμενα, Ενότητα 11.8.2.1.

11.13.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Τα στοιχεία που χρησιμοποιούνται κατά την αξιοποίηση της υπηρεσίας είναι τα ακόλουθα:

- Επωνυμία Δήμου, στον οποίο είναι εγκατεστημένη η επιχείρηση του πολίτη
- Στοιχεία της επιχείρησης του πολίτη
- Στοιχεία κύκλου εργασιών της επιχείρησης του πολίτη για τους μήνες που αυτά δεν έχουν συμπληρωθεί
- Ποσό τέλους
- Στοιχεία ηλεκτρονικής πληρωμής

11.13.3 Επιπτώσεις Απειλών

Ένα σημαντικό θέμα είναι η διαφύλαξη της εμπιστευτικότητας των στοιχείων του κύκλου εργασιών της επιχείρησης. Σε περίπτωση αποκάλυψής τους σε μη εξουσιοδοτημένα πρόσωπα ο φορέας παροχής της ηλεκτρονικής υπηρεσίας μπορεί να υποστεί νομικές συνέπειες καθώς τα προαναφερόμενα δεδομένα καλύπτονται από το φορολογικό απόρρητο. Επίσης είναι εμφανές ότι μεγάλη προσοχή απαιτείται αναφορικά με την ακεραιότητα των δεδομένων καθώς λαμβάνει χώρα ηλεκτρονική πληρωμή, γεγονός που σημαίνει ότι κάποιοι είναι πιθανόν να προσπαθήσουν να το εκμεταλλευτούν με στόχο το οικονομικό όφελος.

11.13.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στην παραπάνω υπηρεσία που θα προσφέρεται ηλεκτρονικά μέσω των ΔΔΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2 του ΠΨΑ.

- *[ΚΥ.4] Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 του ΠΨΑ, εντάσσονται στην κατηγορία «**Οικονομικά Δεδομένα (υπαγόμενα στο Φορολογικό Απόρρητο)**».
- *[ΚΥ.5] Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2 του ΠΨΑ, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 3**.
- Σύμφωνα με τον *[ΚΥ.9]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 3** και **Επίπεδο Αυθεντικοποίησης 2**.
- Σύμφωνα με τον *[ΚΥ.13]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι **ΠΙΣΤΟΠΟΙΗΤΙΚΑ** αποθηκευμένα σε διακριτικά Σκληρής ή Χαλαρής Αποθήκευσης (ό,τι επιλέξει ο φορέας).

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΠΛΗΡΩΜΗ ΔΗΜΟΤΙΚΟΥ ΦΟΡΟΥ ΜΕΣΩ ΔΔΠ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Πληρωμή Δημοτικού Φόρου
Αρμόδιος Φορέας	Δήμοι, Οικονομική υπηρεσία
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	ΑΦΜ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Οικονομικά δεδομένα υπαγόμενα στο Φορολογικό Απόρρητο
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	4
Επίπεδο Εμπιστοσύνης	Επίπεδο 3
Επίπεδο Αυθεντικοποίησης	Επίπεδο 2
Μηχανισμός Αυθεντικοποίησης	Ψηφιακό Πιστοποιητικό αποθηκευμένο σε Διακριτικό Σκληρής ή Χαλαρής Αποθήκευσης (ό,τι επιλέξει ο φορέας)
Επίπεδο Εγγραφής	Επίπεδο 3

Πίνακας 17: Ένταξη Υπηρεσίας Πληρωμής Δημοτικού Φόρου μέσω ΔΔΠ στο ΠΨΑ

11.13.5 Απαιτούμενες Τροποποιήσεις Προτεινόμενης Λύσης

Αναφορικά με την αξιοποίηση των διακριτικών αυθεντικοποίησης θα πρέπει να καταργηθεί η αξιοποίηση των συνθηματικών και να αξιοποιηθούν ψηφιακά πιστοποιητικά.

Σχετικά με τη διαδικασία της εγγραφής θα πρέπει να ακολουθηθούν οι διαδικασίες εγγραφής επιπέδου 3 και ο χρήστης να αποδεικνύει, υποβάλλοντας το κατάλληλο δημόσιο έγγραφο, τον Α.Φ.Μ. του.

11.14 Παράδειγμα Εφαρμογής ΠΨΑ 13: Πληρωμή Προστίμων ΚΟΚ μέσω των ΔΔΠ

11.14.1 Προτεινόμενη Διαδικασία Εγγραφής

Όπως προηγούμενα, Ενότητα 11.8.1.

11.14.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.14.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Όπως προηγούμενα, Ενότητα 11.8.2.1.

11.14.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Τα στοιχεία που χρησιμοποιούνται κατά την αξιοποίηση της υπηρεσίας είναι τα ακόλουθα:

- Αριθμός κυκλοφορίας οχήματος
- Στοιχεία κλήσεων που αφορούν τον αριθμό κυκλοφορίας (περιλαμβάνεται το χρηματικό ποσό)
- Στοιχεία ηλεκτρονικής πληρωμής

11.14.3 Επιπτώσεις Απειλών

Είναι εμφανές ότι μεγάλη προσοχή απαιτείται αναφορικά με την ακεραιότητα των δεδομένων καθώς λαμβάνει χώρα ηλεκτρονική πληρωμή, γεγονός που σημαίνει ότι κάποιοι είναι πιθανόν να προσπαθήσουν να το εκμεταλλευτούν με στόχο το οικονομικό όφελος. Βέβαια το γεγονός ότι το ύψος της συναλλαγής είναι προκαθορισμένο μετριάζει τις πιθανές επιπτώσεις.

11.14.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στην παραπάνω υπηρεσία που θα προσφέρεται ηλεκτρονικά μέσω των ΔΔΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2 του ΠΨΑ.

- *[ΚΥ.4] Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 του ΠΨΑ, εντάσσονται στην κατηγορία «**Οικονομικά Δεδομένα (με προκαθορισμένο ύψος συναλλαγής**».
- *[ΚΥ.5] Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2 του ΠΨΑ, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 2**).
- Σύμφωνα με τον *[ΚΥ.8]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 2** και **Επίπεδο Αυθεντικοποίησης 1**.

- Σύμφωνα με τους *[ΚΥ.10] και [ΚΠ.6]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΣΥΝΘΗΜΑΤΙΚΑ**», ενώ *προαιρετικά* μπορούν να αξιοποιηθούν και «ΣΥΝΘΗΜΑΤΙΚΑ ΜΙΑΣ ΧΡΗΣΗΣ».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΠΛΗΡΩΜΗ ΠΡΟΣΤΙΜΩΝ ΚΟΚ ΜΕΣΩ ΔΔΠ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Πληρωμή Προστίμων ΚΟΚ
Αρμόδιος Φορέας	Δήμοι, Οικονομική υπηρεσία – τμήμα εσόδων του Δήμου
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	Προσκόμιση Κλήσης / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Απλά δεδομένα
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	4
Επίπεδο Εμπιστοσύνης	Επίπεδο 2
Επίπεδο Αυθεντικοποίησης	Επίπεδο 1
Μηχανισμός Αυθεντικοποίησης	Συνθηματικά (Προαιρετικά: Συνθηματικά μιας Χρήσης)
Επίπεδο Εγγραφής	Επίπεδο 2

Πίνακας 18: Ένταξη Υπηρεσίας Πληρωμής Προστίμων ΚΟΚ μέσω ΔΔΠ στο ΠΨΑ

11.14.5 Απαιτούμενες Τροποποιήσεις Προτεινόμενης Λύσης

Όπως προηγούμενα, Ενότητα 11.8.5.

11.15 Παράδειγμα Εφαρμογής ΠΨΑ 14: Πληρωμή Τελών Ύδρευσης μέσω των ΔΔΠ

11.15.1 Προτεινόμενη Διαδικασία Εγγραφής

Όπως προηγούμενα, Ενότητα 11.8.1.

11.15.2 Καταγραφή Αξιοποιούμενων Δεδομένων

11.15.2.1 Δεδομένα που Υποβάλλονται κατά την Εγγραφή

Όπως προηγούμενα, Ενότητα 11.8.2.1.

11.15.2.2 Δεδομένα που Υποβάλλονται κατά την Αξιοποίηση των Υπηρεσιών

Τα στοιχεία που χρησιμοποιούνται κατά την αξιοποίηση της υπηρεσίας είναι τα ακόλουθα:

- Στοιχεία λογαριασμού πολίτη
- Τρόπος πληρωμής
- Στοιχεία ηλεκτρονικής πληρωμής

11.15.3 Επιπτώσεις Απειλών

Είναι εμφανές ότι μεγάλη προσοχή απαιτείται αναφορικά με την ακεραιότητα των δεδομένων καθώς λαμβάνει χώρα ηλεκτρονική πληρωμή, γεγονός που σημαίνει ότι κάποιοι είναι πιθανόν να προσπαθήσουν να το εκμεταλλευτούν με στόχο το οικονομικό όφελος.

11.15.4 Εφαρμογή του ΠΨΑ στις Υπηρεσίες

Η εφαρμογή του ΠΨΑ στην παραπάνω υπηρεσία που θα προσφέρεται ηλεκτρονικά μέσω των ΔΔΠ, θα γίνει σύμφωνα με τους Κανόνες της Ενότητας 10.2 του ΠΨΑ.

- *[ΚΥ.4] Προσδιορισμός Κατηγορίας Δεδομένων:* Τα δεδομένα που αξιοποιούνται στις προαναφερόμενες υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.1 του ΠΨΑ, εντάσσονται στην κατηγορία «**Οικονομικά Δεδομένα (μη προκαθορισμένου ύψους συναλλαγής)**».
- *[ΚΥ.5] Προσδιορισμός Επιπέδου Εμπιστοσύνης:* Οι υπηρεσίες, σύμφωνα με τα οριζόμενα στην ενότητα 9.1.2 του ΠΨΑ, εντάσσονται στο **Επίπεδο Εμπιστοσύνης 3**.
- Σύμφωνα με τον *[ΚΥ.9]*, οι υπηρεσίες θα πρέπει να υιοθετήσουν **Επίπεδο Εγγραφής 3** και **Επίπεδο Αυθεντικοποίησης 2**.
- Σύμφωνα με τον *[ΚΥ.13]*, ο μηχανισμός αυθεντικοποίησης που πρέπει να αξιοποιηθεί είναι «**ΠΙΣΤΟΠΟΙΗΤΙΚΑ** (Διακριτικό Σκληρής Αποθήκευσης)».

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την ένταξη της υπηρεσίας στο ΠΨΑ.

ΠΛΗΡΩΜΗ ΤΕΛΩΝ ΥΔΡΕΥΣΗΣ ΜΕΣΩ ΔΔΠ	
ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ	
Τίτλος Υπηρεσίας	Πληρωμή Τελών Ύδρευσης
Αρμόδιος Φορέας	Δήμοι, Οικονομική υπηρεσία
Αναγνωριστικό / Τρόπος Αυθεντικοποίησης	ΑΦΜ / Συνθηματικά
ΕΝΤΑΞΗ ΥΠΗΡΕΣΙΩΝ ΣΤΟ Π.Ψ.Α.	
Τύπος Δεδομένων	Οικονομικά δεδομένα μη προκαθορισμένου ύψους συναλλαγής
Επίπεδο Ηλεκτρονικής Ολοκλήρωσης	4
Επίπεδο Εμπιστοσύνης	Επίπεδο 3
Επίπεδο Αυθεντικοποίησης	Επίπεδο 2
Μηχανισμός Αυθεντικοποίησης	Ψηφιακό Πιστοποιητικό αποθηκευμένο σε Διακριτικό Σκληρής Αποθήκευσης
Επίπεδο Εγγραφής	Επίπεδο 3

Πίνακας 19: Ένταξη Υπηρεσίας Πληρωμής Τελών Ύδρευσης μέσω ΔΔΠ στο ΠΨΑ

11.15.5 Απαιτούμενες Τροποποιήσεις Προτεινόμενης Λύσης

Αναφορικά με την αξιοποίηση των διακριτικών αυθεντικοποίησης θα πρέπει να καταργηθεί η αξιοποίηση των συνθηματικών και να αξιοποιηθούν ψηφιακά πιστοποιητικά.

Σχετικά με τη διαδικασία της εγγραφής θα πρέπει να ακολουθηθούν οι διαδικασίες εγγραφής επιπέδου 3 και ο χρήστης να αποδεικνύει, υποβάλλοντας το κατάλληλο δημόσιο έγγραφο, τον Α.Φ.Μ. του.

12. ΠΑΡΑΡΤΗΜΑ Α: Βιβλιογραφία και Σύνδεσμοι

Τεχνικά Θέματα

[1] Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens (IDABC), http://www.europa.eu.int/idabc

[2] Ψηφιακή Στρατηγική 2006-2013 και Επιχειρησιακό Πρόγραμμα «Ψηφιακή Σύγκλιση», Ειδική Υπηρεσία Διαχείρισης Ε.Π. «Κοινωνία της Πληροφορίας», Υπουργείο Οικονομίας και Οικονομικών, http://www.infosoc.gr

[3] Επιχειρησιακό Πρόγραμμα «Διοικητική Μεταρρύθμιση», Υπουργείο Εσωτερικών, Γενική Γραμματεία Δημόσιας Διοίκησης & Ηλεκτρονικής Διακυβέρνησης, http://www.gspa.gr

[4] Trust Services- e-Government Strategy Policy Framework and Guidelines, Version 3.0, September 2002, http://www.govtalk.gov.uk/policydocs/policydocs_document.asp?docnum=655&topic=56&topictitle=Security+Framework&subjecttitle=

[5] Confidentiality - e-Government Strategy Policy Framework and Guidelines, Version 3.0, September 2002, http://www.cabinetoffice.gov.uk/csia/documents/pdf/Confidentiality_V3_Sept_2002.pdf

[6] Registration and Authentication - e-Government Strategy Policy Framework and Guidelines, Version 3.0, September 2002, http://www.cabinetoffice.gov.uk/csia/documents/pdf/RegAndAuthentn0209v3.pdf

[7] Broker Security Model www.reach.ie/misc/docs/6%20Broker%20Security%20Model%20v1.0.pdf,

[8] Australian Government - e-Authentication Framework for Individuals - Overview and Principles, June 2006, http://www.agimo.gov.au/infrastructure/authentication

[9] Australian Government - e-Authentication Framework for Business, December 2005, http://www.agimo.gov.au/infrastructure/authentication

[10] New Zealand E-government - Interoperability Framework - (NZ e-GIF) - Version 3.0, March 2006, http://www.e.govt.nz/standards/e-gif/e-gif-v-3/e-gif-v-3-intro.pdf

[11] Guide to Authentication Standards for Online Services State Services Commission, June 2006, Version 1.0, http://www.e.govt.nz/standards/e-gif/authentication/guide-to-auth-standards

[12] Ron Ross, Marianne Swanson , Gary Stoneburner, Stu Katzke, Arnold Johnson – NIST Special Publication 800-37 - Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004, http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf

[13] Joshua B. Bolten, *E-Authentication Guidance for Federal Agencies,* December 16, 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[14] NIST - William E. Burr Donna F. Dodson W. Timothy Polk, Electronic Authentication Guideline, April 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[15] Σωκράτης Κάτσικας, Δημήτριος Γκρίτζαλης, Στέφανος Γκρίτζαλης, Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, 2004

[16] http://sectools.org/crackers.html

[17] Cisneros, R., Bliss, D., and Garcia, M. 2006. Password auditing applications. J. Comput. Small Coll. 21, 4 (Apr. 2006), 196-202.

[18] Pinkas, B. and Sander, T. 2002. Securing passwords against dictionary attacks. In Proceedings of the 9th ACM Conference on Computer and Communications Security (Washington, DC, USA, November 18 - 22, 2002). V. Atluri, Ed. CCS '02. ACM Press, New York, NY, 161-170. DOI= http://doi.acm.org/10.1145/586110.586133

[19] Γεώργιος Καμπουράκης Στέφανος Γκρίτζαλης Σωκράτης Κάτσικας, Ασφάλεια Ασύρματων και Κινητών Δικτύων Επικοινωνιών, Εκδόσεις Παπασωτηρίου, 2006

[20] Neils Ferguson, Bruce Schneier, Practical Cryptography, Wiley Publishing 2003

[21] de Vivo, M., de Vivo, G. O., and Isern, G. 1998. Internet security attacks at the basic levels. SIGOPS Oper. Syst. Rev. 32, 2 (Apr. 1998), 4-15. DOI= http://doi.acm.org/10.1145/506133.506136

[22] On-line Authentication Threats and Attacks - New Zealand and E-government

[23] Mirkovic J.; Dietrich S.; Dittrich D., and P. Reiher, Internet Denial of Service: Attack and Defence Mechanisms. Prentice Hall, 2005

[24] NIST - William E. Burr Donna F. Dodson W. Timothy Polk, Electronic Authentication Guideline, April 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[25] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone , Handbook of Applied Cryptography, CRC Press August 2001

[26] D 8.3 Database on Identity Management Systems and ID Law in the EU, Ioannis Maghiros, Sabine Delaitre, Bert-Jaap Koops, 14-3-2006

[27] US E-Government Authentication Framework and Programs Michael Caloyannides, Dennis R. Copeland, George H. Datesman Jr., and David S. Weitzel

[28] Survey on EU's Electronic -ID Solutions. Amir Hayat, Herbert Leitold, Christian Rechberger, Thomas Rössler

[29] E-government in the Netherlands: a brief history http://ec.europa.eu/idabc/servlets/Doc?id=22685

[30] eGovernment in The Netherlands http://ec.europa.eu/idabc/egovo

[31] Regulatin Electronic commerce in the Netherlands http://www.ejcl.org/64/art64-28.html

[32] Towards the electronic government, http://ec.europa.eu/idabc/en/document/4861/375

[33] The office of the privacy commissioner [Government Guidelines] http://www.privacy.gov.au/government/guidelines/index.html

[34] http://www.e.govt.nz/services/authentication/library/docs/pia-200404

[35] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, http://

[36] Ron Ross, Stu Katzke, Arnold Kohnosn, Mariane Swanson, Gary Stoneburner, George Rogers, Annabelle Lee ,NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems, February 2005

[37] F. Baker, P Savola, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 3704, March 2004

[38] [Krawczyk, H.; Bellare, M.; Canetti, R.; "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997

[39] Ferguson Niels and Bruce Schneier, Practical Cryptography, Wiley Publishing 2003

[40] Thomer M. Gil and Massimiliano Poletto, MULTOPS: a data-structure for bandwidth attack detection, In Proceedings of the 10th USENIX Security Symposium

[41] Chen-Mou Cheng; Kung, H.T.; Koan-Sin TanUse of spectral analysis in defence against DoS attacks, In proceedings of Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE, Vol.3, Iss., 17-21 Nov. 2002

[42] Manikopoulos, C.; Papavassiliou, S.; Network intrusion and fault detection: a statistical anomaly approach ,Communications Magazine, IEEE ,Volume: 40 , Issue: 10 , Oct. 2002, Pages:76 – 82

[43] http://www.cisco.com/en/US/products/ps5892/index.html

[44] Sir Ross. January 20, 2005. A guide to social engineering http://www.astalavista.com/index.php?section=directory&cmd=detail&id=3488

[45] An improved deniable authentication protocol, http://www3.interscience.wiley.com/cgi-bin/abstract/112774772/ABSTRACT

[46] Kerberos: The Network Authentication Protocol, http://web.mit.edu/Kerberos/

[47] Cisco - Protecting Your Core: Infrastructure Protection Access Control Lists, http://www.cisco.com/warp/public/707/iacl.html

[48] Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας, Δημήτριος Γκρίτζαλης, Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης και Ηλεκτρονικού Επιχειρείν, Εκδόσεις Παπασωτηρίου, 2003

Νομικά Θέματα

[1] Άρθρο 29 – Ομάδα εργασίας για την προστασία των δεδομένων, Έγγραφο εργασίας σχετικά με την Ηλεκτρονική διακυβέρνηση, 10593/02/EL, WP 73

[2] Αρμαμέντος Π./Σωτηρόπουλος Β., Προσωπικά Δεδομένα, Αθήνα-Θεσσαλονίκη 2004

[3] Γεωργιάδης Α., Γενικές Αρχές Αστικού Δικαίου. Αθήνα-Κομοτηνή 2002

[4] Δαγτόγλου Π. Δ., «Γενικό Διοικητικό Δίκαιο», πέμπτη έκδοση ενημερωμένη από Π. Μ. Ευστρατίου, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2004

[5] Μήτρου Λ., "*Προστασία Προσωπικών Δεδομένων*" σε Σ. Κάτσικας/Δ.Γκρίτζαλης/Σ. Γκρίτζαλης (επιμ.),"Ασφάλεια Πληροφοριακών Συστημάτων", Αθήνα 2004, σελ. 443-525

[6] Παυλόπουλος Πρ., «Η αστική ευθύνη του Δημοσίου κατά τους κανόνες του δημοσίου δικαίου» στο συλλογικό έργο «Διοικητικό Δίκαιο», Απ.Γέροντας, Σ. Λύτρας, Πρ. Παυλόπουλος, Γλ. Σιούτη, Σ. Φλογαΐτης, επιμέλεια Κ. Γιαννακόπουλος, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα–Κομοτηνή, 2004.

[7] Σπηλιωτόπουλος Επ., «Εγχειρίδιο Διοικητικού Δικαίου», εκδόσεις Αντ. Ν. Σάκκουλα, ενδέκατη έκδοση ενημερωμένη μέχρι και 2002.

[8] Bal A., Quelques réflexions sur l' administration électronique, Lex Electronica, vol. 10, no 1, Hiver 2005

[9] Cimander R./ Kubicek H./Freitter M., Standardised e-Form exchange via EDIAKT II in Austria – Good Practice Case (case study), 2006

[10] *Commission Nationale de l' Informatique et des Libertés (CNIL), La position de la CNIL sur le Programme ADELE (Administration Electronique), Paris 2004*

[11] Council of European Committee of ministers, Recommendation no. r (91) 10 of the committee of ministers to member states on the communication to third parties of personal data held by public bodies *(adopted by the committee of ministers on 9 September 1991 at the 461st meeting of the ministers' deputies)*

[12] *Eifert M., J.O. Püschel, C. Stapel-Schulz (Bundesministerium für Wirtschaft und Arbeit). Rechtskonformes E-Government, Berlin 2003*

[13] Holden S.H./Millett L.I., Authentication, Privacy, and the Federal E-Government, The Information Society, 21, 2005, pp. 367-377

[14] *Hristova R. (Universität St Gallen), Die Bedeutung des Personenidentifikators in der Entwicklung des e-Governments – Working Paper No 9, St. Gallen, 2005*

[15] Modinis (A conceptual framework for European IDM Systems- K.U.Leuven/Lawfort/A-Sit.), Study on Identity Management in eGovernment, Prepared for the eGovernment Unit – DG Information Society and Media, 2006

[16] Office of the e-Envoy, Security – e-Government Strategy Framework Policy and Guidelines, London 2002

[17] *Pinet M.(CNIL), First Reflections on Electronic Administration, Spring Conference of Data Protection Commissioners, Bonn 2002*

[18] *Projektgruppe E-Government im Bundesamt für Sicherheit in der Informationstechnik (BSI)- Hans Bredow-Institut für Medienforschung – Centre for Research in Law and Innovation, Rechtliche Rahmenbedingungen für E-Government, Bonn 2004*

13. ΠΑΡΑΡΤΗΜΑ Β: Πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών

Στο παράρτημα αυτό αποτυπώνεται το πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών (certificate policy framework), στο οποίο προσδιορίζονται όλες οι αναγκαίες διαδικασίες έκδοσης (issue), διαμοιρασμού (distribution) και ανάκλησης (revoke) των διαφορετικού τύπου ψηφιακών πιστοποιητικών που θα είναι δυνατό να εκδίδονται, με βάση το ΠΨΑ. Ακολούθως προσδιορίζονται και οι αντίστοιχες διαδικασίες ελέγχου συμμόρφωσης των πολιτικών ψηφιακών πιστοποιητικών και των κανονισμών λειτουργίας που αφορούν στην έκδοση των ψηφιακών πιστοποιητικών από Υποκείμενες Αρχές Πιστοποίησης (Certification Authorities).

13.1.1 Γενικά

Οι Αρχές Πιστοποίησης και οι Υποκείμενές τους και συνεπώς τα εκδιδόμενα από αυτές ψηφιακά πιστοποιητικά θα πρέπει να ακολουθούν το παρόν πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών. Με βάση το πρότυπο X.509, Πολιτική Ψηφιακών Πιστοποιητικών θεωρείται ένα σύνολο επακριβώς προσδιορισμένων κανόνων, οι οποίοι εξασφαλίζουν την εφαρμοσιμότητα (applicability) ενός ψηφιακού πιστοποιητικού στο πλαίσιο της λειτουργίας ενός συνόλου εφαρμογών, με συγκεκριμένες απαιτήσεις ασφάλειας. Η Πολιτική Ψηφιακών Πιστοποιητικών, γενικά, αποτελεί ένα χρήσιμο εργαλείο για το χρήστη Υποδομών Δημοσίου Κλειδιού (ΥΔΚ) ώστε να αποφασίσει εάν ένα συγκεκριμένο ψηφιακό πιστοποιητικό μπορεί να θεωρείται αξιόπιστο (trustworthy) για χρήση σε κάποια συγκεκριμένη εφαρμογή.

Θα πρέπει να σημειωθεί ότι το παρόν πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών συμμορφώνεται με το de facto standard RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, διάδοχο του RFC 2527.

13.1.2 Σκοπός

Σκοπός της ενότητας αυτής είναι να παρουσιάσει ένα πλαίσιο Πολιτικής Πιστοποιητικών που θα μπορούν να αξιοποιήσουν ως οδηγό οι Υποκείμενες Αρχές Πιστοποίησης δημοσίου ή ιδιωτικού δικαίου για τη συγγραφή Πολιτικών Ψηφιακών Πιστοποιητικών και της αντίστοιχης Δήλωσης Πρακτικής (Practice Statement). Συγκεκριμένα, το πλαίσιο αυτό Ψηφιακών Πιστοποιητικών προκαθορίζει όλα εκείνα τα στοιχεία που απαιτείται να ληφθούν υπόψη για την ορθή λειτουργία των Υποδομών Δημοσίου Κλειδιού.

Οίκοθεν νοείται ότι το πλαίσιο αυτό δεν προσδιορίζει κάποια συγκεκριμένη Πολιτική Πιστοποιητικών, αλλά περιγράφει τις γενικές αρχές που θα πρέπει να ακολουθούνται κατά τη συγγραφή των πολιτικών πιστοποιητικών.

13.1.3 Στόχος

Ο στόχος της ενότητας αυτής είναι ο προσδιορισμός των περιεχομένων της Πολιτικής Ψηφιακών Πιστοποιητικών και συγκεκριμένα η περιγραφή όλων εκείνων των τεχνικών

ρυθμιστικών και κανονιστικών στοιχείων και των αντίστοιχων πληροφοριών που θα πρέπει να λαμβάνονται υπόψη κατά τη συγγραφή της Πολιτικής και της αντίστοιχης Δήλωσης Πρακτικής ψηφιακών πιστοποιητικών.

13.1.4 Πολιτική Ψηφιακών Πιστοποιητικών

Ένα ψηφιακό πιστοποιητικό συσχετίζει ένα ζεύγος ασύμμετρων κρυπτογραφικών κλειδιών, δημόσιο και ιδιωτικό, με ένα σύνολο πληροφοριών που είναι δυνατό να προσδιορίσει μοναδικά την οντότητα που έχει στην κατοχή της το συγκεκριμένο πιστοποιητικό. Η αποδοχή του συσχετισμού αυτού εξαρτάται από την αποτίμηση που πραγματοποιεί ο κάθε χρήστης που επιθυμεί να αξιοποιήσει το δημόσιο αυτό πιστοποιητικό, με βάση την εφαρμογή αξιοποίησης του πιστοποιητικού και την ισχύουσα Πολιτική Πιστοποιητικών που εφαρμόζεται από τον πάροχο ΥΔΚ. Διαφορετικά ψηφιακά πιστοποιητικά θα πρέπει να εκδίδονται για διαφορετικού σκοπού υπηρεσίες, ώστε να διασφαλίζεται ότι σε περίπτωση διακύβευσης ενός ζεύγους κλειδιών, το οποίο συνδέεται με ένα συγκεκριμένο ψηφιακό πιστοποιητικό, οι υπηρεσίες που δεν αξιοποιούν το συγκεκριμένο ψηφιακό πιστοποιητικό θα παραμένουν ανεπηρέαστες.

13.1.5 Προσδιορισμός Πολιτικής Ψηφιακών Πιστοποιητικών

Η πολιτική ψηφιακών πιστοποιητικών καταγράφεται σε κάθε ψηφιακό πιστοποιητικό και αναπαριστάται από ένα μοναδικό προσδιοριστή αντικειμένου (Object Identifier). Για κάθε πολιτική ψηφιακών πιστοποιητικών που προσδιορίζεται από Υποκείμενες Αρχές Πιστοποίησης θα πρέπει να γίνεται καταχώριση του προσδιοριστή αντικειμένου για τη συγκεκριμένη Πολιτική Ψηφιακών Πιστοποιητικών. Η διαδικασία καταχώρισης περιλαμβάνει συγκεκριμένες επιμέρους διαδικασίες, όπως έχουν προσδιοριστεί σε σχετικά πρότυπα των ISO/IEC και ITU. Για παράδειγμα, ο προσδιοριστής της Πολιτικής Πιστοποίησης που χρησιμοποιείται από την Adobe System είναι ο ακόλουθος: 2.16.840.1.113733.1.7.23.3

13.1.5.1 Εφαρμοσιμότητα της Πολιτικής

Όλες οι οντότητες που θα συμμετέχουν σε υπηρεσίες ΥΔΚ θα πρέπει να εφαρμόζουν τις συγκεκριμένες οδηγίες. Οι οντότητες αυτές περιγράφονται αναλυτικά στην ενότητα 13.1.5.2, ενώ οι επιτρεπόμενες χρήσεις των πιστοποιητικών (εφαρμογές στα πλαίσια των οποίων μπορούν να αξιοποιηθούν) αναλύονται στην ενότητα 13.1.6.3.

