

NUMĂRUL DOSARULUI: 2022-
0941

Număr de identificare a
clasificării: 2 2 2

Cadrul de încredere

pentru e-identificarea suedeză

Versiunea din 4 octombrie 2022

1. Context și scop

Cadrul de încredere pentru identificarea electronică suedeză urmărește să stabilească cerințe comune pentru emitenții de documente de identificare electronică revizuite și aprobate de Agenția Suedeză pentru Guvernare Digitală (DIGG). Cerințele sunt împărțite în diferite niveluri de protecție – cunoscute sub denumirea de niveluri de asigurare – care corespund unor grade diferite de siguranță tehnică și operațională din partea emitentului și unor grade diferite de verificare a faptului că persoana căreia îi este emis un document de identificare electronică este într-adevăr cea care pretinde că este.

Cerințele acestui cadru de încredere se aplică nivelurilor de asigurare 2-4, nivelul 4 corespunzând celui mai înalt nivel de protecție.

Conformitatea se interpretează după cum urmează:

- (a) în cazul în care nivelul de asigurare nu este specificat, cerința trebuie îndeplinită la toate nivelurile și
- (b) în cazul în care se specifică nivelul de asigurare, conformitatea se asigură cel puțin la nivelul relevant.

Cerințele stabilite pentru un nivel mai scăzut decât cel relevant nu se iau în considerare.

2. Organizare și guvernare

Cerințe operaționale generale

- K2.1 Emitenții de documente de identificare electronică suedeze, care nu sunt organisme publice, trebuie să funcționeze ca entități juridice înregistrate și să încheie și să mențină asigurarea necesară pentru activitate.
- K2.2 Emitenții de documente de identificare electronică suedeze trebuie să aibă o activitate comercială stabilă, să fie pe deplin operaționali în toate părțile specificate în prezentul document și să fie bine familiarizați cu cerințele legale care le sunt impuse în calitate de emitenți de documente de identificare electronică suedeze.
- K2.3 Emitenții de documente de identificare electronică suedeze trebuie să aibă capacitatea de a-și asuma riscul de răspundere pentru daune și să dispună de resurse financiare suficiente pentru a-și desfășura operațiunile timp de cel puțin un an.

Siguranța informațiilor

K2.4 Emitenții de documente de identificare electronică suedeze trebuie să fi instituit un sistem de management al securității informațiilor (SMSI) pentru părțile activităților lor afectate de cadrul de încredere, care se bazează, după caz, pe ISO/IEC 27001 sau pe principii echivalente pentru gestionarea și controlul activității de securitate a informațiilor, inclusiv următoarele:

- (a) Toate procesele administrative și tehnice esențiale pentru siguranță trebuie să fie documentate și să se bazeze pe o fundație formală, în care rolurile, responsabilitățile și competențele sunt clar definite.
- (b) Emitenții de documente de identificare electronică suedeze se asigură că dispun în orice moment de resurse umane suficiente pentru a-și îndeplini obligațiile.
- (c) Emitenții de documente de identificare electronică suedeze instituie un proces de gestionare a riscurilor care, în mod corespunzător, continuu sau cel puțin o dată la 12 luni, analizează amenințările și vulnerabilitățile din întreprindere și care, prin introducerea unor măsuri de securitate, echilibrează riscurile la niveluri acceptabile.
- (d) Emitenții de documente de identificare electronică suedeze instituie un proces de gestionare a incidentelor care asigură în mod sistematic calitatea serviciului, forme de raportare ulterioară și că se iau măsuri de reacție și preventive adecvate pentru a atenua sau a preveni daunele rezultate în urma unor astfel de evenimente.
- (e) Emitenții de documente de identificare electronică suedeze stabilesc și testează periodic un plan de continuitate care îndeplinește cerințele de accesibilitate ale întreprinderii prin capacitatea de a restabili procesele critice în cazul unei crize sau al unor incidente grave.
- (f) Emitenții de documente de identificare electronică suedeze evaluează periodic activitatea de securitate a informațiilor și introduc măsuri de îmbunătățire în sistemul de management.

K2.5 Domeniul de aplicare și maturitatea sistemului de management:

Nivelul 4: Sistemul de management al securității informațiilor trebuie să fie conform cu SS-ISO/IEC 27001:2017 sau cu versiunile ulterioare sau internaționale echivalente ale standardului și, în domeniul de aplicare al acestuia, să includă toate cerințele impuse emitenților de documente de identificare electronică suedeze.

