

Το πλαίσιο εμπιστοσύνης

για τη σουηδική ηλεκτρονική
ταυτοποίηση

Έκδοση 4 Οκτωβρίου 2022

1. Ιστορικό και σκοπός

Το πλαίσιο εμπιστοσύνης για την ηλεκτρονική ταυτοποίηση στη Σουηδία αποσκοπεί στη θέσπιση κοινών απαιτήσεων για τους εκδότες ηλεκτρονικών ταυτοτήτων που εξετάζονται και εγκρίνονται από τον Σουηδικό Οργανισμό Ψηφιακής Διακυβέρνησης (DIGG). Οι απαιτήσεις διακρίνονται σε διαφορετικά επίπεδα προστασίας —γνωστά ως επίπεδα διασφάλισης— τα οποία αντιστοιχούν σε διαφορετικούς βαθμούς τεχνικής και επιχειρησιακής ασφάλειας από την πλευρά του εκδότη και σε διαφορετικούς βαθμούς επαλήθευσης ότι το πρόσωπο στο οποίο εκδίδεται ηλεκτρονικό έγγραφο ταυτοποίησης είναι πράγματι αυτό που ισχυρίζεται ότι είναι.

Οι απαιτήσεις του εν λόγω πλαισίου εμπιστοσύνης ισχύουν για τα επίπεδα διασφάλισης 2 έως 4, ενώ το επίπεδο 4 αντιστοιχεί στο υψηλότερο επίπεδο προστασίας.

Η συμμόρφωση ερμηνεύεται ως εξής:

- 1) όταν δεν προσδιορίζεται το επίπεδο διασφάλισης, η απαίτηση πρέπει να ικανοποιείται σε όλα τα επίπεδα, και
- 2) όταν καθορίζεται το επίπεδο διασφάλισης, η συμμόρφωση διασφαλίζεται τουλάχιστον στο σχετικό επίπεδο.

Οι απαιτήσεις που καθορίζονται για επίπεδο χαμηλότερο από το αντίστοιχο επίπεδο δεν λαμβάνονται υπόψη.

2. Οργάνωση και διακυβέρνηση

Συνολικές επιχειρησιακές απαιτήσεις

- K2.1 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων (eID) που δεν είναι δημόσιοι φορείς λειτουργούν ως καταχωρισμένες νομικές οντότητες και συνάπτουν και διατηρούν την ασφάλιση που απαιτείται για την επιχείρηση.
- K2.2 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων πρέπει να έχουν καθιερωμένη επιχειρηματική δραστηριότητα, να είναι πλήρως λειτουργικοί σε όλα τα μέρη που προσδιορίζονται στο παρόν έγγραφο και να είναι πλήρως εξοικειωμένοι με τις νομικές απαιτήσεις που τους επιβάλλονται ως εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων.
- K2.3 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων πρέπει να έχουν την ικανότητα να αναλαμβάνουν τον κίνδυνο ευθύνης για ζημιές και να διαθέτουν επαρκείς οικονομικούς πόρους για τη διεξαγωγή των εργασιών τους για τουλάχιστον ένα έτος.

Ασφάλεια πληροφοριών

K2.4 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων έχουν θεσπίσει σύστημα διαχείρισης της ασφάλειας των πληροφοριών (ISMS) για τα τμήματα των δραστηριοτήτων τους που επηρεάζονται από το πλαίσιο εμπιστοσύνης, το οποίο βασίζεται, κατά περίπτωση, στο πρότυπο ISO/IEC 27001 ή σε ισοδύναμες αρχές για τη διαχείριση και τον έλεγχο των εργασιών ασφάλειας πληροφοριών, που περιλαμβάνουν τα εξής:

