Εισαγωγή στο τεχνικό πλαίσιο «Sweden Connect»

2024-12-04

Αριθ. αναφοράς: **2019-267**

Πίνακας περιεχομένων

1. Εισαγωγή

1.1. Επισκόπηση

Το τεχνικό πλαίσιο Sweden Connect έχει προσαρμοστεί για δίκτυα ταυτότητας που βασίζονται στο SAML 2.0.

> Στην τελευταία έκδοση του τεχνικού πλαισίου, έχουν επίσης εισαχθεί προδιαγραφές για το OpenID Connect. Επί του παρόντος δεν υπάρχει υποστήριξη δικτύου για το OpenID Connect. Αυτή θα τεθεί σε εφαρμογή το 2025.

> Τα υπόλοιπα μέρη του παρόντος εγγράφου περιγράφουν μόνο το δίκτυο SAML. Μόλις τεθεί πλήρως σε εφαρμογή το OpenID Connect, το παρόν έγγραφο θα καλύπτει και αυτήν την τεχνολογία.

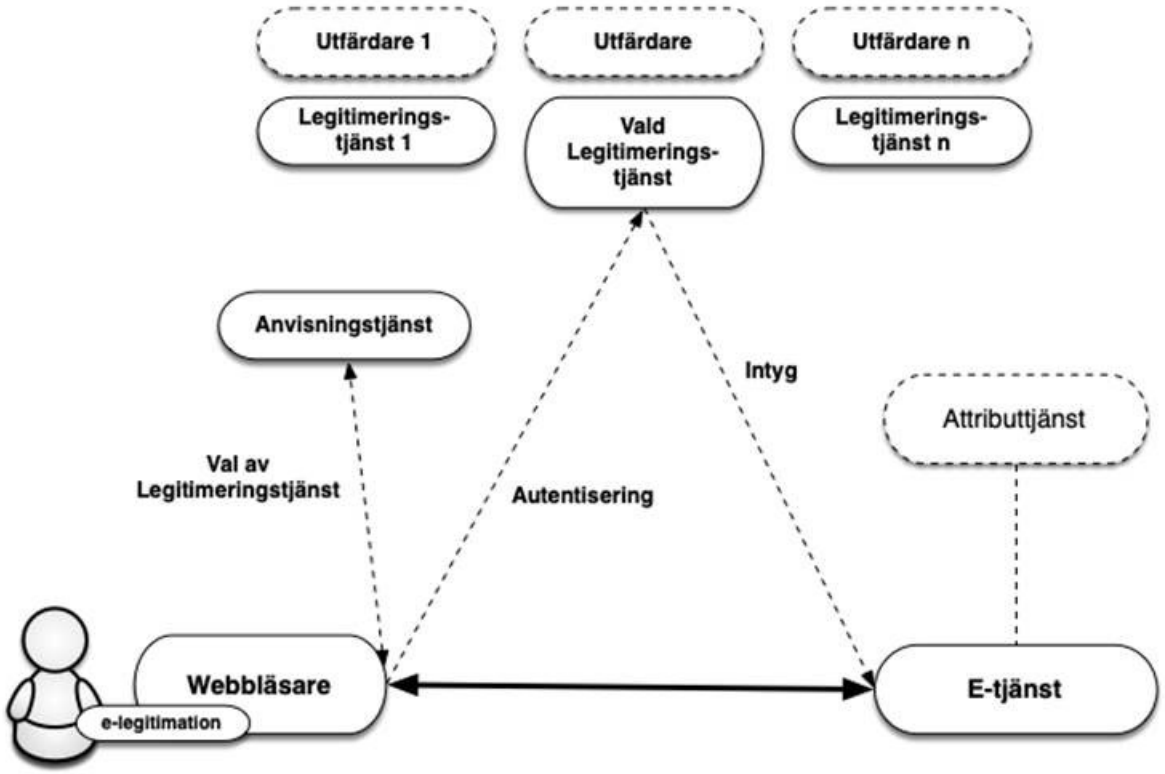
Τα συμβαλλόμενα μέρη λαμβάνουν πιστοποιητικά ταυτότητας σε τυποποιημένη μορφή από μια υπηρεσία ελέγχου ταυτότητας[1].

Οι ηλεκτρονικές υπηρεσίες που απαιτούν υπογραφή δεν χρειάζεται να προσαρμοστούν στις ηλεκτρονικές ταυτότητες των διαφόρων χρηστών για τη δημιουργία ηλεκτρονικών υπογραφών. Αντ' αυτού, η ηλεκτρονική υπηρεσία αναθέτει τη διαδικασία αυτή σε μια υπηρεσία υπογραφής, όπου οι χρήστες, υποστηριζόμενοι από έλεγχο ταυτότητας μέσω μιας υπηρεσίας ελέγχου ταυτότητας, έχουν τη δυνατότητα να υπογράφουν ηλεκτρονικά έγγραφα.

Εντός του δικτύου, οι ηλεκτρονικές υπηρεσίες και τα αντίστοιχα συμβαλλόμενα μέρη αναλαμβάνουν τον ρόλο του παρόχου υπηρεσιών (SP), ενώ οι υπηρεσίες ελέγχου ταυτότητας που εκδίδουν πιστοποιητικά ταυτότητας αναλαμβάνουν τον ρόλο του παρόχου ταυτότητας (IdP) και, επομένως, του ελεγκτή ταυτότητας του χρήστη, ανεξάρτητα από την ηλεκτρονική υπηρεσία για την οποία ελέγχεται η ταυτότητα του χρήστη.

Για τις περιπτώσεις όπου η ηλεκτρονική υπηρεσία χρειάζεται περισσότερες πληροφορίες σχετικά με τον χρήστη, π.χ. πληροφορίες σχετικά με τη δικαιοπρακτική ικανότητα, μπορεί να υποβληθεί ερώτηση σε μια υπηρεσία χαρακτηριστικού, Αρχή Χαρακτηριστικών (AA), εντός του δικτύου, εάν υπάρχει σχετική υπηρεσία χαρακτηριστικού. Μέσω αιτήματος χαρακτηριστικού, η ηλεκτρονική υπηρεσία μπορεί να λάβει τις απαραίτητες πρόσθετες πληροφορίες για την έγκριση του χρήστη και την παροχή πρόσβασης στην ηλεκτρονική υπηρεσία ή σε ισοδύναμο.

Δεδομένου ότι τόσο τα προσωπικά δεδομένα ταυτότητας όσο και άλλα χαρακτηριστικά που σχετίζονται με τους χρήστες παρέχονται μέσω πιστοποιητικών ταυτότητας και πιστοποιητικών χαρακτηριστικών, όλα τα είδη ηλεκτρονικών ταυτοτήτων για τα οποία τα συμβαλλόμενα μέρη έχουν συμφωνήσει και αποτελούν μέρος του δικτύου μπορούν να χρησιμοποιηθούν για έλεγχο ταυτότητας έναντι ηλεκτρονικής υπηρεσίας που απαιτεί τόσο προσωπικό αριθμό ταυτότητας όσο και πρόσθετες πληροφορίες, ακόμη και αν η ηλεκτρονική ταυτότητα δεν περιέχει συγκεκριμένα προσωπικά δεδομένα (π.χ. πλαίσια κωδικών για τη δημιουργία κωδικών πρόσβασης μίας χρήσης).



