IRATSZÁM: 2022-0941
OSZTÁLYOZÁSI AZONOSÍTÓ: 3.2.3

A bizalmi keretrendszer

a svéd e-azonosításhoz

2022. október 4-i változat

1. Háttér és cél

A svéd elektronikus azonosításra vonatkozó bizalmi keretrendszer célja, hogy egységes követelményeket állapítson meg a svéd Digitális Kormányzati Ügynökség (DIGG) által felülvizsgált és jóváhagyott elektronikus azonosítók kibocsátóira vonatkozóan. A követelmények különböző védelmi osztályokra – biztonsági szintekre – oszlanak, amelyek megfelelnek a kibocsátó által biztosított különböző technikai és működési biztonsági szinteknek, valamint az arra vonatkozóan végzett különböző szintű ellenőrzéseknek, hogy az a személy, akinek elektronikus személyazonosító okmányt állítottak ki, valóban az, akinek kiadja magát.

E bizalmi keretrendszer követelményei a 2–4. megbízhatósági szintre vonatkoznak, a 4. szint pedig a legmagasabb szintű védelemnek felel meg.

A megfelelést a következőképpen kell értelmezni:

(a) amennyiben a biztonsági szint nincs meghatározva, a követelményt minden szinten teljesíteni kell, és

(b) amennyiben a biztonsági szintet meghatározták, a megfelelést legalább a vonatkozó szinten biztosítani kell.

A vonatkozó szintnél alacsonyabb szintre megállapított követelményeket figyelmen kívül kell hagyni.

2. Szervezet és irányítás

Általános működési követelmények

K2.1 A svéd elektronikus személyazonosítók azon kibocsátóinak, amelyek nem közjogi szervek, nyilvántartásba vett jogi személyként kell működniük, és meg kell kötniük és fenn kell tartaniuk a vállalkozáshoz szükséges biztosítást.

K2.2 A svéd elektronikus személyazonosítók kibocsátóinak letelepedett vállalkozással kell rendelkezniük, az e dokumentumban meghatározott valamennyi rész tekintetében teljes mértékben működőképesnek kell lenniük, és jól kell ismerniük a svéd elektronikus személyazonosítók kibocsátóiként rájuk vonatkozó jogi követelményeket.

K2.3 A svéd elektronikus személyazonosítók kibocsátóinak viselniük kell tudni a kártérítési felelősség kockázatát, és elegendő pénzügyi forrással kell rendelkezniük ahhoz, hogy legalább egy évig folytassák működésüket.

Információbiztonság

K2.4 A svéd elektronikus személyazonosítók kibocsátóinak a bizalmi keretrendszer által érintett tevékenységeikre vonatkozóan információbiztonsági irányítási rendszert (ISMS) kell létrehozniuk, amely adott esetben az ISO/IEC 27001 szabványon vagy azzal egyenértékű, az információbiztonsági munka irányítására és ellenőrzésére vonatkozó elveken alapul, beleértve a következőket:

(a) A biztonság szempontjából kritikus valamennyi adminisztratív és műszaki folyamatot dokumentálni kell, és azoknak olyan hivatalos alapokon kell nyugodniuk, amelyek egyértelműen meghatározzák a szerepeket, a felelősségi köröket és a hatásköröket.

(b) A svéd elektronikus személyazonosítók kibocsátóinak biztosítaniuk kell, hogy mindenkor elegendő emberi erőforrással rendelkezzenek kötelezettségeik teljesítéséhez.

(c) A svéd elektronikus személyazonosítók kibocsátóinak ki kell alakítaniuk egy olyan kockázatkezelési eljárást, amely megfelelő módon, folyamatosan vagy legalább 12 havonta elemzi az üzleti tevékenységben rejlő fenyegetéseket és sebezhetőségeket, és amely biztonsági intézkedések bevezetésével elfogadható szintre egyensúlyozza a kockázatokat.

(d) A svéd elektronikus személyazonosítók kibocsátóinak ki kell alakítaniuk egy olyan eseménykezelési folyamatot, amely szisztematikusan biztosítja a szolgáltatás minőségét, a folytonos jelentéstétel formáit, valamint azt, hogy megfelelő reaktív és megelőző intézkedéseket hozzanak az ilyen eseményekből eredő károk enyhítésére vagy megelőzésére.