13.1.5.2 Περιγραφή Οντοτήτων Παροχής Υπηρεσιών Δημοσίου Κλειδιού

Στην ενότητα αυτή περιγράφονται αναλυτικά όλες οι οντότητες που πρέπει να συμμετέχουν και να καθορίζονται κατ' ελάχιστον σε κάθε Πολιτική Πιστοποιητικών Υποδομής Δημόσιου Κλειδιού.

13.1.5.2.1 Αρχές Πιστοποίησης

Η Αρχή Πιστοποίησης παρέχει υπηρεσίες πιστοποίησης σε φυσικά ή νομικά πρόσωπα, τα οποία έχουν εγγραφεί ως (τελικοί) χρήστες και κάνουν χρήση ηλεκτρονικών υπηρεσιών της Δημόσιας

Διοίκησης. Ακόμη, είναι επιφορτισμένη με την τεχνική διαχείριση των πιστοποιητικών για ολόκληρο τον κύκλο ζωής τους. Σε αυτή συμπεριλαμβάνονται τα εξής:

- Διαχείριση κλειδιών
    - Δημιουργία κλειδιών
    - Διάσωση και ανάκτηση κλειδιών
    - Ανανέωση κλειδιών και διαχείριση του ιστορικού
- Αποθήκευση και διανομή ψηφιακών πιστοποιητικών
- Ανάκληση ψηφιακών πιστοποιητικών
- Δημοσιοποίηση της Λίστας Ανάκλησης Πιστοποιητικών (Certificate Revocation List)

Κάθε Αρχή Πιστοποίησης που εκδίδει, διαμοιράζει και ανακαλεί ψηφιακά πιστοποιητικά, στο πλαίσιο της αρχιτεκτονικής που υποστηρίζει το παρόν παραδοτέο του ΠΨΑ για την ΚΔΠ ΕΡΜΗΣ, θα πρέπει να λειτουργεί ως Υποκείμενη Αρχή Πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) (ν.3448/2006).

Η ΑΠΕΔ αποτελεί τη ρίζα (root) της σχετικής ιεραρχίας, στο πλαίσιο ενός καθαρού ολοκληρωμένου ιεραρχικού μοντέλου εμπιστοσύνης Αρχών Πιστοποίησης.

Αφού το βάθος του ως άνω ιεραρχικού μοντέλου στη συγκεκριμένη περίπτωση, με την ΑΠΕΔ ως ρίζα και σε πρώτο επίπεδο όλες τις Υποκείμενες Αρχές Πιστοποίησης, είναι το ελάχιστο δυνατό έχοντας την τιμή ένα, αναπτύσσεται μία καλά ορισμένη δομή, χωρίς αυξημένη πολυπλοκότητα και κατά συνέπεια η προταθείσα αρχιτεκτονική δε χρήζει ανάγκης για περαιτέρω βελτιστοποιήσεις δια ενδεχόμενης υιοθέτησης πρόσθετης πολυπλοκότητας από εισαγωγή υπηρεσιών διαπιστοποίησης (cross certification).

13.1.5.2.2 Αρχή Εγγραφής

Η Αρχή Εγγραφής παρέχει τη λειτουργική διεπαφή και επικοινωνία μεταξύ ενός αιτούμενου και του παρόχου που είναι υπεύθυνος για τον έλεγχο και πιστοποίηση των στοιχείων ή του ρόλου μιας οντότητας. Η Αρχή Εγγραφής ελέγχει όλα τα απαραίτητα στοιχεία που απαιτούνται για την έκδοση ενός πιστοποιητικού, όπως αυτά αναφέρονται στο παρόν πλαίσιο (βλέπε ενότητα 8) και διασφαλίζει την ακρίβεια των στοιχείων σύμφωνα με το Προεδρικό Διάταγμα Π.Δ 150/2001 άρθρο 6. Όλες οι έγκυρες αιτήσεις προωθούνται στην Αρχή Πιστοποίησης για την έκδοση του κατάλληλου ψηφιακού πιστοποιητικού μέσω ασφαλών διαύλων επικοινωνίας όπως ορίζονται στην ενότητα 13.1.7.1.

13.1.5.2.3 Τελικοί Χρήστες Πιστοποιητικών

Ως χρήστης ψηφιακού πιστοποιητικού νοείται

- κάθε φυσικό πρόσωπο,
- κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου ιδιωτικού δικαίου και

- κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου δημοσίου δικαίου

που έχει εγγραφεί και κάνει χρήση ηλεκτρονικών υπηρεσιών της Δημόσιας Διοίκησης και ενεργεί είτε στο δικό του όνομα είτε στο όνομα άλλου φυσικού ή νομικού προσώπου ή φορέα. Εφόσον χρήστης ψηφιακού πιστοποιητικού είναι νομικό πρόσωπο, αυτό εκπροσωπείται σύμφωνα με τα οριζόμενα στις εκάστοτε διατάξεις ή στο καταστατικό αυτού.

13.1.5.2.4 Οντότητες Εμπιστοσύνης

Ο φορέας ΥΔΚ θα πρέπει να αναφέρει όλες εκείνες τις οντότητες που εμπιστεύονται τη συγκεκριμένη πολιτική και συνεπώς τα εκδιδόμενα πιστοποιητικά για τις διαφορετικού είδους υπηρεσίες που προσφέρονται από το φορέα.

13.1.5.2.5 Οντότητες Διαχείρισης

Όλοι οι πάροχοι ΥΔΚ υποχρεούνται να δηλώνουν τα πλήρη στοιχεία της υπεύθυνης αρχής που έχει την ευθύνη διαχείρισης της Πολιτικής Πιστοποιητικών και της αντίστοιχης Δήλωσης Πρακτικών. Επιπλέον θα πρέπει να συμπεριλαμβάνονται και στοιχεία επικοινωνίας του φυσικού προσώπου που ενεργεί εκ μέρους της Αρχής Πιστοποίησης και επωμίζεται την ευθύνη διαχείρισης της Πολιτικής Πιστοποιητικών.

13.1.5.2.6 Άλλες οντότητες

Ο φορέας ΥΔΚ θα πρέπει να αναφέρει επιπλέον όλες τις επιπρόσθετες οντότητες με τις οποίες συνεργάζεται για την παροχή ολοκληρωμένων υπηρεσιών ΥΔΚ, εφόσον υπάρχουν.

13.1.5.3 Γενικές Διατάξεις και Όροι

Σε αυτή την ενότητα προσδιορίζονται οι υποχρεώσεις όλων των εμπλεκόμενων οντοτήτων για την παροχή ΥΔΚ. Συγκεκριμένα περιλαμβάνονται:

- Οι υποχρεώσεις:
    - των Αρχών Πιστοποίησης
    - των Αρχών Εγγραφής
    - των κατόχων ψηφιακών πιστοποιητικών
- Ευθύνες
    - των Αρχών Πιστοποίησης
    - των Αρχών Εγγραφής
    - των κατόχων ψηφιακών πιστοποιητικών
- Εγγυήσεις
- Θέματα δημοσιοποίησης των ψηφιακών πιστοποιητικών
- Πολιτική εμπιστευτικότητας

- Μέθοδοι Εγγραφής, Ταυτοποίησης και Αυθεντικοποίησης των χρηστών πριν την έκδοση ενός ψηφιακού πιστοποιητικού
- Μέθοδοι επίλυσης διαφορών

13.1.5.3.1 Υποχρεώσεις των εμπλεκόμενων οντοτήτων

13.1.5.3.1.1 Υποχρεώσεις Αρχών Εγγραφής

Οι κατ' ελάχιστον υποχρεώσεις των Αρχών Εγγραφής, είναι οι ακόλουθες:

- Διαχείριση των αιτήσεων για έκδοση, ανανέωση, ανάκληση πιστοποιητικών των χρηστών
    - Έλεγχος της ορθότητας των στοιχείων των αιτήσεων πιστοποιητικών
    - Προώθηση των έγκυρων αιτήσεων στην Αρχή Πιστοποίησης
    - Ενημέρωση των χρηστών για μη έγκριση της αίτησης τους μέσω ασφαλών διαύλων επικοινωνίας
    - Με βάση την κρισιμότητα του προς έκδοση πιστοποιητικού θα πρέπει να αιτείται ή όχι φυσικής παρουσίας του αιτούντος στην Αρχή Εγγραφής
- Να εφαρμόζουν τις διαδικασίες εγγραφής όπως αυτές ορίζονται για τις υπηρεσίες που κατατάσσονται στο Επίπεδο Εμπιστοσύνης 3.
- Να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν την έκδοση πιστοποιητικών για χρονικό διάστημα τριάντα (30) ετών σύμφωνα με το προεδρικό διάταγμα 150/2001 παράρτημα ΙΙ, στοιχείο θ.
- Να προστατεύουν το ζεύγος κλειδιών τους αξιοποιώντας ασφαλείς διατάξεις σύμφωνα με το προεδρικό διάταγμα 150/2001 παράρτημα ΙΙΙ.
- Να αξιοποιούν τα ζεύγη κλειδιών τους αποκλειστικά για τη διαχείριση των ηλεκτρονικών αιτήσεων πιστοποιητικών φυσικών προσώπων.
- Να εναρμονίζονται σε κάθε περίπτωση με το ισχύον νομικό-θεσμικό πλαίσιο για την παροχή υπηρεσιών ηλεκτρονικής διακυβέρνησης.

13.1.5.3.1.2 Υποχρεώσεις Αρχών Πιστοποίησης

Οι κατ' ελάχιστον υποχρεώσεις των Αρχών Πιστοποίησης, είναι οι ακόλουθες:

- Δημοσιοποίηση της Πολιτικής Πιστοποιητικών και της αντίστοιχης Δήλωσης Πρακτικής.
- Εφαρμογή των πολιτικών που περιγράφονται στις παρούσες οδηγίες.
- Έγκριση της Πολιτικής Πιστοποιητικών από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ή από την αντίστοιχη Αρχή που διασφαλίζει την εφαρμογή της πολιτικής.
- Έλεγχος της ορθότητας των στοιχείων που λαμβάνουν από την Αρχή Εγγραφής.

- Διαχείριση Πιστοποιητικών φυσικών προσώπων
    - Δημιουργία
    - Ανανέωση
    - Ανάκληση
- Δημοσιοποίηση Ενεργών Πιστοποιητικών
- Διαχείριση Λίστας Ανάκλησης Πιστοποιητικών
    - Δημοσίευση
    - Ανανέωση
- Δε θα πρέπει να εκδίδονται περισσότερα από ένα πιστοποιητικά με το ίδιο δημόσιο κλειδί πλην των περιπτώσεων ανανέωσης του πιστοποιητικού και μόνο για ψηφιακά πιστοποιητικά κρυπτογράφησης ή για λόγους που απαιτείται από το νόμο.
- Να προστατεύουν το ζεύγος κλειδιών τους αξιοποιώντας ασφαλείς διατάξεις σύμφωνα με το προεδρικό διάταγμα 150/2001 παράρτημα III.
- Να αξιοποιούν διαφορετικό ζεύγος κλειδιών για την ψηφιακή υπογραφή των πιστοποιητικών από αυτό που αξιοποιείται για την επικοινωνία με τρίτες οντότητες (κρυπτογράφηση και ψηφιακή υπογραφή).
- Δεν θα πρέπει να τηρούν τους κωδικούς των ασφαλών διατάξεων που παρέχουν στα φυσικά πρόσωπα για την αποθήκευση των ζευγών κλειδιών.
- Να καταγράφουν το σύνολο των συναφών πληροφοριών που αφορούν τη διαχείριση πιστοποιητικών εφόσον απαιτείται, για χρονικό διάστημα τριάντα (30) ετών, σύμφωνα με το προεδρικό διάταγμα 150/2001 παράρτημα II, στοιχείο θ.
- Να εναρμονίζονται σε κάθε περίπτωση με το ισχύον νομικό-θεσμικό πλαίσιο.

13.1.5.3.1.3 Υποχρεώσεις Χρηστών

Οι κατ' ελάχιστον υποχρεώσεις των χρηστών, είναι οι ακόλουθες:

- Αληθής και ακριβής δήλωση των στοιχείων που απαιτούνται για την έκδοση ενός πιστοποιητικού κατά τη διαδικασία της εγγραφής.
- Έγκριση και αποδοχή της Πολιτικής Πιστοποιητικών και της αντίστοιχης Δήλωσης Πρακτικής.
- Χρήση των πιστοποιητικών και των αντίστοιχων ζευγών κλειδιών εναρμονισμένη με την αντίστοιχη πολιτική και με βάση τις εφαρμογές των εκδιδόμενων πιστοποιητικών, όπως ορίζονται στις επιτρεπτές χρήσεις των πιστοποιητικών (βλέπε ενότητα 13.1.6.3).
- Προστασία της ασφαλούς διάταξης αποθήκευσης των ζευγών κλειδιών από μη εξουσιοδοτημένους χρήστες:

- Δεν θα πρέπει να διατηρούν στον ίδιο χώρο την ασφαλή διάταξη που αποθηκεύονται τα ζεύγη κλειδιών και τους προσωπικούς τους αριθμούς PIN-PUK.
- Σε καμία περίπτωση δεν πρέπει να αφήνουν εκτεθειμένη την ασφαλή διάταξη που αποθηκεύονται τα ζεύγη κλειδιών τους.
- Έπειτα από κάθε χρήση της ασφαλούς διάταξης θα πρέπει να την αποθηκεύουν σε ασφαλές μέρος.
- Δεν θα πρέπει να δανείζουν την ασφαλή διάταξη που αποθηκεύονται τα ζεύγη κλειδιών ή να γνωστοποιούν τους κωδικούς αριθμούς PIN-PUK σε οποιονδήποτε.

- Άμεση ενημέρωση της Αρχής Πιστοποίησης σε περίπτωση υποψίας διακύβευσης του ιδιωτικού κλειδιού ή απώλεια της ασφαλούς διάταξης.
- Να ακολουθούν τις διαδικασίες εγγραφής που ορίζονται για τις υπηρεσίες Επιπέδου Εμπιστοσύνης 3.
- Προσωρινή ή μόνιμη ανάκληση των πιστοποιητικών που είναι κάτοχοι.

13.1.5.3.2 Ευθύνες των εμπλεκόμενων οντοτήτων

13.1.5.3.2.1 Ευθύνες Αρχής Εγγραφής

Οι ευθύνες της Αρχής Εγγραφής είναι κατ' ελάχιστον οι ακόλουθες:

- Η Αρχή Εγγραφής θα πρέπει να εναρμονίζεται με την Πολιτική Πιστοποιητικών.
- Η Αρχή Εγγραφής πρέπει να τηρεί τις υποχρεώσεις που αναγράφονται στην ενότητα 13.1.5.3.1.1.
- Η Αρχή Εγγραφής δε φέρει καμία υπαιτιότητα σε περίπτωση μη ορθής χρήσης των πιστοποιητικών.
- Η Αρχή Εγγραφής πρέπει να εναρμονίζεται και να εφαρμόζει το Π.Δ 150/2001.

13.1.5.3.2.2 Ευθύνες Αρχής Πιστοποίησης

Οι ευθύνες της Αρχής Πιστοποίησης είναι κατ' ελάχιστον οι ακόλουθες:

- Η Αρχή Πιστοποίησης πρέπει να εφαρμόζει την Πολιτική Πιστοποιητικών.
- Η Αρχή Πιστοποίησης πρέπει να τηρεί τις υποχρεώσεις που αναφέρονται στην ενότητα 13.1.5.3.1.2.
- Η Αρχή Πιστοποίησης πρέπει να εγγυάται την ορθότητα των στοιχείων που αναγράφονται στα πιστοποιητικά.
- Η Αρχή Πιστοποίησης δε φέρει ευθύνη για μη ορθή χρήση πιστοποιητικών εφόσον δεν οφείλεται σε δική της υπαιτιότητα.

- Η Αρχή Πιστοποίησης πρέπει να εναρμονίζεται και να εφαρμόζει το Π.Δ 150/2001.

13.1.5.3.2.3 Ευθύνες Χρηστών

Οι ευθύνες των χρηστών είναι κατ' ελάχιστον οι ακόλουθες:

- Οι χρήστες θα πρέπει να τηρούν τις υποχρεώσεις που αναφέρονται στην ενότητα 13.1.5.3.1.3.

13.1.5.3.2.4 Ευθύνη προς Αποζημίωση

Οι ΥΔΚ θα πρέπει να προσδιορίζουν τις αποζημιώσεις και το όριο οικονομικής ευθύνης που τους αναλογεί με βάση τις επιπτώσεις που μπορεί να προκαλέσει η μη ορθή διαχείριση ενός πιστοποιητικού ή δυσλειτουργία της Αρχής Πιστοποίησης ή οποιουδήποτε λειτουργικού τμήματος, συμπεριλαμβανομένων και των συνεργαζόμενων οντοτήτων, που προκαλεί τη μη παροχή υπηρεσιών ΥΔΚ. Επιπλέον, στον προσδιορισμό του ορίου οικονομικής ευθύνης θα πρέπει να λαμβάνεται υπόψη το είδος των συναλλαγών, σε συνδυασμό με τον τύπο του πιστοποιητικού που αξιοποιείται. Το όριο οικονομικής ευθύνης θα πρέπει να αναγράφεται στα στοιχεία του πιστοποιητικού.

Σε περίπτωση που τα προβλήματα που δημιουργούνται δεν οφείλονται σε δική υπαιτιότητα της ΥΔΚ, δε φέρει καμία οικονομική ευθύνη και συνεπώς δε θα πρέπει να δίνονται αποζημιώσεις.

Σε κάθε περίπτωση, θα πρέπει να διευκρινιστεί ότι εάν οι ΥΔΚ είναι ιδιωτικοί φορείς ισχύουν τα παραπάνω, ενώ εάν πρόκειται για δημόσιο φορέα ισχύουν οι ρυθμίσεις που αφορούν την αστική ευθύνη του Δημοσίου (άρθρο 105 Εισαγωγικού Νόμου ΑΚ, λαμβανομένης υπόψη της σχετικής νομολογίας).

13.1.5.3.3 Εγγυήσεις

Οι πάροχοι ΥΔΚ οφείλουν να προσδιορίσουν συγκεκριμένες εγγυήσεις για την ακρίβεια των δεδομένων που διαχειρίζονται. Για παράδειγμα, θα μπορούσε η ακρίβεια των στοιχείων Αριθμών Φορολογικών Μητρώου που αξιοποιούνται από την ΥΔΚ να επιβεβαιώνονται από το Υπουργείο Οικονομίας και Οικονομικών. Επιπλέον θα πρέπει να προσδιορίσουν και τις περιπτώσεις εκείνες όπου οι εγγυήσεις αυτές δεν εφαρμόζονται.

13.1.5.3.4 Θέματα δημοσιοποίησης ψηφιακών πιστοποιητικών

Η ΥΔΚ θα πρέπει να δημοσιοποιεί όλες εκείνες τις πληροφορίες που αφορούν θέματα διαχείρισης των ψηφιακών πιστοποιητικών. Συγκεκριμένα:

- τις πρακτικές που ακολουθούν σε συνδυασμό με την αντίστοιχη πολιτική πιστοποιητικών
- τα πιστοποιητικά και την τρέχουσα κατάστασή τους
- τη συχνότητα ανανέωσης των δημόσιων πληροφοριών που ορίζονται σε αυτήν την ενότητα

- την έγκυρη Λίστα Ανάκλησης Πιστοποιητικών
- το πρωτόκολλο που μπορούν να αξιοποιούν οι χρήστες για τον έλεγχο της εγκυρότητας ενός συγκεκριμένου πιστοποιητικού (προτείνεται η αξιοποίηση του πρωτοκόλλου OSCP).
- τις μεθόδους που χρησιμοποιούνται για πρόσβαση στις παραπάνω πληροφορίες.

13.1.5.3.5 Πολιτική Εμπιστευτικότητας

Οι πληροφορίες που θεωρούνται εμπιστευτικές κατά τη λειτουργία της ΥΔΚ είναι οι ακόλουθες:

- Ιδιωτικά κλειδιά Αρχής Πιστοποίησης και Αρχής Εγγραφής
- Ιδιωτικά κλειδιά κρυπτογράφησης που αποθηκεύονται στην Αρχή Πιστοποίησης
- Τα πιστοποιητικά και δεδομένα που συλλέγονται από την Αρχή Εγγραφής για την ταυτοποίηση του χρήστη και για την έκδοση του αντίστοιχου πιστοποιητικού

Σε κάθε περίπτωση η ΥΔΚ θα πρέπει να τηρεί τη σχετική νομοθεσία περί προστασίας των προσωπικών δεδομένων. Θα πρέπει να σημειωθεί ότι τα δεδομένα που 'εμφανίζονται' στα πιστοποιητικά των χρηστών και στους δημόσιους καταλόγους της ΥΔΚ δεν θεωρούνται εμπιστευτικά.

Οι Αρχές εγγραφής και Πιστοποίησης παρέχουν εμπιστευτικές πληροφορίες σύμφωνα με το Νόμο και κατόπιν εισαγγελικής παραγγελίας.

13.1.5.3.6 Μέθοδοι Επίλυσης διαφορών

Οι ΥΔΚ θα πρέπει να προσδιορίζουν τις μεθόδους επίλυσης διαφορών που προκύπτουν μεταξύ των εμπλεκόμενων οντοτήτων, έχοντας ως βάση σε κάθε περίπτωση την ισχύουσα νομοθεσία.

13.1.5.3.7 Μέθοδοι Εγγραφής, Ταυτοποίησης και Αυθεντικοποίησης των χρηστών πριν την έκδοση ενός ψηφιακού πιστοποιητικού

13.1.5.3.7.1 Πρότυπο Καταγραφής στοιχείων

Οι Αρχές Εγγραφής θα καταγράφουν ή θα μετατρέπουν τα απαραίτητα στοιχεία για την έκδοση ενός πιστοποιητικού με βάση το πρότυπο του ΕΛΟΤ για απόδοση ελληνικών ονομάτων στην αγγλική γλώσσα.

13.1.5.3.7.2 Ταυτοποίηση και Αυθεντικοποίηση Χρηστών

Η ταυτοποίηση και αυθεντικοποίηση των χρηστών κατά την αρχική τους αίτηση για έκδοση ενός ψηφιακού πιστοποιητικού θα πρέπει να πραγματοποιείται σύμφωνα με τις διαδικασίες που ορίζονται για ηλεκτρονικές υπηρεσίες επιπέδου εμπιστοσύνης 3 (βλέπε ενότητα 8).

13.1.5.3.8 Χρεώσεις

Οι ΥΔΚ θα πρέπει να προσδιορίζουν στην αντίστοιχη ενότητα την πολιτική και εφόσον απαιτείται τα ακόλουθα:

- χρεώσεις έκδοσης/ ανανέωσης πιστοποιητικού
- χρεώσεις πρόσβασης στους δημόσιους καταλόγους
- χρεώσεις ανάκλησης πιστοποιητικού
- χρεώσεις επιπρόσθετων υπηρεσιών

13.1.6 Κατηγορίες Ψηφιακών Πιστοποιητικών

Οι διαφορετικές κατηγορίες ψηφιακών πιστοποιητικών, που μπορούν να αξιοποιηθούν από τους τελικούς χρήστες (βλέπε ενότητα 13.1.5.2.3) για υπηρεσίες ηλεκτρονικής διακυβέρνησης Επιπέδου Εμπιστοσύνης 3, είναι:

- Ψηφιακό πιστοποιητικό για ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων και εγγράφων
- Ψηφιακό πιστοποιητικό για κρυπτογράφηση ηλεκτρονικών μηνυμάτων ή εγγράφων

Τα πιστοποιητικά τελικών χρηστών που ορίζονται ανωτέρω πρέπει να χρησιμοποιούνται αποκλειστικά στο πλαίσιο της εγγραφής των χρηστών και της αξιοποίησης ηλεκτρονικών υπηρεσιών της Δημόσιας Διοίκησης, σύμφωνα με τα οριζόμενα στην ενότητα 13.1.6.3 (επιτρεπτές χρήσεις πιστοποιητικών).

Να τονιστεί ότι τα πιστοποιητικά για ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων και εγγράφων μπορούν να αξιοποιηθούν και από τους Δημόσιους Φορείς. Παρόλα αυτά, δεδομένης της ένταξης όλων των Δημόσιων φορέων στο έργο «Σύζευξις», της Υποδομής Δημόσιου Κλειδιού που έχει αναπτυχθεί για το έργο αυτό και της ιεραρχικής δομής των Υποκειμένων Αρχών Πιστοποίησης υπό την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), δε συντρέχει ανάγκη προσδιορισμού Πολιτικών Πιστοποιητικών για τα ψηφιακά πιστοποιητικά Δημόσιου Φορέα, αφού αυτές υιοθετούνται ως έχουν. Οι διεργασίες που επιτελούν οι Δημόσιοι Φορείς στο ΠΨΑ, συμπεριλαμβανομένης και της ΚΔΠ, περιορίζονται στην ψηφιακή υπογραφή δεδομένων και εγγράφων. Υπενθυμίζεται ότι ο κανονισμός πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) στην §1.2.1.1 αναφέρει: «Η Πολιτική Πιστοποίησης 1 (ΠΠ 1) αναφέρεται σε Αναγνωρισμένα Πιστοποιητικά τελικών χρηστών. Τα πιστοποιητικά που εκδίδονται βάσει της ΠΠ 1 χρησιμοποιούνται για ψηφιακή υπογραφή (προηγμένη ηλεκτρονική υπογραφή) ηλεκτρονικών μηνυμάτων ή εγγράφων». Στον ίδιο κανονισμό, στην §1.4.3 αναφέρεται ότι: «Ως Τελικοί Χρήστες νοούνται τα φυσικά πρόσωπα, κάτοχοι πιστοποιητικών σύμφωνα με τις διατάξεις του παρόντος που έχουν συγκεκριμένη αρμοδιότητα στο πλαίσιο άσκησης των καθηκόντων τους και στη συγκεκριμένη οργανική μονάδα στην οποία υπηρετούν».

13.1.6.1 Προφίλ Ψηφιακών Πιστοποιητικών

Τα ψηφιακά πιστοποιητικά που θα αξιοποιηθούν στις υπηρεσίες ηλεκτρονικής διακυβέρνησης περιλαμβάνουν τα βασικά πεδία που απαιτούνται για αναγνωρισμένα πιστοποιητικά, σύμφωνα με το Π.Δ 150/2001, και είναι τύπου X509 v3.

Πεδίο
Έκδοση (Version)
Αριθμός Σειράς (Serial Number)
Αλγόριθμος Υπογραφής (Signature Algorithm)
Διακριτικό Όνομα Εκδότη (Issuer DN)
Ισχύει Από (Valid From)
Ισχύει Μέχρι (Valid To)
Διακριτικό Όνομα Υποκειμένου (Subject DN)
Δημόσιο Κλειδί Υποκειμένου (Subject Public Key)
Υπογραφή (Signature)

Πίνακας 20: Βασικά Πεδία Προφίλ Πιστοποιητικού

13.1.6.1.1 Αναλυτική περιγραφή πεδίων

- Έκδοση (Version): αναφέρεται στην έκδοση του προτύπου X.509 πιστοποιητικών και υποστηρίζει εκτεταμένα πεδία.
- Αριθμός Σειράς (Serial Number): αποτελείται από το μοναδικό αριθμό του εκδιδόμενου πιστοποιητικού, ο οποίος καθορίζεται από τον εκδότη των πιστοποιητικών με σκοπό τη διάκριση του πιστοποιητικού.
- Αλγόριθμός Υπογραφής (Signature Algorithm): αναφέρεται στον αλγόριθμο σύνοψης (Hash Function) που θα αξιοποιείται από την ΥΔΚ. Προτείνεται η αξιοποίηση αλγορίθμων της οικογενείας SHA (π.χ. SHA-256) σε συνδυασμό με τον αλγόριθμο RSA.
- Διακριτικό Όνομα Εκδότη (Issuer DN): αναφέρεται στο όνομα του εκδότη του πιστοποιητικού και αποτελείται από τα υπό-πεδία Χώρα (Country), Οργανισμός (Organization), Κοινό Όνομα (Common Name) και Ηλεκτρονική Διεύθυνση (E-mail Address). Τα παραπάνω πεδία πλην της Ηλεκτρονικής Διεύθυνσης (E-mail Address) είναι υποχρεωτικά.
- Ισχύει Από (Valid From): περιλαμβάνει την ημερομηνία έκδοσης του πιστοποιητικού.
- Ισχύει Μέχρι (Valid To): περιλαμβάνει την ημερομηνία λήξης του πιστοποιητικού.
- Διακριτικό Όνομα Υποκειμένου (Subject DN): Αναφέρεται στον κάτοχο του πιστοποιητικού και αποτελείται από τα υπό-πεδία Χώρα (Country), Οργανισμός (Organization), Κοινό Όνομα (Common Name) και Ηλεκτρονική Διεύθυνση (E-mail

Address). Τα παραπάνω πεδία πλην της Ηλεκτρονικής Διεύθυνσης (E-mail Address) είναι υποχρεωτικά. Συγκεκριμένα, σύμφωνα με το RFC 3280, η χρήση της ηλεκτρονικής διεύθυνσης στο συγκεκριμένο πεδίο προτείνεται μόνο σε περιπτώσεις που απαιτείται συμβατότητα με προϋπάρχουσες υπηρεσίες και εφαρμογές.