Utfärdare 1	Εκδότης 1
Utfärdare n	Εκδότης n
Legitimeringstjänst 1	Υπηρεσία ελέγχου ταυτότητας 1
Vald legitimeringstjänst	Επιλεγμένη υπηρεσία ελέγχου ταυτότητας
Legitimeringstjänst n	Υπηρεσία ελέγχου ταυτότητας n
Anvisningstjänst	Υπηρεσία εύρεσης
Intyg	Πιστοποιητικό
Val av legitimeringstjänst	Επιλογή της υπηρεσίας ελέγχου ταυτότητας
autentisering	έλεγχος ταυτότητας
attributtjänst	υπηρεσία χαρακτηριστικών
Webbläsare	Φυλλομετρητής
E-tjänst	Ηλεκτρονική υπηρεσία

Σχήμα 1: *Απεικόνιση της επικοινωνίας μεταξύ των διαφόρων υπηρεσιών στο πλαίσιο δικτύου ταυτοτήτων.*

[1]: Η υπηρεσία ελέγχου ταυτότητας αναφέρεται επίσης σε άλλα έγγραφα της Digg ως υπηρεσία ταυτότητας και υπηρεσία πιστοποίησης. Ωστόσο, στο παρόν έγγραφο χρησιμοποιείται μόνο ο όρος «υπηρεσία ελέγχου ταυτότητας».

1.2. Πλαίσιο εμπιστοσύνης και επίπεδα ασφάλειας

Η βάση για την οποία πρέπει να εφαρμόζεται το επίπεδο ασφάλειας κατά τον έλεγχο ταυτότητας ενός χρήστη είναι το επίπεδο διασφάλισης για την ηλεκτρονική ταυτοποίηση που απαιτείται από την ηλεκτρονική υπηρεσία. Για να είναι συγκρίσιμα αυτά τα επίπεδα ασφάλειας στο πλαίσιο του δικτύου, ορίζονται τέσσερα επίπεδα διασφάλισης (1-4) στο

Πλαίσιο Εμπιστοσύνης για τη σουηδική ηλεκτρονική ταυτοποίηση [Digg.Tillit] και τρία επίπεδα διασφάλισης (χαμηλό, βασικό, υψηλό) στον κανονισμό eIDAS της ΕΕ. Όλοι οι εκδότες πιστοποιητικών ταυτότητας πρέπει να αποδεικνύουν ότι ολόκληρη η διαδικασία στην οποία βασίζεται η έκδοση πιστοποιητικών ταυτότητας πληροί τις απαιτήσεις του απαιτούμενου επιπέδου διασφάλισης, μεταξύ άλλων:

- απαιτήσεις για τη δημιουργία του πιστοποιητικού ταυτότητας·
- απαιτήσεις για την ηλεκτρονική ταυτοποίηση (έλεγχος ταυτότητας)·
- απαιτήσεις για τη διαδικασία έκδοσης·
- απαιτήσεις για την ίδια την ηλεκτρονική ταυτότητα και τη χρήση της·
- απαιτήσεις για τον εκδότη της ηλεκτρονικής ταυτότητας·
- απαίτηση για την εξακρίβωση της ταυτότητας του αιτούντος ηλεκτρονική ταυτοποίηση.

1.3. Υπηρεσία συλλογής, διαχείρισης και δημοσίευσης μεταδεδομένων

Ένα δίκτυο SAML παρέχει πληροφορίες σχετικά με τους συμμετέχοντες του δικτύου μέσω μεταδεδομένων SAML. Τόσο οι οντότητες που παρέχουν υπηρεσίες ελέγχου ταυτότητας και χαρακτηριστικών στο δίκτυο όσο και τα συμβαλλόμενα μέρη, δηλαδή οι οντότητες που καταναλώνουν αυτές τις υπηρεσίες, π.χ. ηλεκτρονικές υπηρεσίες, θεωρούνται συμμετέχοντες σε δίκτυο.

Τα μεταδεδομένα του δικτύου επιτρέπουν στους συμμετέχοντες να λαμβάνουν πληροφορίες σχετικά με τις υπηρεσίες άλλων συμμετεχόντων, συμπεριλαμβανομένων των δεδομένων που είναι απαραίτητα για την ασφαλή ανταλλαγή πληροφοριών μεταξύ των συμμετεχόντων. Τα μεταδεδομένα πρέπει να επικαιροποιούνται από κάθε μέρος και σύμφωνα με τους συμβατικούς όρους.

Ο κύριος σκοπός των μεταδεδομένων είναι η παροχή των κλειδιών/πιστοποιητικών που απαιτούνται για την ασφαλή επικοινωνία και ανταλλαγή πληροφοριών μεταξύ των υπηρεσιών. Εκτός από τα κλειδιά, τα μεταδεδομένα περιέχουν επίσης και άλλες πληροφορίες που είναι σημαντικές για την αλληλεπίδραση μεταξύ των υπηρεσιών, όπως διευθύνσεις των απαιτούμενων λειτουργιών, πληροφορίες σχετικά με τα επίπεδα διασφάλισης, τις κατηγορίες υπηρεσιών, τις πληροφορίες διεπαφής χρήστη κ.λπ.

Ένα δίκτυο ταυτοτήτων ορίζεται από ένα μητρώο σε μορφή XML που υπογράφεται με το πιστοποιητικό του φορέα εκμετάλλευσης του δικτύου. Το αρχείο περιέχει πληροφορίες σχετικά με τα μέλη του δικτύου ταυτοτήτων, συμπεριλαμβανομένων των πιστοποιητικών τους. Δεδομένου ότι το αρχείο μεταδεδομένων είναι υπογεγραμμένο, αρκεί η σύγκριση ενός πιστοποιητικού με το αντίστοιχο μεταδεδομένο. Μια υποδομή που βασίζεται σε κεντρικό μητρώο δικτύου απαιτεί το μητρώο να ενημερώνεται συνεχώς και τα μέλη του δικτύου να χρησιμοποιούν πάντα την τελευταία έκδοση του αρχείου.

1.4. Υπηρεσία εύρεσης

Σε ένα δίκτυο ταυτοτήτων, είναι δυνατή η προσφορά και η κατανάλωση μιας κοινής υπηρεσίας εύρεσης, η οποία απαριθμεί τις υπηρεσίες ελέγχου ταυτότητας που είναι διαθέσιμες στον χρήστη για να επιλέξει. Ο σκοπός μιας τέτοιας υπηρεσίας εύρεσης είναι να απαλλάξει τις μεμονωμένες ηλεκτρονικές υπηρεσίες που αποτελούν μέρος του δικτύου ταυτότητας από την εφαρμογή υποστήριξης όσον αφορά τον τρόπο με τον οποίο οι χρήστες επιλέγουν την υπηρεσία ελέγχου ταυτότητας (ή τη μέθοδο σύνδεσης).