(e) A svéd elektronikus személyazonosítók kibocsátóinak létre kell hozniuk (és rendszeresen tesztelniük kell) egy olyan folytonossági tervet, amely válság vagy súlyos események esetén a kritikus folyamatok helyreállításának képessége révén megfelel az üzleti tevékenység akadálymentességi követelményeinek.

(f) A svéd elektronikus személyazonosítók kibocsátóinak rendszeresen értékelniük kell az információbiztonsági munkát, és javító intézkedéseket kell bevezetniük az irányítási rendszerbe.

K2.5 Az irányítási rendszer alkalmazási köre és kiforrottsága:

4. szint: Az információbiztonsági irányítási rendszernek meg kell felelnie az SS-ISO/IEC 27001:2017 szabványnak vagy a szabvány azzal egyenértékű későbbi vagy nemzetközi változatainak, és ennek hatálya alá kell tartoznia a svéd elektronikus személyazonosítók kibocsátóira vonatkozó valamennyi követelménynek.

Alvállalkozási feltételek

K2.6 A svéd elektronikus személyazonosítók azon kibocsátójának, amely egy vagy több, biztonsági szempontból kritikus folyamat elvégzését kiszervezte egy másik félnek, szerződésben kell meghatároznia, hogy mely kritikus folyamatokért felelős az alvállalkozó, és mely követelmények vonatkoznak rájuk, és a kibocsátói nyilatkozatban tisztáznia kell a szerződéses kapcsolatot.

Dokumentumok nyomon követhetősége, törlése és tárolása

K2.7 A svéd elektronikus személyazonosítók kibocsátói a következőket tárolják:

(a) kérelmezési dokumentumok és az elektronikus személyazonosítók kiállításával, átvételével, illetve letiltásával kapcsolatos dokumentumok;

(b) szerződések, szakpolitikai dokumentumok és kibocsátói nyilatkozatok; és

(c) a svéd elektronikus személyazonosítók kibocsátóira vonatkozó követelményeknek való megfelelés igazolásához szükséges feldolgozási előzmények és egyéb olyan dokumentumok, amelyek lehetővé teszik a biztonsági szempontból kritikus folyamatok és ellenőrzések meglétét és hatékonyságát igazoló utókövetést.

K2.8 A tárolási időszak nem lehet öt évnél rövidebb, és az anyagoknak ezen időszak alatt olvasható formában előállíthatóknak kell lenniük, kivéve, ha a törlésre vonatkozó követelmény a magánélet védelme szempontjából szükséges, és azt törvény vagy más rendelet alátámasztja.

Felülvizsgálat és utókövetés

K2.9 A svéd elektronikus személyazonosítók kibocsátóinak létre kell hozniuk egy belső ellenőrzési funkciót, amely rendszeres időközönként felülvizsgálja a kibocsátási tevékenységeket. A belső ellenőrnek a feladatai ellátása során független, objektív és pártatlan felülvizsgálatot biztosító módon kell eljárnia, és rendelkeznie kell a feladatai ellátásához szükséges szakértelemmel és tapasztalattal. A belső ellenőr önállóan megtervezi az ellenőrzés lefolytatását, és ezt egy hároméves időszakra vonatkozó ellenőrzési tervben dokumentálja. Az ellenőrzési elemeket kockázat- és lényegességi elemzés alapján kell kiválasztani, és azoknak a Kibocsátó által a Digitális Kormányzati Ügynökséghez benyújtott műveletleírásokon kell alapulniuk.

3. és 4. szint: A belső ellenőrzést elfogadott ellenőrzési standardok alapján kell elvégezni.

3. Fizikai, adminisztratív és személyorientált biztonság

K3.1 A művelet központi részeit fizikailag védeni kell a környezeti események, jogosulatlan hozzáférés vagy egyéb külső zavarok okozta károktól. A hozzáférés-ellenőrzést oly módon kell alkalmazni, hogy az érzékeny területekre való belépés az arra jogosult személyzetre korlátozódjon, az információhordozó eszközöket biztonságosan tárolják és ártalmatlanítsák, és az e védett területekre való belépést folyamatosan figyelemmel kísérjék.