Condiții de subcontractare

- K2.6 Un emitent de documente de identificare electronică suedeze care a externalizat executarea unuia sau mai multor procese critice din punctul de vedere al securității către o altă parte trebuie să definească prin contract procesele critice de care este responsabil subcontractantul și cerințele care se aplică acestora și să clarifice relația contractuală în declarația emitentului.

Trasabilitatea, ștergerea și stocarea documentelor

- K2.7 Emitenții de documente de identificare electronică suedeze stochează:
- (a) documentele aferente cererii și documentele referitoare la emiterea, primirea sau blocarea documentelor de identificare electronică;
 - (b) contractele, documentele de politică și declarațiile emitentului; și
 - (c) istoricul prelucrării și alte documente de acest tip necesare pentru a dovedi conformitatea cu cerințele impuse emitenților de cărți de identitate electronice suedeze și care permit o monitorizare care să demonstreze că procesele și controalele critice din punctul de vedere al securității sunt instituite și eficace.
- K2.8 Perioada de stocare nu trebuie să fie mai mică de cinci ani, iar materialul trebuie să poată fi produs într-o formă lizibilă pe parcursul acestei perioade, cu excepția cazului în care o cerință de ștergere este necesară din punctul de vedere al vieții private și este susținută de lege sau de alte reglementări.

Reexaminare și urmărire

- K2.9 Emitenții de documente de identificare electronică suedeze instituie o funcție de audit intern care examinează periodic activitățile de emitere. Auditorul intern este independent în îndeplinirea îndatoririlor sale într-un mod care să asigure o examinare obiectivă și imparțială și are competența și experiența necesare pentru îndeplinirea îndatoririlor sale. Auditorul intern planifică în mod independent efectuarea auditului și consemnează acest lucru într-un plan de audit care acoperă o perioadă de trei ani. Elementele de audit sunt selectate pe baza unei analize a riscurilor și a semnificației și se bazează pe descrierile operațiunilor prezentate de emitent Agenției pentru Guvernare Digitală.

Nivelurile 3 și 4: Auditul intern se efectuează pe baza standardelor de audit acceptate.

3. Securitate fizică, administrativă și orientată spre persoane

- K3.1 Părțile centrale ale operațiunii sunt protejate fizic împotriva daunelor cauzate de evenimente de mediu, de accesul neautorizat sau de alte perturbări externe. Controlul accesului se aplică astfel încât accesul în zonele sensibile să fie limitat la personalul autorizat, mediile purtătoare de informații să fie stocate și eliminate în siguranță, iar accesul în aceste zone protejate să fie monitorizat în permanență.
- K3.2 Înainte ca o persoană să își asume oricare dintre rolurile identificate în conformitate cu punctul K2.4 litera (a) și care au o importanță deosebită pentru securitate, emitentul de cărți de identitate electronice suedeze trebuie să fi efectuat verificări ale antecedentelor pentru a se asigura că persoana poate fi considerată de încredere și că persoana deține calificările și formarea necesare pentru a îndeplini în condiții de siguranță și securitate sarcinile care decurg din rol.
- K3.3 Emitenții trebuie să dispună de proceduri pentru a se asigura că numai personalul autorizat în mod specific are acces la datele colectate și păstrate în conformitate cu K2.7.
- K3.4 **Nivelurile 3 și 4:** Emitenții se asigură, de-a lungul întregului lanț al procesului de emitere, că separarea sarcinilor se aplică astfel încât nicio persoană să nu poată obține o identificare electronică în numele altei persoane.

4. Securitate tehnică

- K4.1 Emitenții de documente de identificare electronică suedeze se asigură că controalele tehnice în vigoare sunt suficiente pentru a atinge nivelul de protecție considerat necesar în ceea ce privește natura, domeniul de aplicare și alte circumstanțe ale activității și că aceste controale funcționează și sunt eficace.

- K4.2 Mijloacele electronice de comunicare utilizate pentru transmiterea datelor sensibile trebuie să fie protejate împotriva interceptării, manipulării și reproducerii.
- K4.3 Materialele criptografice sensibile utilizate pentru emiterea de documente de identificare electronică, identificarea titularilor și eliberarea de certificate de identitate trebuie să fie protejate astfel încât:
- (a) accesul să fie limitat, din punct de vedere logic și fizic, la rolurile și aplicațiile care sunt strict necesare;
 - (b) materialul cu chei criptografice să nu fie niciodată stocat în text simplu pe suporturi de stocare persistente;
 - (c) materialul cu chei criptografice să fie protejat prin utilizarea unui modul hardware criptografic cu mecanisme de securitate active care contracarează atât încercările fizice, cât și cele logice de a compromite materialul cu chei criptografice;
 - (d) mecanismele de securitate pentru protecția materialelor cu chei criptografice sunt transparente și se bazează pe standarde recunoscute și bine stabilite; și
 - (e) **Nivelurile 3 și 4:** datele de activare pentru protecția materialului cu chei criptografice sunt gestionate prin controlul mai multor persoane.
- K4.4 Emitenții dispun de proceduri documentate pentru a se asigura că nivelul necesar de protecție în mediul informatic relevant poate fi menținut în timp și în legătură cu modificările, inclusiv evaluări periodice ale vulnerabilității și pregătirea adecvată pentru a face față nivelurilor de risc în schimbare și incidentelor care apar.