Δεδομένου ότι η υπηρεσία εύρεσης είναι διαθέσιμη στο πλαίσιο του δικτύου ταυτοτήτων, οι ηλεκτρονικές υπηρεσίες μπορούν να κατευθύνουν τους χρήστες τους εκεί προκειμένου να επιλέξουν την υπηρεσία ελέγχου ταυτότητας. Η υπηρεσία εύρεσης αλληλεπιδρά με τον χρήστη ο οποίος προβαίνει στην επιλογή του και, στη συνέχεια, ο χρήστης, μαζί με την επιλογή του, ανακατευθύνεται στην ηλεκτρονική υπηρεσία, η οποία πλέον γνωρίζει σε ποια υπηρεσία ελέγχου ταυτότητας θα πρέπει να αποσταλεί ο χρήστης για έλεγχο ταυτότητας.

> Προς το παρόν δεν υπάρχει κοινή υπηρεσία εύρεσης για το δίκτυο Sweden Connect.

1.5. Ενσωμάτωση στο συμβαλλόμενο μέρος

Τα συμβαλλόμενα μέρη, π.χ. οι ηλεκτρονικές υπηρεσίες, ενσωματώνονται με υπηρεσίες ελέγχου ταυτότητας μέσω τυποποιημένων μηνυμάτων και καταναλώνουν πιστοποιητικά ταυτότητας που διαθέτουν επίσης τυποποιημένους μορφότυπους.

Το τεχνικό πλαίσιο Sweden Connect επηρεάζεται από το προφίλ διαλειτουργικότητας «SAML V2.0 Προφίλ ανάπτυξης για διαλειτουργικότητα δικτύου» [SAML2Int]. Το προφίλ υποστηρίζεται από μια σειρά εμπορικών προϊόντων και λύσεων ανοιχτού κώδικα, που διευκολύνουν την ενσωμάτωση στις ηλεκτρονικές υπηρεσίες.

Πολλές ηλεκτρονικές υπηρεσίες χρησιμοποιούν αυτόνομες λύσεις ελέγχου ταυτότητας, πράγμα που σημαίνει ότι η προσαρμογή της ενσωμάτωσης ώστε να συμμορφώνεται με το τεχνικό πλαίσιο έχει περιορισμένο αντίκτυπο στην ίδια την ηλεκτρονική υπηρεσία.

1.6. Υπογραφή

Κατά την υπογραφή, το τεχνικό πλαίσιο Sweden Connect καθιστά δυνατή τη χρήση διαφορετικών τύπων ηλεκτρονικής ταυτοποίησης, ακόμη και εκείνων που δεν βασίζονται σε πιστοποιητικά, χωρίς την ανάγκη ειδικών προσαρμογών στην ηλεκτρονική υπηρεσία. Αυτό οφείλεται στο γεγονός ότι το ηλεκτρονικά εκδοθέν πιστοποιητικό ταυτότητας (που χρησιμοποιείται για την ταυτοποίηση των χρηστών κατά την υπογραφή) έχει τον ίδιο μορφότυπο ανεξάρτητα από τον τύπο της ηλεκτρονικής ταυτοποίησης που χρησιμοποιεί ο χρήστης.

Μια υπηρεσία υπογραφής έχει ως στόχο να καταστήσει δυνατές τις υπογραφές εντός δικτύων ταυτοτήτων που συμμορφώνονται με το τεχνικό πλαίσιο, υποστηριζόμενες από όλους τους τύπους ηλεκτρονικής ταυτοποίησης που προσφέρουν επαρκή βαθμό ασφάλειας.

Με την προμήθεια[1] και την εισαγωγή μιας υπηρεσίας υπογραφής, ένα συμβαλλόμενο μέρος του δικτύου μπορεί να επιτρέψει σε έναν χρήστη να υπογράψει ένα ηλεκτρονικό έγγραφο με την υποστήριξη της υπηρεσίας υπογραφής. Η ηλεκτρονική υπογραφή του χρήστη και το

σχετικό πιστοποιητικό υπογραφής δημιουργούνται από την υπηρεσία υπογραφής αφού ο χρήστης συμφωνήσει στη υπογραφή προβαίνοντας σε έλεγχο της ταυτότητάς του έναντι της υπηρεσίας υπογραφής[2].

[1]: Είναι επίσης δυνατή η υλοποίηση μιας υπηρεσίας υπογραφής με βάση τις προδιαγραφές του τεχνικού πλαισίου ή η απόκτηση υπηρεσίας υπογραφής με άλλο τρόπο.

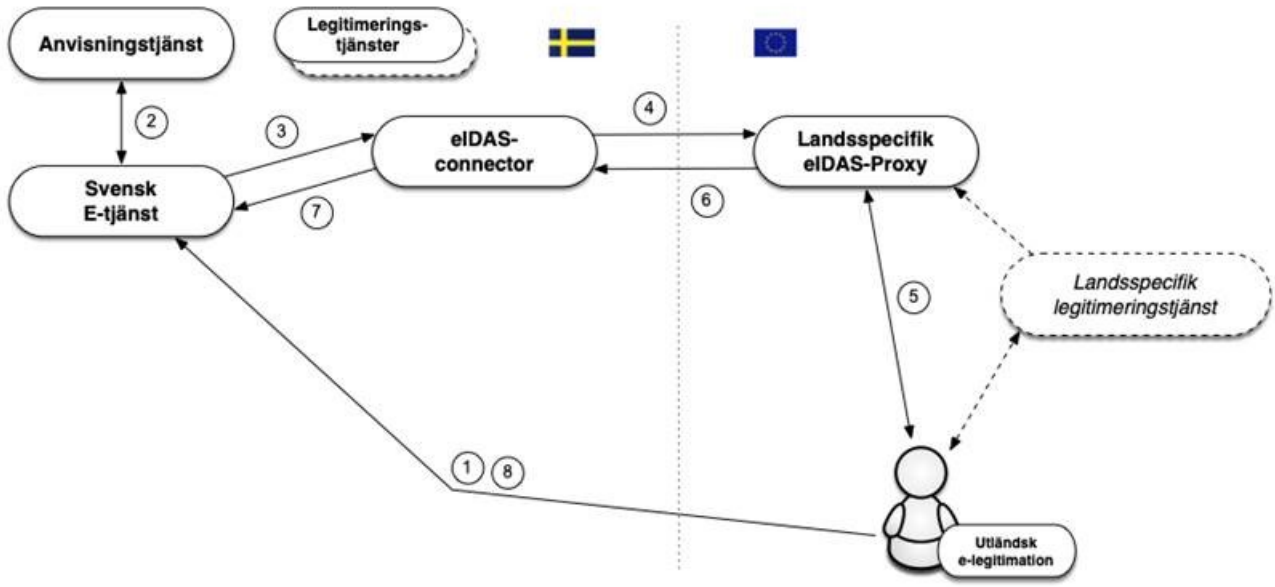
[2]: Είναι σημαντικό να σημειωθεί ότι είναι υψίστης σημασίας ο χρήστης να αντιλαμβάνεται αυτήν τη διαδικασία ως υπογραφή ενός εγγράφου. Ως εκ τούτου, θα πρέπει να χρησιμοποιείται ροή υπογραφής για τις ηλεκτρονικές ταυτότητες που το υποστηρίζουν σε σχέση με τον «έλεγχο ταυτότητας για υπογραφή».