K3.2 Még mielőtt egy személy betöltené a K2.4(a) ponttal összhangban meghatározott és a biztonság szempontjából különösen fontos szerepek valamelyikét, a svéd elektronikus személyazonosítók kibocsátójának háttérellenőrzéseket kell végeznie annak biztosítása érdekében, hogy az adott személy megbízhatónak tekinthető, és hogy az adott személy rendelkezik a szerepből eredő feladatok biztonságos és védett ellátásához szükséges képesítéssel és képzettséggel.

K3.3 A kibocsátóknak eljárásokkal kell rendelkezniük annak biztosítására, hogy csak a külön engedéllyel rendelkező személyzet férhessen hozzá a K2.7. ponttal összhangban gyűjtött és megőrzött adatokhoz.

K3.4 **3. és 4. szint:** A kibocsátóknak a kibocsátási folyamat teljes láncolatában biztosítaniuk kell, hogy a feladatok elkülönítése oly módon történjen, hogy egyetlen személy se kaphasson elektronikus személyazonosítót egy másik személy nevében.

4. Műszaki biztonság

K4.1 A svéd elektronikus személyazonosítók kibocsátóinak biztosítaniuk kell, hogy a bevezetett technikai ellenőrzések elegendőek legyenek a vállalkozás jellegére, tevékenységi körére és egyéb körülményeire tekintettel szükségesnek ítélt védelmi szint eléréséhez, és hogy ezek az ellenőrzések működjenek és hatékonyak legyenek.

K4.2 Az érzékeny adatok továbbításához használt elektronikus kommunikációs eszközöket védeni kell a lehallgatással, manipulációval és visszajátszással szemben.

K4.3 Az elektronikus személyazonosítók kibocsátásához, a birtokosok azonosításához és a személyazonosító igazolványok kiállításához használt érzékeny kriptográfiai kulcsanyagokat oly módon kell védeni, hogy:

(a) a hozzáférés logikailag és fizikailag a feltétlenül szükséges szerepekre és alkalmazásokra korlátozódjon;

(b) a kulcsanyagot sohase tárolják egyszerű szövegként tartós adathordozón;

(c) a kulcsanyagot olyan aktív biztonsági mechanizmusokkal rendelkező kriptográfiai hardvermodul használatával védik, amely ellensúlyozza a kulcsanyag veszélyeztetésére irányuló fizikai és logikai kísérleteket;

(d) a kulcsanyagok védelmét szolgáló biztonsági mechanizmusok átláthatóak és elismert, jól bevált szabványokon alapulnak; és

(e) **3. és 4. szint:** A kulcsanyag védelméhez szükséges aktiválási adatok kezelése többszemélyes kontrollal történik.

K4.4 A kibocsátóknak dokumentált eljárásokkal kell rendelkezniük annak biztosítására, hogy az adott informatikai környezetben a szükséges védelmi szint a változásokkal összefüggésben az idő múlásával is fenntartható legyen, beleértve a rendszeres sebezhetőségi értékeléseket és a megfelelő felkészültséget a változó kockázati szinteknek és a bekövetkező eseményeknek való megfelelésre.

5. Kérelem, azonosítás és nyilvántartásba vétel

Tájékoztatás a feltételekről

K5.1 A svéd elektronikus személyazonosítók kibocsátói tájékoztatást nyújtanak a szerződésekről, a szerződéses feltételekről, valamint a kapcsolódó információkról és a szolgáltatás használatára vonatkozó korlátozásokról a csatlakoztatott felhasználók, az e-szolgáltatók és minden olyan további fél számára, aki a kibocsátó szolgáltatására támaszkodhat.

K5.2 A svéd elektronikus személyazonosítók kibocsátójának egyértelműen hivatkoznia kell a szerződéses feltételekre, és úgy kell megterveznie az eljárásokat, hogy a feltételeket a kiállítási folyamat során a kérelmező számára biztosítsa.