Με στόχο την εξασφάλιση της μοναδικότητας του Διακριτικού Ονόματος Υποκειμένου ανά Πάροχο Υπηρεσιών Πιστοποίησης και συνεπώς τη διευκόλυνση της διαχείρισης των πιστοποιητικών, την προώθηση της διαλειτουργικότητας και την ομοιομορφία στη διαδικασία αυθεντικοποίησης που ακολουθούν οι πάροχοι των υπηρεσιών, προτείνεται η υιοθέτηση ενός «Κωδικού Διαχείρισης Πιστοποιητικού» ως μέρος του Διακριτικού Ονόματος του Υποκειμένου και συγκεκριμένα του Κοινού Ονόματος (Common Name). Ο κωδικός αυτός προτείνεται να δημιουργείται από ένα αριθμητικό μέρος (π.χ. αύξων αριθμός) και κάποιο χαρακτηριστικό του κατόχου (π.χ. αρχικά του ονόματός του). Ο συνδυασμός των πεδίων «Οργανισμός» (που αποτυπώνει τον πάροχο υπηρεσιών πιστοποίησης) και «Κοινό Όνομα» (που αποτυπώνει τον προαναφερόμενο κωδικό διαχείρισης πιστοποιητικού) πρέπει να είναι μοναδικός. Εξυπακούεται ότι το Διακριτικό Όνομα Υποκειμένου, και συνεπώς και τα πεδία «Οργανισμός» και «Κοινό Όνομα» για τα οποία γίνεται λόγος, πρέπει να είναι τα ίδια για το σύνολο των πιστοποιητικών που εκδίδονται για το συγκεκριμένο πρόσωπο από το συγκεκριμένο ΠΥΠ, ώστε κάθε φορέας να μπορεί να τα αξιοποιήσει για να συνδέσει τα πιστοποιητικά του χρήστη με τα στοιχεία που διατηρεί γι' αυτόν στο σύστημά του.

Θα πρέπει να τονιστεί ότι για τον προαναφερόμενο Κωδικό Διαχείρισης Πιστοποιητικών θα πρέπει να εξασφαλιστεί ότι:

- τηρούνται οι προϋποθέσεις της σχετικής νομοθεσίας σχετικά με τη διασύνδεση αρχείων που περιέχουν προσωπικά δεδομένα (άρθρο 8 του ν. 2472/97)
- δεν δημιουργούνται κατ' αποτέλεσμα οι προϋποθέσεις για χρήση μοναδικού αναγνωριστικού αριθμού – εφόσον δεν υπάρχει αντίστοιχο νομικό υπόβαθρο
- η χρήση του αποσκοπεί ή/και περιορίζεται στην εκπλήρωση του σκοπού επεξεργασίας και δεν εκτείνεται σε άλλους σκοπούς που δεν αφορούν την ταυτοποίηση/ψηφιακή αυθεντικοποίηση του χρήστη της συγκεκριμένης αιτούμενης υπηρεσίας, εφόσον δεν υπάρχει αυτοτελής νόμιμη βάση (όπως π.χ. συγκατάθεση του χρήστη, ρητή διάταξη νόμου, υπέρτερο συμφέρον).

- Δημόσιο Κλειδί Υποκειμένου (Subject Public Key): αποτελείται από το Δημόσιο Κλειδί του Υποκειμένου (Ιδιοκτήτη του ψηφιακού πιστοποιητικού).
- Υπογραφή (Signature): αποτελείται από την ψηφιακή υπογραφή του εκδότη του ψηφιακού πιστοποιητικού.

13.1.6.2 Επεκτάσεις Ψηφιακών Πιστοποιητικών

Τα ψηφιακά πιστοποιητικά X.509 ver.3 των χρηστών που θα μπορούν να αξιοποιηθούν σε υπηρεσίες ηλεκτρονικής διακυβέρνησης Επιπέδου Εμπιστοσύνης 3, θα είναι σύμφωνα με όσα

περιλαμβάνονται στο *RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* και θα περιλαμβάνουν τις ακόλουθες επεκτάσεις:

- Χρήση Κλειδιού (Key Usage): αναφέρεται ποια θα είναι η χρήση του δημόσιου κλειδιού που περιλαμβάνεται στο ψηφιακό πιστοποιητικό.
    - Για επαλήθευση Ψηφιακής Υπογραφής ηλεκτρονικών μηνυμάτων ή εγγράφων τα πεδία «digitalSignature» και «nonRepudiation» ορίζονται.
    - Για Κρυπτογράφηση ηλεκτρονικών μηνυμάτων ή εγγράφων τα πεδία «dataEncipherment» και «keyEncipherment» ορίζονται.
- Εναλλακτικό Όνομα Υποκειμένου (Subject Alternative Name): περιλαμβάνεται ένα εναλλακτικό όνομα για τον κάτοχο του ψηφιακού πιστοποιητικού. Δεδομένης της ταυτόχρονης ύπαρξης του πεδίου *Διακριτικό Όνομα Υποκειμένου (Subject DN)*, συνάγεται ότι στο παρόν πεδίο θα μπορούσε να περιληφθεί σχετικό αναγνωριστικό του ιδιοκτήτη για ηλεκτρονικές υπηρεσίες (π.χ. ΑΦΜ) ή οποιαδήποτε άλλη πληροφορία του τελικού χρήστη που κρίνεται σκόπιμη από την αντίστοιχη υπηρεσία, όπως για παράδειγμα η ηλεκτρονική διεύθυνσή του (e-mail address). Με τον τρόπο αυτό θα μπορούσε να επιτευχθεί αξιοποίηση των σχετικών στοιχείων, στην κατεύθυνση της βελτίωσης της ευελιξίας και διαλειτουργικότητας με υπό ανάπτυξη και με λειτουργούντα πληροφοριακά συστήματα. Σημειώνεται, όμως, ότι η χρήση των αναγνωριστικών αυτών είναι νόμιμη, εφόσον – και στο βαθμό που:
    - τηρούνται οι προϋποθέσεις της σχετικής νομοθεσίας σχετικά με τη διασύνδεση αρχείων που περιέχουν προσωπικά δεδομένα (άρθρο 8 του ν. 2472/97)
    - δεν δημιουργούνται κατ' αποτέλεσμα οι προϋποθέσεις για χρήση μοναδικού αναγνωριστικού αριθμού – εφόσον δεν υπάρχει αντίστοιχο νομικό υπόβαθρο
    - η χρήση των αναγνωριστικών αποσκοπεί ή/και περιορίζεται στην εκπλήρωση του σκοπού επεξεργασίας και δεν εκτείνεται σε άλλους σκοπούς που δεν αφορούν την ταυτοποίηση/ψηφιακή αυθεντικοποίηση του χρήστη της συγκεκριμένης αιτούμενης υπηρεσίας, εφόσον δεν υπάρχει αυτοτελής νόμιμη βάση (όπως π.χ. συγκατάθεση του χρήστη, ρητή διάταξη νόμου, υπέρτερο συμφέρον)
- Ταυτοποίηση Χρήστη (Clientauth): αναφέρει εάν το συγκεκριμένο πιστοποιητικό μπορεί να χρησιμοποιηθεί για την ταυτοποίηση του χρήστη. Στα ψηφιακά πιστοποιητικά για ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων ή εγγράφων το συγκεκριμένο πεδίο ορίζεται (set), ενώ στα ψηφιακά πιστοποιητικά για κρυπτογράφηση ηλεκτρονικών μηνυμάτων ή εγγράφων το πεδίο δεν ορίζεται.
- Σημεία Διανομής Καταλόγου Ανακληθέντων Πιστοποιητικών (CRL distribution List): αναφέρονται τα σημεία διανομής της Λίστας Ανακληθέντων Πιστοποιητικών, σε μορφή URL διεύθυνσης.

- Πολιτικές Πιστοποιητικού (Certificate Policies): αναφέρεται το σημείο εύρεσης του κειμένου των Πολιτικών που διέπουν το ψηφιακό πιστοποιητικό, σε μορφή URL διεύθυνσης.

Κάθε ΥΔΚ θα προκαθορίζει τις επιτρεπτές και μη χρήσεις στην Πολιτική Πιστοποιητικών, με βάση τις ανάγκες που δημιουργούνται από το περιβάλλον εφαρμογής, σε περιπτώσεις που δεν καλύπτονται από το παρόν πλαίσιο.

Θα πρέπει να σημειωθεί ότι για την ενσωμάτωση πιστοποιητικών άλλου τύπου θα πρέπει να προσδιοριστούν οι επιτρεπτές και μη χρήσεις αυτών από τον πάροχο της αντίστοιχης ΥΔΚ. Επιπλέον, στην προσδιοριζόμενη Πολιτική Πιστοποιητικών θα πρέπει να ορίζεται εάν το υποκείμενο που αξιοποιεί το αντίστοιχο πιστοποιητικό είναι εξυπηρετητής ή χρήστης και να προσδιορίσει τα αντίστοιχα στοιχεία.

	Ψηφιακό πιστοποιητικό τελικού χρήστη επίπεδου εμπιστοσύνης 3 για *ψηφιακή υπογραφή* ηλεκτρονικών μηνυμάτων και εγγράφων	Ψηφιακό πιστοποιητικό τελικού χρήστη επιπέδου εμπιστοσύνης 3 για *κρυπτογράφηση* ηλεκτρονικών μηνυμάτων ή εγγράφων
Κρισιμότητα (critical)	Μη ορισμένο	Μη ορισμένο
Ψηφιακή Υπογραφή (digitalSignature)	Ορισμένο	Μη Ορισμένο
Μη αποποίηση (nonRepudiation)	Ορισμένο	Μη ορισμένο
Κρυπτογράφηση Κλειδιού (keyEncipherment)	Μη Ορισμένο	Ορισμένο
Κρυπτογράφηση Δεδομένων (dataEncipherment)	Μη Ορισμένο	Ορισμένο
Συμφωνία Δεδομένων (keyAgreement)	Μη Ορισμένο	Μη Ορισμένο
Κλειδί Υπογραφής Πιστοποιητικού (keyCertSign)	Μη Ορισμένο	Μη Ορισμένο
Υπογραφή Καταλόγου Ανακληθέντων Πιστοποιητικών (cRLSign)	Μη Ορισμένο	Μη Ορισμένο
(Μόνο Κρυπτογράφηση) (encipherOnly)	Μη Ορισμένο	Μη Ορισμένο
(Μόνο αποκρυπτογράφηση) (decipherOnly)	Μη Ορισμένο	Μη Ορισμένο

Πίνακας 21: Ρυθμίσεις Επέκτασης Χρήσης Κλειδιού

13.1.6.3 Επιτρεπτές Χρήσεις των ψηφιακών πιστοποιητικών

13.1.6.3.1 Ψηφιακό πιστοποιητικό κρυπτογράφησης

- Για τη διασφάλιση της εμπιστευτικότητας σε κάθε είδους ηλεκτρονική υπηρεσία της Δημόσιας Διοίκησης, επιπέδου εμπιστοσύνης 3, που προσφέρεται μέσω της ΚΔΠ.

Να τονιστεί ότι η χρήση του πιστοποιητικού «απαιτείται» μόνο στο πλαίσιο υπηρεσιών που έχουν ενταχθεί σε επίπεδο εμπιστοσύνης 3. Παρόλα αυτά, αν ο φορέας το επιλέξει, το πιστοποιητικό μπορεί να αξιοποιηθεί, επιπλέον, και για υπηρεσίες που έχουν ενταχθεί στα χαμηλότερα επίπεδα εμπιστοσύνης 1 και 2.

13.1.6.3.2 Ψηφιακό πιστοποιητικό ψηφιακής υπογραφής

- Για ταυτοποίηση και αυθεντικοποίηση του υποκειμένου σε κάθε είδους ηλεκτρονική υπηρεσία της Δημόσιας Διοίκησης, επιπέδου εμπιστοσύνης 3, που προσφέρεται μέσω της ΚΔΠ.
- Για δημιουργία ψηφιακών υπογραφών σε κάθε είδους ηλεκτρονική υπηρεσία της Δημόσιας Διοίκησης, επιπέδου εμπιστοσύνης 3, που προσφέρεται μέσω της ΚΔΠ.

Να τονιστεί ότι η χρήση του πιστοποιητικού «απαιτείται» μόνο στο πλαίσιο υπηρεσιών που έχουν ενταχθεί σε επίπεδο εμπιστοσύνης 3. Παρόλα αυτά, αν ο φορέας το επιλέξει, το πιστοποιητικό μπορεί να αξιοποιηθεί, επιπλέον, και για υπηρεσίες που έχουν ενταχθεί στα χαμηλότερα επίπεδα εμπιστοσύνης 1 και 2.

13.1.6.4 Μη επιτρεπτές Χρήσεις των ψηφιακών πιστοποιητικών

13.1.6.4.1 Ψηφιακό πιστοποιητικό κρυπτογράφησης

- Για συναλλαγές που δεν ορίζονται ρητά στην ενότητα Επιτρεπτές Χρήσεις Ψηφιακού πιστοποιητικού κρυπτογράφησης (βλέπε ενότητα 13.1.6.3.1).

13.1.6.4.2 Ψηφιακό πιστοποιητικό ψηφιακής υπογραφής

- Για συναλλαγές που δεν ορίζονται ρητά στην ενότητα Επιτρεπτές Χρήσεις Ψηφιακού πιστοποιητικού ψηφιακής υπογραφής (βλέπε ενότητα 13.1.6.3.2).

13.1.7 Απαιτήσεις Λειτουργίας

Σε αυτή την ενότητα περιγράφονται οι απαιτήσεις που πρέπει να καλύπτουν οι Αρχές Πιστοποίησης και παρουσιάζονται στην αντίστοιχη ενότητα Πολιτικής Πιστοποιητικών, όσον αφορά στις διαδικασίες που πρέπει να ακολουθούνται κατά τη διάρκεια λειτουργίας μιας Αρχής Πιστοποίησης.

13.1.7.1 Θέματα επικοινωνίας μεταξύ των οντοτήτων ΥΔΚ

Οι επικοινωνίες που πραγματοποιούνται μεταξύ Αρχής Εγγραφής και Αρχής Πιστοποίησης πρέπει να διασφαλίζουν απαιτήσεις εμπιστευτικότητας και ακεραιότητας, αξιοποιώντας οποιοδήποτε πρωτόκολλο ή μηχανισμό που παρέχει σχετικές υπηρεσίες, όπως SSL ή IPsec ή S/MIME. Επιπλέον, στην περίπτωση που ένας χρήστης επικοινωνεί με την Αρχή Πιστοποίησης θα πρέπει να διασφαλίζεται υποχρεωτικά η ακεραιότητα και εμπιστευτικότητα των ανταλλασσόμενων μηνυμάτων.

13.1.7.2 Διαχείριση Κλειδιών

13.1.7.2.1 Δημιουργία κλειδιών

13.1.7.2.1.1 Οντότητες Δημιουργίας Κλειδιών

Οι οντότητες που επιφορτίζονται με τη δημιουργία του ζεύγους κλειδιών προσδιορίζονται από την ΥΔΚ.

13.1.7.2.1.2 Μήκος κλειδιών

Το μήκος των κλειδιών που εκδίδονται για τους χρήστες θα πρέπει να είναι τουλάχιστον 1024 bits. Το μέγεθος μπορεί να απαιτηθεί να είναι ακόμη μεγαλύτερο, ανάλογα με τις εξελίξεις στα επιστημονικά δρώμενα στη γνωστική περιοχή της κρυπτολογίας.

13.1.7.2.1.3 Παράμετροι Ασφάλειας

Τα κλειδιά θα πρέπει να δημιουργούνται με την αξιοποίηση ορθών παραμέτρων, με στόχο την επίτευξη δημιουργίας ασφαλών κλειδιών.

13.1.7.2.1.4 Μέθοδοι δημιουργίας των κλειδιών ψηφιακής υπογραφής

Τα ζεύγη κλειδιών, τα οποία θα αξιοποιούνται για την ψηφιακή υπογραφή, θα δημιουργούνται αποκλειστικά και μόνο από τους τελικούς χρήστες κάνοντας χρήση ασφαλών διατάξεων, συμβατών με τις σχετικές απαιτήσεις του προεδρικού διατάγματος Π.Δ. 150/2001, που τους έχουν χορηγηθεί κατά τη διαδικασία εγγραφής σε υπηρεσίες εμπιστοσύνης επιπέδου 3. Στην περίπτωση δημιουργίας πιστοποιητικών χαλαρής αποθήκευσης, ο πάροχος υπηρεσιών δημοσίου κλειδιού θα πρέπει να παρέχει στους χρήστες το κατάλληλο λογισμικό για τη δημιουργία των κλειδιών ψηφιακής υπογραφής. Για τη δημιουργία του ζεύγους κλειδιών θα αξιοποιούνται οι κατάλληλοι κωδικοί πρόσβασης. Καμία οντότητα δεν θα δύναται να δημιουργήσει κλειδιά ψηφιακής υπογραφής για λογαριασμό κάποιου χρήστη.

13.1.7.2.1.5 Μέθοδοι δημιουργίας των κλειδιών κρυπτογράφησης

Τα ζεύγη κλειδιών κρυπτογράφησης θα δημιουργούνται κεντρικοποιημένα από την Αρχή Πιστοποίησης, αξιοποιώντας ασφαλείς διατάξεις, συμβατές με τις σχετικές απαιτήσεις του προεδρικού διατάγματος Π.Δ. 150/2001, οι οποίες θα αποθηκεύουν τα ζεύγη κλειδιών τόσο στις ασφαλείς διατάξεις των χρηστών όσο και σε αντίστοιχες εφεδρικές συσκευές. Θα πρέπει

να σημειωθεί ότι η εξαγωγή των κλειδιών από τις συσκευές αυτές θα μπορεί να γίνει μόνο από αποκλειστικά εξουσιοδοτημένες οντότητες. Να τονιστεί ότι για τους δημόσιους υπαλλήλους, χρήστες του ΣΥΖΕΥΞΙΣ, προβλέπεται ρητά η δημιουργία και αποθήκευση των ιδιωτικών κλειδιών αποκρυπτογράφησης εκτός του διακριτικού αποθήκευσης, για αντιμετώπιση προβλημάτων σε περιπτώσεις απώλειας. Όσον αφορά στους ιδιώτες, μπορεί να παραμένει στη διακριτική τους ευχέρεια η επιλογή, είτε για ενδεχόμενη κεντρική δημιουργία και αποθήκευση, είτε για δημιουργία στην πλευρά του χρήστη, με βάση πάντοτε το ως άνω σκεπτικό.

13.1.7.2.1.6 Τρόποι αξιοποίησης των κλειδιών

Τα κλειδιά που δημιουργούνται και διαμοιράζονται στους χρήστες θα πρέπει να αξιοποιούνται σύμφωνα με τα όσα προδιαγράφονται στην ενότητα «Επιτρεπτές χρήσεις των ψηφιακών πιστοποιητικών» (βλέπε ενότητα 13.1.6.3).

13.1.7.2.1.7 Δίαυλοι μεταφοράς των ιδιωτικών κλειδιών κρυπτογράφησης στον κάτοχό τους

Τα ιδιωτικά κλειδιά κρυπτογράφησης του χρήστη θα παραδίδονται στον κάτοχό τους αποθηκευμένα σε ασφαλή διάταξη, σύμφωνα με όσα προβλέπονται από το επίπεδο εγγραφής 3. Σε περίπτωση που δε γίνεται χρήση ασφαλούς διάταξης, τα κλειδιά θα παραδίδονται στον κάτοχό τους σε φορητό μέσο αποθήκευσης (π.χ. ψηφιακό δίσκο) είτε ηλεκτρονικά με την χρήση του προτύπου PKCS#12 μέσω ασφαλούς διαύλου επικοινωνίας. Σε κάθε περίπτωση, τα μεταφερόμενα κλειδιά θα πρέπει να προστατεύονται με κωδικό, ο οποίος θα παραδίδεται στο χρήστη σύμφωνα με τα προβλεπόμενα στο επίπεδο εγγραφής 3. Σε περίπτωση ανανέωσης των κρυπτογραφικών κλειδιών, βλέπε ενότητες 13.1.7.2.3.5 και 13.1.7.3.6.3.

13.1.7.2.1.8 Τρόποι παροχής του δημοσίου κλειδιού στην Αρχή Πιστοποίησης

Το δημόσιο κλειδί, που αξιοποιείται στη διαδικασία της κρυπτογράφησης, βρίσκεται στη διάθεση της Αρχής Πιστοποίησης, καθώς τα κλειδιά αυτά δημιουργούνται κεντρικά, ενώ το δημόσιο κλειδί για την επαλήθευση της ψηφιακής υπογραφής αποθηκεύεται στην Αρχή Πιστοποίησης με την έκδοση του αντίστοιχου ψηφιακού πιστοποιητικού, το οποίο και συμπεριλαμβάνεται στην αντίστοιχη αίτηση έκδοσης πιστοποιητικού μορφής PKCS#10.

13.1.7.2.1.9 Μηχανισμοί και πρότυπα που αξιοποιούνται για τη δημιουργία των κλειδιών

Οι διατάξεις που χρησιμοποιούνται για τη δημιουργία του ζεύγους κλειδιών θα πρέπει να τηρούν πλήρως τις προϋποθέσεις που ορίζονται στο Π.Δ. 150/2001 προκειμένου να χαρακτηρίζονται ως «ασφαλείς». Ως εκ τούτου όλες οι συσκευές που αξιοποιούνται για την δημιουργία των κλειδιών θα πρέπει κατ' ελάχιστο να ακολουθούν τις προδιαγραφές FIPS 140-2 επιπέδου 3, είτε να είναι πιστοποιημένες σε CC EAL4.

13.1.7.2.2 Ανάκληση Κλειδιών

13.1.7.2.2.1 Περιπτώσεις ανάκλησης κλειδιών αυτομάτως από την Αρχή Πιστοποίησης

Η Αρχή Πιστοποίησης έχει τη δυνατότητα ανάκλησης των πιστοποιητικών στις ακόλουθες περιπτώσεις:

- Λήξη του πιστοποιητικού του χρήστη όπως αυτή ορίζεται στο πεδίο Valid to, του βασικού προφίλ πιστοποιητικού
- Μη συμμόρφωση του χρήστη με την παρούσα πολιτική
- Διακύβευση του ιδιωτικού κλειδιού
- Απώλεια της ασφαλούς διάταξης αποθήκευσης των κλειδιών
- Τερματισμός λειτουργίας της Αρχής Πιστοποίησης

13.1.7.2.2.2 Οντότητες ανάκλησης κλειδιών

Οι οντότητες που επιφορτίζονται τη διαδικασία ανάκλησης κλειδιών καθορίζονται από την εκάστοτε ΥΔΚ.

13.1.7.2.2.3 Οντότητες που μπορούν να αιτηθούν την ανάκληση κλειδιών

Οι οντότητες που μπορούν να αιτηθούν την ανάκληση των πιστοποιητικών είναι:

- Οι Χρήστες των ψηφιακών πιστοποιητικών
    - κάθε φυσικό πρόσωπο
    - κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου ιδιωτικού δικαίου
    - κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου δημοσίου δικαίου
- Η Αρχή Πιστοποίησης

13.1.7.2.2.4 Μέθοδοι ανάκλησης ζεύγους κλειδιών

Τα ζεύγη κλειδιών θα διαγράφονται από το διακριτικό στο οποίο αποθηκεύονται, εφόσον γίνεται αποδεκτή η αίτηση ανάκλησης.

13.1.7.2.2.5 Διαδικασία ανάκλησης κλειδιών

Οι οντότητες που επιθυμούν να ανακαλέσουν ένα ζεύγος κλειδιών θα πρέπει να χρησιμοποιήσουν την κατάλληλη υπηρεσία ανάκλησης στα πλαίσια της οποίας θα συμπληρώσουν αίτηση, θα την υπογράψουν ψηφιακά και θα την υποβάλλουν ηλεκτρονικά, εφόσον βέβαια είναι ενεργό το διακριτικό αποθήκευσης. Σε διαφορετική περίπτωση ο χρήστης θα πρέπει να μεταβεί αυτοπροσώπως στην Αρχή Εγγραφής και να υποβάλει την αίτηση

ανάκλησης. Αφού διαπιστωθεί η εγκυρότητα των στοιχείων από την Αρχή Εγγραφής, η αίτηση προωθείται στην Αρχή Πιστοποίησης για περαιτέρω επεξεργασία και την τελική ανάκληση των κλειδιών, με τη διαγραφή τους από το διακριτικό αποθήκευσης, την ανάκληση των αντίστοιχων πιστοποιητικών, καθώς και την ενημέρωση της λίστας ανακλημένων πιστοποιητικών.

13.1.7.2.2.6 Μέθοδοι αυθεντικοποίησης οντοτήτων που αιτούνται την ανάκληση κλειδιών

Οι οντότητες που αιτούνται την ανάκληση κλειδιών είναι δυνατόν να αυθεντικοποιηθούν μέσω της ισχύουσας ηλεκτρονικής υποδομής αυθεντικοποίησης, όπως αυτή προσδιορίζεται για το επίπεδο εμπιστοσύνης 3, είτε με τη φυσική παρουσία τους στην Αρχή Εγγραφής ή την Αρχή Πιστοποίησης.

13.1.7.2.3 Επαναδημιουργία – Ανανέωση Κλειδιού

13.1.7.2.3.1 Περιπτώσεις επαναδημιουργίας – ανανέωσης κλειδιού κρυπτογράφησης

Η ανανέωση-επαναδημιουργία των κλειδιών κρυπτογράφησης μπορεί να πραγματοποιηθεί για μη ανακλημένα πιστοποιητικά στις ακόλουθες περιπτώσεις:

1. Απώλεια του Διακριτικού Αποθήκευσης των κλειδιών
2. Αστοχία υλικού στο διακριτικό αποθήκευσης των κλειδιών (μοναδική περίπτωση επαναδημιουργίας)
3. Δημοσίευση επιθέσεων οι οποίες επηρεάζουν τα υπάρχοντα ζεύγη κλειδιών
4. Καθιερωμένη ανανέωση κλειδιών πριν τη λήξη του πιστοποιητικού

13.1.7.2.3.2 Περιπτώσεις επαναδημιουργίας – ανανέωσης κλειδιού ψηφιακής υπογραφής

Σε καμία περίπτωση δεν θα πρέπει να πραγματοποιείται επαναδημιουργία (ίδιων) κλειδιών ψηφιακής υπογραφής. Η ανανέωση του ζεύγους κλειδιών για την ψηφιακή υπογραφή γίνεται είτε λόγω λήξης του πιστοποιητικού είτε λόγω δημοσίευσης επιθέσεων που επηρεάζουν τα υπάρχοντα ζεύγη κλειδιών. Ουσιαστικά, ως ανανέωση του ζεύγους κλειδιών νοείται η έκδοση νέου ζεύγους κλειδιών ψηφιακής υπογραφής.

13.1.7.2.3.3 Οντότητες επαναδημιουργίας - ανανέωσης Ζεύγους Κλειδιών

Οι οντότητες που επιφορτίζονται τη διαδικασία επαναδημιουργίας-ανανέωσης ζεύγους κλειδιών καθορίζονται από την ΥΔΚ.

13.1.7.2.3.4 Αυθεντικοποίηση οντοτήτων που αιτούνται την ανανέωση κλειδιών και πιστοποιητικών

Οι οντότητες που αιτούνται την ανανέωση κλειδιών είναι δυνατό να αυθεντικοποιηθούν με την αξιοποίηση της υπάρχουσας ηλεκτρονικής υποδομής αυθεντικοποίησης, όπως αυτή προβλέπεται για το επίπεδο εμπιστοσύνης 3. Επίσης η αυθεντικοποίηση μπορεί να γίνει με τη φυσική παρουσία τους στην Αρχή Εγγραφής ή την Αρχή Πιστοποίησης.

13.1.7.2.3.5 Διαδικασία ανανέωσης κρυπτογραφικών κλειδιών

Για την ανανέωση των κρυπτογραφικών κλειδιών ο χρήστης θα πρέπει να ακολουθήσει τη διαδικασία επανέκδοσης-ανανέωσης του ψηφιακού πιστοποιητικού (για λεπτομέρειες βλέπε ενότητα 13.1.7.3.6.3).

13.1.7.2.3.6 Διαδικασία επαναδημιουργίας κρυπτογραφικών κλειδιών

Κρυπτογραφικά κλειδιά επαναδημιουργούνται μόνο στην περίπτωση αστοχίας υλικού στο διακριτικό αποθήκευσης. Σε αυτή την περίπτωση ο χρήστης θα πρέπει αυτοπροσώπως να υποβάλει στην Αρχή Εγγραφής αίτηση επαναδημιουργίας κρυπτογραφικών κλειδιών αφού παραδώσει το διακριτικό αποθήκευσης που είχε στην κατοχή του. Η Αρχή Εγγραφής ελέγχει την ορθότητα των στοιχείων της αίτησης και την προωθεί στην Αρχή Πιστοποίησης για την αντιγραφή των κλειδιών κρυπτογράφησης από τα αντίγραφα προστασίας σε νέο διακριτικό αποθήκευσης. Όλες οι προαναφερθείσες διαδικασίες θα πρέπει να πραγματοποιούνται μέσω ασφαλών διατάξεων όπως ορίζεται στο προεδρικό διάταγμα Π.Δ. 150/2001 παράρτημα III.

13.1.7.2.4 Προστασία κλειδιών

13.1.7.2.4.1 Τρόποι προστασίας ιδιωτικών κλειδιών της Αρχής Πιστοποίησης

Τα ιδιωτικά κλειδιά της Αρχής Πιστοποίησης θα πρέπει να αποθηκεύονται σε ασφαλείς διατάξεις όπως ορίζεται στο προεδρικό διάταγμα Π.Δ. 150/2001. Ως εκ τούτου οι συσκευές που αξιοποιούνται για την αποθήκευση των κλειδιών θα πρέπει κατ' ελάχιστο να είναι συμβατές με τις προδιαγραφές FIPS 140-2 επιπέδου 3, είτε να είναι πιστοποιημένες σε CC EAL4. Επιπροσθέτως μόνο εξουσιοδοτημένες οντότητες θα πρέπει να έχουν πρόσβαση στις συσκευές αυτές και συνεπώς στα αντίστοιχα ιδιωτικά κλειδιά. Επιπρόσθετοι τρόποι προστασίας των ιδιωτικών κλειδιών της Αρχής Πιστοποίησης θα πρέπει να προσδιορίζονται από τον εκάστοτε φορέα ΥΔΚ.