1.7. Τεχνικό πλαίσιο και eIDAS

Ο κανονισμός (ΕΕ) αριθ. 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης, eIDAS, απαιτεί από τους σουηδικούς δημόσιους φορείς να αναγνωρίζουν τις ηλεκτρονικές ταυτότητες που έχουν κοινοποιήσει άλλες χώρες του eIDAS. Αυτό σημαίνει ότι μια δημόσια σουηδική ηλεκτρονική υπηρεσία που βασίζεται σε ορισμένους κανόνες πρέπει να είναι σε θέση να δέχεται σύνδεση που πραγματοποιείται με τη χρήση ηλεκτρονικής ταυτότητας που έχει εκδοθεί σε άλλη χώρα.

1.7.1. Έλεγχος ταυτότητας με χρήση ξένων eID

Οι τεχνικές προδιαγραφές για το eIDAS βασίζονται, όπως και το τεχνικό πλαίσιο, σε πρότυπα SAML, και παρόλο που υπάρχουν πολλές ομοιότητες, υπάρχουν επίσης διαφορές σε αυτές τις προδιαγραφές. Ωστόσο, μια σουηδική ηλεκτρονική υπηρεσία δεν θα πρέπει να σχετίζεται άμεσα με τις τεχνικές προδιαγραφές του eIDAS. Η παρακάτω εικόνα δείχνει τον τρόπο με τον οποίο ο σουηδικός κόμβος eIDAS (*σύνδεσμος eIDAS*) λειτουργεί ως γέφυρα μεταξύ άλλων χωρών και του σουηδικού δικτύου όταν γίνεται έλεγχος ταυτότητα ενός προσώπου με τη χρήση ξένης ηλεκτρονικής ταυτότητας σε σουηδική ηλεκτρονική υπηρεσία. Ο σουηδικός κόμβος eIDAS συμμορφώνεται με το τεχνικό πλαίσιο.



Anvisningstjänst	Υπηρεσία εύρεσης
Legitimeringstjänster	Υπηρεσίες ελέγχου ταυτότητας
Svensk E-tjänst	Σουηδική ηλεκτρονική υπηρεσία
EiDAS-connector	σύνδεσμος eiDAS
Landsspecifik Eidas Proxy	Ειδική ανά χώρα υπηρεσία μεσολάβησης eIDAS
Landsspecifik legitimeringstjänst	Υπηρεσία ελέγχου ταυτότητας ανά χώρα
utländsk e-legitimation	ξένη eID

Η ροή έχει ως εξής:

1. Ένας χρήστης με ξένη ηλεκτρονική ταυτότητα ζητεί πρόσβαση σε σουηδική ηλεκτρονική υπηρεσία (δηλ. συνδέεται).

2. Η ηλεκτρονική υπηρεσία επιτρέπει στον χρήστη να επιλέξει τη μέθοδο σύνδεσης χρησιμοποιώντας μια υπηρεσία εύρεσης. Εμφανίζεται η επιλογή «Ξένη eID», η οποία επιλέγεται από τον χρήστη στην περίπτωση eIDAS.

3. Η ηλεκτρονική υπηρεσία δημιουργεί αίτημα ελέγχου ταυτότητας σύμφωνα με το παρόν τεχνικό πλαίσιο και κατευθύνει τον χρήστη στον σουηδικό κόμβο eIDAS (*σύνδεσμος*) για τον οποίο είναι υπεύθυνη η DIGG. Ο κόμβος eIDAS λειτουργεί ως υπηρεσία ελέγχου ταυτότητας (*Πάροχος ταυτότητας*) στο δίκτυο έναντι των σουηδικών συμβαλλόμενων μερών, πράγμα που σημαίνει ότι η επικοινωνία με αυτήν την υπηρεσία πραγματοποιείται με τον ίδιο τρόπο όπως και με άλλες υπηρεσίες ελέγχου ταυτότητας εντός δικτύων που συμμορφώνονται με το τεχνικό πλαίσιο.

4. Το αίτημα που λαμβάνεται διεκπεραιώνεται και ο κόμβος eIDAS εμφανίζει μια σελίδα επιλογής στην οποία ο χρήστης επιλέγει «τη χώρα του»[1]. Ο σουηδικός κόμβος eIDAS μετατρέπει τώρα το αίτημα ελέγχου ταυτότητας που έχει παραληφθεί σε αίτημα ελέγχου ταυτότητας eIDAS και κατευθύνει τον χρήστη στην «υπηρεσία μεσολάβησης eIDAS» της επιλεγμένης χώρας.

5. Όταν το αίτημα ελέγχου ταυτότητας παραλαμβάνεται από την υπηρεσία μεσολάβησης eIDAS για την επιλεγμένη χώρα, αναλαμβάνει η τεχνολογία ελέγχου ταυτότητας αυτής της χώρας. Δεν χρησιμοποιούν όλες οι χώρες eIDAS το SAML για έλεγχο ταυτότητας, αλλά εάν αυτό συνέβαινε στο παράδειγμά μας, ο χρήστης θα ανακατευθυνόταν σε μια υπηρεσία ελέγχου ταυτότητας (*Πάροχος ταυτότητας*) και πριν από αυτό ίσως και σε υπηρεσία εύρεσης για την επιλογή της υπηρεσίας ελέγχου ταυτότητας.

6. Μετά τη διενέργεια του ελέγχου ταυτότητας, δημιουργείται πιστοποιητικό (*Παραδοχή*) σύμφωνα με τις προδιαγραφές του eIDAS. Το εν λόγω πιστοποιητικό περιλαμβάνει χαρακτηριστικά ειδικά για το eIDAS που ταυτοποιούν τον χρήστη. Το πιστοποιητικό αυτό διαβιβάζεται στη συνέχεια στον σουηδικό κόμβο eIDAS.

7. Ο κόμβος λαμβάνει το πιστοποιητικό και επικυρώνει την ορθότητά του. Το εν λόγω πιστοποιητικό μετατρέπεται από μορφότυπο eIDAS σε πιστοποιητικό μορφοποιημένο σύμφωνα με το τεχνικό πλαίσιο και αποστέλλεται στην ηλεκτρονική υπηρεσία.