K5.3 A svéd elektronikus személyazonosítók kibocsátóinak gondoskodniuk kell egy kibocsátói nyilatkozatról, amely a következőket tartalmazza:

(a) a kibocsátó kiléte és elérhetőségei;

(b) a kibocsátó által nyújtott szolgáltatások és megoldások rövid leírása, beleértve az alkalmazásra, a kibocsátásra és a letiltásra alkalmazott módszereket;

(c) a nyújtott szolgáltatáshoz kapcsolódó feltételek, beleértve a felhasználónak az elektronikus személyazonosító védelmére vonatkozó kötelezettségeit, a kibocsátó kötelezettségeit és felelősségét, a nyújtott garanciákat és az ígért rendelkezésre állást;

(d) tájékoztatás a személyes adatok kezeléséről és annak módjáról; és

(e) a nyújtott szolgáltatás szerződéses feltételeinek, illetve egyéb feltételeinek módosítására vonatkozó intézkedések, beleértve a szolgáltatás ellenőrzött módon történő megszüntetése érdekében teendő lépéseket.

K5.4 **3. és 4. szint:** A svéd elektronikus személyazonosítók (eID) kibocsátói a Digitális Kormányzati Ügynökség (DIGG) vagy a kibocsátó által nyújtott szolgáltatásokra támaszkodó más szerződő fél kérésére tájékoztatást nyújtanak a vállalkozás tulajdonlásáról és irányításáról.

K5.5 A tevékenységét megszüntető svéd eID-kibocsátónak a szolgáltatás megszüntetésére előre meghatározott tervet kell követnie. A tervnek tartalmaznia kell a szolgáltatás valamennyi felhasználójának és a DIGG-nek a tájékoztatását. A kibocsátó a megszűnést követően a K2.7 és K2.8 ponttal összhangban továbbra is hozzáférhetővé teszi az archivált anyagokat.

Kérelem

K5.6 Svéd elektronikus személyazonosítót csak a kérelmező kérésére vagy más egyenértékű átvételi eljárás keretében lehet kiállítani, és csak azt követően, hogy a kérelmezőt tájékoztatták a személyazonosító kiállításának feltételeiről és a rá háruló felelősségről.

Az ugyanazon kibocsátó által korábban kiállított érvényes vagy nemrégiben letiltott elektronikus személyazonosító okmányt helyettesítő vagy kiegészítő elektronikus személyazonosító kiállítására azonban előzetes kérelmezési eljárás nélkül is sor kerülhet.

K5.7 A svéd elektronikus személyazonosító iránti kérelmet személyazonosító számhoz vagy koordinációs számhoz, valamint a kibocsátó számára az ilyen elektronikus személyazonosító megadásához egyébként szükséges információkhoz kell kapcsolni.

A kérelmező személyazonosságának megállapítása

K5.8 A svéd elektronikus személyazonosítók kibocsátóinak ellenőrizniük kell, hogy a kérelemhez kapcsolódó információk hiánytalanok-e, és megfelelnek-e a hivatalos nyilvántartásban rögzített információknak.

K5.9 Amennyiben a hivatalos nyilvántartásban ellenőrizendő információkat bizalmasként („védett személyazonosság”) jelölik meg, a szükséges ellenőrzéseket más, ezzel egyenértékű módon is el lehet végezni.

K5.10 A kérelmező azonosítása személyes látogatás során:

A svéd elektronikus személyazonosítók kibocsátói személyes látogatás során ugyanúgy ellenőrizhetik a kérelmező személyazonosságát, mint a szabványos személyazonosító okmány kiállításakor.

K5.11 A kérelmező távoli azonosítása a jelenlegi jogviszonyban:

3. szint: Azon svéd eID-kibocsátók, akik gazdasági vagy jogi szempontból jelentős ügyleteket érintő jogviszonyban már azonosították a kérelmezőt, és amennyiben a kérelmező távolról is azonosítható a svéd eID minőségi védjegy 3. szintű követelményeivel egyenértékű egyéb megbízható eszközökkel, használhatják ezt a módszert a kérelmező személyazonosságának megállapítására.

4. szint: Nem alkalmazható.

K5.12 Azonosítás svéd elektronikus személyazonosítóval:

A svéd elektronikus személyazonosítók kibocsátója távolról is azonosíthatja a kérelmezőt egy legalább a kiállítandóval azonos biztonsági szintű, meglévő érvényes svéd elektronikus személyazonosítóval, ha szerződéses akadályok nélkül ezt az azonosítást használhatja az új elektronikus személyazonosító kiállításának alapjául.

4. szint: Az újonnan kibocsátott elektronikus személyazonosító érvényességi ideje nem haladhatja meg a meglévő elektronikus személyazonosító érvényességi idejét.