- 1) Όλες οι κρίσιμες για την ασφάλεια διοικητικές και τεχνικές διαδικασίες πρέπει να τεκμηριώνονται και να βασίζονται σε επίσημη βάση, όπου οι ρόλοι, οι αρμοδιότητες και οι εξουσίες καθορίζονται με σαφήνεια.
- 2) Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων διασφαλίζουν ότι διαθέτουν ανά πάσα στιγμή επαρκείς ανθρώπινους πόρους για την εκπλήρωση των υποχρεώσεών τους.
- 3) Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων θεσπίζουν διαδικασία διαχείρισης κινδύνου η οποία, με κατάλληλο τρόπο, συνεχώς ή τουλάχιστον κάθε 12 μήνες, αναλύει τις απειλές και τα τρωτά σημεία της επιχείρησης και, μέσω της θέσπισης μέτρων ασφαλείας, εξισορροπεί τους κινδύνους σε αποδεκτά επίπεδα.
- 4) Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων θεσπίζουν διαδικασία διαχείρισης συμβάντων η οποία διασφαλίζει συστηματικά την ποιότητα της υπηρεσίας, τις μορφές περαιτέρω αναφοράς και τη λήψη κατάλληλων αντιδραστικών και προληπτικών μέτρων για τον μετριασμό ή την πρόληψη ζημιών που προκύπτουν από τέτοια γεγονότα.
- 5) Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων καταρτίζουν και δοκιμάζουν τακτικά σχέδιο συνέχισης δραστηριοτήτων που πληροί τις απαιτήσεις προσβασιμότητας της επιχείρησης μέσω της ικανότητας αποκατάστασης κρίσιμων διαδικασιών σε περίπτωση κρίσης ή σοβαρών συμβάντων.
- 6) Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων αξιολογούν τακτικά τις εργασίες ασφάλειας των πληροφοριών και εισάγουν μέτρα βελτίωσης στο σύστημα διαχείρισης.

K2.5 Πεδίο εφαρμογής και ωριμότητα του συστήματος διαχείρισης:

Επίπεδο 4: Το σύστημα διαχείρισης της ασφάλειας των πληροφοριών συμμορφώνεται με το πρότυπο SS-ISO/IEC 27001:2017 ή ισοδύναμες μεταγενέστερες ή διεθνείς εκδόσεις του προτύπου, και εντός του πεδίου εφαρμογής αυτού περιλαμβάνονται όλες οι απαιτήσεις που επιβάλλονται στους εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων.

Όροι υπερβολίας

- K2.6 Ο εκδότης σουηδικών ηλεκτρονικών ταυτοτήτων που έχει αναθέσει την εκτέλεση μιας ή περισσότερων διαδικασιών κρίσιμης σημασίας για την ασφάλεια σε άλλο μέρος καθορίζει με σύμβαση για ποιες κρίσιμες διαδικασίες είναι υπεύθυνος ο υπεργολάβος και ποιες απαιτήσεις ισχύουν για αυτές, και αποσαφηνίζει τη συμβατική σχέση στη δήλωση του εκδότη.

Ιχνηλασιμότητα, διαγραφή και αποθήκευση εγγράφων

- K2.7 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων αποθηκεύουν:
- 1) έγγραφα αίτησης και έγγραφα σχετικά με την έκδοση, την παραλαβή ή το κλείδωμα ηλεκτρονικών ταυτοτήτων·
 - 2) συμβάσεις, έγγραφα πολιτικής και δηλώσεις εκδότη· και
 - 3) ιστορικό επεξεργασίας και άλλα έγγραφα τεκμηρίωσης που απαιτούνται για να αποδειχθεί η συμμόρφωση με τις απαιτήσεις που επιβάλλονται στους εκδότες των σουηδικών ηλεκτρονικών ταυτοτήτων και τα οποία καθιστούν δυνατή την παρακολούθηση που αποδεικνύει ότι οι κρίσιμες για την ασφάλεια διαδικασίες και έλεγχοι εφαρμόζονται και είναι αποτελεσματικά.
- K2.8 Η περίοδος αποθήκευσης δεν είναι μικρότερη από πέντε έτη και το υλικό μπορεί να παραχθεί σε ευανάγνωστη μορφή καθ' όλη τη διάρκεια αυτής της περιόδου, εκτός εάν απαιτείται διαγραφή από την άποψη της ιδιωτικότητας και υποστηρίζεται από νόμο ή άλλο κανονισμό.

