Παράρτημα ΙΙΙ: **Κανόνες και πρότυπα για την εγγραφή, ταυτοποίηση και ηλεκτρονική αναγνώριση πολιτών και επιχειρήσεων σε ηλεκτρονικές υπηρεσίες του δημόσιου τομέα.**

1. Καθορισμός «επιπέδων εμπιστοσύνης» για τις ηλεκτρονικές υπηρεσίες

Η κατηγοριοποίηση των υπηρεσιών σε επίπεδα εμπιστοσύνης γίνεται με βάση την κατηγορία των δεδομένων που αξιοποιούν (απλά ,ευαίσθητα και οικονομικά), αλλά και τις πιθανές επιπτώσεις που μπορεί να προκληθούν σε περίπτωση μη ορθής λειτουργίας ή διαχείρισής τους. Τα επίπεδα εμπιστοσύνης που ορίζει το ΠΗΔ είναι τα ακόλουθα:

- **Επίπεδο Εμπιστοσύνης 0**

Στο επίπεδο εμπιστοσύνης 0 εντάσσονται οι 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.

- **Επίπεδο Εμπιστοσύνης 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.

- **Επίπεδο Εμπιστοσύνης 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.

- **Επίπεδο Εμπιστοσύνης 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.

2. **Καθορισμός των μηχανισμών αυθεντικοποίησης σε σχέση με τα επίπεδα εμπιστοσύνης**

Μηχανισμοί Αυθεντικοποίησης

Τα συστήματα αυθεντικοποίησης είναι δυνατό να κατηγοριοποιηθούν με βάση τα διακριτικά που χρησιμοποιούνται για τον έλεγχο της ορθότητας της ηλεκτρονικής ταυτότητας των χρηστών ενός συστήματος. Ανάλογα με το επιθυμητό επίπεδο ασφάλειας υιοθετείται και ο αντίστοιχος συνδυασμός διακριτικών όπως περιγράφονται παρακάτω:

- **Συνθηματικά**

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

- **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.

- **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.

- **Διακριτικά Υλικού – Σκληρής Αποθήκευσης (hard tokens)**

Τα διακριτικά υλικού σκληρής αποθήκευσης αναφέρονται σε συσκευές υλικού οι οποίες αποθηκεύουν τα απαιτούμενα μυστικά κλειδιά και προσφέρουν αυξημένη 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.

Επίπεδα Αυθεντικοποίησης

Ανάλογα με τις απαιτήσεις αυθεντικοποίησης επιλέγονται ένα από τα παρακάτω επίπεδα αυθεντικοποίησης

- **Επίπεδο Αυθεντικοποίησης 0**

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. Δεν απαιτείται μηχανισμός αυθεντικοποίησης.

- **Επίπεδο Αυθεντικοποίησης 1**

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. Οι μηχανισμοί αυθεντικοποίησης που προτείνονται για το συγκεκριμένο επίπεδο συμπεριλαμβάνουν: συνθηματικά και συνθηματικά μιας χρήσης.

- **Επίπεδο Αυθεντικοποίησης 2**

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.

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 Αρχή Χρονοσήμανσης (Time Stamping Authority - TSA). 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.

Σύνοψη Συσχετισμού Επιπέδων Εμπιστοσύνης & Αυθεντικοποίησης

Στον παρακάτω πίνακα συνοψίζεται η συσχέτιση μεταξύ Επιπέδων Εμπιστοσύνης και Επιπέδων Αυθεντικοποίησης.

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

3. Προσδιορισμός των απαιτήσεων των διαδικασιών εγγραφής των χρηστών στις ηλεκτρονικές υπηρεσίες ανάλογα με το μηχανισμό αυθεντικοποίησης.

Με τον όρο *εγγραφή* ενός χρήστη *σε μια υπηρεσία* ορίζεται το σύνολο των διαδικασιών μέσω των οποίων ο χρήστης 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.

Στην ενότητα αυτή αποτυπώνονται οι διαδικασίες που απαιτούνται για την εγγραφή ενός χρήστη 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.

Τύποι χρηστών

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

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

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», η οποία ουσιαστικά θα παρέχει τη λειτουργική διεπαφή και επικοινωνία μεταξύ των δύο οντοτήτων και θα είναι υπεύθυνη για τον έλεγχο και την 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 είναι δημόσια.

- **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. Δεν απαιτείται κάποια συγκεκριμένη διαδικασία εγγραφής.

- **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).