8. Το συμβαλλόμενο μέρος προσθέτει τυχόν πρόσθετες πληροφορίες και καθορίζει αν ο χρήστης θα πρέπει να έχει πρόσβαση στην υπηρεσία.

Ως εκ τούτου, οι σουηδικές ηλεκτρονικές υπηρεσίες πρέπει να υποστηρίζουν μόνο το τεχνικό πλαίσιο για να χειρίζονται έναν έλεγχο ταυτότητας που πραγματοποιείται με τη χρήση ευρωπαϊκής ηλεκτρονικής ταυτότητας. Ωστόσο, η ηλεκτρονική υπηρεσία πρέπει να είναι σε θέση να χειριστεί την ταυτότητα που παρουσιάζεται, η οποία δεν είναι απαραίτητα προσωπικός αριθμός ταυτότητας. Ως εκ τούτου, μπορεί να υπάρχουν περιπτώσεις όπου μια ηλεκτρονική υπηρεσία ελέγχει την ταυτότητα χρήστη μέσω του πλαισίου eIDAS, αλλά η ταυτότητα που παρουσιάζεται από τον χρήστη δεν μπορεί να χρησιμοποιηθεί στην ηλεκτρονική υπηρεσία. Περισσότερα σχετικά με αυτό στο κεφάλαιο 1.7.3 που ακολουθεί.

> [1]: Επί του παρόντος, ο χρήστης επιλέγει την «υπηρεσία μεσολάβησης eIDAS» στην οποία θα πρέπει να προωθηθεί το αίτημα. Αυτό εξαρτάται από τη χώρα στην οποία ανήκει ο εκδότης της ηλεκτρονικής ταυτότητας του χρήστη.

1.7.2. Υπογραφές με χρήση ξένων eID

Όπως έχει ήδη περιγραφεί, εφαρμόζεται ένα μοντέλο ηλεκτρονικής υπογραφής εντός αυτού του τεχνικού πλαισίου που ονομάζεται συνενωμένη υπογραφή. Μια υπηρεσία υπογραφής που βασίζεται σε διακομιστή συνδέεται με την ηλεκτρονική υπηρεσία, η οποία με τη σειρά της ζητεί υπογραφή. Όταν ένας χρήστης υπογράφει ένα έγγραφο, η ηλεκτρονική υπηρεσία στέλνει ένα αίτημα υπογραφής στην υπηρεσία υπογραφής. Στη συνέχεια, η υπηρεσία υπογραφής ζητεί από τον χρήστη να πιστοποιήσει την ταυτότητά του. Στο πλαίσιο του ελέγχου ταυτότητας, ο χρήστης εγκρίνει την υπογραφή. Η υπηρεσία υπογραφής στέλνει τα δεδομένα πίσω στην ηλεκτρονική υπηρεσία και στη συνέχεια αποθηκεύονται τα δεδομένα υπογραφής που σχετίζονται με το έγγραφο που έχει υπογραφεί.

Η διαδικασία αυτή καθιστά δυνατή την υπογραφή και με τη χρήση ξένου eID, καθώς η υπηρεσία υπογραφής μπορεί να επιλέξει να ελέγξει την ταυτότητα του χρήστη με χρήση ξένης eID σύμφωνα με τη διαδικασία που περιγράφεται ανωτέρω στην ενότητα 1.7.1.

Κατά την υπογραφή, σε αυτήν την περίπτωση, ο σουηδικός κόμβος eIDAS είναι υπεύθυνος να ενημερώσει τον χρήστη ότι ο σκοπός του ελέγχου ταυτότητας είναι η υπογραφή εγγράφου, ποιος ζήτησε την υπογραφή, καθώς και να παράσχει κάθε πληροφορία σχετικά με το τι υπογράφεται. Ένα πιστοποιητικό ταυτότητας εκδίδεται μόνο αφού ο χρήστης έχει επικυρώσει τον εαυτό του (για υπογραφή) και αυτό αποστέλλεται στην υπηρεσία υπογραφής, η οποία με τη σειρά της δημιουργεί την υπογραφή.

1.7.3. Διαχείριση ταυτοτήτων

Τα πιστοποιητικά ταυτότητας από άλλες χώρες συμμορφώνονται με τις τεχνικές προδιαγραφές σε επίπεδο ΕΕ που έχουν αναπτυχθεί στο πλαίσιο του κανονισμού eIDAS. Τα χαρακτηριστικά που πρέπει πάντα να περιλαμβάνει κάθε χώρα για τα φυσικά πρόσωπα, καθώς και για τους οργανισμούς («Ελάχιστο Σύνολο Δεδομένων», MDS) καθορίζονται στον εν λόγω κανονισμό. Κάθε χώρα πρέπει να περιλαμβάνει μοναδικό αναγνωριστικό ανά ηλεκτρονική ταυτότητα που να αντιπροσωπεύει μόνο ένα φυσικό πρόσωπο. Από ορισμένες χώρες, αυτά τα αναγνωριστικά θα είναι μοναδικά και συνεπή ανά άτομο με τον ίδιο τρόπο όπως, για παράδειγμα, οι σουηδικοί προσωπικοί αριθμοί ταυτότητας, αλλά αυτά τα αναγνωριστικά μπορούν να έχουν πολύ διαφορετικές συνθέσεις και χαρακτηριστικά. Ένα

χαρακτηριστικό που μπορεί να ποικίλλει είναι το πόσο διαρκεί ένα τέτοιο αναγνωριστικό, δηλαδή αν ένα τέτοιο αναγνωριστικό παραμένει αμετάβλητο κατά τη διάρκεια της ζωής ενός ατόμου ή αλλάζει εάν, για παράδειγμα, το άτομο μετακομίσει σε άλλη περιοχή, αλλάξει το όνομά του ή απλώς αλλάξει την ηλεκτρονική ταυτότητά του. Από ορισμένες χώρες (π.χ. το Ηνωμένο Βασίλειο), το αναγνωριστικό θα διαφέρει ανάλογα με το ποια από τις ηλεκτρονικές ταυτότητες της χώρας επιλέγει να χρησιμοποιήσει ο χρήστης.