13.1.7.2.4.2 Τρόποι προστασίας των δημιουργούμενων ζευγών κλειδιών

Η Αρχή Πιστοποίησης θα πρέπει να δημιουργεί τα ζεύγη κλειδιών σε ασφαλείς διατάξεις όπως ορίζεται στο προεδρικό διάταγμα Π.Δ. 150/2001. Ως εκ τούτου οι συσκευές που αξιοποιούνται για τη δημιουργία των ζευγών κλειδιών θα πρέπει κατ' ελάχιστο να είναι συμβατές με τις προδιαγραφές FIPS 140-2 επιπέδου 3, είτε να είναι πιστοποιημένες σε CC EAL4. Επιπρόσθετοι τρόποι προστασίας των δημιουργούμενων ζευγών κλειδιών θα πρέπει να προσδιορίζονται από τον εκάστοτε φορέα ΥΔΚ.

13.1.7.2.4.3 Τρόποι προστασίας των αποθηκευμένων κλειδιών

Τα ιδιωτικά κλειδιά θα πρέπει:

- να αποθηκεύονται σε tamper proof συσκευές (π.χ έξυπνες κάρτες)
- να μην είναι δυνατή η ανάγνωσή τους (εκτός της συσκευής) (read protection)
- η τροποποίησή τους θα πρέπει να είναι δυνατή μόνο με την αξιοποίηση των αντίστοιχων κρυπτογραφικών κλειδιών
- η ενεργοποίηση των κλειδιών θα πραγματοποιείται με την αξιοποίηση του αντίστοιχου PIN

Σε κάθε περίπτωση η αποθήκευση των ιδιωτικών κλειδιών πρέπει να γίνει σε ασφαλείς διατάξεις, όπως ορίζεται στο προεδρικό διάταγμα Π.Δ. 150/2001. Επιπλέον σε περιπτώσεις όπου τα ζεύγη κλειδιών αποθηκεύονται και στην Αρχή Πιστοποίησης, θα πρέπει μόνο εξουσιοδοτημένες οντότητες να έχουν πρόσβαση σε αυτά και μόνο σε ειδικές περιπτώσεις.

13.1.7.2.4.4 Τρόποι ενεργοποίησης των κλειδιών

Η ενεργοποίηση των κλειδιών θα πραγματοποιείται με την αξιοποίηση του αντίστοιχου PIN/PUK.

13.1.7.2.5 Άλλα θέματα διαχείρισης κλειδιών

Οι πάροχοι ΥΔΚ θα πρέπει να προσδιορίζουν θέματα διαχείρισης κλειδιών που δεν εμπίπτουν στις παραπάνω κατηγορίες.

13.1.7.3 Διαχείριση Πιστοποιητικών

13.1.7.3.1 Οντότητες που μπορούν να αιτηθούν την έκδοση πιστοποιητικών

Οι οντότητες που μπορούν να πραγματοποιήσουν αιτήσεις για την έκδοση ενός ψηφιακού πιστοποιητικού είναι:

- κάθε φυσικό πρόσωπο
- κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου ιδιωτικού δικαίου
- κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου δημοσίου δικαίου

που θέλει να αξιοποιήσει το ψηφιακό πιστοποιητικό στα πλαίσια των ηλεκτρονικών υπηρεσιών που προσφέρονται μέσω της ΚΔΠ.

13.1.7.3.2 Αίτηση έκδοσης πιστοποιητικών

Οι οντότητες που αιτούνται την έκδοση πιστοποιητικών θα πρέπει να εφαρμόζουν και να αποδέχονται, σε κάθε περίπτωση, την Πολιτική Πιστοποιητικών που εφαρμόζει η εκάστοτε ΥΔΚ. Για να είναι δυνατή η αίτηση έκδοσης πιστοποιητικών, ο χρήστης θα πρέπει να έχει παραλάβει το διακριτικό αποθήκευσης στο οποίο είναι αποθηκευμένα τα ζεύγη κλειδιών του,

αφού βέβαια έχει πρώτα υποβάλει αίτηση εγγραφής σε υπηρεσίες επιπέδου εμπιστοσύνης 3, ακολουθώντας τις διαδικασίες εγγραφής που προβλέπονται για το επίπεδο 3.

Εφόσον έχει παραλάβει το διακριτικό αποθήκευσης είναι σε θέση να αιτηθεί την έκδοση των πιστοποιητικών, αξιοποιώντας την ηλεκτρονική υπηρεσία έκδοσης ψηφιακών πιστοποιητικών. Συγκεκριμένα, για την έκδοση πιστοποιητικού ψηφιακής υπογραφής ο χρήστης υποβάλει ηλεκτρονικά, στην Αρχή Εγγραφής, αίτηση στην οποία ενσωματώνει το δημόσιο κλειδί του, ψηφιακά υπογεγραμμένο από το αντίστοιχο ιδιωτικό που βρίσκεται αποθηκευμένο στο διακριτικό αποθήκευσής του. Οι ψηφιακές αυτές αιτήσεις θα πρέπει να ακολουθούν το πρότυπο PKCS#10. Η Αρχή Εγγραφής, εφόσον ελέγξει την ορθότητα των στοιχείων της αίτησης και την εγκρίνει, προωθεί την αίτηση στην Αρχή Πιστοποίησης για τη δημιουργία του πιστοποιητικού ψηφιακής υπογραφής. Η έγκριση των στοιχείων πρέπει να πραγματοποιείται σύμφωνα με τις μεθόδους που παρουσιάζονται στην ενότητα 13.1.5.3.7.2 «Ταυτοποίηση και αυθεντικοποίηση του χρήστη πριν την εγγραφή». Η εγκεκριμένη και υπογεγραμμένη αίτηση έκδοσης πιστοποιητικού θα πρέπει να μεταφέρεται από την Αρχή Εγγραφής στην Αρχή Πιστοποίησης με ασφαλή τρόπο, όπως έχει προδιαγραφεί στην ενότητα «Θέματα επικοινωνίας μεταξύ των οντοτήτων ΥΔΚ» (βλέπε ενότητα 13.1.7.1). Η Αρχή Πιστοποίησης, με τη σειρά της, εκδίδει το αντίστοιχο πιστοποιητικό ψηφιακής υπογραφής με βάση τα στοιχεία που υπάρχουν στην αίτηση, και ενημερώνει το χρήστη ότι μπορεί να το παραλάβει από τους χώρους αποθήκευσης που διατηρεί η ΥΔΚ.

Αναφορικά με την έκδοση ψηφιακών πιστοποιητικών κρυπτογράφησης, λόγω του ότι τα αντίστοιχα ζεύγη κλειδιών δεν πρέπει να αξιοποιούνται για δημιουργία ψηφιακής υπογραφής και συνεπώς δεν μπορούν να αξιοποιηθούν για τη δημιουργία αντίστοιχου ηλεκτρονικού αιτήματος, θα δημιουργούνται κεντρικά κατά την έκδοση του ζεύγους κλειδιών και θα μπορούν να παραληφθούν από τους χώρους αποθήκευσης που διατηρεί η ΥΔΚ.

13.1.7.3.3 Έκδοση πιστοποιητικών

Όλα τα εκδιδόμενα πιστοποιητικά θα πρέπει να αξιοποιούν κάποια από τις μεθόδους ταυτοποίησης που ορίζεται στην ενότητα 6, για τον προσδιορισμό της ταυτότητας των οντοτήτων που κατέχουν ψηφιακά πιστοποιητικά. Η Αρχή Πιστοποίησης μπορεί να απορρίψει την έκδοση του πιστοποιητικού και οφείλει να ενημερώνει για τους λόγους απόρριψης της έκδοσης. Σε περίπτωση έκδοσης του πιστοποιητικού οφείλει, επίσης, να ενημερώνει το συνδρομητή για την έκδοσή του είτε στην ηλεκτρονική διεύθυνσή του ή στην ταχυδρομική με βάση την επιθυμία του χρήστη. Η βασική δομή του πιστοποιητικού περιγράφεται στην ενότητα 13.1.6.1. Όλα τα εκδιδόμενα πιστοποιητικά θα πρέπει να ακολουθούν τις προδιαγραφές PKCS#6.

13.1.7.3.4 Αποδοχή Πιστοποιητικού

Για την ενεργοποίηση του πιστοποιητικού ψηφιακής υπογραφής, μετά την έκδοση, ο τελικός χρήστης θα πρέπει να στείλει ένα υπογεγραμμένο μήνυμα στην Αρχή Πιστοποίησης μέσα σε εύλογο διάστημα (π.χ. εντός 30 ημερών, χρόνος που θα προσδιοριστεί από την ΥΔΚ), διαφορετικά το πιστοποιητικό δε θα δημοσιεύεται στον κατάλογο των ενεργών πιστοποιητικών,

συνεπώς δε θα θεωρείται έγκυρο. Αναφορικά με τα πιστοποιητικά κρυπτογράφησης θα ενεργοποιούνται αυτόματα με τη δημιουργία τους και αφού δημοσιευθούν στον αντίστοιχο κατάλογο ενεργών πιστοποιητικών.

Εναλλακτικά, η αποδοχή του πιστοποιητικού ψηφιακής υπογραφής από τον τελικό χρήστη θα μπορούσε να θεωρηθεί δεδομένη και να δημοσιεύεται κατευθείαν στον κατάλογο των ενεργών πιστοποιητικών. Σε περίπτωση που ο χρήστης το επιθυμεί θα μπορεί να αιτηθεί, μέσα σε εύλογο χρονικό διάστημα κάποιων ωρών από την παραλαβή του, το πιστοποιητικό να καταστεί μη έγκυρο.

13.1.7.3.5 Ανάκληση πιστοποιητικών

13.1.7.3.5.1 Περιπτώσεις ανάκλησης πιστοποιητικών αυτομάτως από την Αρχή Πιστοποίησης

Βλέπε ενότητα 13.1.7.2.2.

13.1.7.3.5.2 Οντότητες που αιτούνται την ανάκληση πιστοποιητικών

Οι οντότητες που μπορούν να αιτηθούν την ανάκληση πιστοποιητικών είναι:

- Οι χρήστες που έχουν στην κατοχή τους ψηφιακό πιστοποιητικό και συγκεκριμένα:
    - κάθε φυσικό πρόσωπο
    - κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου ιδιωτικού δικαίου
    - κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου δημοσίου δικαίου
- Η Αρχή Πιστοποίησης

13.1.7.3.5.3 Χρονικό διάστημα επεξεργασίας αιτήματος ανάκλησης

Το χρονικό διάστημα στο οποίο θα πρέπει να πραγματοποιείται η ανάκληση πιστοποιητικών θα πρέπει να καθορίζεται από την ΥΔΚ (ενδεικτικός χρόνος επεξεργασίας είναι μία ημέρα).

13.1.7.3.5.4 Μέθοδοι που αξιοποιούνται για την ανάκληση πιστοποιητικών

Δεν ορίζονται.

13.1.7.3.5.5 Διαδικασία ανάκλησης πιστοποιητικών

Οι οντότητες που επιθυμούν να ανακαλέσουν ένα πιστοποιητικό θα πρέπει να χρησιμοποιήσουν την κατάλληλη υπηρεσία ανάκλησης, μέσω της οποίας θα συμπληρώσουν την αντίστοιχη αίτηση, θα την υπογράψουν ψηφιακά και θα την υποβάλλουν ηλεκτρονικά, εφόσον βέβαια είναι ενεργό το διακριτικό αποθήκευσης. Σε διαφορετική περίπτωση ο χρήστης θα πρέπει να μεταβεί αυτοπροσώπως στην Αρχή Εγγραφής και να υποβάλει την αίτηση ανάκλησης του

πιστοποιητικού προσκομίζοντας τα απαραίτητα δικαιολογητικά που προβλέπονται από το επίπεδο εγγραφής 3. Αφού διαπιστωθεί η εγκυρότητα των στοιχείων της υποβληθείσας αίτησης, ανεξαρτήτως του τρόπου υποβολής της, η αίτηση προωθείται από την Αρχή Εγγραφής στην Αρχή Πιστοποίησης για περαιτέρω επεξεργασία και την τελική ανάκληση των κλειδιών, με τη διαγραφή τους από το διακριτικό αποθήκευσης, την ανάκληση των αντίστοιχων πιστοποιητικών, καθώς και την ενημέρωση της λίστας ανακλημένων πιστοποιητικών.

Προκειμένου να εξασφαλιστεί η δυνατότητα άμεσης ανάκλησης ενός πιστοποιητικού, θα μπορούσε να εξεταστεί η δημιουργία ειδικής υπηρεσίας, όπου θα απευθύνεται τηλεφωνικά ο χρήστης για να αιτηθεί ανάκλησης του πιστοποιητικού του, αφού πρώτα ταυτοποιηθεί τηλεφωνικά, για παράδειγμα δια της αξιοποίησης σχετικού κωδικού που θα προμηθεύεται κατά την αρχική παραλαβή του πιστοποιητικού του. Σε συνέχεια της αίτησης αυτής, το πιστοποιητικό θα τίθεται προσωρινά εκτός ισχύος και θα ανακαλείται πλήρως μετά την κατάθεση αντίστοιχης αίτησης στην Αρχή Εγγραφής.

Αξίζει να τονιστεί ότι η τηλεφωνική ταυτοποίηση του χρήστη δεν αντιστοιχεί στο επίπεδο εμπιστοσύνης 3 που εντάσσονται οι υπηρεσίες που αξιοποιούν ψηφιακά πιστοποιητικά. Ως εκ τούτου, σε περίπτωση που επιτραπεί η διαδικασία τηλεφωνικής προσωρινής ανάκλησης πιστοποιητικών, το αποτέλεσμα θα είναι ότι οι αντίστοιχες υπηρεσίες θα εντάσσονται πρακτικά σε χαμηλότερα επίπεδα εμπιστοσύνης και συνεπώς δεν θα καλύπτουν τις απαραίτητες απαιτήσεις ασφάλειας ως προς τη συνιστώσα της διαθεσιμότητας.

13.1.7.3.5.6 Μέθοδος ενημέρωσης της Λίστας Ανάκλησης Πιστοποιητικών

Δεν ορίζεται.

13.1.7.3.5.7 Θέματα χρόνου ανανέωσης της Λίστας Ανάκλησης Πιστοποιητικών

Η Λίστα Ανάκλησης Πιστοποιητικών θα πρέπει να ενημερώνεται άμεσα κατά την ανάκληση ενός πιστοποιητικού (σε διάστημα μιας μέρας) και τουλάχιστον μια ημέρα πριν την τυπική λήξη της.

13.1.7.3.5.8 Θέματα δημοσιοποίησης της Λίστας Ανάκλησης Πιστοποιητικών

Η λίστα ανάκλησης πιστοποιητικών θα δημοσιοποιείται μέσω του ιστοχώρου που συντηρεί η ΥΔΚ, ενώ εναλλακτικά θα μπορεί να αποστέλλεται στους χρήστες μέσω υπογεγραμμένου μηνύματος ηλεκτρονικού ταχυδρομείου.

13.1.7.3.5.9 Άλλες περιπτώσεις ανάκλησης πιστοποιητικών

Επιπρόσθετες περιπτώσεις ανάκλησης πιστοποιητικών θα πρέπει να προσδιορίζονται από τον εκάστοτε φορέα ΥΔΚ.

13.1.7.3.5.10 Δομή της Λίστας Ανάκλησης Πιστοποιητικών

Η δομή της λίστας θα πρέπει να συμμορφώνεται με το πρότυπο X509v3 CRLv2. Συγκεκριμένα θα πρέπει να έχει τη δομή που παρουσιάζεται στην παρακάτω Εικόνα.

Αριθμός Έκδοσης
Αλγόριθμός ψηφ. Υπογ.
Ψηφιακή υπογραφή
Εκδότης
Ημερομήνία έκδοσης
Ημερομηνία ανανέωσης
Λίστα ανάκλησης πιστοποιητικών
Προεκτάσεις

Εικόνα 6: Βασικά Πεδία Ανάκλησης Πιστοποιητικών

13.1.7.3.5.11 Μέθοδοι αυθεντικοποίησης των οντοτήτων που αιτούνται την ανάκληση πιστοποιητικών

Οι οντότητες που αιτούνται ανάκληση πιστοποιητικών μπορούν να αυθεντικοποιηθούν μέσω της υπάρχουσας ηλεκτρονικής υποδομής αυθεντικοποίησης, όπως αυτή προσδιορίζεται για το επίπεδο εμπιστοσύνης 3.

13.1.7.3.6 Επανέκδοση-Ανανέωση πιστοποιητικών

Με τον όρο «επανέκδοση ενός πιστοποιητικού» νοείται η έκδοση νέου πιστοποιητικού σε κάποιο χρήστη, για τις ακόλουθες περιπτώσεις:

- Τροποποίηση των στοιχείων του πιστοποιητικού
- Εγγραφή σε νέα υπηρεσία
- Τροποποίηση των κλειδιών του πιστοποιητικού
- Απώλεια του Διακριτικού Αποθήκευσης των κλειδιών
- Αστοχία υλικού στο διακριτικό αποθήκευσης των κλειδιών
- Δημοσίευση επιθέσεων οι οποίες επηρεάζουν τα υπάρχοντα ζεύγη κλειδιών
- Καθιερωμένη ανανέωση κλειδιών πριν τη λήξη του πιστοποιητικού

13.1.7.3.6.1 Οντότητες που μπορούν να αιτηθούν την επανέκδοση-ανανέωση πιστοποιητικού

Οι οντότητες που μπορούν να ζητήσουν την επανέκδοση πιστοποιητικού είναι οι νόμιμοι κάτοχοι πιστοποιητικών.

13.1.7.3.6.2 Οντότητες που πραγματοποιούν την επανέκδοση-ανανέωση του πιστοποιητικού

Οι οντότητες που πραγματοποιούν την επανέκδοση-ανανέωση του πιστοποιητικού προσδιορίζονται από την εκάστοτε ΥΔΚ.

13.1.7.3.6.3 Διαδικασίες επανέκδοσης-ανανέωσης του πιστοποιητικού

Για την επανέκδοση ενός ψηφιακού πιστοποιητικού ο χρήστης θα πρέπει να συμπληρώσει την απαραίτητη αίτηση επανέκδοσης του ψηφιακού πιστοποιητικού και να την υποβάλλει στη Αρχή Εγγραφής (σε ηλεκτρονική μορφή εφόσον το διακριτικό αποθήκευσης βρίσκεται σε λειτουργία ή έντυπα σε όλες τις άλλες περιπτώσεις). Η Αρχή Εγγραφής, αφού ελέγξει την ορθότητα της αίτησης, την προωθεί στην Αρχή Πιστοποίησης για την επανέκδοση του ψηφιακού πιστοποιητικού και ενημερώνει το χρήστη για την επιτυχή έκδοσή του. Θα πρέπει να σημειωθεί ότι στην περίπτωση της καθιερωμένης ανανέωσης του πιστοποιητικού, ο χρήστης θα ενημερώνεται αρκετά πριν τη λήξη του πιστοποιητικού, με ψηφιακά υπογεγραμμένο ηλεκτρονικό μήνυμα της Αρχής Εγγραφής. Αξίζει να αναφερθεί ότι τα κλειδιά κρυπτογράφησης που αντιστοιχούν σε ανανέωση θα παραδίδονται στο χρήστη μέσω SSL και θα αποθηκεύονται αυτόματα σε ασφαλή διάταξη, αξιοποιώντας το μηχανισμό PKCS#11 (βλέπε και ενότητα 13.1.7.3.3).

13.1.7.3.6.4 Μέθοδοι αυθεντικοποίησης των οντοτήτων που αιτούνται επανέκδοση πιστοποιητικού

Οι οντότητες που αιτούνται την επανέκδοση πιστοποιητικών, είναι δυνατόν να αυθεντικοποιηθούν μέσω της υπάρχουσας ηλεκτρονικής υποδομής αυθεντικοποίησης (εφόσον δεν υπάρχει αστοχία υλικού), όπως αυτή προσδιορίζεται από το επίπεδο εμπιστοσύνης 3. Σε διαφορετική περίπτωση απαιτείται η φυσική τους παρουσία στην Αρχή Εγγραφής για τη συμπλήρωση της αίτησης και την ταυτοποίησή τους.

13.1.7.3.7 Υπηρεσίες ελέγχου κατάστασης πιστοποιητικού

Η ΥΔΚ θα πρέπει να προσδιορίσει τις υπηρεσίες που προσφέρονται για τον έλεγχο της κατάστασης των πιστοποιητικών, καθώς και τα επιπλέον χαρακτηριστικά αυτών των υπηρεσιών. Προτείνεται η αξιοποίηση του πρωτοκόλλου OCSP.

13.1.7.3.8 Λήξη Συνδρομής

Η ΥΔΚ θα πρέπει να προσδιορίσει τις διαδικασίες που ακολουθούνται με το πέρας της συνδρομής ενός χρήστη. Κατ' ελάχιστο, σύμφωνα με το Π.Δ. 150/2001, η ΥΔΚ είναι υποχρεωμένη να διατηρεί όλα τα δεδομένα που σχετίζονται με τα αναγνωρισμένα ψηφιακά πιστοποιητικά για χρονικό διάστημα τριάντα (30) ετών. Επιπροσθέτως θα πρέπει να ενημερώνει άμεσα τη λίστα ανάκλησης ψηφιακών πιστοποιητικών και να διαγράφει τα κλειδιά από τη συσκευή του χρήστη.

13.1.7.4 Υπηρεσίες Χρονοσήμανσης

Η ΥΔΚ θα πρέπει να προσδιορίσει, εάν προσφέρονται υπηρεσίες χρονοσήμανσης, σε ποιες περιπτώσεις απαιτείται η αξιοποίησή τους, καθώς επίσης και τις περιπτώσεις όπου οι υπηρεσίες χρονοσήμανσης κάνουν χρήση έμπιστης πηγής χρόνου. Προτείνεται η χρήση υπηρεσιών χρονοσήμανσης στις περιπτώσεις όπου απαιτείται η τήρηση συγκεκριμένων χρονικών ορίων.

13.1.7.5 Ελεγκτικές Διαδικασίες κατά τη λειτουργία

13.1.7.5.1 Γεγονότα που καταγράφονται από την Αρχή Εγγραφής

Κατά τη λειτουργία της Αρχής Εγγραφής θα πρέπει να καταγράφονται τα ακόλουθα γεγονότα:

- Αιτήσεις Έκδοσης Πιστοποιητικών – Κλειδιών
- Αιτήσεις Ανάκλησης Πιστοποιητικών – Κλειδιών
- Αιτήσεις Επαναδημιουργίας Πιστοποιητικών – Κλειδιών
- Εγκεκριμένες αιτήσεις έκδοσης-ανάκλησης και επαναδημιουργίας Πιστοποιητικών-Κλειδιών

13.1.7.5.2 Γεγονότα που καταγράφονται από την Αρχή Πιστοποίησης

Κατά τη λειτουργία της Αρχής Πιστοποίησης θα πρέπει να καταγράφονται τα ακόλουθα γεγονότα:

- Αιτήσεις Έκδοσης Πιστοποιητικών – Κλειδιών
- Αιτήσεις Ανάκλησης Πιστοποιητικών – Κλειδιών
- Αιτήσεις Επαναδημιουργίας Πιστοποιητικών – Κλειδιών
- Εκδιδόμενα Πιστοποιητικά-Κλειδιά
- Ανανέωση της Λίστας Ανακληθέντων Πιστοποιητικών
- Εφεδρικά αντίτυπα Πιστοποιητικών-Κλειδιών
- Πρόσβαση στους χώρους έκδοσης Πιστοποιητικών-Κλειδιών

13.1.7.5.3 Συχνότητα επεξεργασίας των καταγεγραμμένων γεγονότων

Τα αρχεία καταγραφής υφίστανται επεξεργασία σε καθημερινή και εβδομαδιαία βάση.

13.1.7.5.4 Περίοδος διατήρησης των καταγεγραμμένων γεγονότων

Σύμφωνα με το Π.Δ. 150/2001, τα δεδομένα τα οποία σχετίζονται με αναγνωρισμένα πιστοποιητικά θα πρέπει να διατηρούνται για χρονικό διάστημα τριάντα (30) ετών.

13.1.7.5.5 Μέθοδοι προστασίας των καταγεγραμμένων γεγονότων

Σε κάθε περίπτωση θα πρέπει να διασφαλίζεται η ακεραιότητα των καταγεγραμμένων γεγονότων με την αξιοποίηση κατάλληλων μηχανισμών. Επιπλέον μόνο εξουσιοδοτημένες οντότητες θα πρέπει να έχουν πρόσβαση σε αυτά.

13.1.7.5.6 Θέματα διατήρησης αντιγράφων ασφαλείας των καταγεγραμμένων γεγονότων

Θα πρέπει να τηρούνται αντίγραφα ασφαλείας των καταγεγραμμένων γεγονότων αξιοποιώντας διαφορετικά μέσα αποθήκευσης (π.χ. σκληρό δίσκο, CD κλπ.). Σε κάθε περίπτωση θα πρέπει να σημειωθεί ότι τα αντίγραφα ασφαλείας θα πρέπει να διατηρούνται σε διαφορετικούς χώρους της ΥΔΚ.

13.1.7.6 Μέθοδοι ανάκαμψης σε περιπτώσεις καταστροφών και διακύβευσης

Η ΥΔΚ θα πρέπει να προσδιορίσει τις περιπτώσεις καταστροφών ή διακύβευσης των ψηφιακών κλειδιών βάσει των οποίων θα προδιαγράψει τις διαδικασίες που ακολουθούνται όσον αφορά:

- τη γνωστοποίηση του γεγονότος σε όλες τις εμπλεκόμενες οντότητες της ΥΔΚ
- την ανάκαμψη-επαναλειτουργία της ΥΔΚ (ενδεικτικά υπάρχει η δυνατότητα μέσω της ΑΠΕΔ)

13.1.7.7 Τερματισμός λειτουργίας Αρχής Πιστοποίησης

Σε περίπτωση τερματισμού λειτουργίας της Αρχής Πιστοποίησης θα πρέπει όλες οι εμπλεκόμενες οντότητες να ενημερωθούν άμεσα (τουλάχιστον ένα μήνα πριν τον τερματισμό της λειτουργίας) μέσω:

- Ψηφιακά υπογεγραμμένων ηλεκτρονικών μηνυμάτων της Αρχής Πιστοποίησης στις αντίστοιχες ηλεκτρονικές διευθύνσεις τους
- Ανακοίνωσης στον ιστοχώρο της Αρχής Πιστοποίησης

Επιπροσθέτως οι χρήστες θα πρέπει να ενημερωθούν αναφορικά με το χρόνο εγκυρότητας των πιστοποιητικών, καθώς και για τα θέματα επεξεργασίας-καταστροφής των αποθηκευμένων δεδομένων που διατηρεί η Αρχή Πιστοποίησης. Σε κάθε περίπτωση τα δεδομένα των πιστοποιητικών θα πρέπει να διατηρηθούν για χρονικό διάστημα τριάντα (30) ετών, σύμφωνα με το προεδρικό διάταγμα Π.Δ. 150/2001.

13.1.7.8 Επιπρόσθετα μέτρα ασφάλειας

Η ΥΔΚ στην Πολιτική Πιστοποιητικών, στα πλαίσια της γενικότερης πολιτικής ασφάλειας που ακολουθεί, θα πρέπει να προδιαγράψει τα επιπλέον μέτρα ασφάλειας και τους αντίστοιχους ελέγχους που πραγματοποιούνται για την προστασία των υπολογιστικών πόρων και συγκεκριμένα για τα ακόλουθα:

- Ασφάλεια Υπολογιστικών συστημάτων
    - Μέθοδοι Εξουσιοδότησης
    - Καταγραφή Γεγονότων Ασφάλειας
    - Διαδικασίες ελέγχου ασφάλειας και εισβολής
    - Αξιολόγηση ασφάλειας

- Ασφάλεια Δικτυακών συστημάτων
    - Firewall
    - Συστήματα Ανίχνευσης Εισβολών
    - Διαδικασίες ελέγχου ασφάλειας και εισβολής
- Αξιολόγηση ασφάλειας των υπολογιστικών συστημάτων της ΥΔΚ. Η αξιολόγηση αυτή θα μπορούσε να βασιστεί, για παράδειγμα, στα ακόλουθα:
    - Common Criteria for Information Technology Security Evaluation
    - Trusted Computers System Evaluation Criteria
    - European Information Technology Security Evaluation Criteria

13.1.7.9 Φυσική ασφάλεια, έλεγχος ασφάλειας διαδικασιών και προσωπικού

Σε αυτή την ενότητα οι ΥΔΚ θα προδιαγράφουν τα στοιχεία εκείνα που σχετίζονται με τα ακόλουθα ώστε να διασφαλίζεται η αξιόπιστη και ασφαλή λειτουργία της ΥΔΚ:

- Φυσική ασφάλεια:
    - Πηροσδιορισμός χώρων υψηλής ασφάλειας
    - Μέθοδοι ελέγχου φυσικής πρόσβασης στους χώρους της ΥΔΚ
    - Τροφοδοσία ρεύματος και κλιματισμός
    - Πλημμύρες
    - Προστασία από πυρκαγιά
    - Εναλλακτικά αντίγραφα ασφάλειας των δεδομένων λειτουργίας
- Έλεγχος των διαδικασιών:
    - Προσδιορισμός ρόλων και αρμοδιοτήτων για την ορθή διεκπεραίωση των διαδικασιών
    - Μέθοδοι ταυτοποίησης και αυθεντικοποίησης των ρόλων
- Έλεγχος ασφαλείας προσωπικού:
    - Προσόντα, εμπειρία που απαιτούνται για κάθε ρόλο που συμμετέχει στις διαδικασίες της ΥΔΚ
    - Επιπρόσθετοι έλεγχοι που πραγματοποιούνται από την ΥΔΚ κατά τη διαδικασία πρόσληψης προσωπικού. Για παράδειγμα, θα μπορούσε να απαιτείται προσκόμιση αντίγραφου ποινικού μητρώου των διαχειριστών, αφού βεβαίως ληφθεί υπόψη το ισχύον νομοθετικό πλαίσιο.
    - Έλεγχος ενεργειών προσωπικού
    - Θέματα εκπαίδευσης

- Θέματα εναλλαγής ρόλων
- Θέματα προσωπικού με συμβάσεις
- Κυρώσεις
- Έγγραφα που παρέχονται στους εργαζομένους

13.1.7.10 Διαχείριση Πολιτικής Πιστοποιητικών

Η ΥΔΚ θα πρέπει να ενημερώνει, με ηλεκτρονικό τρόπο, όλους τους χρήστες για περιπτώσεις όπου η ανανέωση της πολιτικής σχετίζεται με τροποποιήσεις των διαδικασιών διαχείρισης κλειδιών και πιστοποιητικών. Για την εφαρμογή της κάθε τροποποίησης θα πρέπει να υπάρχει σχετική άδεια από την αρμόδια Αρχή Πιστοποίησης. Σε περιπτώσεις σημαντικών αλλαγών, θα πρέπει να τροποποιείται αντίστοιχα ο προσδιοριστής της πολιτικής καθώς και να ενημερώνονται αντίστοιχα όλα τα πιστοποιητικά.