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 ηλεκτρονικά, 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. το 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, δίνεται πρόσβαση στην υπηρεσία από το λογαριασμό του χρήστη που υπέβαλε αίτηση. Σε κάθε περίπτωση διασφαλίζεται η ενημέρωση του χρήστη 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.

- **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.

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.

Ο χρήστης μετά την υποβολή του ηλεκτρονικού αιτήματος μπορεί να προσέλθει στην αρμόδια υπηρεσία για να 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. Σε περίπτωση που ο φορέας κάποιας υπηρεσίας επιθυμεί την προσκόμιση κάποιου ακόμα εγγράφου, ο χρήστης θα ενημερώνεται σχετικά κατά τη διάρκεια της ηλεκτρονικής αίτησης και θα πρέπει να το προσκομίσει μαζί με τα υπόλοιπα ώστε να αποκτήσει πρόσβαση στην υπηρεσία.

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

- **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.

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. 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 και υποβάλλοντας τα δημόσια έγγραφα που απαιτούνται αντίστοιχα με αυτά του επιπέδου 2. Μετά την παραλαβή του διακριτικού αυθεντικοποίησης ο προσωπικός κωδικός πρόσβασης (PIN – Personal Identification Number) του διακριτικού γνωστοποιείται με ασφαλή τρόπο στο 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.

- **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 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.

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 Γενικού Εμπορικού Μητρώου, 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.

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.

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
- 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).

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.

4. Οδηγίες και κανόνες, βασισμένοι στο ισχύον νομικό – κανονιστικό πλαίσιο, για την κατηγοριοποίηση των δεδομένων που επεξεργάζονται οι ηλεκτρονικές υπηρεσίες με βάση τις αρχές για τη προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

[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. 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

[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.

[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 το υφιστάμενο νομικό πλαίσιο (Ν. 2472/97 & Ν 2690/99 & Κώδικας φορολογίας εισοδήματος) στις κάτωθι κατηγορίες: • Απλά δεδομένα • Ευαίσθητα δεδομένα • Οικονομικά δεδομένα

[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 παρούσα.

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

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

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

[ΚΥ.9]	Υπηρεσίες που έχουν ενταχθεί στο Επίπεδο Εμπιστοσύνης 3 ΘΑ ΠΡΕΠΕΙ ΝΑ υιοθετήσουν: a. Επίπεδο Εγγραφής 3 και b. 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 εξασφαλίσει πρόσβαση στην υπηρεσία για το λογαριασμό του χρήστη και να γνωστοποιήσει με ασφαλή τρόπο στο χρήστη 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 εξασφαλίσει πρόσβαση στην υπηρεσία για το λογαριασμό του χρήστη και να γνωστοποιήσει με ασφαλή τρόπο στο χρήστη τα διαπιστευτήρια για τη χρήση της υπηρεσίας. Ο ενδιαφερόμενος ΘΑ ΠΡΕΠΕΙ ΝΑ ενημερωθεί ότι μπορεί να ενεργοποιηθούν 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 και υποβάλλοντας

	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 γνωστοποιηθεί με ασφαλή τρόπο στο χρήστη.

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

[ΚΜ.1]	Μεταξύ της Πύλης ΕΡΜΗΣ 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 πύλη ΕΡΜΗΣ 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 πύλη ΕΡΜΗΣ ΔΕΝ ΠΡΕΠΕΙ ΝΑ αποθηκεύει κανένα επιπλέον στοιχείο αναφορικά με το χρήστη ή την υπηρεσία. Για την άρτια λειτουργία του μηχανισμού ελέγχου (auditing), η πύλη ΕΡΜΗΣ 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 πύλης ΕΡΜΗΣ και εξυπηρετητή υπηρεσίας, όσο και στο τμήμα επικοινωνίας μεταξύ πύλης ΕΡΜΗΣ και χρήστη.

[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 δημοσιεύσει την Πολιτική Ψηφιακών Πιστοποιητικών στον ιστοχώρο της, σε εμφανές σημείο.

[ΚΥ.20]	ΠΡΕΠΕΙ ΝΑ διενεργούνται τακτικοί έλεγχοι της πολιτικής ψηφιακών πιστοποιητικών από στελέχη της μονάδας πληροφορικής της Υποκείμενης Αρχής Πιστοποίησης.

[ΚΥ.21]	Τα εκδιδόμενα πιστοποιητικά ΠΡΕΠΕΙ ΝΑ συμμορφώνονται με το επίπεδο εμπιστοσύνης στο οποίο εντάσσεται η υπηρεσία για την οποία εκδίδονται.