Προκειμένου να απλουστευθεί η διαχείριση των χρηστών στις σουηδικές ηλεκτρονικές υπηρεσίες, ο σουηδικός κόμβος eIDAS δημιουργεί ένα τυποποιημένο αναγνωριστικό χαρακτηριστικό για τους χρήστες που έχουν πιστοποιηθεί με τη χρήση ξένης ηλεκτρονικής ταυτότητας, γνωστό ως *προσωρινό αναγνωριστικό* (συντομογραφία PRID). Επιπλέον, δημιουργείται ένα σχετικό χαρακτηριστικό που δηλώνει την αναμενόμενη διάρκεια ζωής αυτού του χαρακτηριστικού ταυτότητας. Το χαρακτηριστικό PRID δημιουργείται με βάση τις τιμές χαρακτηριστικών που λαμβάνονται από τον ξένο έλεγχο ταυτότητας σύμφωνα με καθορισμένες μεθόδους για τη συγκεκριμένη χώρα. Κάθε συνδυασμός χώρας και μεθόδου κατηγοριοποιείται από την άποψη της αναμενόμενης διάρκειας, δηλαδή πόσο πιθανό είναι μια ταυτότητα να αλλάξει με την πάροδο του χρόνου για το ίδιο πρόσωπο. Αυτό επιτρέπει στις σουηδικές ηλεκτρονικές υπηρεσίες να προσαρμόζουν την επικοινωνία με τον χρήστη και να παρέχουν προορατικά χαρακτηριστικά που διευκολύνουν έναν χρήστη του οποίου η ταυτότητα έχει αλλάξει να ανακτήσει τον έλεγχο των πληροφοριών του στην ηλεκτρονική υπηρεσία.

Σε ορισμένες περιπτώσεις, ένα πρόσωπο που έχει επικυρωθεί με τη χρήση ξένης ηλεκτρονικής ταυτότητας μπορεί επίσης να κατέχει σουηδικό αριθμό προσωπικής ταυτότητας. Το πρόσωπο αυτό μπορεί, για παράδειγμα, να είναι Σουηδός υπήκοος ο οποίος έχει μετακομίσει στο εξωτερικό και έχει αποκτήσει ξένη ηλεκτρονική ταυτότητα ή αλλοδαπός υπήκοος ο οποίος είναι εγγεγραμμένος στη Σουηδία και στον οποίο έχει χορηγηθεί προσωπικός αριθμός ταυτότητας.

Το γεγονός ότι ένα πρόσωπο με ξένη ηλεκτρονική ταυτότητα διαθέτει σουηδικό αριθμό ταυτότητας δεν είναι συνήθως γνωστό στην αλλοδαπή υπηρεσία ελέγχου ταυτότητας και, ως εκ τούτου, οι πληροφορίες αυτές δεν περιλαμβάνονται στο πιστοποιητικό ταυτότητας της χώρας στην οποία πιστοποιείται το πρόσωπο. Ο σουηδικός κόμβος, από την άλλη πλευρά, έχει τη δυνατότητα να αναζητήσει μια υπηρεσία χαρακτηριστικού στη Σουηδία[1] όσον αφορά το κατά πόσον υπάρχει καταχωρισμένος αριθμός ταυτότητας για το πρόσωπο που επικυρώνεται και μπορεί, στην περίπτωση αυτή, να προσθέσει τις πληροφορίες αυτές στο πιστοποιητικό ταυτότητας που αποστέλλεται στην ηλεκτρονική υπηρεσία.

> [1]: Κατά τον χρόνο σύνταξης, δεν υπάρχει υπηρεσία χαρακτηριστικού που να δημιουργεί σύνδεση μεταξύ των ταυτοτήτων eIDAS και των σουηδικών αριθμών προσωπικής ταυτότητας.

1.7.4. Σουηδικές eID σε ξένες ηλεκτρονικές υπηρεσίες

Η Σουηδία έχει κοινοποιήσει τις σουηδικές ηλεκτρονικές ταυτότητες στα επίπεδα διασφάλισης βασικό και υψηλό σύμφωνα με το eIDAS.

Αίτημα ελέγχου ταυτότητας από ξένη ηλεκτρονική υπηρεσία υποβάλλεται στον σουηδικό κόμβο eIDAS (υπηρεσία μεσολάβησης) μέσω συνδέσμου eIDAS στη χώρα της ηλεκτρονικής υπηρεσίας. Στον σουηδικό κόμβο eIDAS, ο χρήστης επιλέγει τη σουηδικό eID που επιθυμεί

να χρησιμοποιήσει για να επαληθεύσει την ταυτότητά του και, στη συνέχεια, αποστέλλεται αίτημα ελέγχου ταυτότητας στην υπηρεσία ελέγχου ταυτότητας (*Identity Provider*) που χειρίζεται την επιλεγμένη ηλεκτρονική ταυτότητα. Το αίτημα αυτό μορφοποιείται σύμφωνα με τεχνικό πλαίσιο, πράγμα που σημαίνει ότι μια σουηδική υπηρεσία ελέγχου ταυτότητας δεν υποχρεούται να συμμορφώνεται με τις τεχνικές προδιαγραφές eIDAS.

Ο χρήστης επικυρώνεται από τη σουηδική υπηρεσία ελέγχου ταυτότητας και εκδίδεται πιστοποιητικό ταυτότητας (σύμφωνα με το τεχνικό πλαίσιο). Το εν λόγω πιστοποιητικό λαμβάνεται από τη σουηδική υπηρεσία μεσολάβησης eIDAS και μετατρέπεται σε πιστοποιητικό σύμφωνα με τις προδιαγραφές του eIDAS πριν από τη διαβίβασή του στον σύνδεσμο eIDAS της αλλοδαπής και στη συνέχεια στην ηλεκτρονική υπηρεσία που το ζήτησε (*Πάροχος υπηρεσιών*).

2. Τεχνικές προδιαγραφές

Το παρόν κεφάλαιο περιέχει προδιαγραφές και προφίλ για δίκτυα ταυτοτήτων που συμμορφώνονται με το τεχνικό πλαίσιο Sweden Connect και ορισμένες συναφείς υπηρεσίες. Εκτός εάν ορίζεται διαφορετικά, τα έγγραφα αυτά είναι δεσμευτικά για την παροχή υπηρεσιών εντός δικτύων ταυτότητας που εφαρμόζουν το τεχνικό πλαίσιο.

2.1. Προφίλ και προδιαγραφές για SAML

Τα δίκτυα ταυτοτήτων που συμμορφώνονται με το τεχνικό πλαίσιο Sweden Connect βασίζονται στο «Προφίλ ανάπτυξης για το σουηδικό πλαίσιο ηλεκτρονικής ταυτοποίησης», [SAML.Profile]. Το προφίλ αυτό επηρεάζεται, αλλά όχι περιοριστικά, από το «Προφίλ Ανάπτυξης SAML V2.0 για τη Διαλειτουργικότητα δικτύων» [SAML2Int]. Το [SAML.Profile] περιέχει επίσης κανόνες και κατευθυντήριες γραμμές ειδικά για το τεχνικό πλαίσιο της Sweden Connect.