13.1.8 Θεσμικό-Κανονιστικό Πλαίσιο

Αν και προσανατολισμένες καταρχήν στις ανάγκες αναγνώρισης των ηλεκτρονικών υπογραφών και παροχής υπηρεσιών πιστοποίησης στο πεδίο των σχέσεων μεταξύ ιδιωτών, οι διατάξεις για τις ηλεκτρονικές υπογραφές μπορούν – mutatis mutandis – να βρουν εφαρμογή και όσον αφορά στην ταυτοποίηση και στην παροχή υπηρεσιών πιστοποίησης στο δημόσιο τομέα.

Όπως επισημαίνεται στο Προοίμιο (19) της Οδηγίας 99/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, οι ηλεκτρονικές υπογραφές θα χρησιμοποιούνται στο δημόσιο τομέα στο πλαίσιο εθνικών και κοινοτικών διοικητικών υπηρεσιών, ενώ ο κοινοτικός νομοθέτης επιτρέπει στα κράτη μέλη να εξαρτούν τη χρήση ηλεκτρονικών υπογραφών στο δημόσιο τομέα από ενδεχόμενες πρόσθετες απαιτήσεις, οι οποίες αναφέρονται μόνο στα ειδικά χαρακτηριστικά της συγκεκριμένης εφαρμογής (άρθρο 3 § 7 της Οδηγίας 99/93/ΕΚ). Πρέπει επίσης να επισημανθεί ότι πρόσφατες μελέτες, όπως η μελέτη FIDIS (Μάρτιος 2006), καταλήγουν στο συμπέρασμα ότι η Οδηγία 99/93/ΕΚ αποτελεί επαρκή και πρόσφορη νομική βάση για την εισαγωγή μιας πανευρωπαϊκής ηλεκτρονικής ταυτότητας.

Ο Έλληνας νομοθέτης, ήδη πριν την έκδοση του Π.Δ. 150/2001 που ενσωμάτωσε την Οδηγία 99/93 στην ελληνική έννομη τάξη, είχε ρυθμίσει αποσπασματικά το θέμα της ψηφιακής υπογραφής με το άρθρο 14 του ν. 2672/1998, όσον αφορά στη διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των υπηρεσιών του Δημοσίου, των ΝΠΔΔ και των ΟΤΑ ή μεταξύ αυτών και των ενδιαφερόμενων φυσικών προσώπων ή ΝΠΙΔ και ενώσεων προσώπων (άρθρο 14 §1 του ν. 2672/1998).

Κατά το άρθρο 14 § 4 ν. 2672/1998 «μεταξύ των υπηρεσιών του άρθρου 14 §1 ν. 2672/1998 διακινούνται με ηλεκτρονικό ταχυδρομείο κατά τις διατάξεις του άρθρου 14 ν. 2672/1998 μηνύματα που έχουν ως περιεχόμενο γνωμοδοτήσεις, ερωτήματα, αιτήσεις, απαντήσεις, εγκυκλίους, οδηγίες, εκθέσεις, μελέτες, πρακτικά, στατιστικά στοιχεία, υπηρεσιακά σημειώματα και έγγραφες εισηγήσεις. Κατά τον παραπάνω τρόπο διακινούνται μεταξύ των υπηρεσιών αυτών και των φυσικών προσώπων και ΝΠΙΔ μηνύματα που έχουν ως περιεχόμενο αιτήσεις

παροχής πληροφοριών και σχετικές απαντήσεις» (εξαιρέσεις προβλέπονται από το άρθρο 14 § 6 ν. 2672/1998).

Κατά το άρθρο 14§ 2, περ. ε΄ του ν. 2672/1998 για την εφαρμογή του παρόντος άρθρου ορίζεται ως ψηφιακή υπογραφή η ψηφιακής μορφής υπογραφή σε δεδομένα ή συνημμένη σε δεδομένα ή λογικά συσχετιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη αποδοχής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή:

1. συνδέεται μονοσήμαντα με τον υπογράφοντα,
2. ταυτοποιεί τον υπογράφοντα,
3. δημιουργείται με μέσα, τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του
4. συνδέεται με τα δεδομένα, στα οποία αναφέρεται, κατά τρόπο, ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.

Ο ορισμός αυτός αποδίδει ουσιαστικά αυτούσιο τον ορισμό της προηγμένης ηλεκτρονικής υπογραφής του άρθρου 2 περ. 2 της Οδηγίας 1999/93/ΕΚ, ο οποίος με τη σειρά του αποδίδεται κατόπιν αυτούσιος και στο άρθρο 2 περ. 2 του Π.Δ. 150/2001, όπου δίδεται ο ορισμός της προηγμένης ηλεκτρονικής ή ψηφιακής υπογραφής κατά το εσωτερικό μας πλέον δίκαιο.

Κατά το άρθρο 14 § 17 ν. 2672/1998 το μήνυμα ηλεκτρονικού ταχυδρομείου θεωρείται ότι έχει περιέλθει στο λήπτη, εφόσον υπάρχει σχετική ηλεκτρονική επιβεβαίωση. Αν το οικείο σύστημα του ηλεκτρονικού ταχυδρομείου δεν υποστηρίζει την αυτόματη επιβεβαίωση της λήψης του μηνύματος, ο παραλήπτης του, εφόσον τούτο ζητηθεί από τον αποστολέα, υποχρεούται στην παραπάνω επιβεβαίωση. Επίσης, η αποστολή μηνύματος με ηλεκτρονικό υπολογιστή δε συνεπάγεται έναρξη των προθεσμιών άσκησης διοικητικών προσφυγών, ενδίκων βοηθημάτων και ενδίκων μέσων (άρθρο 14 § 17 ν. 2672/1998).

Με το άρθρο 20 του ν. 3448/2006 καθορίζονται οι όροι και οι προϋποθέσεις για την παροχή των υπηρεσιών πιστοποίησης από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) και τις Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), οι οποίες καθορίζονται σύμφωνα με τις διατάξεις της παραγράφου 4 του άρθρου 20 του προαναφερόμενου νόμου. Επί τη βάσει της κανονιστικής εξουσιοδότησης που αυτός περιέχει κυρώθηκε με την ΥΑ 256/2006 (Β'/1654) ο Κανονισμός Πιστοποίησης της ΑΠΕΔ. Ο Κανονισμός αυτός αποτελεί τη Δήλωση Πρακτικής της ΑΠΕΔ, ως Πρωτεύουσας Αρχής Πιστοποίησης για την παροχή υπηρεσιών πιστοποίησης κατά τα προβλεπόμενα στις διατάξεις του Κανονισμού 248/71/2002 της ΕΕΤΤ (ΦΕΚ 603/Β) και του ΠΔ 150/2001 (ΦΕΚ 125/Α) για την έκδοση "αναγνωρισμένων πιστοποιητικών".

Τα πιστοποιητικά της ΑΠΕΔ, αν και αποτελούν πιστοποιητικά για γενική χρήση, έχουν περιορισμούς στη χρήση τους όπως ορίζεται στη παράγραφο 7 του Κανονισμού. Σε κάθε περίπτωση οι διατάξεις του Κανονισμού δε θίγουν α) διατάξεις που ισχύουν αναφορικά με τη σύναψη και την ισχύ συμβάσεων ή εν γένει τη σύσταση νομικών υποχρεώσεων, β) διατάξεις που επιβάλλουν τη χρήση ορισμένου τύπου γ) διατάξεις που αναφέρονται στην αποδεικτική ή άλλη χρήση εγγράφων δ) διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να

καθίστανται γνωστά έγγραφα ορισμένων κατηγοριών και δεδομένα προσωπικού χαρακτήρα, σύμφωνα και με τις διατάξεις του άρθρου 1 § 2 του Π.Δ. 150/2001.

Ελλείψει ειδικότερης ρύθμισης και επί τη βάσει της ρύθμισης του άρθρου 7 του Π.Δ. 150/2001 εφαρμόζονται οι ρυθμίσεις της νομοθεσίας για την προστασία προσωπικών δεδομένων που περιέχονται στον ν. 2472/97 όπως ισχύει και κατά περίπτωση του ν. 3471/06 (που αντικατέστησε τον ν. 2774/99). Το άρθρο 7 περιέχει ειδική ρύθμιση ως προς τα δεδομένα που πρέπει να συλλέγονται για την έκδοση πιστοποιητικών. Ενόψει όμως της χρήσης των πιστοποιητικών στο πλαίσιο συναλλαγών με το δημόσιο τομέα θα πρέπει να επανεξεταστεί η ρύθμιση της παραγράφου 3, σύμφωνα με την οποία επιτρέπεται στους παρόχους υπηρεσιών πιστοποίησης να αναγράφουν στο αναγνωρισμένο πιστοποιητικό ψευδώνυμο αντί του ονόματος.

13.1.9 Οδηγίες εφαρμογής

Το Πλαίσιο Πολιτικής Ψηφιακών Πιστοποιητικών αποτελεί 'οδηγό' για τη συγγραφή Πολιτικής Ψηφιακών Πιστοποιητικών και της αντίστοιχης Δήλωσης Πρακτικής για τους παρόχους ΥΔΚ. Στο υπάρχον πλαίσιο καλύπτεται μια σειρά από διαφορετικά θέματα που απαιτούνται για την ορθή και αξιόπιστη λειτουργία μιας ΥΔΚ στα πλαίσια της ηλεκτρονικής διακυβέρνησης. Ανάλογα με τις υπηρεσίες και την κρισιμότητα αυτών που προσφέρονται από τις ΥΔΚ θα πρέπει να προδιαγράφονται και τα αντίστοιχα στοιχεία της Πολιτικής Πιστοποιητικών, όπως αναλύονται στο παρόν πλαίσιο.

Το πλαίσιο αυτό δεν είναι αυστηρό στην εφαρμογή του, σε περιπτώσεις όπου δεν είναι αναγκαία η περιγραφή κάποιων ενοτήτων θα πρέπει να αναφέρεται ρητώς στην αντίστοιχη ενότητα «δεν ορίζεται», η οποία όμως μπορεί να τροποποιηθεί σε νεώτερη έκδοση της πολιτικής. Σε περίπτωση που το παρόν πλαίσιο δεν προβλέπει κάποια χαρακτηριστικά της Πολιτικής Πιστοποιητικών οι ΥΔΚ είναι ελεύθερες για την εισαγωγή των επιπρόσθετων χαρακτηριστικών.

Η γενική δομή της Πολιτικής Πιστοποιητικών πρέπει να εναρμονίζεται με την ακόλουθη δομή:

1 Πολιτική Ψηφιακών Πιστοποιητικών

- 1.1 Εφαρμοσιμότητα της πολιτικής
- 1.2 Οντότητες Παροχής Υπηρεσιών Δημοσίου Κλειδιού
  - 1.2.1 Αρχή Πιστοποίησης
  - 1.2.2 Αρχή Εγγραφής
  - 1.2.3 Τελικοί Χρήστες Πιστοποιητικών
  - 1.2.4 Οντότητες Εμπιστοσύνης
  - 1.2.5 Οντότητες Διαχείρισης
  - 1.2.6 Άλλες οντότητες

1.3 Γενικές Διατάξεις και Όροι

1.3.1 Υποχρεώσεις των εμπλεκόμενων οντοτήτων

1.3.1.1 Υποχρεώσεις Αρχών Εγγραφής

1.3.1.2 Υποχρεώσεις Αρχών Πιστοποίησης

1.3.1.3 Υποχρεώσεις Χρηστών

1.3.2 Ευθύνες των εμπλεκόμενων οντοτήτων

1.3.2.1 Ευθύνες Αρχής Εγγραφής

1.3.2.2 Ευθύνες Αρχής Πιστοποίησης

1.3.2.3 Ευθύνες χρηστών

1.3.2.4 Ευθύνη προς Αποζημίωση

1.3.3 Εγγυήσεις

1.3.4 Θέματα δημοσιοποίησης ψηφιακών πιστοποιητικών

1.3.5 Πολιτική εμπιστευτικότητας

1.3.6 Μέθοδοι Επίλυση διαφορών

1.3.7 Μέθοδοι Εγγραφής, Ταυτοποίησης και Αυθεντικοποίησης των χρηστών πριν την έκδοση ενός ψηφιακού πιστοποιητικού

1.3.7.1 Πρότυπο Καταγραφής στοιχείων

1.3.7.2 Ταυτοποίηση και Αυθεντικοποίηση χρηστών

1.3.8 Χρεώσεις

1.4 Κατηγορίες Εκδιδόμενων Ψηφιακών Πιστοποιητικών

1.4.1 Προφίλ Ψηφιακών Πιστοποιητικών

1.4.2 Επεκτάσεις Ψηφιακών Πιστοποιητικών

1.4.3 Επιτρεπτές Χρήσεις των ψηφιακών πιστοποιητικών

1.4.3.1 Ψηφιακό πιστοποιητικό κρυπτογράφησης

1.4.3.2 Ψηφιακό πιστοποιητικό ψηφιακής υπογραφής

1.4.4 Μη επιτρεπτές Χρήσεις των ψηφιακών πιστοποιητικών

1.4.4.1 Ψηφιακό πιστοποιητικό κρυπτογράφησης

1.4.4.2 Ψηφιακό πιστοποιητικό ψηφιακής υπογραφής

1.5 Απαιτήσεις Λειτουργίας

1.5.1 Θέματα επικοινωνίας μεταξύ των οντοτήτων ΥΔΚ

1.5.2 Διαχείριση Κλειδιών

14. ΠΑΡΑΡΤΗΜΑ Γ: Πλαίσιο Πολιτικής Τομεακών Ψηφιακών Πιστοποιητικών

Στο παράρτημα αυτό αποτυπώνεται το πλαίσιο Πολιτικής Τομεακών Ψηφιακών Πιστοποιητικών (certificate policy framework), στο οποίο προσδιορίζονται όλες οι αναγκαίες διαδικασίες έκδοσης (issue), διαμοιρασμού (distribution) και ανάκλησης (revoke) των ψηφιακών πιστοποιητικών που θα εκδίδονται για χρήση σε ηλεκτρονικές υπηρεσίες που θα προσφέρουν κατευθείαν (όχι μέσω της Κεντρικής Διαδικτυακής Πύλης) οι φορείς και θα περιέχουν σε κρυπτογραφημένη μορφή τα αναγνωριστικά που θα καθορίζει ο φορέας. Εξυπακούεται ότι σε πολλές περιπτώσεις οι απαιτήσεις ταυτίζονται με αυτές που προβλέπονται από την ενότητα 13 για τα πιστοποιητικά υπογραφής και κρυπτογράφησης. Ως εκ τούτου συγκεκριμένες απαιτήσεις/ διατάξεις επαναλαμβάνονται ή υπάρχουν παραπομπές στην ενότητα 13.

14.1.1 Γενικά

Οι Αρχές Πιστοποίησης και οι Υποκείμενές τους και συνεπώς τα εκδιδόμενα από αυτές τομεακά ψηφιακά πιστοποιητικά θα πρέπει να ακολουθούν το παρόν πλαίσιο Πολιτικής Τομεακών Ψηφιακών Πιστοποιητικών. Ειδικότερα το παρόν πλαίσιο καταγράφει τις ελάχιστες απαιτήσεις με τις οποίες θα πρέπει να συμμορφώνονται όλες οι εμπλεκόμενες οντότητες για την παροχή υπηρεσιών ΥΔΚ για τομεακές εφαρμογές.

Θα πρέπει να σημειωθεί ότι το παρόν πλαίσιο Πολιτικής Τομεακών Ψηφιακών Πιστοποιητικών συμμορφώνεται με το de facto standard RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, διάδοχο του RFC 2527.

14.1.2 Σκοπός

Σκοπός της ενότητας αυτής είναι να παρουσιάσει ένα πλαίσιο Πολιτικής Πιστοποιητικών που θα μπορούν να αξιοποιήσουν ως οδηγό οι Υποκείμενες Αρχές Πιστοποίησης δημοσίου ή ιδιωτικού δικαίου για τη συγγραφή της Πολιτικής Τομεακών Πιστοποιητικών και της αντίστοιχης Δήλωσης Πρακτικής (Practice Statement).

Οικοθεν νοείται ότι το πλαίσιο αυτό δεν προσδιορίζει κάποια συγκεκριμένη Πολιτική Πιστοποιητικών, αλλά περιγράφει τις γενικές αρχές που θα πρέπει να ακολουθούνται κατά τη συγγραφή των πολιτικών Τομεακών Πιστοποιητικών.

14.1.3 Στόχος

Ο στόχος της ενότητας αυτής είναι ο προσδιορισμός των περιεχομένων της Πολιτικής Τομεακών Ψηφιακών Πιστοποιητικών και συγκεκριμένα η περιγραφή όλων εκείνων των τεχνικών, ρυθμιστικών και κανονιστικών στοιχείων και των αντίστοιχων πληροφοριών που θα πρέπει να λαμβάνονται υπόψη κατά τη συγγραφή της Πολιτικής και της αντίστοιχης Δήλωσης Πρακτικής Τομεακών Ψηφιακών πιστοποιητικών.

14.1.4 Πολιτική Τομεακών Ψηφιακών Πιστοποιητικών

Ισχύει τα αναγραφόμενα στην Ενότητα 13.1.4.

14.1.5 Προσδιορισμός Πολιτικής Ψηφιακών Πιστοποιητικών

Ισχύει τα αναγραφόμενα στην Ενότητα 13.1.5.

14.1.5.1 Εφαρμοσιμότητα της Πολιτικής

Όλες οι οντότητες που θα συμμετέχουν σε υπηρεσίες ΥΔΚ και σχετίζονται με τομεακές (όχι μέσω ΚΔΠ) ηλεκτρονικές υπηρεσίες, θα πρέπει να εφαρμόζουν τις συγκεκριμένες οδηγίες. Οι οντότητες αυτές περιγράφονται αναλυτικά στην ενότητα 14.1.5.2, ενώ οι επιτρεπτές χρήσεις των πιστοποιητικών (εφαρμογές στα πλαίσια των οποίων μπορούν να αξιοποιηθούν) αναλύονται στην ενότητα 14.1.6.3.

14.1.5.2 Περιγραφή Οντοτήτων Παροχής Υπηρεσιών Δημοσίου Κλειδιού

Στην ενότητα αυτή περιγράφονται αναλυτικά όλες οι οντότητες που πρέπει να συμμετέχουν και να καθορίζονται κατ' ελάχιστον σε κάθε Πολιτική Τομεακών Πιστοποιητικών Υποδομής Δημόσιου Κλειδιού.

14.1.5.2.1 Αρχές Πιστοποίησης

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.2.1. Προτείνεται η αξιοποίηση διαφορετικής αρχής πιστοποίησης για τη διαχείριση των τομεακών πιστοποιητικών για ολόκληρο τον κύκλο ζωής τους.

14.1.5.2.2 Αρχή Εγγραφής

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.2.2. Δεν προτείνεται η δημιουργία νέας Αρχής Εγγραφής για την κάλυψη των αναγκών των τομεακών ψηφιακών πιστοποιητικών καθώς οι διαδικασίες εγγραφής είναι αντίστοιχες με αυτές των πιστοποιητικών υπογραφής και κρυπτογράφησης.

14.1.5.2.3 Τελικοί Χρήστες Τομεακών Ψηφιακών Πιστοποιητικών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.2.3 με τη διαφορά ότι αφορούν ηλεκτρονικές υπηρεσίες που προσφέρονται κατευθείαν (όχι μέσω της ΚΔΠ) από τους φορείς.

14.1.5.2.4 Οντότητες Εμπιστοσύνης

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.2.4.

14.1.5.2.5 Άλλες οντότητες

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.2.5.

14.1.5.3 Γενικές Διατάξεις και Όροι

Σε αυτή την ενότητα προσδιορίζονται οι υποχρεώσεις όλων των εμπλεκόμενων οντοτήτων για την παροχή ΥΔΚ που σχετίζονται με τις υπηρεσίες των τομεακών πιστοποιητικών. Συγκεκριμένα περιλαμβάνονται:

- Οι υποχρεώσεις:
    - των Αρχών Πιστοποίησης
    - των Αρχών Εγγραφής
    - των κατόχων ψηφιακών πιστοποιητικών
- Ευθύνες
    - των Αρχών Πιστοποίησης
    - των Αρχών Εγγραφής
    - των κατόχων ψηφιακών πιστοποιητικών
- Εγγυήσεις
- Θέματα δημοσιοποίησης των ψηφιακών πιστοποιητικών
- Πολιτική εμπιστευτικότητας
- Μέθοδοι Εγγραφής, Ταυτοποίησης και Αυθεντικοποίησης των χρηστών πριν την έκδοση ενός ψηφιακού πιστοποιητικού
- Μέθοδοι επίλυσης διαφορών

14.1.5.3.1 Υποχρεώσεις των εμπλεκόμενων οντοτήτων

14.1.5.3.1.1 Υποχρεώσεις Αρχών Εγγραφής

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.1.1.

14.1.5.3.1.2 Υποχρεώσεις Αρχών Πιστοποίησης

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.1.2.

14.1.5.3.1.3 Υποχρεώσεις Χρηστών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.1.3.

14.1.5.3.2 Ευθύνες των εμπλεκόμενων οντοτήτων

14.1.5.3.2.1 Ευθύνες Αρχής Εγγραφής

Οι ευθύνες της Αρχής Εγγραφής είναι κατ' ελάχιστον οι ακόλουθες:

- Η Αρχή Εγγραφής θα πρέπει να εναρμονίζεται με την Πολιτική Τομεακών Πιστοποιητικών.

- Η Αρχή Εγγραφής πρέπει να τηρεί τις υποχρεώσεις που αναγράφονται στην ενότητα 14.1.5.3.1.1.
- Η Αρχή Εγγραφής δε φέρει καμία υπαιτιότητα σε περίπτωση μη ορθής χρήσης των τομεακών πιστοποιητικών.
- Η Αρχή Εγγραφής πρέπει να εναρμονίζεται και να εφαρμόζει το προεδρικό διάταγμα Π.Δ 150/2001.

14.1.5.3.2.2 Ευθύνες Αρχής Πιστοποίησης

Οι ευθύνες της Αρχής Πιστοποίησης είναι κατ' ελάχιστον οι ακόλουθες:

- Η Αρχή Πιστοποίησης πρέπει να εφαρμόζει την Πολιτική Τομεακών Πιστοποιητικών.
- Η Αρχή Πιστοποίησης πρέπει να τηρεί τις υποχρεώσεις που αναφέρονται στην ενότητα 14.1.5.3.1.2.
- Η Αρχή Πιστοποίησης πρέπει να εγγυάται την ορθότητα των στοιχείων που αναγράφονται στα τομεακά πιστοποιητικά.
- Η Αρχή Πιστοποίησης δε φέρει ευθύνη για μη ορθή χρήση των τομεακών πιστοποιητικών εφόσον δεν είναι δική της υπαιτιότητα.
- Η Αρχή Πιστοποίησης πρέπει να εναρμονίζεται και να εφαρμόζει το προεδρικό διάταγμα Π.Δ 150/2001.

14.1.5.3.2.3 Ευθύνες Χρηστών

Οι ευθύνες των χρηστών είναι κατ' ελάχιστον οι ακόλουθες:

- Οι χρήστες θα πρέπει να τηρούν τις υποχρεώσεις που αναφέρονται στην ενότητα 14.1.5.3.1.3.

14.1.5.3.2.4 Ευθύνη προς Αποζημίωση

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.2.4.

14.1.5.3.3 Εγγυήσεις

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.3.

14.1.5.3.4 Θέματα δημοσιοποίησης τομεακών ψηφιακών πιστοποιητικών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.4.

14.1.5.3.5 Πολιτική εμπιστευτικότητας

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.5, με μοναδική επιπρόσθετη απαίτηση τη διασφάλιση της εμπιστευτικότητας των τομεακών αναγνωριστικών (π.χ. ΑΦΜ) που αποθηκεύονται στα πιστοποιητικά.

14.1.5.3.6 Μέθοδοι Επίλυσης διαφορών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.6.

14.1.5.3.7 Μέθοδοι Εγγραφής, Ταυτοποίησης και Αυθεντικοποίησης των χρηστών πριν την έκδοση ενός ψηφιακού πιστοποιητικού

14.1.5.3.7.1 Πρότυπο Καταγραφής στοιχείων

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.7.1.

14.1.5.3.7.2 Ταυτοποίηση και Αυθεντικοποίηση Χρηστών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.7.2, καθώς επίσης και οι όποιες επιπρόσθετες απαιτήσεις θέτει ο κάθε φορέας του δημοσίου για την απόδειξη κατοχής των αναγνωριστικών του χρήστη.

14.1.5.3.8 Χρεώσεις

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.5.3.8.

14.1.6 Κατηγορίες Τομεακών Ψηφιακών Πιστοποιητικών

Για την κάλυψη ειδικών αναγκών ανά τομέα του Δημοσίου και συγκεκριμένα για την αξιοποίηση ηλεκτρονικών υπηρεσιών που προσφέρονται κατευθείαν (όχι μέσω ΚΔΠ) από τους φορείς, θα εκδίδονται (για τους τελικούς χρήστες – όπως αυτοί ορίζονται στην ενότητα 14.1.5.2.3), πιστοποιητικά του παρακάτω τύπου:

- Τομεακό ψηφιακό πιστοποιητικό για αυθεντικοποίηση & ψηφιακή υπογραφή ηλεκτρονικών μηνυμάτων και εγγράφων

14.1.6.1 Προφίλ Τομεακών Ψηφιακών Πιστοποιητικών

Τα τομεακά ψηφιακά πιστοποιητικά περιλαμβάνουν τα βασικά πεδία που απαιτούνται για αναγνωρισμένα πιστοποιητικά, σύμφωνα με το Π.Δ 150/2001, και είναι τύπου X509 v3.

Πεδίο
Έκδοση (Version)
Αριθμός Σειράς (Serial Number)
Αλγόριθμος Υπογραφής (Signature Algorithm)
Διακριτικό Όνομα Εκδότη (Issuer DN)
Ισχύει Από (Valid From)
Ισχύει Μέχρι (Valid To)
Διακριτικό Όνομα Υποκειμένου (Subject DN)

Πεδίο
Δημόσιο Κλειδί Υποκειμένου (Subject Public Key)
Υπογραφή (Signature)

Πίνακας 22: Βασικά Πεδία Προφίλ Τομεακού Πιστοποιητικού

14.1.6.1.1 Αναλυτική περιγραφή πεδίων

- Έκδοση (Version): αναφέρεται στην έκδοση του προτύπου X.509 πιστοποιητικών και υποστηρίζει εκτεταμένα πεδία.
- Αριθμός Σειράς (Serial Number): αποτελείται από το μοναδικό αριθμό του εκδιδόμενου πιστοποιητικού, ο οποίος καθορίζεται από τον εκδότη των πιστοποιητικών με σκοπό τη διάκριση του πιστοποιητικού.
- Αλγόριθμός Υπογραφής (Signature Algorithm): αναφέρεται στον αλγόριθμό σύνοψης (Hash Function) που θα αξιοποιείται από την ΥΔΚ. Προτείνεται η αξιοποίηση του SHA-1.
- Διακριτικό Όνομα Εκδότη (Issuer DN): αναφέρεται στο όνομα του εκδότη του πιστοποιητικού και αποτελείται από τα υπό-πεδία Χώρα (Country), Οργανισμός (Organization), Κοινό Όνομα (Common Name) και Ηλεκτρονική Διεύθυνση (E-mail Address). Τα παραπάνω πεδία πλην της Ηλεκτρονικής Διεύθυνσης (E-mail Address) είναι υποχρεωτικά.
- Ισχύει Από (Valid From): περιλαμβάνει την ημερομηνία έκδοσης του πιστοποιητικού.
- Ισχύει Μέχρι (Valid To): περιλαμβάνει την ημερομηνία λήξης του πιστοποιητικού.
- Διακριτικό Όνομα Υποκειμένου (Subject DN): Αναφέρεται στον κάτοχο του πιστοποιητικού και αποτελείται από τα υπό-πεδία Χώρα (Country), Οργανισμός (Organization), Κοινό Όνομα (Common Name) και Ηλεκτρονική Διεύθυνση (E-mail Address). Τα παραπάνω πεδία πλην της Ηλεκτρονικής Διεύθυνσης (E-mail Address) είναι υποχρεωτικά. Συγκεκριμένα, σύμφωνα με το RFC 3280, η χρήση της ηλεκτρονικής διεύθυνσης στο συγκεκριμένο πεδίο προτείνεται μόνο σε περιπτώσεις που απαιτείται συμβατότητα με προϋπάρχουσες υπηρεσίες και εφαρμογές.