Επανεξέταση και παρακολούθηση

- K2.9 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων ορίζουν λειτουργία εσωτερικού ελέγχου που επανεξετάζει περιοδικά τις δραστηριότητες έκδοσης. Ο εσωτερικός ελεγκτής είναι ανεξάρτητος κατά την εκτέλεση των καθηκόντων του κατά τρόπο που εξασφαλίζει αντικειμενικό και αμερόληπτο έλεγχο και διαθέτει τις ικανότητες και την πείρα που απαιτούνται για την άσκηση των καθηκόντων του. Ο εσωτερικός ελεγκτής προγραμματίζει ανεξάρτητα τη διενέργεια του ελέγχου και την τεκμηριώνει σε πρόγραμμα ελέγχου που καλύπτει περίοδο τριών ετών. Τα στοιχεία ελέγχου επιλέγονται βάσει ανάλυσης κινδύνου και σημαντικότητας και βασίζονται στις περιγραφές των πράξεων που υποβάλλει ο εκδότης στον Οργανισμό Ψηφιακής Διακυβέρνησης.

Επίπεδα 3 και 4: Ο εσωτερικός έλεγχος διενεργείται βάσει αποδεκτών ελεγκτικών προτύπων.

3. Φυσική, διοικητική και ανθρωποκεντρική ασφάλεια

- K3.1 Τα κεντρικά τμήματα της λειτουργίας προστατεύονται φυσικά από ζημιές που προκαλούνται από περιβαλλοντικά γεγονότα, μη εξουσιοδοτημένη πρόσβαση ή άλλες εξωτερικές διαταραχές. Ο έλεγχος πρόσβασης εφαρμόζεται κατά τρόπο ώστε η πρόσβαση σε ευαίσθητες περιοχές να περιορίζεται στο εξουσιοδοτημένο προσωπικό, τα μέσα μεταφοράς πληροφοριών να αποθηκεύονται και να απορρίπτονται με ασφάλεια και η πρόσβαση στις εν λόγω προστατευόμενες περιοχές να παρακολουθείται συνεχώς.
- K3.2 Προτού ένα πρόσωπο αναλάβει οποιονδήποτε από τους ρόλους που προσδιορίζονται σύμφωνα με την παράγραφο K2.4 στοιχείο α) και οι οποίοι έχουν ιδιαίτερη σημασία για την ασφάλεια, ο εκδότης των σουηδικών ηλεκτρονικών ταυτοτήτων πρέπει να έχει διενεργήσει ελέγχους ιστορικού προκειμένου να διασφαλίσει ότι το πρόσωπο μπορεί να θεωρηθεί αξιόπιστο και διαθέτει τα προσόντα και την κατάρτιση που απαιτούνται για την ασφαλή εκτέλεση των καθηκόντων που απορρέουν από τον ρόλο.
- K3.3 Οι εκδότες διαθέτουν διαδικασίες που διασφαλίζουν ότι μόνο ειδικά εξουσιοδοτημένο προσωπικό έχει πρόσβαση στα δεδομένα που συλλέγονται και διατηρούνται σύμφωνα με την παράγραφο K2.7.
- K3.4 **Επίπεδα 3 και 4:** Οι εκδότες διασφαλίζουν σε όλη την αλυσίδα της διαδικασίας έκδοσης ότι ο διαχωρισμός των καθηκόντων εφαρμόζεται κατά τρόπο ώστε κανείς δεν έχει τη δυνατότητα να αποκτήσει ηλεκτρονική ταυτότητα εξ ονόματος άλλου προσώπου.