2.1.1. Προφίλ ανάπτυξης για το σουηδικό πλαίσιο ηλεκτρονικής ταυτοποίησης

Το έγγραφο «Προφίλ ανάπτυξης για το σουηδικό πλαίσιο ηλεκτρονικής ταυτοποίησης», [SAML.Profile], είναι το κύριο τεχνικό έγγραφο-πλαίσιο και προσδιορίζει, μεταξύ άλλων:

- τον τρόπο με τον οποίο κατασκευάζονται και ερμηνεύονται τα μεταδεδομένα SAML·
- τον τρόπο μορφοποίησης του αιτήματος ελέγχου ταυτότητας·
- τον τρόπο χειρισμού του αιτήματος ελέγχου ταυτότητας και τον τρόπο με τον οποίο σχεδιάζεται, επαληθεύεται και διεκπεραιώνεται το πιστοποιητικό ταυτότητας·
- απαιτήσεις ασφάλειας·
- ειδικές απαιτήσεις SAML για υπηρεσίες υπογραφής και «έλεγχο ταυτότητας για υπογραφή».

2.1.2. Σουηδικό πλαίσιο ηλεκτρονικής ταυτοποίησης – Μητρώο αναγνωριστικών

Η εφαρμογή μιας σουηδικής υποδομής ηλεκτρονικής ταυτοποίησης απαιτεί διάφορες μορφές αναγνωριστικών για την αναπαράσταση αντικειμένων σε δομές δεδομένων. Το έγγραφο

«Sweden Connect — Μητρώο αναγνωριστικών» [SC.Registry] ορίζει τη δομή των αναγνωριστικών που εκχωρούνται βάσει του τεχνικού πλαισίου, καθώς και ένα μητρώο καθορισμένων αναγνωριστικών.

2.1.3. Καθορισμός χαρακτηριστικών για το σουηδικό πλαίσιο ηλεκτρονικής ταυτοποίησης

Η προδιαγραφή «Καθορισμός χαρακτηριστικών για το σουηδικό πλαίσιο eID», [SAML.Attributes], δηλώνει τα SAML προφίλ χαρακτηριστικών που χρησιμοποιούνται εντός δικτύων ταυτότητας που συμμορφώνονται με το τεχνικό πλαίσιο, συμπεριλαμβανομένων αυτών που συνδέονται με το eIDAS μέσω του σουηδικού κόμβου eIDAS.

2.1.4. Κατηγορίες οντοτήτων για το σουηδικό πλαίσιο eID

Οι κατηγορίες οντοτήτων χρησιμοποιούνται εντός του δικτύου για διάφορους σκοπούς:

- Κατηγορίες οντοτήτων υπηρεσιών — Χρησιμοποιούνται σε μεταδεδομένα για να αντιπροσωπεύουν τις απαιτήσεις των ηλεκτρονικών υπηρεσιών για τα επίπεδα διασφάλισης και τα ζητούμενα χαρακτηριστικά, καθώς και για την εκπλήρωση των επιπέδων διασφάλισης από τις υπηρεσίες ελέγχου ταυτότητας και την παροχή χαρακτηριστικών.

- Κατηγορίες Ιδιοτήτων Υπηρεσιών — Χρησιμοποιούνται για να αντιπροσωπεύουν ένα συγκεκριμένο χαρακτηριστικό μιας υπηρεσίας.

- Κατηγορίες Οντοτήτων Τύπων Υπηρεσιών — Χρησιμοποιούνται για να αντιπροσωπεύουν διαφορετικούς τύπους υπηρεσιών εντός του δικτύου.

- Κατηγορίες Οντοτήτων Συμβάσεων Υπηρεσιών — Χρησιμοποιούνται από τις υπηρεσίες για να ανακοινώσουν έντυπα συμφωνίας και παρόμοια.

- Γενικές Κατηγορίες Οντοτήτων — κατηγορίες οντοτήτων που δεν εμπίπτουν σε καμία από τις παραπάνω κατηγορίες.

Η προδιαγραφή «Κατηγορίες οντοτήτων για το σουηδικό πλαίσιο ηλεκτρονικής ταυτοποίησης» [SAML.EntCat] προσδιορίζει τις κατηγορίες οντοτήτων που ορίζονται από το τεχνικό πλαίσιο και περιγράφει τη σημασία τους.

2.1.5. Προδιαγραφή Κατασκευασμένων Χαρακτηριστικών eIDAS για το Σουηδικό Πλαίσιο Ηλεκτρονικής Ταυτοποίησης

Η προδιαγραφή «Προδιαγραφή Κατασκευασμένων Χαρακτηριστικών eIDAS για το Σουηδικό Πλαίσιο eID», [SC.eIDAS.Attrs], προσδιορίζει διαδικασίες και κανόνες για το πώς ταχαρακτηριστικά ταυτότητας κατασκευάζονται με βάση τα χαρακτηριστικά που λαμβάνονται κατά τη διάρκειατου ελέγχου ταυτότητας στο eIDAS.

2.1.6. Προφίλ εφαρμογής για παρόχους ταυτότητας BankID εντός του σουηδικού πλαισίου ηλεκτρονικής ταυτοποίησης

Η προδιαγραφή «Προφίλ Εφαρμογής για Παρόχους Ταυτότητας BankID εντός του σουηδικού πλαισίου eID», [SAML.BankID], καθορίζει κανόνες για το πώς μια υπηρεσία ελέγχου ταυτότητας που υλοποιεί υποστήριξη για BankID πρέπει να σχεδιαστεί.

> **Παρακαλείστε να σημειώσετε τα εξής:** Η παρούσα προδιαγραφή δεν είναι δεσμευτική για τη συμμόρφωση με τεχνικό πλαίσιο. Έχει σημασία μόνο για τις υπηρεσίες ελέγχου ταυτότητας που εφαρμόζουν υποστήριξη για το BankID και τις ηλεκτρονικές υπηρεσίες που το χρησιμοποιούν. Ωστόσο, οι υπηρεσίες ελέγχου ταυτότητας που εφαρμόζουν υποστήριξη για το BankID και επιθυμούν να συνδεθούν με την ομοσπονδία Sweden Connect πρέπει να συμμορφώνονται με αυτήν την προδιαγραφή.

2.1.7. Κύρια επιλογή στα αιτήματα ελέγχου ταυτότητας SAML

Η προδιαγραφή «Κυρία επιλογή στα αιτήματα ελέγχου ταυτότητας SAML» [SAML.Principal] ορίζει μια επέκταση της SAML που επιτρέπει σε ένα συμβαλλόμενο μέρος να ενημερώνει μια υπηρεσία ελέγχου ταυτότητας σχετικά με την ταυτότητα που επιθυμεί να ελεγχθεί.

2.1.8. Επέκταση μηνύματος χρήστη σε αιτήματα ελέγχου ταυτότητας SAML

Η προδιαγραφή «Επέκταση μηνύματος χρήστη σε αιτήματα ελέγχου ταυτότητας SAML» [SAML.UMessage] ορίζει μια επέκταση σε SAML που επιτρέπει σε ένα συμβαλλόμενο μέρος να συμπεριλάβει ένα μήνυμα εμφάνισης στο αίτημα ελέγχου ταυτότητας που αποστέλλεται στην υπηρεσία ελέγχου ταυτότητας. Η υπηρεσία ελέγχου ταυτότητας μπορεί στη συνέχεια να εμφανίσει αυτό το μήνυμα στον χρήστη κατά το στάδιο ελέγχου ταυτότητας.