  Με στόχο την εξασφάλιση της μοναδικότητας του Διακριτικού Ονόματος Υποκειμένου ανά Πάροχο Υπηρεσιών Πιστοποίησης και συνεπώς τη διευκόλυνση της διαχείρισης των πιστοποιητικών, την προώθηση της διαλειτουργικότητας και την ομοιομορφία στη διαδικασία αυθεντικοποίησης που ακολουθούν οι πάροχοι των υπηρεσιών, προτείνεται η υιοθέτηση ενός «Κωδικού Διαχείρισης Πιστοποιητικού» ως μέρος του Διακριτικού Ονόματος του Υποκειμένου και συγκεκριμένα του Κοινού Ονόματος (Common Name). Ο κωδικός αυτός προτείνεται να δημιουργείται από ένα αριθμητικό μέρος (π.χ. αύξων αριθμός) και κάποιο χαρακτηριστικό του κατόχου (π.χ. αρχικά του ονόματός του). Ο συνδυασμός των πεδίων «Οργανισμός» (που αποτυπώνει τον πάροχο υπηρεσιών πιστοποίησης) και «Κοινό Όνομα» (που αποτυπώνει τον προαναφερόμενο κωδικό

διαχείρισης πιστοποιητικού) πρέπει να είναι μοναδικός. Εξυπακούεται ότι το Διακριτικό Όνομα Υποκειμένου, και συνεπώς και τα πεδία «Οργανισμός» και «Κοινό Όνομα» για τα οποία γίνεται λόγος, πρέπει να είναι τα ίδια για το σύνολο των πιστοποιητικών που εκδίδονται για το συγκεκριμένο πρόσωπο από τον συγκεκριμένο ΠΥΠ, ώστε κάθε φορέας να μπορεί να τα αξιοποιήσει για να συνδέσει τα πιστοποιητικά του χρήστη με τα στοιχεία που διατηρεί γι' αυτόν στο σύστημά του.

Θα πρέπει να τονιστεί ότι για τον προαναφερόμενο Κωδικό Διαχείρισης Πιστοποιητικών θα πρέπει να εξασφαλιστεί ότι:

- τηρούνται οι προϋποθέσεις της σχετικής νομοθεσίας σχετικά με τη διασύνδεση αρχείων που περιέχουν προσωπικά δεδομένα (άρθρο 8 του ν. 2472/97)
- δεν δημιουργούνται κατ' αποτέλεσμα οι προϋποθέσεις για χρήση μοναδικού αναγνωριστικού αριθμού – εφόσον δεν υπάρχει αντίστοιχο νομικό υπόβαθρο
- η χρήση του αποσκοπεί ή/και περιορίζεται στην εκπλήρωση του σκοπού επεξεργασίας και δεν εκτείνεται σε άλλους σκοπούς που δεν αφορούν την ταυτοποίηση/ψηφιακή αυθεντικοποίηση του χρήστη της συγκεκριμένης αιτούμενης υπηρεσίας, εφόσον δεν υπάρχει αυτοτελής νόμιμη βάση (όπως π.χ. συγκατάθεση του χρήστη, ρητή διάταξη νόμου, υπέρτερο συμφέρον).

- Δημόσιο Κλειδί Υποκειμένου (Subject Public Key): αποτελείται από το Δημόσιο Κλειδί του Υποκειμένου (Ιδιοκτήτη του ψηφιακού πιστοποιητικού).
- Υπογραφή (Signature): αποτελείται από την ψηφιακή υπογραφή του εκδότη του ψηφιακού πιστοποιητικού.

14.1.6.2 Επεκτάσεις Ψηφιακών Πιστοποιητικών Χρηστών

Τα τομεακά ψηφιακά πιστοποιητικά X.509 ver.3 των χρηστών που θα μπορούν να αξιοποιηθούν σε ηλεκτρονικές υπηρεσίες που προσφέρονται κατευθείαν (όχι μέσω ΚΔΠ) από τους φορείς, θα είναι σύμφωνα με όσα περιλαμβάνονται στο *RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* και θα περιλαμβάνουν τις ακόλουθες επεκτάσεις:

- Χρήση Κλειδιού (Key Usage): αναφέρεται ποια θα είναι η χρήση του δημόσιου κλειδιού που περιλαμβάνεται στο ψηφιακό πιστοποιητικό. Καθώς το τομεακό πιστοποιητικό χρησιμεύει μόνο για επαλήθευση Ψηφιακής Υπογραφής, τα πεδία που ορίζονται είναι τα «digitalSignature» και «nonRepudiation».
- Εναλλακτικό Όνομα Υποκειμένου (Subject Alternative Name): περιλαμβάνεται ένα εναλλακτικό όνομα για τον κάτοχο του ψηφιακού πιστοποιητικού. Δεδομένης της ταυτόχρονης ύπαρξης του πεδίου *Διακριτικό Όνομα Υποκειμένου (Subject DN)*, στο παρόν πεδίο θα περιληφθεί κρυπτογραφημένο (αξιοποιώντας τις οδηγίες του PKCS#1) το σχετικό αναγνωριστικό του χρήστη που επιθυμεί ο δημόσιος φορέας που προσφέρει την υπηρεσία (π.χ. ΑΦΜ).

Η κρυπτογράφηση των τομεακών αναγνωριστικών θα γίνεται με το δημόσιο κλειδί του χρήστη ώστε να μπορεί να αποκρυπτογραφηθεί μόνο με τη συγκατάθεσή του (δηλαδή τη χρήση του ιδιωτικού κλειδιού του). Σε κάθε περίπτωση η όποια τεχνική λύση υιοθετηθεί για τη κρυπτογράφηση του αναγνωριστικού θα πρέπει να εξασφαλίζει α) ότι η αποκρυπτογράφηση δεν μπορεί να γίνει χωρίς τη συγκατάθεση του χρήστη και β) τη δυνατότητα της ανεξάρτητης επαλήθευσής του συμπεριλαμβανομένου στο πιστοποιητικό αναγνωριστικού από τον πάροχο της υπηρεσίας.

Μια ενδεικτική λύση που εξασφαλίζει κάτι τέτοιο είναι η ακόλουθη: Κατά την έκδοση του πιστοποιητικού ο πάροχος υπηρεσιών πιστοποίησης κρυπτογραφεί τη συνένωση ΑΦΜ + Padding[6] με το δημόσιο κλειδί του χρήστη. Ο Πάροχος Υπηρεσιών Πιστοποίησης δεν θα πρέπει να αρχειοθετεί τον ΑΦΜ αλλά ούτε το Padding. Για την επαλήθευση του αναγνωριστικού από τον πάροχο της υπηρεσίας ο χρήστης θα πρέπει να αποστείλει το ψηφιακό πιστοποιητικό του και ταυτόχρονα να αποδείξει ότι είναι κάτοχος του σχετικού ιδιωτικού κλειδιού με κάποια τυπική διαδικασία challenge – response[7]. Στη συνέχεια ο χρήστης αποκρυπτογραφεί την τιμή που είναι αποθηκευμένη στο ψηφιακό πιστοποιητικό του, χρησιμοποιώντας το ιδιωτικό του κλειδί και αποστέλλει το αποτέλεσμα της αποκρυπτογράφησης, που είναι το ΑΦΜ + Padding, στον πάροχο της υπηρεσίας. Ο πάροχος της υπηρεσίας αναπαράγει το κρυπτόγραμμα που είναι αποθηκευμένο στο πιστοποιητικό (κρυπτογραφώντας το ΑΦΜ + Padding με το δημόσιο κλειδί του χρήστη) ώστε να επιβεβαιώσει ότι το ΑΦΜ το οποίο ισχυρίζεται ο χρήστης ότι κατέχει είναι πράγματι αυτό που αναγράφεται στο πιστοποιητικό του.

Να τονιστεί ότι για την κρυπτογράφηση – επαλήθευση του αναγνωριστικού μπορούν να υιοθετηθούν πολλοί εναλλακτικοί τρόποι, μεταξύ των οποίων και αυτοί που ορίζονται στο RFC 4683 που αξιοποιούν συναρτήσεις κατακερματισμού.

- Ταυτοποίηση Χρήστη (Clientauth): αναφέρει εάν το συγκεκριμένο πιστοποιητικό μπορεί να χρησιμοποιηθεί για την ταυτοποίηση του χρήστη. Στα τομεακά ψηφιακά πιστοποιητικά, το συγκεκριμένο πεδίο ορίζεται (set).
- Σημεία Διανομής Καταλόγου Ανακληθέντων Πιστοποιητικών (CRL distribution List): αναφέρονται τα σημεία διανομής της Λίστας Ανακληθέντων Πιστοποιητικών, σε μορφή URL διεύθυνσης.

[6] Το Padding είναι μια τυχαία ακολουθία δεδομένων προτεινόμενου μήκους 256 bits, απαραίτητη για την προστασία απέναντι σε περιπτώσεις δημιουργίας πίνακα αντιστοίχησης μεταξύ καθαρού και κρυπτογραφημένου ΑΦΜ.

[7] Η απόδειξη της κατοχής του ιδιωτικού κλειδιού είναι απαραίτητη για να διασφαλιστεί ότι το ΑΦΜ που θα αποσταλεί αμέσως μετά είναι πράγματι το αποτέλεσμα της αποκρυπτογράφησης της τιμής που είχε αποθηκευθεί στο πιστοποιητικό και όχι προϊόν υποκλοπής από κάποιο τρίτο πρόσωπο.

- Πολιτικές Πιστοποιητικού (Certificate Policies): αναφέρεται το σημείο εύρεσης του κειμένου των Πολιτικών που διέπουν το ψηφιακό πιστοποιητικό, σε μορφή URL διεύθυνσης.

	Τομεακό Ψηφιακό πιστοποιητικό τελικού χρήστη για *ψηφιακή υπογραφή* ηλεκτρονικών μηνυμάτων και εγγράφων
Κρισιμότητα (critical)	Μη ορισμένο
Ψηφιακή Υπογραφή (digitalSignature)	Ορισμένο
Μη αποποίηση (nonRepudiation)	Ορισμένο
Κρυπτογράφηση Κλειδιού (keyEncipherment)	Μη Ορισμένο
Κρυπτογράφηση Δεδομένων (dataEncipherment)	Μη Ορισμένο
Συμφωνία Δεδομένων (keyAgreement)	Μη Ορισμένο
Κλειδί Υπογραφής Πιστοποιητικού (keyCertSign)	Μη Ορισμένο
Υπογραφή Καταλόγου Ανακληθέντων Πιστοποιητικών (cRLSign)	Μη Ορισμένο
(Μόνο Κρυπτογράφηση) (encipherOnly)	Μη Ορισμένο
(Μόνο αποκρυπτογράφηση) (decipherOnly)	Μη Ορισμένο

Πίνακας 23: Ρυθμίσεις Επέκτασης Χρήσης Κλειδιού

14.1.6.3 Επιτρεπτές Χρήσεις Τομεακών ψηφιακών πιστοποιητικών ψηφιακής υπογραφής

- Για ταυτοποίηση και αυθεντικοποίηση του υποκειμένου στις (τομεακές) ηλεκτρονικές υπηρεσίες που προσφέρονται κατευθείαν (όχι μέσω ΚΔΠ) από Φορείς του Δημοσίου.
- Για δημιουργία ψηφιακών υπογραφών στις (τομεακές) ηλεκτρονικές υπηρεσίες που προσφέρονται κατευθείαν (όχι μέσω ΚΔΠ) από Φορείς του Δημοσίου.

- Για την κρυπτογράφηση/ αποκρυπτογράφηση των τομεακών αναγνωριστικών που συμπεριλαμβάνονται στα αντίστοιχα ψηφιακά πιστοποιητικά.

14.1.6.4 Μη επιτρεπτές Χρήσεις Τομεακών ψηφιακών πιστοποιητικών ψηφιακής υπογραφής

- Για συναλλαγές που δεν ορίζονται ρητά στην ενότητα 14.1.6.3.

14.1.7 Απαιτήσεις Λειτουργίας

Σε αυτή την ενότητα περιγράφονται οι απαιτήσεις που πρέπει να καλύπτουν οι Αρχές Πιστοποίησης και παρουσιάζονται στην αντίστοιχη ενότητα Πολιτικής Τομεακών Πιστοποιητικών, όσον αφορά στις διαδικασίες που πρέπει να ακολουθούνται κατά τη διάρκεια λειτουργίας της Αρχής Πιστοποίησης που επιφορτίζεται με τη διαχείριση των τομεακών πιστοποιητικών.

14.1.7.1 Θέματα επικοινωνίας μεταξύ των οντοτήτων ΥΔΚ

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.1.

14.1.7.2 Διαχείριση Κλειδιών

14.1.7.2.1 Δημιουργία κλειδιών

14.1.7.2.1.1 Οντότητες Δημιουργίας Κλειδιών

Οι οντότητες που επιφορτίζονται με τη δημιουργία του ζεύγους κλειδιών προσδιορίζονται από την ΥΔΚ.

14.1.7.2.1.2 Μήκος κλειδιών

Το μήκος των κλειδιών θα πρέπει να είναι τουλάχιστον 1024 bits. Το μέγεθος μπορεί να απαιτηθεί να είναι ακόμη μεγαλύτερο, ανάλογα με τις εξελίξεις στα επιστημονικά δρώμενα στη γνωστική περιοχή της κρυπτολογίας.

14.1.7.2.1.3 Παράμετροι Ασφάλειας

Τα κλειδιά θα πρέπει να δημιουργούνται με την αξιοποίηση ορθών παραμέτρων (n,q), με στόχο την επίτευξη δημιουργίας ασφαλών κλειδιών.

14.1.7.2.1.4 Μέθοδοι δημιουργίας των κλειδιών

Τα ζεύγη κλειδιών, τα οποία θα αξιοποιούνται για τη ψηφιακή υπογραφή σε τομεακές ηλεκτρονικές υπηρεσίες, θα δημιουργούνται αποκλειστικά και μόνο από τους τελικούς χρήστες κάνοντας χρήση ασφαλών διατάξεων, συμβατών με τις σχετικές απαιτήσεις του προεδρικού διατάγματος Π.Δ. 150/2001, που τους έχουν χορηγηθεί κατά τη διαδικασία εγγραφής σε υπηρεσίες εμπιστοσύνης επιπέδου 3. Για τη δημιουργία του ζεύγους κλειδιών θα αξιοποιούνται

οι κατάλληλοι κωδικοί πρόσβασης. Καμία οντότητα δεν θα δύναται να δημιουργήσει κλειδιά ψηφιακής υπογραφής για λογαριασμό κάποιου χρήστη.

14.1.7.2.1.5 Τρόποι αξιοποίησης των κλειδιών

Τα κλειδιά που δημιουργούνται και διαμοιράζονται στους χρήστες θα πρέπει να αξιοποιούνται σύμφωνα με τα όσα προδιαγράφονται στην ενότητα επιτρεπτές χρήσεις των πιστοποιητικών (βλέπε ενότητα 14.1.6.3).

14.1.7.2.1.6 Τρόποι παροχής του δημοσίου κλειδιού στην Αρχή Πιστοποίησης

Το δημόσιο κλειδί για την επαλήθευση της ψηφιακής υπογραφής αποθηκεύεται στην Αρχή Πιστοποίησης με την έκδοση του αντίστοιχου ψηφιακού πιστοποιητικού, το οποίο και συμπεριλαμβάνεται στην αντίστοιχη αίτηση έκδοσης του ψηφιακού τομεακού πιστοποιητικού μορφής PKCS#10.

14.1.7.2.1.7 Μηχανισμοί και πρότυπα που αξιοποιούνται για τη δημιουργία των κλειδιών

Οι διατάξεις που χρησιμοποιούνται για τη δημιουργία του ζεύγους κλειδιών θα πρέπει να τηρούν πλήρως τις προϋποθέσεις που ορίζονται στο Π.Δ. 150/2001 προκειμένου να χαρακτηρίζονται ως «ασφαλείς». Ως εκ τούτου όλες οι συσκευές που αξιοποιούνται για την δημιουργία των κλειδιών θα πρέπει κατ' ελάχιστο να ακολουθούν τις προδιαγραφές FIPS 140-2 επιπέδου 3.

14.1.7.2.2 Ανάκληση Κλειδιών

14.1.7.2.2.1 Περιπτώσεις ανάκλησης κλειδιών αυτομάτως από την Αρχή Πιστοποίησης

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.2.2.1. Επιπλέον η Αρχή Πιστοποίησης τομεακών ψηφιακών πιστοποιητικών έχει τη δυνατότητα ανάκλησης των πιστοποιητικών μετά από σχετικό αίτημα του Δημόσιου Φορέα που αξιοποιεί το πιστοποιητικό.

14.1.7.2.2.2 Οντότητες ανάκλησης κλειδιών

Οι οντότητες που επιφορτίζονται τη διαδικασία ανάκλησης κλειδιών καθορίζονται από την εκάστοτε ΥΔΚ.

14.1.7.2.2.3 Οντότητες που μπορούν να αιτηθούν την ανάκληση κλειδιών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.2.2.3. Επιπρόσθετα ανάκληση πιστοποιητικών μπορεί να αιτηθεί ο Δημόσιος Φορέας για τον οποίο εκδίδονται τα αντίστοιχα τομεακά πιστοποιητικά.

14.1.7.2.2.4 Μέθοδοι ανάκλησης ζεύγους κλειδιών

Τα ζεύγη κλειδιών θα διαγράφονται από το διακριτικό στο οποίο αποθηκεύονται, εφόσον γίνεται αποδεκτή η αίτηση ανάκλησης.

14.1.7.2.2.5 Διαδικασία ανάκλησης κλειδιών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.2.2.5. Στις περιπτώσεις όπου ο χρήστης υποβάλει την αίτηση αυτοπροσώπως, θα πρέπει να αποδείξει την κατοχή του αντίστοιχου αναγνωριστικού υποβάλλοντας τα απαραίτητα έγγραφο

14.1.7.2.2.6 Μέθοδοι αυθεντικοποίησης οντοτήτων που αιτούνται την ανάκληση κλειδιών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.2.2.6.

14.1.7.2.3 Επαναδημιουργία – Ανανέωση Κλειδιού

14.1.7.2.3.1 Περιπτώσεις επαναδημιουργίας – ανανέωσης κλειδιού

Σε καμία περίπτωση δεν θα πρέπει να πραγματοποιείται επαναδημιουργία (ίδιων) κλειδιών ψηφιακής υπογραφής. Η ανανέωση του ζεύγους κλειδιών για την ψηφιακή υπογραφή γίνεται είτε λόγω λήξης του τομεακού πιστοποιητικού είτε λόγω δημοσίευσης επιθέσεων που επηρεάζουν τα υπάρχοντα ζεύγη κλειδιών. Ουσιαστικά, ως ανανέωση του ζεύγους κλειδιών νοείται η έκδοση νέου ζεύγους κλειδιών ψηφιακής υπογραφής.

14.1.7.2.3.2 Οντότητες Επαναδημιουργίας-Ανανέωσης Ζεύγους Κλειδιών

Οι οντότητες που επιφορτίζονται τη διαδικασία επαναδημιουργίας-ανανέωσης ζεύγους κλειδιών καθορίζονται από την ΥΔΚ.

14.1.7.2.3.3 Αυθεντικοποίηση οντοτήτων που αιτούνται την ανανέωση κλειδιών και πιστοποιητικών

Οι οντότητες που αιτούνται την ανανέωση κλειδιών είναι δυνατό να αυθεντικοποιηθούν με την αξιοποίηση της υπάρχουσας ηλεκτρονικής υποδομής αυθεντικοποίησης, όπως αυτή προβλέπεται για το επίπεδο εμπιστοσύνης 3. Επίσης η αυθεντικοποίηση μπορεί να γίνει με τη φυσική παρουσία τους στην Αρχή Εγγραφής ή την Αρχή Πιστοποίησης.

14.1.7.2.4 Προστασία κλειδιών

14.1.7.2.4.1 Τρόποι προστασίας ιδιωτικών κλειδιών της Αρχής Πιστοποίησης

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.2.4.1.

14.1.7.2.4.2 Τρόποι προστασίας των δημιουργούμενων κλειδιών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.2.4.2.

14.1.7.2.4.3 Τρόποι προστασίας των αποθηκευμένων κλειδιών

Τα ιδιωτικά κλειδιά θα πρέπει:

- να αποθηκεύονται σε tamper proof συσκευές (π.χ έξυπνες κάρτες)
- να μην είναι δυνατή η ανάγνωσή τους (εκτός της συσκευής) (read protection)
- η τροποποίησή τους θα πρέπει να είναι δυνατή μόνο με την αξιοποίηση των αντίστοιχων κρυπτογραφικών κλειδιών
- Η ενεργοποίηση των κλειδιών θα πραγματοποιείται με την αξιοποίηση του αντίστοιχου PIN

Σε κάθε περίπτωση η αποθήκευση των ιδιωτικών κλειδιών πρέπει να γίνει σε ασφαλείς διατάξεις, όπως ορίζεται στο προεδρικό διάταγμα Π.Δ. 150/2001.

14.1.7.2.4.4 Τρόποι ενεργοποίησης των κλειδιών

Η ενεργοποίηση των κλειδιών θα πραγματοποιείται με την αξιοποίηση του αντίστοιχου PIN/PUK.

14.1.7.2.5 Άλλα θέματα διαχείρισης κλειδιών

Οι πάροχοι ΥΔΚ θα πρέπει να προσδιορίζουν θέματα διαχείρισης κλειδιών που δεν εμπίπτουν στις παραπάνω κατηγορίες.

14.1.7.3 Διαχείριση Πιστοποιητικών

14.1.7.3.1 Οντότητες που μπορούν να αιτηθούν την έκδοση τομεακών πιστοποιητικών

Οι οντότητες που μπορούν να πραγματοποιήσουν αιτήσεις για την έκδοση ενός τομεακού ψηφιακού πιστοποιητικού είναι:

- κάθε φυσικό πρόσωπο
- κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου ιδιωτικού δικαίου
- κάθε νόμιμα εξουσιοδοτημένος εκπρόσωπος νομικού προσώπου δημοσίου δικαίου

που θέλει να αξιοποιήσει το τομεακό ψηφιακό πιστοποιητικό στα πλαίσια των ηλεκτρονικών υπηρεσιών που προσφέρονται κατευθείαν (όχι μέσω ΚΔΠ) από κάποιον Δημόσιο Φορέα.

14.1.7.3.2 Αίτηση έκδοσης πιστοποιητικών

Οι οντότητες που αιτούνται την έκδοση πιστοποιητικών θα πρέπει να εφαρμόζουν και να αποδέχονται, σε κάθε περίπτωση, την Πολιτική Τομεακών Πιστοποιητικών που εφαρμόζει η εκάστοτε ΥΔΚ. Για να είναι δυνατή η αίτηση έκδοσης πιστοποιητικών, ο χρήστης θα πρέπει να έχει παραλάβει το διακριτικό αποθήκευσης στο οποίο είναι αποθηκευμένα τα ζεύγη κλειδιών του, αφού βέβαια έχει πρώτα υποβάλει αίτηση εγγραφής σε υπηρεσίες επιπέδου εμπιστοσύνης

3 ακολουθώντας τις διαδικασίες εγγραφής που προβλέπονται για το επίπεδο 3. Επιπρόσθετα θα πρέπει να αποδεικνύει την κατοχή του τομεακού αναγνωριστικού που θα αποθηκευτεί στο πιστοποιητικό.

Εφόσον έχει παραλάβει το διακριτικό αποθήκευσης είναι σε θέση να αιτηθεί την έκδοση των τομεακών πιστοποιητικών, αξιοποιώντας την ηλεκτρονική υπηρεσία έκδοσης ψηφιακών πιστοποιητικών. Συγκεκριμένα, για την έκδοση πιστοποιητικού ψηφιακής υπογραφής ο χρήστης υποβάλει ηλεκτρονικά, στην Αρχή Εγγραφής, αίτηση στην οποία ενσωματώνει το δημόσιο κλειδί του, ψηφιακά υπογεγραμμένο από το αντίστοιχο ιδιωτικό που βρίσκεται αποθηκευμένο στο διακριτικό αποθήκευσής του. Οι ψηφιακές αυτές αιτήσεις θα πρέπει να ακολουθούν το πρότυπο PKCS#10. Η Αρχή Εγγραφής, εφόσον ελέγξει την ορθότητα των στοιχείων της αίτησης και την εγκρίνει, προωθεί την αίτηση στην Αρχή Πιστοποίησης για τη δημιουργία του τομεακού πιστοποιητικού ψηφιακής υπογραφής. Η έγκριση των στοιχείων πρέπει να πραγματοποιείται σύμφωνα με τις μεθόδους που παρουσιάζονται στην ενότητα 14.1.5.3.7.2. Η εγκεκριμένη και υπογεγραμμένη αίτηση έκδοσης πιστοποιητικού θα πρέπει να μεταφέρεται από την Αρχή Εγγραφής στην Αρχή Πιστοποίησης με ασφαλή τρόπο, όπως έχει προδιαγραφεί στην ενότητα 14.1.7.1. Η Αρχή Πιστοποίησης, με τη σειρά της, εκδίδει το αντίστοιχο πιστοποιητικό ψηφιακής υπογραφής, με βάση τα στοιχεία που υπάρχουν στην αίτηση, και ενημερώνει το χρήστη ότι μπορεί να το παραλάβει από τους χώρους αποθήκευσης που διατηρεί η ΥΔΚ.

Επίσης όλα τα αναγνωριστικά, για τα οποία μέσω της παρούσας αίτησης έκδοσης πιστοποιητικού ο χρήστης έχει δώσει τη ρητή συγκατάθεσή του να αξιοποιούνται από Δημόσιους Φορείς, πρέπει να κρυπτογραφούνται με τα δημόσια κλειδιά των φορέων και να ενσωματώνονται στην αίτηση που υποβάλει και όχι να κρυπτογραφούνται από την Αρχή Πιστοποίησης, ώστε σε κάθε περίπτωση να διασφαλίζεται η ακεραιότητά τους.

14.1.7.3.3 Έκδοση πιστοποιητικών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.3.3.

Η βασική δομή του πιστοποιητικού περιγράφεται στην ενότητα 14.1.6.1.

14.1.7.3.4 Αποδοχή Πιστοποιητικού

Για την ενεργοποίηση του πιστοποιητικού, μετά την έκδοση, ο τελικός χρήστης θα πρέπει να στείλει ένα υπογεγραμμένο μήνυμα στην Αρχή Πιστοποίησης μέσα σε εύλογο διάστημα (π.χ. εντός 30 ημερών, χρόνος που θα προσδιοριστεί από την ΥΔΚ), διαφορετικά το πιστοποιητικό δε θα δημοσιεύεται στον κατάλογο ενεργών πιστοποιητικών και συνεπώς δε θα θεωρείται έγκυρο.

14.1.7.3.5 Ανάκληση πιστοποιητικών

14.1.7.3.5.1 Περιπτώσεις ανάκλησης πιστοποιητικών αυτομάτως από την Αρχή Πιστοποίησης

Βλέπε ενότητα 14.1.7.2.2.1.

14.1.7.3.5.2 Οντότητες που αιτούνται την ανάκληση πιστοποιητικών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.3.5.2. Επίσης την ανάκληση του τομεακού πιστοποιητικού μπορεί να αιτηθεί ο δημόσιος φορέας για τις υπηρεσίες του οποίου έχει εκδοθεί το πιστοποιητικό.

14.1.7.3.5.3 Χρονικό διάστημα επεξεργασίας αιτήματος ανάκλησης

Το χρονικό διάστημα στο οποίο θα πρέπει να πραγματοποιείται η ανάκληση πιστοποιητικών θα πρέπει να καθορίζεται από την ΥΔΚ (ενδεικτικός χρόνος επεξεργασίας είναι μία ημέρα).

14.1.7.3.5.4 Μέθοδοι που αξιοποιούνται για την ανάκληση πιστοποιητικών

Δεν ορίζονται.

14.1.7.3.5.5 Διαδικασία ανάκλησης πιστοποιητικών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.3.5.5. Στις περιπτώσεις όπου ο χρήστης υποβάλει την αίτηση αυτοπροσώπως, θα πρέπει να αποδείξει την κατοχή του αντίστοιχου αναγνωριστικού υποβάλλοντας τα απαραίτητα έγγραφα.

14.1.7.3.5.6 Μέθοδοι ενημέρωσης της Λίστας Ανάκλησης Πιστοποιητικών

Δεν ορίζονται.

14.1.7.3.5.7 Θέματα χρόνου ανανέωσης της Λίστας Ανάκλησης Πιστοποιητικών

Η Λίστα Ανάκλησης Πιστοποιητικών θα πρέπει να ενημερώνεται άμεσα κατά την ανάκληση ενός πιστοποιητικού (σε διάστημα μιας ημέρας) και τουλάχιστον μια ημέρα πριν την τυπική λήξη της.

14.1.7.3.5.8 Θέματα δημοσιοποίησης της Λίστας Ανάκλησης Πιστοποιητικών

Η λίστα ανάκλησης πιστοποιητικών θα δημοσιοποιείται μέσω του ιστοχώρου που συντηρεί η ΥΔΚ και ο εμπλεκόμενος δημόσιος φορέας, ενώ θα μπορεί να αποστέλλεται και μέσω υπογεγραμμένου e-mail στους χρήστες για την άμεση ενημέρωσή τους.

14.1.7.3.5.9 Άλλες περιπτώσεις ανάκλησης πιστοποιητικών

Δεν ορίζονται.

14.1.7.3.5.10 Δομή της Λίστας Ανάκλησης Πιστοποιητικών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.3.5.10.

14.1.7.3.5.11 Μέθοδοι αυθεντικοποίησης των οντοτήτων που αιτούνται την ανάκληση πιστοποιητικών

Οι οντότητες που αιτούνται ανάκληση πιστοποιητικών μπορούν να αυθεντικοποιηθούν μέσω της υπάρχουσας ηλεκτρονικής υποδομής αυθεντικοποίησης, όπως αυτή προσδιορίζεται για το επίπεδο εμπιστοσύνης 3.

14.1.7.3.6 Επανέκδοση Τομεακών πιστοποιητικών

Με τον όρο «επανέκδοση ενός τομεακού πιστοποιητικού» νοείται η έκδοση νέου τομεακού πιστοποιητικού σε κάποιο χρήστη, για τους λόγους που αναφέρονται στην ενότητα 13.1.7.3.6 όπως επίσης και σε περιπτώσεις τροποποίησης των τομεακών αναγνωριστικών που είναι αποθηκευμένα στο πιστοποιητικό.