4. Τεχνική ασφάλεια

- K4.1 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων διασφαλίζουν ότι οι τεχνικοί έλεγχοι που εφαρμόζονται επαρκούν για την επίτευξη του επιπέδου προστασίας που κρίνεται αναγκαίο όσον αφορά τη φύση, το πεδίο εφαρμογής και άλλες περιστάσεις της επιχειρηματικής δραστηριότητας, και ότι οι εν λόγω έλεγχοι λειτουργούν και είναι αποτελεσματικοί.
- K4.2 Τα ηλεκτρονικά μέσα επικοινωνίας που χρησιμοποιούνται για τη διαβίβαση ευαίσθητων δεδομένων προστατεύονται από υποκλοπή, παραποίηση και επανάληψη.
- K4.3 Το ευαίσθητο υλικό κρυπτογράφησης που χρησιμοποιείται για την έκδοση ηλεκτρονικών ταυτοτήτων, την ταυτοποίηση των κατόχων και την έκδοση πιστοποιητικών ταυτότητας προστατεύεται κατά τρόπο ώστε:
- 1) η πρόσβαση να είναι περιορισμένη, λογικά και φυσικά, στους ρόλους και τις εφαρμογές που είναι απολύτως αναγκαίοι·
 - 2) το υλικό κρυπτογράφησης να μην αποθηκεύεται ποτέ σε απλό κείμενο σε σταθερά μέσα αποθήκευσης·
 - 3) το υλικό κρυπτογράφησης να προστατεύεται με τη χρήση κρυπτογραφικού υλικού με ενεργούς μηχανισμούς ασφάλειας που εξουδετερώνουν τόσο τις φυσικές όσο και τις λογικές απόπειρες πρόκλησης ζημίας στο υλικό κρυπτογράφησης·
 - 4) οι μηχανισμοί ασφάλειας για την προστασία του υλικού κρυπτογράφησης είναι διαφανείς και βασίζονται σε αναγνωρισμένα και καθιερωμένα πρότυπα· και
 - 5) **Επίπεδα 3 και 4:** η διαχείριση των δεδομένων ενεργοποίησης για την προστασία του υλικού κρυπτογράφησης διενεργείται μέσω ελέγχου πολλαπλών προσώπων.
- K4.4 Οι εκδότες διαθέτουν τεκμηριωμένες διαδικασίες που διασφαλίζουν ότι το απαιτούμενο επίπεδο προστασίας στο σχετικό περιβάλλον ΤΠ μπορεί να διατηρηθεί με την πάροδο του χρόνου και σε σχέση με αλλαγές, συμπεριλαμβανομένων τακτικών αξιολογήσεων τρωτότητας και κατάλληλης ετοιμότητας για την αντιμετώπιση των μεταβαλλόμενων επιπέδων κινδύνου και των συμβάντων που συμβαίνουν.

5. Αίτηση, αναγνώριση και καταχώριση

Πληροφορίες σχετικά με τις προϋποθέσεις

- K5.1 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων παρέχουν πληροφορίες σχετικά με τις συμβάσεις, τους όρους και τις προϋποθέσεις, καθώς και σχετικές πληροφορίες και τυχόν περιορισμούς στη χρήση της υπηρεσίας, σε συνδεδεμένους χρήστες, παρόχους ηλεκτρονικών υπηρεσιών και άλλους που ενδέχεται να βασίζονται στην υπηρεσία του εκδότη.
- K5.2 Ο εκδότης σουηδικών ηλεκτρονικών ταυτοτήτων αναφέρεται σαφώς στους όρους και τις προϋποθέσεις και σχεδιάζει τις διαδικασίες έτσι ώστε οι όροι και οι προϋποθέσεις να παρέχονται στον αιτούντα κατά τη διαδικασία έκδοσης.
- K5.3 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων υποβάλλουν δήλωση εκδότη η οποία περιλαμβάνει:
- 1) την ταυτότητα και τα στοιχεία επικοινωνίας του εκδότη·
 - 2) σύντομες περιγραφές των υπηρεσιών και των λύσεων που παρέχει ο εκδότης, συμπεριλαμβανομένων των εφαρμοζόμενων μεθόδων για την εφαρμογή, την έκδοση και το κλείδωμα·
 - 3) τους όρους που συνδέονται με την παρεχόμενη υπηρεσία, συμπεριλαμβανομένων των υποχρεώσεων του χρήστη για την προστασία της ηλεκτρονικής ταυτότητάς του, των υποχρεώσεων και ευθυνών του εκδότη, των τυχόν εγγυήσεων που παρέχονται και της υπόσχεσης διαθεσιμότητας·
 - 4) πληροφορίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τον τρόπο με τον οποίο πραγματοποιείται· και
 - 5) ρυθμίσεις για την τροποποίηση των όρων ή άλλων προϋποθέσεων της παρεχόμενης υπηρεσίας, συμπεριλαμβανομένων των μέτρων που πρέπει να ληφθούν για τη διακοπή της υπηρεσίας με ελεγχόμενο τρόπο.
- K5.4 **Επίπεδα 3 και 4:** Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων, κατόπιν αιτήματος του Οργανισμού Ψηφιακής Διακυβέρνησης (DIGG) ή άλλου συμβαλλόμενου μέρους που βασίζεται σε υπηρεσίες που παρέχονται από τον εκδότη, παρέχουν πληροφορίες σχετικά με τον τρόπο ιδιοκτησίας και διαχείρισης της επιχείρησης.
- K5.5 Ο εκδότης σουηδικών ηλεκτρονικών ταυτοτήτων που παύει τις δραστηριότητές του ακολουθεί προκαθορισμένο σχέδιο διακοπής της υπηρεσίας. Το σχέδιο περιλαμβάνει την ενημέρωση όλων των χρηστών της υπηρεσίας και του DIGG. Ο εκδότης διατηρεί περαιτέρω διαθέσιμο αρχειοθετημένο υλικό σύμφωνα με τις παραγράφους K2.7 και K2.8 μετά τη διακοπή λειτουργίας.