5. Cerere, identificare și înregistrare

Informații privind condițiile

- K5.1 Emitenții de documente de identificare electronică suedeze furnizează informații cu privire la contracte, termeni și condiții, precum și informații conexe și orice restricții privind utilizarea serviciului, utilizatorilor conectați, furnizorilor de servicii electronice și altor persoane care se pot baza pe serviciul emitentului.
- K5.2 Un emitent de documente de identificare electronică suedeze face trimitere în mod clar la termeni și condiții și concepe procedurile astfel încât termenii și condițiile să fie puse la dispoziția solicitantului în cadrul procesului de emitere.
- K5.3 Emitenții de documente de identificare electronică suedeze furnizează o declarație a emitentului care include:
- (a) identitatea și datele de contact ale emitentului;
 - (b) scurte descrieri ale serviciilor și soluțiilor furnizate de emitent, inclusiv metodele aplicate pentru aplicare, emitere și blocare;
 - (c) condițiile asociate cu serviciul furnizat, inclusiv obligațiile utilizatorului de a-și proteja identitatea electronică, obligațiile și responsabilitățile emitentului, orice garanție oferită și disponibilitatea promisă;
 - (d) informații privind prelucrarea datelor cu caracter personal și modul în care aceasta este efectuată; și
 - (e) modalitățile de modificare a termenilor sau a altor condiții ale serviciului furnizat, inclusiv măsurile care trebuie luate pentru a întrerupe serviciul în mod controlat.
- K5.4 **Nivelurile 3 și 4:** Emitenții de documente de identificare electronică suedeze trebuie să furnizeze, la cererea Agenției pentru Guvernare Digitală (DIGG) sau a unei alte părți contractante care se bazează pe serviciile furnizate de emitent, informații cu privire la modul în care întreprinderea este deținută și gestionată.
- K5.5 Un emitent de documente de identificare electronică suedeze care își încetează activitățile urmează un plan prestabilit pentru întreruperea serviciului. Planul include informarea tuturor utilizatorilor serviciului și a DIGG. Emitentul păstrează, de asemenea, materialele arhivate disponibile în conformitate cu K2.7 și K2.8 după întrerupere.

Cererea

K5.6 O carte de identitate electronică suedeză poate fi eliberată numai la cererea solicitantului sau printr-o altă procedură de acceptare echivalentă și numai după ce solicitantul a fost informat cu privire la condițiile în care este eliberată și la responsabilitatea care îi va reveni.

Cu toate acestea, emiterea unei cărți de identitate electronice care înlocuiește sau completează un document de identitate electronică valabil sau recent blocat emis anterior de același emitent poate avea loc fără nicio procedură de solicitare prealabilă.

K5.7 O cerere pentru un document electronic de identificare suedez trebuie să fie legată de un număr personal de identificare sau de un număr de coordonare, precum și de informațiile care sunt altfel necesare emitentului pentru a furniza un astfel de document electronic de identificare.

Stabilirea identității solicitantului

K5.8 Emitenții de documente de identificare electronică suedeze trebuie să verifice dacă informațiile legate de cerere sunt complete și corespund informațiilor înregistrate într-un registru oficial.

K5.9 În cazul în care informațiile care trebuie verificate într-un registru oficial sunt marcate ca fiind confidențiale („identitate protejată”), controalele necesare pot fi efectuate prin alte mijloace echivalente.

K5.10 Identificarea solicitantului în timpul unei vizite față în față:

Emitenții de documente de identificare electronică suedeze pot verifica identitatea solicitantului în timpul unei vizite față în față, în același mod ca atunci când eliberează un document de identitate standard.

K5.11 Identificarea de la distanță a solicitantului în relația existentă:

Nivelul 3: Emitenții de documente de identificare electronică suedeze care au identificat deja solicitantul într-o relație care implică tranzacții semnificative din punct de vedere economic sau juridic și în cazul în care solicitantul poate fi identificat de la distanță prin alte mijloace fiabile echivalente cu cerințele de nivel 3 ale mărcii de calitate eID suedeze pot utiliza această metodă pentru a stabili identitatea solicitantului.