14.1.7.3.6.1 Οντότητες που μπορούν να αιτηθούν επανέκδοσης τομεακού πιστοποιητικού

Οι οντότητες που μπορούν να ζητήσουν την επανέκδοση πιστοποιητικού είναι οι νόμιμοι κάτοχοι των πιστοποιητικών καθώς και οι δημόσιοι φορείς που τα αξιοποιούν.

14.1.7.3.6.2 Οντότητες που πραγματοποιούν την επανέκδοση του πιστοποιητικού

Οι οντότητες που πραγματοποιούν την επανέκδοση του πιστοποιητικού προσδιορίζονται από την εκάστοτε ΥΔΚ.

14.1.7.3.6.3 Διαδικασίες επανέκδοσης του πιστοποιητικού

Για την επανέκδοση ενός ψηφιακού πιστοποιητικού ο χρήστης θα πρέπει να συμπληρώσει την απαραίτητη αίτηση επανέκδοσης του ψηφιακού πιστοποιητικού και να την υποβάλλει στη Αρχή Εγγραφής (σε ηλεκτρονική μορφή εφόσον το διακριτικό αποθήκευσης βρίσκεται σε λειτουργία ή έντυπα σε όλες τις άλλες περιπτώσεις). Η Αρχή Εγγραφής αφού ελέγξει την ορθότητα της αίτησης, την προωθεί στην Αρχή Πιστοποίησης για την επανέκδοση του ψηφιακού πιστοποιητικού και ενημερώνει το χρήστη για την επιτυχή έκδοσή του.

14.1.7.3.6.4 Μέθοδοι αυθεντικοποίησης των οντοτήτων που αιτούνται επανέκδοση πιστοποιητικού

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.3.6.4.

14.1.7.3.7 Υπηρεσίες ελέγχου κατάστασης πιστοποιητικού

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.3.7.

14.1.7.3.8 Λήξη Συνδρομής

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.3.8.

14.1.7.4 Υπηρεσίες Χρονοσήμανσης

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.4.

14.1.7.5 Ελεγκτικές Διαδικασίες κατά τη λειτουργία

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.5.

14.1.7.6 Διαχείριση Πολιτικής Πιστοποιητικών

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.7.10.

14.1.8 Θεσμικό-Κανονιστικό Πλαίσιο

Ισχύουν τα αναγραφόμενα στην ενότητα 13.1.8.

15. ΠΑΡΑΡΤΗΜΑ Δ: ΟΜΟΣΠΟΝΔΕΣ ΤΑΥΤΟΤΗΤΕΣ (FEDERATED IDENTITIES)

15.1 Εισαγωγή

Ως **Ομοσπονδία** ορίζεται το σύνολο δύο ή περισσοτέρων επιχειρηματικών συνεργατών που έχουν κοινούς πελάτες και στοχεύουν στην αναβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών και ταυτόχρονα στη μείωση του κόστους διαχείρισης ταυτοτήτων. Για παράδειγμα, ένα χρηματοοικονομικό ίδρυμα μπορεί να προσφέρει, σε συγκεκριμένους πελάτες, συνεχή πρόσβαση σε πληροφορίες της οικονομικής αγοράς μέσω κάποιας τρίτης ερευνητικής εταιρείας. Κυβερνητικοί οργανισμοί μπορεί να συνεργαστούν ώστε να παρέχουν ένα ενιαίο μονοπάτι ηλεκτρονικής επικοινωνίας των πολιτών με αυτούς. Μία μικρή online επιχείρηση μπορεί να επιλέξει η διαχείριση των αρχείων των πελατών της να γίνεται από κάποιο οικονομικό ίδρυμα που παρέχει τέτοιου τύπου υπηρεσίες. Σε όλες αυτές τις περιπτώσεις, οι επιχειρήσεις χρειάζεται να δημιουργήσουν μια επιχειρησιακή ομοσπονδία.

Οι επιχειρησιακές ομοσπονδίες βασίζονται στις σχέσεις εμπιστοσύνης. Οι σχέσεις αυτές δημιουργούνται χρησιμοποιώντας νομικές συμφωνίες μεταξύ των συμμετεχόντων και είναι απαραίτητο να ισχύσουν πριν την έναρξη λειτουργίας της ομοσπονδίας. Αφού οριστούν οι επιχειρήσεις και οι μεταξύ τους συμφωνίες, οι συνεργάτες πρέπει να αξιοποιούν κάποια τεχνολογία που υποστηρίζει τις συμφωνίες της ομοσπονδίας, δηλαδή κατ' ελάχιστον: δυνατότητες διαχείρισης της ομοσπονδίας και της μεταξύ τους εμπιστοσύνης, κρυπτογραφική υποστήριξη και εφαρμογές πρωτοκόλλων που επιτρέπουν τη διεκπεραίωση μιας ασφαλούς συνεργασίας στο διαδικτυακό περιβάλλον.

Στην τεχνολογία πληροφορίας (information technology - IT), η ομόσπονδη ταυτότητα (federated identity) έχει δύο γενικές έννοιες:

- Τη διαδικασία αυθεντικοποίησης ενός χρήστη, διαμέσου πολλαπλών IT συστημάτων ή οργανισμών.
- Την εικονική ένωση (ή assembled identity), των πληροφοριών ενός χρήστη (ή μιας αρχής) που είναι αποθηκευμένες σε πολλαπλά διακριτά συστήματα διαχείρισης ταυτότητας. Τα δεδομένα συνενώνονται μεταξύ τους χρησιμοποιώντας ένα κοινό στοιχείο, συνήθως το όνομα του χρήστη.

Η ομόσπονδη ταυτότητα μπορεί να επιτευχθεί μέσω ενός μεγάλου αριθμού μεθόδων, μερικές εκ των οποίων κάνουν χρήση επίσημων προτύπων του Διαδικτύου, όπως το OASIS SAML, ή δημοσιευμένων προδιαγραφών για τεχνολογίες ανοικτού κώδικα (π.χ. Information Cards, OpenID, the Higgins trust framework, Novell's Bandit project).

15.2 Διαχείριση Ομόσπονδης Ταυτότητας

Κάθε άτομο μπορεί να αναγνωριστεί μέσω πολλών κατηγοριών προσωπικών δεδομένων. Διαφορετικοί συνδυασμοί των δεδομένων αυτών μπορούν να ταυτοποιήσουν κάποιο άτομο μοναδικά. Δεδομένης της πληθώρας πληροφοριών που συνδέονται με την ταυτότητα ενός ατόμου και τον τρόπο που αυτή ορίζεται, ανάλογα με το πλαίσιο χρήσης, είναι απαραίτητη η δημιουργία ενός συστήματος που θα επιτρέπει τη διαχείριση των πληροφοριών αυτών στον ψηφιακό χώρο. Στη διεθνή βιβλιογραφία υπάρχει ομοφωνία ως προς τον ορισμό της διαχείρισης ταυτότητας ως διοικητικής διαδικασίας. Πρόκειται για το σύνολο των διαδικασιών που επιτρέπουν τη δημιουργία, διατήρηση και κατάργηση των πληροφοριών που ορίζουν μοναδικά κάθε χρήστη ενός συνόλου πληροφοριακών συστημάτων.

Συνεπώς μια βασική απαίτηση για την καθιέρωση της επιχειρησιακής ομοσπονδίας είναι η διαχείριση των ταυτοτήτων σε ολόκληρη την ομοσπονδία. Η διαδικασία αυτή ονομάζεται διαχείριση ομόσπονδης ταυτότητας (federated identity management) και είναι απαραίτητη για την εγκαθίδρυση ασφαλούς και οικονομικώς αποδοτικής επιχειρησιακής συνεργασίας, με τον έλεγχο του ποιος συνδέεται σε ποιες εφαρμογές και σε ποιους πόρους.

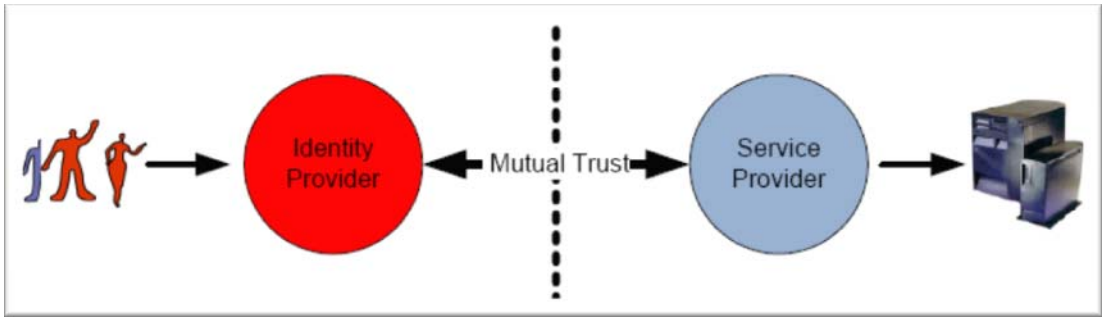
Η διαχείριση ταυτότητας εστιάζει κυρίως στα εξής ζητήματα:

- Στον προσδιορισμό των επιχειρηματικών διαδικασιών που απαιτούν ταυτοποίηση των χρηστών
- Στο βαθμό ταυτοποίησης των χρηστών στο σύστημα, δηλαδή στο πόσο ισχυρή είναι η ταυτότητα που δημιουργείται από το σύστημα και αν είναι ανθεκτική σε αντιγραφή ή κακή χρήση της
- Στη διακριτική προσπέλαση των χρηστών σε διάφορες υπηρεσίες που προσφέρει το σύστημα
- Στην επιλογή εργαλείων που θα διαχειρίζονται αποτελεσματικά τις ταυτότητες των χρηστών και θα υλοποιούν ένα ασφαλές περιβάλλον χωρίς προβλήματα

Η διαχείριση ομόσπονδης ταυτότητας καθιστά εφικτό, για μια ήδη αυθεντικοποιημένη οντότητα, να αναγνωρίζεται και να παίρνει μέρος σε υπηρεσίες σε διαφορετικούς τομείς. Οι χρήστες μπορούν να αυθεντικοποιηθούν από έναν οργανισμό ή ιστοσελίδα, να αναγνωρίζονται και να τους παραδίδεται προσωπικό περιεχόμενο και υπηρεσίες και από άλλους τομείς, χωρίς να χρειάζεται να αυθεντικοποιηθούν πάλι. Έτσι, παρέχεται η δυνατότητα αυξημένης πρόσβαση σε πληροφορίες εντός και εκτός των ορίων ενός και μόνο οργανισμού.

Η διαχείριση ομόσπονδης ταυτότητας παρέχει ένα άμεσο όφελος στους χρήστες της ομοσπονδίας. Ο χρήστης είναι απαραίτητο να θυμάται μόνο τα διαπιστευτήριά του προκειμένου να πιστοποιηθεί και να αυθεντικοποιηθεί. Η αυθεντικοποίηση σε άλλους οργανισμούς της ομοσπονδίας μπορεί να είναι μια μοναδική διαδικασία χωρίς την ανάγκη για άμεση αλληλεπίδραση με το χρήστη. Αυτή η μοναδική επικύρωση μειώνει τον αριθμό των διαπιστευτηρίων που απαιτείται από τους χρήστες να θυμούνται και το συνολικό αριθμό παροχής τους για πρόσβαση σε υπηρεσίες.

Οι πιο σημαντικοί ρόλοι σε μια ομοσπονδία είναι ο **πάροχος ταυτότητας (identity provider)** και ο **πάροχος υπηρεσίας (service provider)**. Ο πάροχος ταυτότητας είναι ο εγγυητής σε μία ομοσπονδία. Είναι υπεύθυνος για τη διαχείριση των χρηστών και των ταυτοτήτων τους, για την έκδοση πιστοποιητικών, την αυθεντικοποίησή τους και εγγυάται για την ταυτότητα των χρηστών. Ο πάροχος υπηρεσιών είναι υπεύθυνος για τον έλεγχο πρόσβασης σε υπηρεσίες, επικυρώνει τις πληροφορίες των ταυτοτήτων για τον πάροχο ταυτότητας, παρέχει πρόσβαση βασιζόμενος στις ταυτότητες και διαχειρίζεται μόνο τοπικά χαρακτηριστικά των χρηστών και όχι ολόκληρο το προφίλ τους. Η αμοιβαία εμπιστοσύνη μεταξύ των δύο παρόχων που δημιουργείται σε μία ομοσπονδία παρουσιάζεται στο παρακάτω σχήμα.



Σχήμα 3: Επιχειρησιακή ομοσπονδία με πάροχο ταυτότητας και πάροχο υπηρεσιών

Σε κάποια επιχειρησιακά σενάρια ένας οργανισμός μπορεί να ενεργεί τόσο ως πάροχος ταυτότητας όσο και ως πάροχος υπηρεσιών. Για παράδειγμα όταν κάποιες δημόσιες υπηρεσίες έχουν πρόσβαση στις μεταξύ τους εφαρμογές, κάθε υπηρεσία παίζει το ρόλο είτε του παρόχου ταυτότητας είτε των παρόχου υπηρεσιών, βασιζόμενη στο ποιος οργανισμός παρέχει τις εφαρμογές σε κάθε περίπτωση.

15.3 Διαχείριση Ταυτότητας στην Ηλεκτρονική Διακυβέρνηση

Συνήθη θέματα που σχετίζονται με την έννοια της ταυτότητας στο ηλεκτρονικό περιβάλλον, και συγκεκριμένα στο Διαδίκτυο, είναι τα παρακάτω:

- αυξημένη ανάγκη ταυτοποίησης των συναλλασσομένων
- επιθυμία των χρηστών να διατηρήσουν τις συνήθειες του «πραγματικού» κόσμου δηλαδή να διατηρούν την ανωνυμία τους στις συναλλαγές
- επικράτηση μιας κουλτούρας όπου ο κάθε χρήστης όχι μόνο δεν αποκαλύπτει την ταυτότητά του κατά την περιήγησή του στο Διαδίκτυο αλλά χρησιμοποιεί ένα ή περισσότερα ψευδώνυμα
- δυνατότητα εταιρειών να συλλέξουν σημαντικές πληροφορίες για τις συνήθειες των συναλλασσομένων, οι οποίες μπορούν να οδηγήσουν σε πιο στοχευμένες πωλήσεις και σε μεγαλύτερα κέρδη

Στο πλαίσιο της ηλεκτρονικής διακυβέρνησης, το ζήτημα της διαχείρισης ταυτότητας είναι ίσως πιο έντονο σε σχέση με τη μέχρι σήμερα σημασία του στις εμπορικές συναλλαγές. Αν και ο βασικός στόχος των συστημάτων διαχείρισης ταυτότητας παραμένει η προστασία των συναλλασσομένων από κακόβουλες συναλλαγές, μια σειρά ζητημάτων λαμβάνουν διαφορετική υπόσταση δεδομένου του πλαισίου εφαρμογής τους. Συγκεκριμένα, το ζήτημα της ανωνυμίας κατά τις συναλλαγές με το Δημόσιο δεν θεωρείται ιδιαίτερα σημαντικό και αναφέρεται κυρίως στην απόκτηση πληροφοριών. Το σύνολο των συναλλαγών με το Δημόσιο απαιτεί την πιστοποίηση της ταυτότητας του ατόμου. Οι βασικές αντιρρήσεις των πολιτών αφορούν κυρίως στα δεδομένα που το κάθε κράτος επιλέγει να απαρτίζουν την πληροφοριακή τους ταυτότητα (informational identity). Στο ηλεκτρονικό εμπόριο, η ταυτότητα του ατόμου διαμορφώνεται εν μέρει με τη δική του συμβολή. Στην ηλεκτρονική διακυβέρνηση κάτι τέτοιο δεν είναι εφικτό, αφού το Κράτος προσδιορίζει τις πληροφοριακές ανάγκες του και τα περιθώρια δράσης είναι συχνά περιορισμένα. Οι φόβοι που εγείρει η διαχείριση ταυτότητας στα πλαίσια της Ηλεκτρονικής Διακυβέρνησης σχετίζονται κυρίως με τους φορείς ταυτοποίησης και αυθεντικοποίησης, οι οποίοι συγκεντρώνουν ευαίσθητα και μοναδικά στοιχεία του ατόμου για τα οποία μέχρι πρότινος φορέας ήταν το ίδιο το άτομο.

Η ομόσπονδη διαχείριση ξεπερνά τα εμπόδια της κεντρικής αποθήκευσης προσωπικών πληροφοριών ενώ επιτρέπει στους χρήστες να συνδέουν πληροφορίες της ταυτότητάς τους μεταξύ διαφορετικών λογαριασμών. Από τη στιγμή που οι χρήστες μπορούν να ελέγξουν πότε και πώς οι λογαριασμοί και οι πληροφορίες τους συνδέονται και διαμοιράζονται, διατηρούν τον μεγαλύτερο έλεγχο πάνω σε αυτές.

Η ομοσπονδιακή διαχείριση ταυτότητας:

- Θεσπίζει έναν μηχανισμό τόσο για την ανταλλαγή όσο και για τη διαχείριση πληροφοριών ταυτότητας καθώς αυτές διακινούνται μεταξύ διαφορετικών οργανισμών.
- Προσφέρει έναν οικονομικό τρόπο για την καθιέρωση του μηχανισμού μοναδιαίας αυθεντικοποίησης (single sign-on) σε πληροφορίες διαφορετικών οργανισμών.
- Καθιστά δυνατό στους οργανισμούς να διαχειρίζονται πολλαπλά security domains με έναν αποδοτικό μηχανισμό ο οποίος συνδέει όλες τις ταυτότητες και επιτρέπει μοναδιαία αυθεντικοποίηση μεταξύ των security domains.

Η ιδέα που οδήγησε στη δημιουργία ομόσπονδων ταυτοτήτων είναι ότι η υπάρχουσα, ετερογενής φύση των αρχιτεκτονικών των πληροφοριακών συστημάτων των οργανισμών δεν θα πρέπει να είναι αναγκαίο να αλλάξει. Ο στόχος των ομόσπονδων ταυτοτήτων είναι να επιτυγχάνεται, αποδοτικά και με ασφάλεια, η πρόσβαση σε πόρους διαφορετικών οργανισμών με αποτέλεσμα να αυξάνεται η παραγωγικότητα, η λειτουργική αποδοτικότητα και η ανταγωνιστική διαφοροποίηση.

Η διαλειτουργικότητα είναι μια απαίτηση μεταξύ οργανισμών αλλά και κυβερνήσεων. Μια ομόσπονδη αρχιτεκτονική επιτρέπει στα διάφορα συστήματα να αλληλεπιδρούν ενώ διατηρούν

την αυτονομία τους. Ένας κύκλος εμπιστοσύνης παρέχει στους συμμετέχοντες οργανισμούς ένα πλαίσιο ώστε να διασφαλίσουν ότι η διαλειτουργικότητα αυτή είναι έμπιστη και ασφαλής.

Ίσως, σε κανέναν άλλο τομέα επικοινωνιών δεν είναι τόσο επιτακτική η ανάγκη για ασφαλή αλλά και ανοιχτή πρόσβαση όσο στην επικοινωνία κυβέρνησης - πολίτη. Όλες οι κυβερνήσεις ανά τον κόσμο επενδύουν στην ηλεκτρονική διακυβέρνηση με σκοπό να παρέχουν στους πολίτες τους τα οφέλη της τεχνολογίας. Στο δημόσιο τομέα, τα διάφορα κυβερνητικά τμήματα προσφέρουν στους πολίτες και τους οργανισμούς διαδικτυακή πρόσβαση στις υπηρεσίες τους. Η ομόσπονδη προσέγγιση είναι ιδανική για να αποφευχθεί η διασύνδεση δημόσιων πληροφοριών οι οποίες μπορεί να περιέχουν προσωπικές πληροφορίες, καθώς διασφαλίζει ότι τα δεδομένα δεν υπάρχουν δύο φορές σε μια κεντρική βάση.

Μεμονωμένες κυβερνητικές αρχές μπορούν να δράσουν ως πάροχοι ταυτότητας εγκαθιδρύοντας κύκλους εμπιστοσύνης και προσφέροντας μια πλήρη γκάμα υπηρεσιών μεταξύ διαφορετικών τομέων. Επιπροσθέτως, με ισχυρή αυθεντικοποίηση, οι κυβερνήσεις μπορούν να διασφαλίσουν ότι μόνο εξουσιοδοτημένοι χρήστες χρησιμοποιούν τις υπηρεσίες τους.

15.4 Προγράμματα Διαχείρισης Ομόσπονδων Ταυτοτήτων

Οι πιο γνωστές μελέτες όσον αφορά τη διαχείριση ομόσπονδων ταυτοτήτων είναι η Liberty Alliance και η Shibboleth. Τα έργα αυτά και ο τρόπος με τον οποίο πραγματοποιούν τη διαχείριση ταυτοτήτων περιγράφονται συνοπτικά στη συνέχεια, καθώς επίσης επισημαίνονται και οι διαφορές μεταξύ τους.

15.4.1 Liberty Alliance

Το πρόγραμμα Liberty Alliance σχηματίστηκε το 2001 από περίπου 30 οργανισμούς από όλο τον κόσμο για να καθιερώσει ανοιχτά πρότυπα και πρακτικές για τη διαχείριση ομόσπονδων ταυτοτήτων. Το Liberty Alliance πέτυχε το σκοπό του με την έκδοση του Liberty Federation το 2002, ενός βιομηχανικού προτύπου για Online διαχείριση.

Επιτρέπει στους χρήστες των υπηρεσιών του Διαδικτύου καθώς και στους χρήστες εφαρμογών ηλεκτρονικού εμπορίου να αυθεντικοποιούνται και να έχουν πρόσβαση σ' ένα ολόκληρο δίκτυο ή τομέα, απολαμβάνοντας υπηρεσίες από πολλαπλές και διαφορετικές τοποθεσίες. Αυτή η ομόσπονδη προσέγγιση δεν απαιτεί επαναυθεντικοποίηση του χρήστη, ενώ παράλληλα παρέχει διασφάλιση της ιδιωτικότητας των χρηστών.

Το Liberty Alliance επιπλέον ανέπτυξε το Liberty Web Services το 2003, ενώ τα μέλη του, που έφτασαν τα 150, αποτελούνται από πωλητές, καταναλωτές, εκπαιδευτικούς οργανισμούς και κυβερνήσεις απ' όλο τον κόσμο. Είναι ανοιχτού κώδικα με σκοπό την ανάπτυξη και τη διαχείριση διάφορων υπηρεσιών που βασίζονται στην ταυτότητα (Identity-based Web Services). Με τη συνεχή ανάπτυξη του Liberty Federation και του Liberty Web Services, το Liberty Alliance ιχνηλάτησε περισσότερες από ένα δισεκατομμύριο ταυτότητες και συσκευές μέχρι το τέλος του 2006. Αυτή η μεγάλης κλίμακας ανάπτυξη συνδυαζόμενη με τις απαιτήσεις των καταναλωτών και των βιομηχανιών, για καλύτερη προστασία από online απάτες και

υποκλοπή ταυτοτήτων, οδήγησε στη δημιουργία του Liberty's Strong Authentication Expert Group (SAEG). Αυτή η ομάδα εργάζεται για λύσεις ισχυρής αυθεντικοποίησης όπως hardware και software tokens, smart cards, SMS-based systems και biometrics, σε ένα ομόσπονδο διαδικτυακό περιβάλλον.

Λεπτομέρειες για το Liberty Alliance μπορούν να βρεθούν στο http://www.projectliberty.org/.

15.4.2 Shibboleth

Το Shibboleth είναι ένα πρότυπο βασισμένο σε ανοικτού κώδικα λογισμικό που έχει υλοποιηθεί για την αυθεντικοποίηση και την εξουσιοδότηση ομόσπονδης ταυτότητας. Η υποδομή του βασίζεται στο OASIS' Security Assertion Markup Language (SAML).

Με τη χρήση της ομόσπονδης ταυτότητας παρέχονται, με ασφάλεια, πληροφορίες σε άλλους οργανισμούς της ίδιας ομοσπονδίας. Έτσι επιτρέπεται η μοναδιαία αυθεντικοποίηση (single sign-on) διαμέσου ή εντός οργανισμών, χωρίς να επιβαρύνεται κάθε οργανισμός με τη διατήρηση των usernames και passwords. Συγκεκριμένα οι πάροχοι ταυτότητας διαθέτουν πληροφορίες για τον κάθε χρήστη, ενώ οι πάροχοι υπηρεσιών – οργανισμοί χρησιμοποιούν αυτή την πληροφορία. Έτσι γνωρίζουν αν κάποιος είναι εξουσιοδοτημένος ή όχι, ενώ ταυτόχρονα προστατεύεται και η ιδιωτικότητα του χρήστη.

Οι οργανισμοί που χρησιμοποιούν το Shibboleth για πρόσβαση σε διαθέσιμους πόρους πρέπει να ενταχθούν ή να δημιουργήσουν μια ομοσπονδία, η οποία και δημιουργεί έναν 'Κύκλο Εμπιστοσύνης' για τους συμμετέχοντες οργανισμούς - πόρους. Κάθε ομοσπονδία έχει τα δικά της κριτήρια ένταξης οργανισμών καθώς και συγκεκριμένα επίπεδα εμπιστοσύνης για την πρόσβαση στους πόρους αυτούς. Το έργο της Shibboleth έχει ήδη εγκαθιδρύσει δύο ομοσπονδίες, την InQueue και την InCommon. Η πρώτη αποσκοπεί στη δοκιμή του Shibboleth από οργανισμούς που το έχουν υλοποιήσει και η δεύτερη είναι για εμπορική χρήση. Άλλες ομοσπονδίες έχουν αναπτυχθεί από την Swiss SWITCH AAI, την EDINA SDSS και την Eduserv.

Λεπτομέρειες για το Shibboleth μπορούν να βρεθούν στο http://shibboleth.internet2.edu/.

15.4.3 Ομοιότητες και διαφορές του Liberty Alliance και του Shibboleth

Ομοιότητες

Τόσο το Liberty Alliance όσο και το Shibboleth υποστηρίζουν μοναδιαία αυθεντικοποίηση (single sign-on) και ανταλλαγή ιδιοτήτων του χρήστη (user attributes), όπως όνομα, e-mail κ.λ.π., που μπορούν να χρησιμοποιηθούν για σκοπούς εξουσιοδότησης. Ακόμη παρέχουν single log-out, δηλαδή όταν ο χρήστης αποσυνδέεται, η αποσύνδεση πραγματοποιείται από όλες τις υπηρεσίες με τις οποίες είχε προηγουμένως συνδεθεί.

Επιπλέον, και τα δύο βασίζονται στην γλώσσα Security Assertion Markup Language (SAML) και χρησιμοποιούν το πρωτόκολλο SOAP. Ένα ακόμη κοινό χαρακτηριστικό είναι η χρήση του κύκλου εμπιστοσύνης μεταξύ των διαφόρων οργανισμών που συμμετέχουν στην ομοσπονδία.

Διαφορές

Η χρήση του Liberty Alliance είναι κυρίως εμπορική, σε αντίθεση με του Shibboleth που μέχρι στιγμής έχει χρησιμοποιηθεί κυρίως σε εκπαιδευτικά προγράμματα, δηλαδή ο πάροχος της υπηρεσίας είναι διαφορετικός σε κάθε περίπτωση. Επιπλέον στο Shibboleth υπάρχουν λίγες ομοσπονδίες σε αντίθεση με το Liberty Alliance που είναι πολλές. Έτσι οι πελάτες στο Shibboleth έχουν μεγαλύτερη ευελιξία.

Η κύρια διαφορά τους είναι ότι το Liberty Alliance βασίζεται στο διαμοιρασμό πληροφοριών της ταυτότητας μεταξύ έμπιστων πηγών και συνεπώς οι πληροφορίες είναι διαθέσιμες απευθείας στους οργανισμούς. Αντίθετα το Shibboleth επιτρέπει στο άτομο να καθορίσει απευθείας ποια υπηρεσία θα χρησιμοποιήσει και η υπηρεσία απαντάει με συγκεκριμένες και απρόσωπες πληροφορίες.

Το Liberty Alliance βασίζεται κυρίως στη διατήρηση των πελατών σε αντίθεση με το Shibboleth που επιθυμεί ευελιξία για τους πελάτες του. Το Liberty Alliance είναι identity provider–oriented ενώ το Shibboleth είναι resource–oriented. Η διαλειτουργικότητα της ομοσπονδίας επιτυγχάνεται με τις μεταξύ τους συμφωνίες στο Shibboleth. Στο Liberty Alliance οι λογαριασμοί των χρηστών είναι αποθηκευμένοι στον εκάστοτε πάροχο ταυτοτήτων. Τέλος ο κώδικας του Shibboleth είναι διαθέσιμος σε αντίθεση με τον κώδικα του Liberty Alliance που δεν είναι.

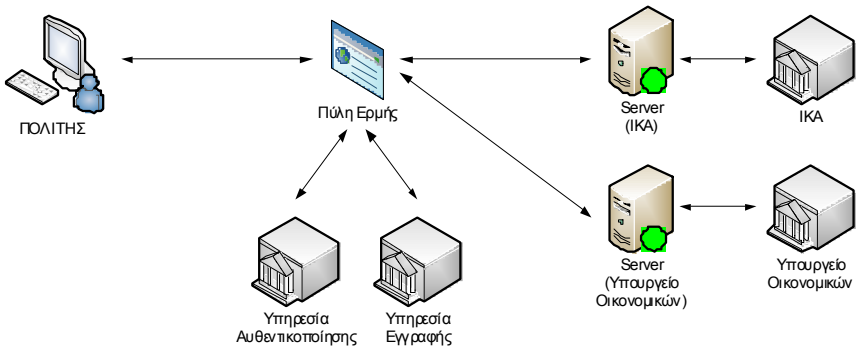
15.5 Σενάρια Διαχείρισης Ομόσπονδης Ταυτότητας σε Περιβάλλον Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα

Η πληθώρα πληροφοριακών συστημάτων που αναπτύχθηκαν στα αρχικά στάδια της ηλεκτρονικής διακυβέρνησης οδήγησαν σταδιακά σε μια κατάσταση όπου ναι μεν παρέχονταν ηλεκτρονικές υπηρεσίες στους πολίτες αλλά τα διάφορα πληροφοριακά συστήματα που τις υποστήριζαν δεν μπορούσαν να επικοινωνήσουν μεταξύ τους. Πρόκειται ουσιαστικά για την αδυναμία μεταφοράς και αξιοποίησης της πληροφορίας με ομοιογενή και αποτελεσματικό τρόπο μεταξύ διαφόρων οργανισμών. Αυτή η αδυναμία οδηγεί, όπως είναι αναμενόμενο, σε χρονοβόρες διαδικασίες ανταλλαγής πληροφοριών μεταξύ των δημοσίων υπηρεσιών, ακυρώνοντας τα οφέλη της ηλεκτρονικής διακυβέρνησης.