Εφαρμογή

K5.6 Μια σουηδική ηλεκτρονική ταυτότητα μπορεί να εκδοθεί μόνο κατόπιν αιτήματος του αιτούντος ή μέσω άλλης ισοδύναμης διαδικασίας αποδοχής και μόνον αφού ο αιτών λάβει γνώση των όρων υπό τους οποίους εκδίδεται και της ευθύνης που θα του ανατεθεί.

Ωστόσο, η έκδοση ηλεκτρονικής ταυτοποίησης που αντικαθιστά ή συμπληρώνει έγκυρο ή πρόσφατα αποκλεισμένο έγγραφο ηλεκτρονικής ταυτοποίησης το οποίο είχε εκδοθεί προηγουμένως από τον ίδιο εκδότη μπορεί να πραγματοποιηθεί χωρίς προηγούμενη διαδικασία υποβολής αίτησης.

K5.7 Η αίτηση για σουηδική ηλεκτρονική ταυτότητα συνδέεται με προσωπικό αριθμό ταυτότητας ή αριθμό συντονισμού, καθώς και με τις πληροφορίες που είναι άλλως απαραίτητες για την παροχή της ηλεκτρονικής ταυτότητας από τον εκδότη.

Προσδιορισμός της ταυτότητας του αιτούντος

K5.8 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων πρέπει να επαληθεύουν ότι οι πληροφορίες που συνδέονται με την αίτηση είναι πλήρεις και αντιστοιχούν σε πληροφορίες που έχουν καταχωριστεί σε επίσημο μητρώο.

K5.9 Όταν οι πληροφορίες που πρέπει να ελέγχονται σε επίσημο μητρώο επισημαίνονται ως εμπιστευτικές («προστατευόμενη ταυτότητα»), οι αναγκαίοι έλεγχοι μπορούν να διενεργούνται με άλλα ισοδύναμα μέσα.

K5.10 Ταυτοποίηση του αιτούντος κατά τη διάρκεια διά ζώσης συνάντησης:

Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων μπορούν να επαληθεύουν την ταυτότητα του αιτούντος κατά τη διάρκεια διά ζώσης συνάντησης, με τον ίδιο τρόπο όπως και κατά την έκδοση τυποποιημένου εγγράφου ταυτότητας.

K5.11 Εξ αποστάσεως ταυτοποίηση του αιτούντος στην υπάρχουσα σχέση:

Επίπεδο 3: Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων που έχουν ήδη ταυτοποιήσει τον αιτούντα σε σχέση που περιλαμβάνει οικονομικά ή νομικά σημαντικές συναλλαγές, και όταν ο αιτών μπορεί να ταυτοποιηθεί εξ αποστάσεως με άλλα αξιόπιστα μέσα ισοδύναμα με τις απαιτήσεις επιπέδου 3 του σουηδικού σήματος ποιότητας eID, μπορούν να χρησιμοποιούν αυτή τη μέθοδο για να εξακριβώσουν την ταυτότητα του αιτούντος.

Επίπεδο 4: Άνευ αντικειμένου.

K5.12 Ταυτοποίηση μέσω σουηδικής eID:

Ο εκδότης σουηδικών ηλεκτρονικών ταυτοτήτων μπορεί να προσδιορίσει τον αιτούντα εξ αποστάσεως μέσω υφιστάμενης ισχύουσας σουηδικής ηλεκτρονικής ταυτότητας τουλάχιστον του ίδιου επιπέδου διασφάλισης με εκείνο που πρόκειται να εκδοθεί, εάν μπορεί, χωρίς συμβατικά εμπόδια, να χρησιμοποιήσει τον εν λόγω προσδιορισμό ως βάση για την έκδοση νέας ηλεκτρονικής ταυτότητας.