2.2. Προφίλ και προδιαγραφές για το OpenID Connect

2.2.1. Προφίλ OpenID Connect για το Sweden Connect

Το προφίλ «Προφίλ OpenID Connect για το Sweden Connect» [OIDC.Profile] βασίζεται στο σουηδικό προφίλ OpenID Connect το οποίο είναι ένα προφίλ OpenID Connect που αναπτύχθηκε από την OIDC Sweden για την προώθηση της διαλειτουργικότητας και της ασφάλειας στο πλαίσιο των σουηδικών λύσεων OIDC.

Το [OIDC.Profile] προσθέτει πρόσθετες απαιτήσεις σχετικά με το δίκτυο Sweden Connect.

2.2.2. Προδιαγραφή Απαιτήσεων και Πεδίων OpenID Connect για το Sweden Connect

Η προδιαγραφή «Προδιαγραφή Απαιτήσεων και Πεδίων OpenID Connect για το Sweden Connect» [OIDC.Claims] βασίζεται στην προδιαγραφή απαιτήσεων και πεδίων για το σουηδικό προφίλ OpenID Connect της OIDC Σουηδίας.

2.3. Προδιαγραφές για την υπογραφή

Η παρούσα ενότητα περιέχει παραπομπές στα έγγραφα που καθορίζουν τις υπηρεσίες υπογραφής εντός δικτύων που συμμορφώνονται με το τεχνικό πλαίσιο Sweden Connect.

2.3.1. Προφίλ εφαρμογής για τη χρήση του OASIS DSS στις κεντρικές υπηρεσίες υπογραφής

Το προφίλ εφαρμογής «Προφίλ Εφαρμογής για τη χρήση του OASIS DSS στις κεντρικές υπηρεσίες υπογραφής» [Sign.DSS.Profile] προσδιορίζει ένα προφίλ για την υπογραφή αιτήματος και απάντησης σύμφωνα με το πρότυπο OASIS «Υπηρεσία Ψηφιακής Υπογραφής βασικών πρωτοκόλλων, στοιχείων και δεσμεύσεων» [DSS].

2.3.2. Επέκταση DSS για Συνενωμένες Κεντρικές Υπηρεσίες Υπογραφής

Η «επέκταση του συστήματος DSS για συνενωμένες κεντρικές υπηρεσίες υπογραφής», [Sign.DSS.Ext], είναι επέκταση του προτύπου OASIS «Πρωτόκολλα, στοιχεία και δεσμεύσεις της υπηρεσίας ψηφιακής υπογραφής», [DSS], το οποίο καθορίζει τους ορισμούς που απαιτούνται για την υπογραφή βάσει του τεχνικού πλαισίου.

2.3.3. Προφίλ πιστοποιητικού για πιστοποιητικά που εκδίδονται από τις κεντρικές υπηρεσίες υπογραφής

Το προφίλ πιστοποιητικού «Προφίλ πιστοποιητικού για πιστοποιητικά που εκδίδονται από κεντρικές υπηρεσίες υπογραφής» [Sign.Cert.Profile] προσδιορίζει το περιεχόμενο των πιστοποιητικών υπογραφής. Αυτό το προφίλ εφαρμόζει μια νέα επέκταση πιστοποιητικού για την υποστήριξη υπηρεσιών υπογραφής.

Αυτό το προφίλ αναφέρεται στην «επέκταση πιστοποιητικού πλαισίου ελέγχου ταυτότητας», [AuthContext], η οποία περιγράφει τον τρόπο με τον οποίο το «Πλαίσιο ελέγχου ταυτότητας» αναπαρίσταται στα πιστοποιητικά X.509.

2.3.4. Πρωτόκολλο ενεργοποίησης υπογραφής για τη συνενωμένη υπογραφή

Η προδιαγραφή «Πρωτόκολλο ενεργοποίησης υπογραφής για συνενωμένη υπογραφή», [Sign.Activation], ορίζει ένα «Πρωτόκολλο Ενεργοποίησης Υπογραφής» (SAP) για την εφαρμογή της «διασφάλισης μοναδικού ελέγχου επιπέδου 2» (SCAL2) σύμφωνα με το πρότυπο «prEN 419241 — Αξιόπιστα Συστήματα Υποστήριξης Διακομιστή Υπογραφής».

3. Κατάλογος αναφοράς

3.1. DIGG

[Digg.Tillit]

Πλαίσιο εμπιστοσύνης για τη σουηδική ηλεκτρονική ταυτοποίηση.

[SC.Registry]

Sweden Connect — Μητρώο αναγνωριστικών.

[SAML.Profile]

Προφίλ ανάπτυξης για το σουηδικό πλαίσιο eID.

[SAML.Attributes]

Προδιαγραφές χαρακτηριστικών για το σουηδικό πλαίσιο eID.

[SAML.EntCat]

Κατηγορίες οντοτήτων για το σουηδικό πλαίσιο eID.

[SC.eIDAS.Attrs]

Προδιαγραφές Κατασκευασμένων Χαρακτηριστικών eIDAS για το σουηδικό πλαίσιο eID.

[SAML.BankID]

Προφίλ εφαρμογής για παρόχους ταυτότητας BankID εντός του σουηδικού πλαισίου eID.

[SAML.Principal]

Κύρια επιλογή στα αιτήματα ελέγχου ταυτότητας SAML.

[SAML.UMessage]

Επέκταση μηνύματος χρήστη σε αιτήματα ελέγχου ταυτότητας SAML.

[OIDC.Profile]

Προφίλ OpenID Connect για το Sweden Connect.

[OIDC.Claims]

Προδιαγραφή Απαιτήσεων και Πεδίων OpenID Connect για το Sweden Connect.

[Sign.DSS.Profile]

Προφίλ εφαρμογής για τη χρήση του OASIS DSS στις κεντρικές υπηρεσίες υπογραφής.

[Sign.DSS.Ext]

Επέκταση DSS για Συνενωμένες Κεντρικές Υπηρεσίες Υπογραφής.

[Sign.Cert.Profile]

Προφίλ πιστοποιητικού για πιστοποιητικά που εκδίδονται από τις Κεντρικές Υπηρεσίες Υπογραφής.

[Sign.Activation]

Πρωτόκολλο Ενεργοποίησης Υπογραφής για Συνενωμένη Υπογραφή.

3.2. Άλλες αναφορές

[SAML2Int]

Προφίλ ανάπτυξης SAML V2.0 για τη διαλειτουργικότητα του δικτύου.

[DSS]

Πρότυπο OASIS – Πρωτόκολλα, Στοιχεία και Δεσμεύσεις Υπηρεσιών Ψηφιακής Υπογραφής, έκδοση 1.0, 11 Απριλίου 2007.

[AuthContext]

RFC-7773. Επέκταση πιστοποιητικού πλαισίου ελέγχου ταυτότητας.