Nivelul 4: Nu se aplică.

K5.12 Identificare printr-un document de identificare electronică suedez:

Un emitent de documente de identificare electronică suedeze poate identifica solicitantul de la distanță prin intermediul unui document de identificare electronică suedez valabil existent, având cel puțin același nivel de asigurare ca cel care urmează să fie emis, dacă poate, fără obstacole contractuale, să utilizeze o astfel de identificare ca bază pentru emiterea unui nou document de identificare electronică.

Nivelul 4: Perioada de valabilitate a noilor documente de identificare electronică emise este limitată astfel încât să nu depășească perioada de valabilitate a identificării electronice existente.

K5.13 Identificarea de la distanță a solicitantului:

Nivelul 2: Emitenții de documente de identificare electronică suedeze pot utiliza înregistrări fiabile ale imaginilor unui document de identitate standard valabil și ale imaginii faciale a solicitantului ca bază pentru stabilirea identității solicitantului de la distanță, în cazul în care comparația nu dă naștere la îndoieli cu privire la identitatea reală a solicitantului.

Nivelul 3: Emitenții de documente de identificare electronică suedeze pot, prin citirea securizată a unui document de identitate standard valabil care conține date biometrice stocate electronic, să stabilească identitatea solicitantului de la distanță pe baza acestor date, dacă datele biometrice corespunzătoare ale persoanei care urmează să fie identificată pot fi colectate într-un mod suficient de sigur, astfel încât să se poată efectua o comparație cu o fiabilitate echivalentă cu cea din cazul unei vizite față în față și în cazul în care comparația nu dă naștere unor îndoieli cu privire la identitatea reală a solicitantului.

Nivelul 4: Nu se aplică.

Înregistrare

- K5.14 Emitenții de documente de identificare electronică suedeze trebuie să țină, respectând normele aplicabile privind protecția datelor cu caracter personal, un registru al utilizatorilor conectați și al documentelor de identificare electronică alocate și să actualizeze acest registru.

6. Emiterea și blocarea documentelor de identificare electronică

Proiectarea mijloacelor tehnice

K6.1 Mijloace tehnice:

Nivelurile 2 și 3: Mijloacele tehnice de identificare electronică prin documente de identificare electronică cu marca de calitate suedeză eID trebuie să fie concepute conform principiului celor doi factori, conform căruia o parte constă în informații stocate electronic pe care utilizatorul trebuie să le dețină, iar cealaltă parte constă în ceea ce utilizatorul trebuie să utilizeze pentru a activa documentele de identificare electronică.

Nivelul 4: Mijloacele tehnice de identificare electronică prin documente de identificare electronică cu marca de calitate suedeză eID trebuie să fie concepute conform principiului celor doi factori, conform căruia o parte constă într-un modul de securitate personal pe care utilizatorul trebuie să îl dețină, iar cealaltă parte constă în ceea ce utilizatorul trebuie să utilizeze pentru a activa modulul de securitate.

K6.2 Mecanismul de activare și codul personalizat trebuie să fie proiectate astfel încât să fie puțin probabil ca terții să încalce protecția, chiar și prin mijloace mecanice.

Nivelurile 3 și 4: Protecția include mecanisme de prevenire a copierii și manipulării documentului de identificare electronică.

K6.3 Utilizatorii identificării electronice cu marca de calitate suedeză a identificării electronice pot, din proprie inițiativă, în perioada de valabilitate a identificării electronice, în mod gratuit și fără inconveniente semnificative, să schimbe sau să solicite un nou cod personal și, prin îndrumare sau producție automată, să fie ajutați să mențină cerințele de la punctul K6.2.

În cazul în care documentul de identificare electronică este conceput astfel încât un cod personalizat să nu poată fi schimbat, utilizatorul ar trebui, în schimb, în aceleași condiții, să poată obține cu promptitudine o nouă identificare electronică cu un nou cod personalizat care să îl înlocuiască pe cel anterior printr-o procedură de blocare.

K6.4 Emitenții de documente de identificare electronică suedeze se asigură că datele înregistrate pentru identificarea electronică a titularilor reprezintă în mod unic solicitantul și sunt atribuite persoanei în cauză atunci când eliberează documentul de identificare electronică.

K6.5 Perioada de valabilitate a documentelor de identificare electronică emise este limitată, ținând seama de elementele de securitate ale documentului de identificare electronică și de riscurile de utilizare abuzivă. Perioada maximă de valabilitate a documentului de identificare electronică este de cinci ani.