Επίπεδο 4: Η περίοδος ισχύος της νεοεκδοθείσας ηλεκτρονικής ταυτότητας περιορίζεται ώστε να μην υπερβαίνει την περίοδο ισχύος της υφιστάμενης ηλεκτρονικής ταυτότητας.

K5.13 Εξ αποστάσεως ταυτοποίηση του αιτούντος:

Επίπεδο 2: Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων μπορούν να χρησιμοποιούν αξιόπιστες εγγραφές εικόνων έγκυρου τυποποιημένου εγγράφου ταυτότητας και της εικόνας προσώπου του αιτούντος ως βάση για την εξ αποστάσεως εξακρίβωση της ταυτότητας του αιτούντος, εάν η σύγκριση δεν δημιουργεί αμφιβολίες ως προς την πραγματική ταυτότητα του αιτούντος.

Επίπεδο 3: Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων μπορούν, μέσω ασφαλούς ανάγνωσης έγκυρου τυποποιημένου εγγράφου ταυτότητας που περιέχει ηλεκτρονικά αποθηκευμένα βιομετρικά δεδομένα, να εξακριβώσουν την ταυτότητα του αιτούντος εξ αποστάσεως βάσει των εν λόγω δεδομένων, εάν τα αντίστοιχα βιομετρικά δεδομένα του προσώπου που πρόκειται να ταυτοποιηθεί μπορούν να συλλεχθούν κατά τρόπο αρκούντως ασφαλή ώστε να είναι δυνατή η σύγκριση με ισοδύναμη αξιοπιστία όπως στην περίπτωση διά ζώσης συνάντησης, και όταν η σύγκριση δεν δημιουργεί αμφιβολίες ως προς την πραγματική ταυτότητα του αιτούντος.

Επίπεδο 4: Άνευ αντικειμένου.

Καταχώριση

- K5.14 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων, λαμβάνοντας υπόψη τους ισχύοντες κανόνες για την προστασία των δεδομένων προσωπικού χαρακτήρα, τηρούν μητρώο συνδεδεμένων χρηστών και τα χορηγηθέντα ηλεκτρονικά έγγραφα ταυτοποίησης και επικαιροποιούν το μητρώο αυτό.

6. Έκδοση και κλείδωμα της ηλεκτρονικής ταυτότητας (eID)

Σχεδιασμός τεχνικών μέσων

K6.1 Τεχνικά μέσα:

Επίπεδα 2 και 3: Τα τεχνικά μέσα ηλεκτρονικής ταυτοποίησης μέσω eID με το σουηδικό σήμα ποιότητας eID σχεδιάζονται σύμφωνα με μια αρχή δύο παραγόντων, σύμφωνα με την οποία το ένα μέρος αποτελείται από ηλεκτρονικά αποθηκευμένες πληροφορίες τις οποίες πρέπει να κατέχει ο χρήστης και το άλλο μέρος συνίσταται σε αυτό που χρησιμοποιεί ο χρήστης για να ενεργοποιήσει την ηλεκτρονική ταυτότητα.

Επίπεδο 4: Τα τεχνικά μέσα ηλεκτρονικής ταυτοποίησης μέσω eID με το σουηδικό σήμα ποιότητας eID σχεδιάζονται σύμφωνα με μια αρχή δύο παραγόντων, σύμφωνα με την οποία το ένα μέρος αποτελείται από μια ενότητα προσωπικής ασφάλειας που πρέπει να διαθέτει ο χρήστης και το άλλο μέρος συνίσταται σε αυτό που χρησιμοποιεί ο χρήστης για να ενεργοποιήσει τη μονάδα ασφάλειας.

K6.2 Ο μηχανισμός ενεργοποίησης και ο εξατομικευμένος κωδικός σχεδιάζονται κατά τρόπο ώστε να είναι απίθανο τρίτοι να παραβιάζουν την προστασία, ακόμη και με μηχανικά μέσα.

Επίπεδα 3 και 4: Η προστασία περιλαμβάνει μηχανισμούς για την πρόληψη της αντιγραφής και της παραποίησης του ηλεκτρονικού εγγράφου ταυτοποίησης.