Δεδομένου του περιορισμένου αριθμού συστημάτων εν λειτουργία, η Ελληνική Δημόσια Διοίκηση δεν αντιμετώπισε άμεσα το πρόβλημα της αδυναμίας επικοινωνίας μεταξύ των πληροφοριακών συστημάτων που προσφέρουν υπηρεσίες ηλεκτρονικής διακυβέρνησης. Παρ' όλα αυτά έχει αφουγκραστεί τη διεθνή εμπειρία και προχωρά στη δημιουργία αφενός μιας Κεντρικής Δικτυακής Πύλης (Εθνική Πύλη ΕΡΜΗΣ) για την ηλεκτρονική διακυβέρνηση και αφετέρου του Πλαισίου Ηλεκτρονικής Διακυβέρνησης. Αναφορικά με το ζήτημα της διαχείρισης ταυτοτήτων, η Ελλάδα υιοθετεί τη βασική τεχνολογική λύση που έχει ακολουθήσει το σύνολο των χωρών με συστήματα ηλεκτρονικής διακυβέρνησης, δηλαδή την ανάπτυξη υποδομής δημοσίου κλειδιού.

15.5.1 Κεντρική Διαδικτυακή Πύλη ως Πάροχος Ταυτότητας

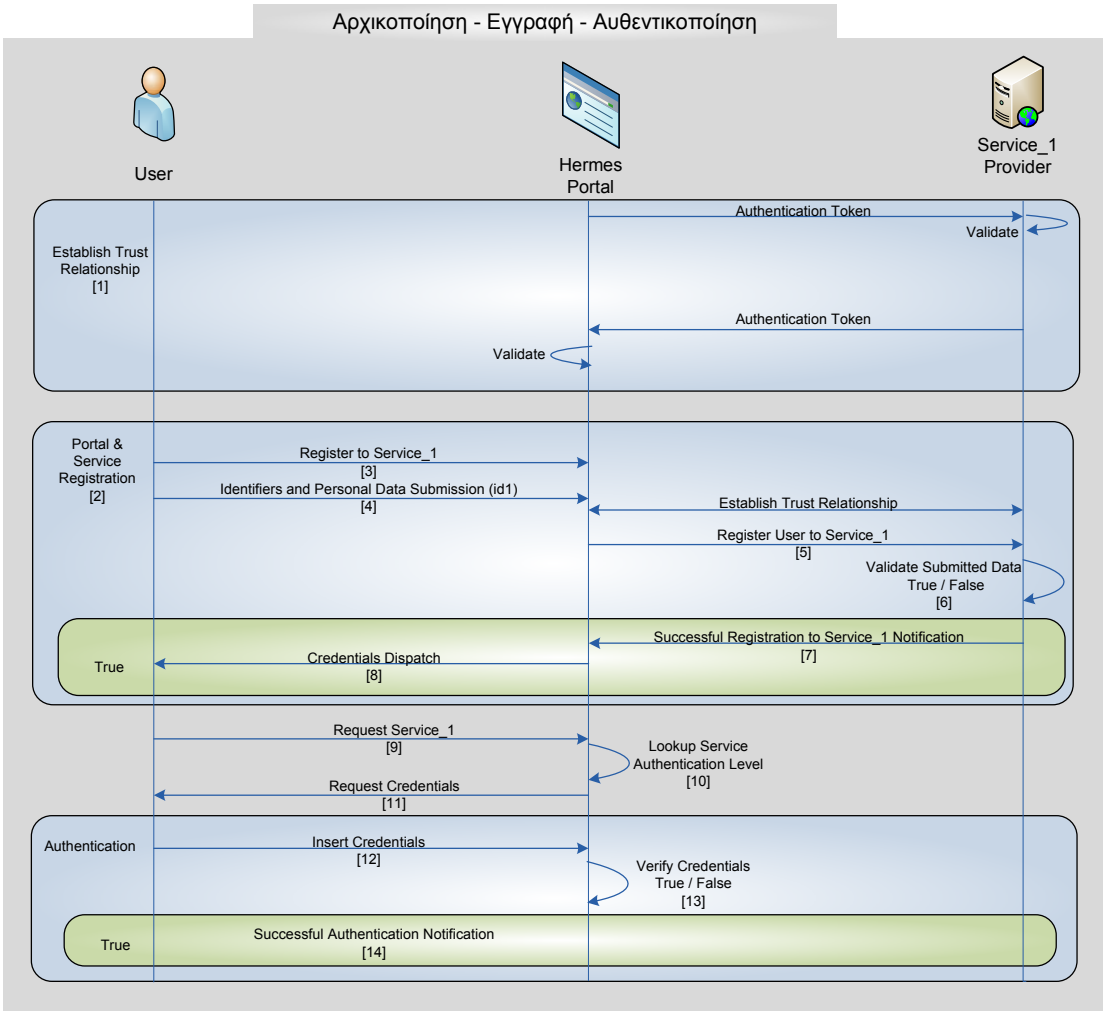
Το πρώτο σενάριο διαχείρισης ομόσπονδης ταυτότητας προϋποθέτει τη χρήση μιας Κεντρικής Διαδικτυακής Πύλης (ΚΔΠ) μέσω της οποίας θα πραγματοποιούνται όλες οι συναλλαγές του πολίτη με τις δημόσιες υπηρεσίες. Η ύπαρξη της ΚΔΠ έχει ως σκοπό την ενιαία αυθεντικοποίηση των χρηστών, ανεξάρτητα από το φορέα ή την υπηρεσία που επιθυμούν αυτοί να προσπελάσουν.



Εικόνα 7: Αξιοποίηση Κεντρικής Διαδικτυακής Πύλης ως Παρόχου Ταυτότητας

Στο μοντέλο αυτό υπάρχουν ο Service_1 Provider (Υπουργείο Οικονομικών) και ο Service_2 Provider (ΙΚΑ). Τα id_1 και id_2 είναι τα αναγνωριστικά που απαιτεί η κάθε υπηρεσία για την ταυτοποίηση του χρήστη.

Στο παρακάτω σχήμα φαίνεται η διαδικασία εγγραφής και αυθεντικοποίησης σε κάποια από τις προσφερόμενες υπηρεσίες.



Εικόνα 8: Αρχικοποίηση - Εγγραφή – Αυθεντικοποίηση

Αρχικά, η ΚΔΠ εγκαθιδρύει σχέσεις εμπιστοσύνης μεταξύ αυτής και των φορέων παροχής υπηρεσιών [1].

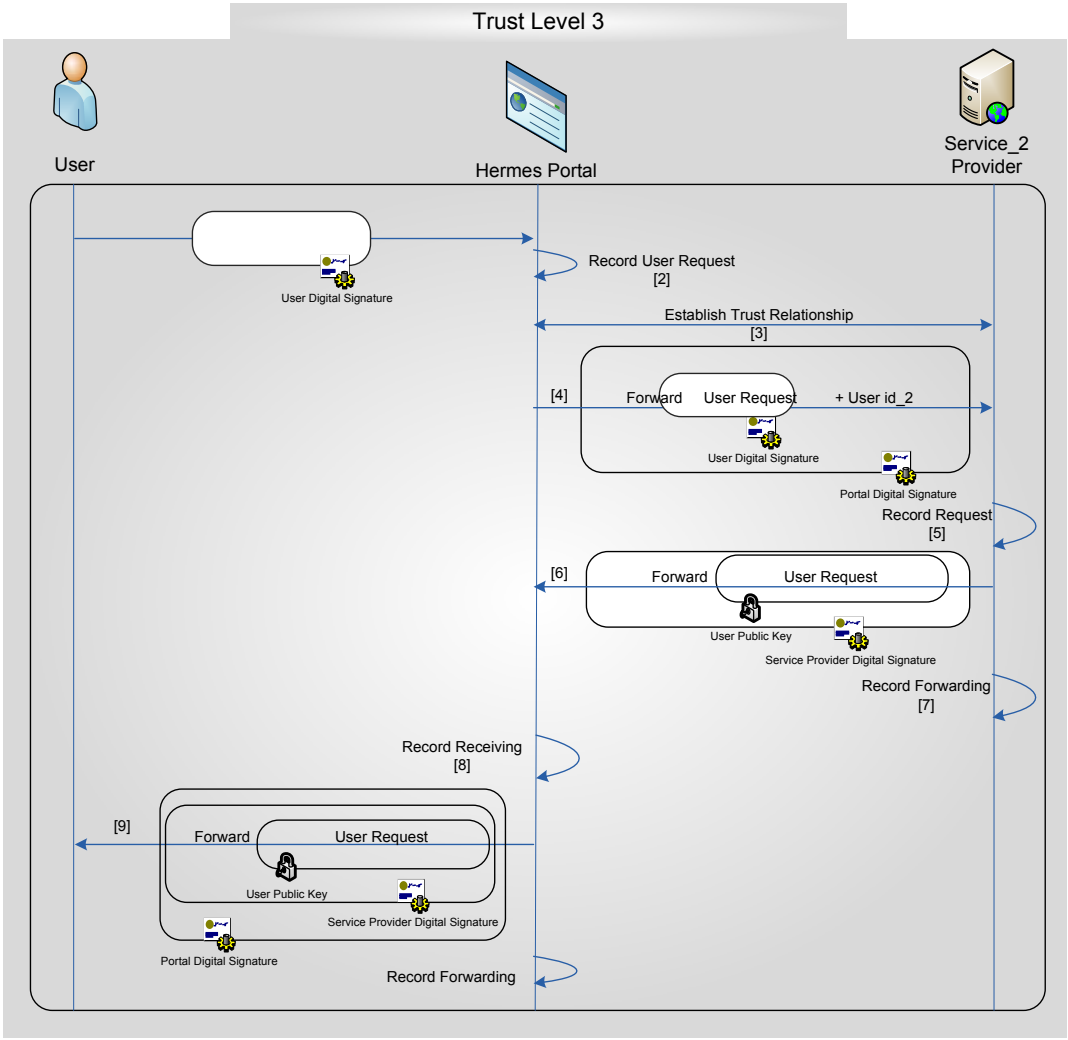
Στη συνέχεια ο χρήστης μπορεί να προχωρήσει και να εγγραφεί στην υπηρεσία που επιθυμεί [2]. Έπειτα, επιλέγει την υπηρεσία [3], στο παράδειγμά μας είναι η Service 1 από τον Service 1 Provider (Υπουργείο Οικονομικών). Στη συνέχεια, παρέχει στην ΚΔΠ τα στοιχεία (αναγνωριστικά) που απαιτούνται για την ταυτοποίησή του [4]. Η ΚΔΠ, με τη σειρά της, εγγράφει το χρήστη στην κατάλληλη υπηρεσία και στον κατάλληλο φορέα [5]. Ο φορέας ελέγχει τα στοιχεία που έχει δώσει ο χρήστης [6] και απαντάει στην ΚΔΠ αν ο χρήστης μπορεί να αξιοποιήσει την υπηρεσία ή όχι [7]. Αν η εγγραφή ολοκληρωθεί χωρίς πρόβλημα, ο χρήστης λαμβάνει μήνυμα επιτυχούς εγγραφής στην υπηρεσία [8].

Ο χρήστης είναι τώρα έτοιμος να χρησιμοποιήσει την υπηρεσία (Service_1). Αρχικά στέλνει στην ΚΔΠ μια αίτηση χρήσης της Υπηρεσίας [9]. Η ΚΔΠ ελέγχει το επίπεδο εμπιστοσύνης της υπηρεσίας [10] και ζητάει από το χρήστη τα διακριτικά αυθεντικοποίησης που απαιτούνται [11].

Ο χρήστης παρέχει στην ΚΔΠ τα διακριτικά αυθεντικοποίησης που απαιτούνται [12]. Η ΚΔΠ ελέγχει την ορθότητά τους [13] και αν είναι σωστά ο χρήστης έχει αυθεντικοποιηθεί και μπορεί να χρησιμοποιήσει την υπηρεσία [14].

Στη συνέχεια, υποθέτουμε ότι ο χρήστης επιθυμεί να χρησιμοποιήσει μια υπηρεσία (Service_2) του ΙΚΑ (Service_2 Provider). Υποθέτουμε επίσης ότι τα διακριτικά αυθεντικοποίησης που κατέχει του επιτρέπουν να αξιοποιήσει υπηρεσίες επιπέδου εμπιστοσύνης 3.

Στο παρακάτω σχήμα φαίνεται η διαδικασία που ακολουθείται για τη χρήση της συγκεκριμένης υπηρεσίας.



Εικόνα 9: Αξιοποίηση Υπηρεσίας Επιπέδου Εμπιστοσύνης 3

Αρχικά, ο χρήστης αποστέλλει, προς την ΚΔΠ, το αίτημά του [1], το οποίο και υπογράφει ψηφιακά. Η ΚΔΠ καταγράφει το συγκεκριμένο αίτημα του χρήστη [2] και εγκαθιδρύει μια σχέση εμπιστοσύνης με τον πάροχο της συγκεκριμένης υπηρεσίας [3].

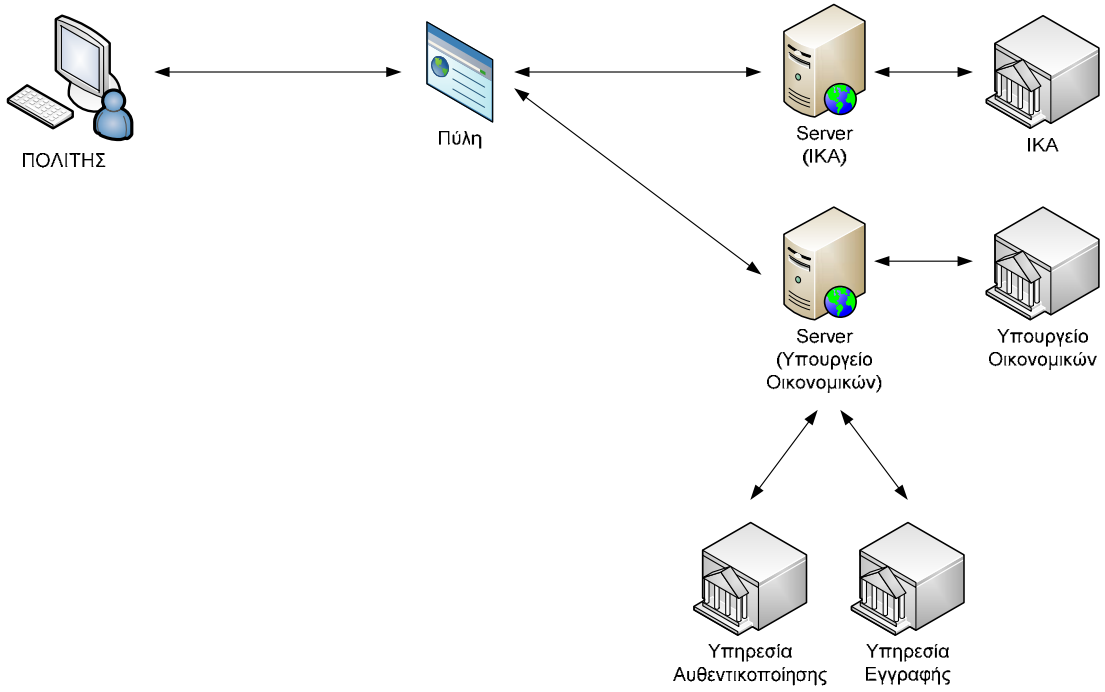
Αφού εγκαθιδρυθεί η σχέση εμπιστοσύνης, η ΚΔΠ προωθεί στον αντίστοιχο φορέα το αίτημα του χρήστη, το οποίο είναι υπογεγραμμένο ψηφιακά από την ΚΔΠ, μαζί με τα αντίστοιχα

αναγνωριστικά (id_2) που απαιτούνται από τη συγκεκριμένη υπηρεσία [4]. Θεωρούμε ότι όλα τα αναγνωριστικά έχουν παρασχεθεί στην ΚΔΠ κατά την πρώτη εγγραφή. Αν δεν είχε γίνει κάτι τέτοιο, η ΚΔΠ θα τα ζητούσε από το χρήστη εκείνη τη στιγμή και η διαδικασία θα συνεχιζόταν ως έχει.

Ο πάροχος της υπηρεσίας καταγράφει το αίτημα [5], στέλνει στην ΚΔΠ την απάντηση [6] και καταγράφει την ενέργεια [7]. Η απάντηση αυτή είναι ψηφιακά υπογεγραμμένη από τον πάροχο ενώ τα στοιχεία που απευθύνονται στον χρήστη είναι κρυπτογραφημένα με το δημόσιο κλειδί του. Αφού λάβει την απάντηση, η ΚΔΠ καταγράφει ότι την έλαβε [8] και την προωθεί, αφού πρώτα την υπογράψει και αυτή με τη σειρά της, στο χρήστη [9].

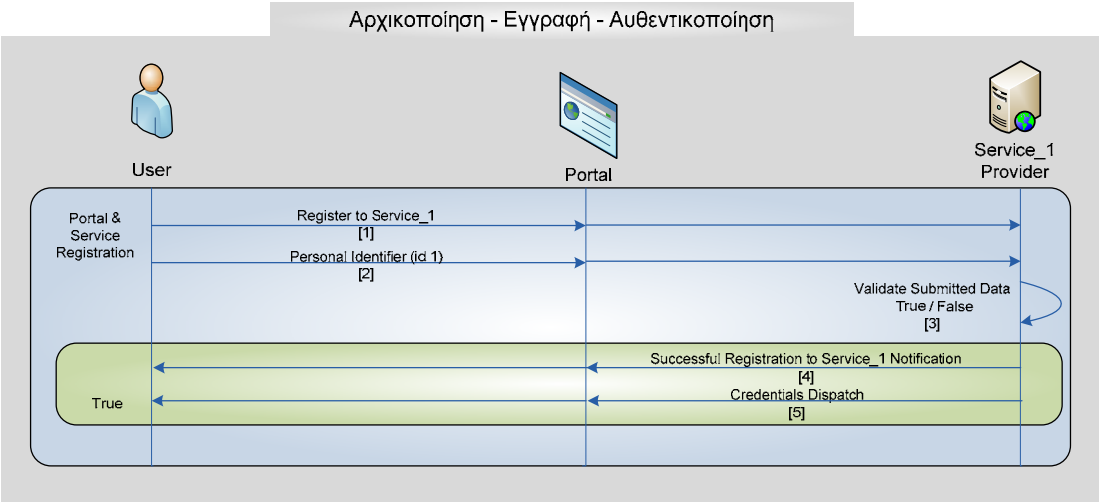
15.5.2 Αξιοποίηση του Εκάστοτε Παρόχου Υπηρεσίας ως Παρόχου Ταυτότητας

Στο σενάριο αυτό έχουμε ξανά τους 2 παρόχους υπηρεσιών (Υπουργείο Οικονομικών και ΙΚΑ), τις 2 υπηρεσίες (Service_1 και Service_2) και τα αντίστοιχα αναγνωριστικά (id_1 και id_2). Η διαφορά έγκειται στο ότι ο εκάστοτε πάροχος, στον οποίο ο χρήστης θα εγγραφεί πρώτα, λειτουργεί ως πάροχος ταυτότητας αντί της ΚΔΠ.



Εικόνα 10: Αξιοποίηση του εκάστοτε Παρόχου Υπηρεσίας ως Παρόχου Ταυτότητας

Στο παρακάτω σχήμα φαίνεται η διαδικασία εγγραφής και αυθεντικοποίησης σε μια υπηρεσία.



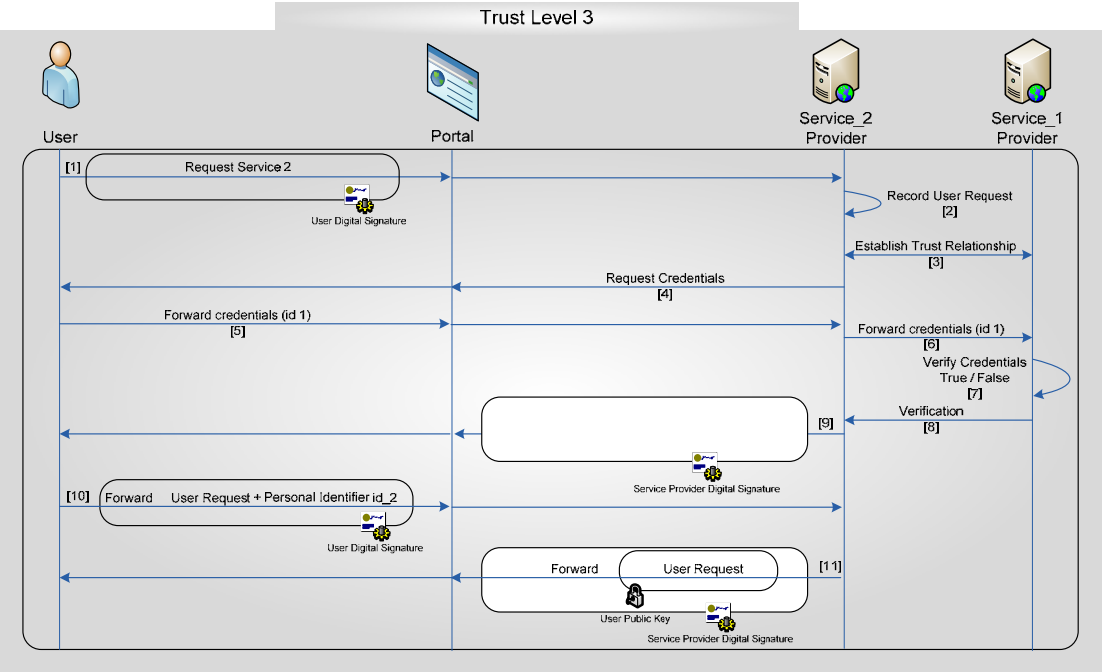
Εικόνα 11: Αρχικοποίηση - Εγγραφή – Αυθεντικοποίηση

Αρχικά ο χρήστης, μέσα από το κεντρικό portal επικοινωνεί με τον Service_1 Provider (Υπουργείο Οικονομικών) και αιτείται την υπηρεσία (Service_1) [1]. Επίσης, αποστέλλει τα αναγνωριστικά (id_1) που απαιτούνται για την υπηρεσία αυτή [2].

Στη συνέχεια, ο πάροχος ελέγχει τα στοιχεία που του έδωσε ο χρήστης [3] και αν είναι σωστά του παρέχει δικαίωμα χρήσης της υπηρεσίας μέσω της αποστολής διακριτικών αυθεντικοποίησης που αντιστοιχούν στο επίπεδο εμπιστοσύνης της υπηρεσίας [4] [5].

Στη συνέχεια, υποθέτουμε ότι ο χρήστης επιθυμεί να χρησιμοποιήσει μια υπηρεσία (Service_2) του ΙΚΑ (Service_2 Provider) για την οποία δεν έχει διακριτικά αυθεντικοποίησης (αυτό έχει συμβεί είτε διότι δεν απαιτείται καθόλου εγγραφή στην υπηρεσία ή διότι κατά την εγγραφή δεν εκδόθηκαν νέα διακριτικά αυθεντικοποίησης). Υποθέτουμε επίσης ότι τα διακριτικά αυθεντικοποίησης που κατέχει του επιτρέπουν να αξιοποιήσει υπηρεσίες επιπέδου εμπιστοσύνης 3.

Στο παρακάτω σχήμα φαίνεται η διαδικασία που ακολουθείται για τη χρήση της συγκεκριμένης υπηρεσίας.



Εικόνα 12: Αξιοποίηση Υπηρεσίας Επιπέδου Εμπιστοσύνης 3

Αρχικά, ο χρήστης, μέσω της κεντρικής πύλης, ζητάει από τον Service_2 Provider (ΙΚΑ) να χρησιμοποιήσει την υπηρεσία του [1], δηλώνοντας ότι έχει στην κατοχή του διακριτικά αυθεντικοποίησης που έχουν εκδοθεί από τον Service_1 Provider. Την αίτησή του την υπογράφει ψηφιακά. Ο πάροχος της υπηρεσίας καταγράφει το αίτημα του χρήστη [2] και εγκαθιδρύει σχέση εμπιστοσύνης με τον πάροχο στον οποίο ο χρήστης είχε αρχικά εγγραφεί [3].

Στη συνέχεια, ο Service_2 Provider ζητάει από τον χρήστη τα αναγνωριστικά με τα οποία είχε αρχικά εγγραφεί καθώς και τα διακριτικά αυθεντικοποίησης που του είχαν παρασχεθεί [4], [5]. Τα στοιχεία αυτά τα στέλνει στον Service_1 Provider [6] ο οποίος τα ελέγχει [7] και απαντάει για το αν τα εγκρίνει ή όχι [8].

Αν τα στοιχεία είναι σωστά, ο πάροχος, του οποίου ο χρήστης αιτείται την υπηρεσία, ζητά από το χρήστη τα αναγνωριστικά (id_2) που απαιτεί η υπηρεσία αυτή [9] και υπογράφει ψηφιακά την αίτησή του. Ο χρήστης αποστέλλει στον πάροχο της υπηρεσίας τα απαραίτητα αναγνωριστικά (id_2) υπογεγραμμένα ψηφιακά [10]. Τέλος, ο πάροχος αποστέλλει στο χρήστη την απάντηση στο αίτημά του (αποτέλεσμα της υπηρεσίας), η οποία είναι κρυπτογραφημένη με το δημόσιο κλειδί του χρήστη και υπογεγραμμένη ψηφιακά από τον πάροχο [11].

15.5.3 Συγκριτική Αξιολόγηση

Το μεγαλύτερο πλεονέκτημα του πρώτου σεναρίου είναι πως η διαχείριση των χρηστών και των διαπιστευτηρίων τους γίνεται από την ΚΔΠ και όχι από τον ίδιο τον φορέα. Έτσι, εξυπηρετείται καλύτερα ο πολίτης αφού χρειάζεται να αυθεντικοποιηθεί μόνο μια φορά και

επίσης, προστατεύεται η ιδιωτικότητά του μιας και τα προσωπικά του στοιχεία παραμένουν μεταξύ αυτού και της πύλης, και αποστέλλονται ανάλογα μόνο στις υπηρεσίες που επιθυμεί να προσπελάσει. Επίσης, παρά την ύπαρξη της ΚΔΠ, οι δημόσιοι φορείς συνεχίζουν να διατηρούν την αυτονομία τους. Ακόμη, υπάρχει μόνο μια βάση δεδομένων για τις καταχωρήσεις των στοιχείων των πολιτών μειώνοντας με τον τρόπο αυτό τυχόν διπλοεγγραφές, ενώ ταυτόχρονα γίνεται καλύτερη διαχείριση των αιτήσεων που πραγματοποιούν οι πολίτες αφού υπάρχει μια κεντρική πύλη η οποία ελέγχει και διαχειρίζεται καλύτερα τις παρεχόμενες υπηρεσίες.

Βέβαια, με τη χρήση του συγκεκριμένου σεναρίου προκύπτει ένα ζήτημα ως προς το ποια χαρακτηριστικά της ταυτότητας του πολίτη (αναγνωριστικά) πρέπει να αποστέλλονται σε κάθε φορέα, αφού ο καθένας χρησιμοποιεί διαφορετικά στοιχεία ταυτοποίησης. Το συγκεκριμένο όμως θέμα όμως μπορεί να λυθεί και να ελεγχθεί σε επίπεδο υλοποίησης.

Από την άλλη μεριά, στο δεύτερο σενάριο η αυθεντικοποίηση των χρηστών γίνεται από τους ίδιους τους φορείς, οι οποίοι για να αποφασίσουν αν θα επιτρέψουν την παροχή της υπηρεσίας στο χρήστη του ζητούν τα διακριτικά αυθεντικοποίησης που του έχουν παρασχεθεί ως αποτέλεσμα της εγγραφής του σε κάποια άλλη υπηρεσία. Στην περίπτωση αυτή, ο πάροχος ταυτότητας μπορεί να είναι ένας οποιοσδήποτε φορέας, ομοίως και ο πάροχος υπηρεσιών.

Εδώ όμως προκύπτουν προβλήματα ιδιωτικότητας αφού ένας φορέας, για να αυθεντικοποιήσει το χρήστη, ζητάει αναγνωριστικά με τα οποία ο χρήστης έχει εγγραφεί σε άλλη υπηρεσία, ώστε να τα στείλει, μαζί με τα αντίστοιχα διακριτικά αυθεντικοποίησης, στον αντίστοιχο πάροχο ο οποίος τα ελέγχει και αποφαίνεται για το αν ο χρήστης μπορεί να συνδεθεί ή όχι.

Η υλοποίηση του δεύτερου σεναρίου θεωρείται πιο δύσκολη αφού οι σχέσεις των φορέων γίνονται πιο περίπλοκες ενώ το εύρος του τομέα στον οποίο θέλουμε να λάβει χώρα η υλοποίηση είναι δυναμικό, γεγονός που σημαίνει ότι η εκ των υστέρων ένταξη κάποιου φορέα στο σύστημα θα δημιουργεί επιπλέον προβληματισμούς αφού ο κύκλος εμπιστοσύνης θα πρέπει να αναπροσαρμόζεται.

Συμπερασματικά, το πρώτο σενάριο υπερέχει σημαντικά του δεύτερου τόσο σε θέματα ασφαλείας όσο και σε θέματα διαλειτουργικότητας.