Furnizarea documentului de identificare electronică

K6.6 Furnizare de la distanță:

Nivelul 2: Un emitent de documente de identificare electronică suedeze furnizează documentul -de identificare electronică într-un mod care confirmă datele de contact păstrate în registrul oficial sau astfel de informații înregistrate în legătură cu procedura electronică conform K5.13 Nivelul 2.

Nivelul 3: Un emitent de documente de identificare electronică suedeze care furnizează o document de identificare electronică prin procedură electronică în conformitate cu K5.11 Nivelul 3, K5.12 Nivelul 3 sau K5.13 Nivelul 3 trebuie să se asigure, atunci când este emis recent, separat și independent de furnizarea în materie de securitate, că utilizatorul este informat că un astfel de document de identitate electronică a fost predat sau, prin alte măsuri, să asigure un grad echivalent de control asupra faptului că persoana este avertizată cu privire la riscul de furt de identitate în legătură cu furnizarea.

Nivelul 4: Un emitent de documente de identificare electronică suedeze care furnizează un document de identificare electronică printr-o procedură electronică conformă cu K5.12 Nivelul 4 trebuie să se asigure, atunci când este emis recent, separat și independent de furnizarea în materie de securitate, că utilizatorul este informat că un astfel de document de identificare electronică a fost predat.

K6.7 Furnizarea în timpul unei vizite față în față:

În timpul unei vizite față în față și după un control al identității în conformitate cu K5.10, un emitent de documente de identificare electronică suedeze furnizează documentul de identificare electronică pe baza unei confirmări de primire semnate și furnizează, de asemenea, partea pe care utilizatorul o utilizează pentru a activa documentul de identificare electronică separat și independent de furnizarea documentului de identificare electronică în ceea ce privește securitatea, pe baza datelor de contact păstrate într-un registru oficial sau a altor informații cu o credibilitate echivalentă.

Serviciu de blocare

K6.8 Emitenții de documente de identificare electronică suedeze trebuie să furnizeze un serviciu de blocare cu o bună accesibilitate pentru ca utilizatorul să își poată bloca documentul de identificare electronică

K6.9 Emitenții de documente de identificare electronică suedeze trebuie să prelucreze și să efectueze cu promptitudine și în condiții de siguranță cererile de blocare și să ia măsuri pentru a preveni utilizarea abuzivă sistematică a serviciului de blocare sau alte acțiuni intenționate care conduc la blocarea pe scară largă a documentelor de identificare electronică, asigurându-se că documentele de identificare electronică ale utilizatorilor sunt disponibile atunci când este necesar

7. Verificarea documentelor de identificare electronică ale titularilor

K7.1 Emitenții de documente de identificare electronică suedeze se asigură că, atunci când verifică identitatea titularului, se efectuează verificări fiabile ale autenticității și valabilității documentului de identificare electronică.

K7.2 Emitenții de documente de identificare electronică suedeze se asigură că au fost implementate controale tehnice de securitate atunci când verifică identitățile electronice ale titularilor, astfel încât este puțin probabil ca terțe părți, prin presupuneri, interceptare, reluare sau manipulare a procesului, să poată încălca mecanismele de protecție.

8. Eliberarea certificatelor de identitate

Emitenții de documente de identificare electronică suedeze care furnizează un serviciu de eliberare a certificatelor de identitate pentru serviciile electronice care se bazează pe acestea respectă, de asemenea, dispozițiile prezentei secțiuni.

- K8.1 Emitenții de documente de identificare electronică suedeze se asigură că serviciul de eliberare a certificatelor de identitate are o bună accesibilitate și că eliberarea certificatelor de identitate este precedată de o identificare fiabilă în conformitate cu dispozițiile secțiunii 7.

Nivelul 4: Certificatele includ o trimitere la materialul criptografic de chei verificat de emitent ca fiind în posesia exclusivă a titularului.

- K8.2 Certificatele de identitate prezentate sunt valabile numai atât timp cât este necesar pentru a permite accesul utilizatorului la serviciul -electronic solicitat și să fie protejate astfel încât informațiile să poată fi citite numai de destinatarul preconizat și autenticitatea certificatelor să poată fi verificată de destinatarii certificatelor.
- K8.3 Emitenții de documente de identificare electronică suedeze, ținând seama de riscurile de utilizare abuzivă a serviciului de certificare, limitează perioada de timp în care pot fi eliberate mai multe certificate de identitate consecutive unui anumit titular înainte ca titularul să fie identificat din nou în conformitate cu dispozițiile secțiunii 7.