K6.3 Οι χρήστες ηλεκτρονικής ταυτοποίησης με το σουηδικό σήμα ποιότητας eID μπορούν, με δική τους πρωτοβουλία, εντός της περιόδου ισχύος της ηλεκτρονικής ταυτότητας, δωρεάν και χωρίς σημαντικά προβλήματα, να ανταλλάξουν ή να ζητήσουν νέο προσωπικό κωδικό και, μέσω καθοδήγησης ή αυτόματης παραγωγής, να βοηθηθούν στη διατήρηση των απαιτήσεων του K6.2.

Εάν η ηλεκτρονική ταυτότητα έχει σχεδιαστεί κατά τρόπον ώστε να μην είναι δυνατή η ανταλλαγή εξατομικευμένου κωδικού, ο χρήστης θα πρέπει αντ' αυτού, υπό τις ίδιες συνθήκες, να είναι σε θέση να αποκτήσει αμέσως νέα ηλεκτρονική ταυτότητα με νέο εξατομικευμένο κωδικό που αντικαθιστά τον προηγούμενο μέσω διαδικασίας κλειδώματος.

K6.4 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων διασφαλίζουν ότι τα δεδομένα που έχουν καταχωριστεί για την ηλεκτρονική ταυτοποίηση των κατόχων αντιπροσωπεύουν μοναδικά τον αιτούντα και αποδίδονται στο εν λόγω πρόσωπο κατά την έκδοση του εγγράφου ηλεκτρονικής ταυτοποίησης.

K6.5 Η διάρκεια ισχύος των εκδοθεισών ηλεκτρονικών ταυτοτήτων είναι περιορισμένη, λαμβανομένων υπόψη των χαρακτηριστικών ασφαλείας του εγγράφου ηλεκτρονικής ταυτοποίησης και των κινδύνων κατάχρησης. Η μέγιστη περίοδος ισχύος της ηλεκτρονικής ταυτότητας είναι πέντε έτη.

Παροχή εγγράφου ηλεκτρονικής ταυτότητας

K6.6 Εξ αποστάσεως παροχή:

Επίπεδο 2: Ο εκδότης σουηδικών ηλεκτρονικών ταυτοτήτων παρέχει το έγγραφο e-ID κατά τρόπο που επιβεβαιώνει τα στοιχεία επικοινωνίας που τηρούνται στο επίσημο μητρώο ή τις πληροφορίες που καταγράφονται σε σχέση με την ηλεκτρονική διαδικασία σύμφωνα με το K5.13 Επίπεδο 2.

Επίπεδο 3: Ο εκδότης σουηδικών ηλεκτρονικών ταυτοτήτων που παρέχει ηλεκτρονική ταυτότητα μέσω ηλεκτρονικής διαδικασίας που είναι σύμφωνη με το K5.11 Επίπεδο 3, το K5.12 Επίπεδο 3 ή το K5.13 Επίπεδο 3, εξασφαλίζει, όταν εκδίδεται πρόσφατα, χωριστά και ανεξάρτητα από τη διάταξη όσον αφορά την ασφάλεια, ότι ο χρήστης ενημερώνεται ότι το εν λόγω έγγραφο e-ID έχει παραδοθεί, ή με άλλα μέτρα διασφαλίζει ισοδύναμο βαθμό ελέγχου ότι το πρόσωπο ενημερώνεται για τον κίνδυνο κλοπής ταυτότητας σε σχέση με τη διάταξη.

Επίπεδο 4: Ο εκδότης σουηδικών ηλεκτρονικών ταυτοτήτων που παρέχει ηλεκτρονική ταυτότητα μέσω ηλεκτρονικής διαδικασίας σύμφωνης με το K5.12 Επίπεδο 4, όταν εκδίδεται πρόσφατα, διασφαλίζει χωριστά και ανεξάρτητα από τη διάταξη όσον αφορά την ασφάλεια, ότι ο χρήστης ενημερώνεται ότι το εν λόγω έγγραφο ηλεκτρονικής ταυτοποίησης έχει παραδοθεί.

K6.7 Παροχή κατά τη διάρκεια διά ζώσης συνάντησης:

Ο εκδότης σουηδικών ηλεκτρονικών ταυτοτήτων παρέχει, κατά τη διάρκεια διά ζώσης συνάντησης και μετά από έλεγχο ταυτότητας σύμφωνα με την παράγραφο K5.10, το ηλεκτρονικό έγγραφο ταυτοποίησης έναντι υπογεγραμμένης απόδειξης και παρέχει περαιτέρω το μέρος που χρησιμοποιεί ο χρήστης για να ενεργοποιήσει την ηλεκτρονική ταυτότητα χωριστά και ανεξάρτητα από την παροχή του εγγράφου ηλεκτρονικής ταυτοποίησης όσον αφορά την ασφάλεια, με βάση τα στοιχεία επικοινωνίας που τηρούνται σε επίσημο μητρώο ή άλλες πληροφορίες ισοδύναμης αξιοπιστίας.

Υπηρεσία κλειδώματος

- K6.8 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων παρέχουν μια υπηρεσία κλειδώματος με καλή προσβασιμότητα ώστε ο χρήστης να είναι σε θέση να κλειδώσει την ηλεκτρονική ταυτότητά του.
- K6.9 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων επεξεργάζονται αμέσως και με ασφάλεια τα αιτήματα κλειδώματος και λαμβάνουν μέτρα για την πρόληψη της συστηματικής κατάχρησης της υπηρεσίας κλειδώματος ή άλλων εσκεμμένων ενεργειών που συνεπάγονται το ευρύ κλείδωμα των εγγράφων ηλεκτρονικής ταυτοποίησης, διασφαλίζοντας ότι οι ηλεκτρονικές ταυτότητες των χρηστών είναι διαθέσιμες, όταν χρειάζεται

7. Επαλήθευση των ηλεκτρονικών ταυτοτήτων των κατόχων

- K7.1 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων διασφαλίζουν ότι, κατά την επαλήθευση της ταυτότητας του κατόχου, διενεργούνται αξιόπιστοι έλεγχοι σχετικά με τη γνησιότητα και την εγκυρότητα του εγγράφου ηλεκτρονικής ταυτοποίησης.
- K7.2 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων διασφαλίζουν ότι έχουν εφαρμοστεί τεχνικές διαδικασίες ασφάλειας κατά την επαλήθευση των ηλεκτρονικών ταυτοτήτων των κατόχων, έτσι ώστε να είναι απίθανο τρίτα μέρη, μέσω εικασιών, υποκλοπών, επαναλήψεων ή χειραγώγησης της διαδικασίας, να παραβιάζουν τους μηχανισμούς προστασίας.

8. Έκδοση πιστοποιητικών ταυτότητας

Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων που παρέχουν υπηρεσία έκδοσης πιστοποιητικών ταυτότητας για τη χρήση ηλεκτρονικών υπηρεσιών συμμορφώνονται επίσης με τις διατάξεις του παρόντος τμήματος.

- K8.1 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων διασφαλίζουν ότι η υπηρεσία έκδοσης πιστοποιητικών ταυτότητας έχει καλή προσβασιμότητα και ότι πριν από την έκδοση πιστοποιητικών ταυτότητας προηγείται αξιόπιστη ταυτοποίηση σύμφωνα με τις διατάξεις της ενότητας 7.

Επίπεδο 4: Τα πιστοποιητικά περιλαμβάνουν αναφορά σε υλικό κρυπτογράφησης που επαληθεύεται από τον εκδότη ότι βρίσκεται στην αποκλειστική κατοχή του κατόχου.

- K8.2 Τα υποβληθέντα πιστοποιητικά ταυτότητας ισχύουν μόνο για όσο χρονικό διάστημα είναι απαραίτητο για την πρόσβαση του χρήστη στη ζητούμενη e-υπηρεσία, και προστατεύονται έτσι ώστε οι πληροφορίες να μπορούν να διαβαστούν μόνο από τον παραλήπτη για τον οποίο προορίζονται και ότι η γνησιότητα των πιστοποιητικών μπορεί να επαληθευτεί από τους αποδέκτες των πιστοποιητικών.
- K8.3 Οι εκδότες σουηδικών ηλεκτρονικών ταυτοτήτων, λαμβάνοντας υπόψη τους κινδύνους κατάχρησης της υπηρεσίας πιστοποίησης, περιορίζουν το χρονικό διάστημα εντός του οποίου μπορούν να εκδοθούν περισσότερα διαδοχικά πιστοποιητικά ταυτότητας σε συγκεκριμένο κάτοχο πριν από την εκ νέου ταυτοποίηση του κατόχου σύμφωνα με τις διατάξεις της ενότητας 7.