K5.13 A kérelmező távoli azonosítása:

2. szint: A svéd elektronikus személyazonosítók kibocsátói a kérelmező személyazonosságának távoli megállapításához felhasználhatják az érvényes szabványos személyazonosító okmányról készült megbízható képfelvételeket és a kérelmező arcképmását, amennyiben az összehasonlítás nem vet fel kétségeket a kérelmező valódi személyazonosságát illetően.

3. szint: A svéd elektronikus személyazonosítók kibocsátói az elektronikusan tárolt biometrikus adatokat tartalmazó érvényes szabványos személyazonosító okmány biztonságos leolvasásával ezen adatok alapján távolról is megállapíthatják a kérelmező személyazonosságát, ha az azonosítandó személy megfelelő biometrikus adatai kellően biztonságos módon összegyűjthetők ahhoz, hogy az összehasonlítás ugyanolyan megbízhatósággal elvégezhető legyen, mint a személyes látogatás esetében, és ha az összehasonlítás nem vet fel kétségeket a kérelmező valódi személyazonosságát illetően.

4. szint: Nem alkalmazható.

Nyilvántartás

K5.14 A svéd elektronikus személyazonosítók kibocsátói a személyes adatok védelmére vonatkozó alkalmazandó szabályok figyelembevételével nyilvántartást vezetnek a csatlakoztatott felhasználókról és a kiosztott elektronikus személyazonosító okmányokról, és ezt a nyilvántartást naprakészen tartják.

6. Az elektronikus személyazonosító kibocsátása és letiltása

A technikai eszközök kialakítása

K6.1 Technikai eszközök:

2. és 3. szint: A svéd eID minőségi jelöléssel ellátott elektronikus azonosítás technikai eszközeit kéttényezős elv alapján kell megtervezni, amelynek értelmében az egyik rész a felhasználó által birtokolandó, elektronikusan tárolt információkból áll, a másik rész pedig abból, amit a felhasználónak az eID aktiválásához használnia kell.

4. szint: A svéd eID minőségi jelöléssel ellátott elektronikus azonosítás technikai eszközeit kéttényezős elv szerint kell megtervezni, amelynek értelmében az egyik rész egy személyes biztonsági modulból áll, amellyel a felhasználónak rendelkeznie kell, a másik rész pedig abból, amit a felhasználónak a biztonsági modul aktiválásához használnia kell.

K6.2 Az aktiválási mechanizmust és a személyre szabott kódot úgy kell megtervezni, hogy harmadik felek számára még mechanikai eszközökkel is valószínűtlen legyen a védelem megsértése.

3. és 4. szint: A védelemnek olyan mechanizmusokat kell magában foglalnia, amelyek megakadályozzák az elektronikus azonosító okmány másolását és manipulálását.

K6.3 A svéd eID minőségi védjeggyel ellátott elektronikus személyazonosító felhasználói számára lehetővé kell tenni, hogy saját kezdeményezésükre, az eID érvényességi ideje alatt díjmentesen és jelentős kényelmetlenség nélkül cseréljenek vagy kérjenek új személyes kódot, és iránymutatás formájában vagy automatikus legenerálás útján segítséget kapjanak a K6.2. pont követelményeinek fenntartásához.

Ha az elektronikus személyazonosítót úgy alakították ki, hogy a személyre szabott kód nem cserélhető, a felhasználó számára ehelyett lehetővé kell tenni, hogy azonos feltételek mellett haladéktalanul egy új, személyre szabott kóddal ellátott elektronikus személyazonosítót szerezzen be, amely egy letiltási eljárás révén felváltja az előzőt.

K6.4 A svéd elektronikus személyazonosítók kibocsátói biztosítják, hogy a birtokosok elektronikus azonosítása céljából nyilvántartásba vett adatok egyedileg képviseljék a kérelmezőt, és azokat az elektronikus személyazonosító okmány kiállításakor hozzárendeljék a szóban forgó személyhez.

K6.5 A kibocsátott elektronikus személyazonosítók érvényességi idejét korlátozni kell, figyelembe véve az elektronikus személyazonosító okmány biztonsági jellemzőit és a visszaélés kockázatát. Az elektronikus azonosító maximális érvényességi ideje öt év.

Elektronikus személyazonosító okmány rendelkezésre bocsátása

K6.6 Távoli rendelkezésre bocsátás:

2. szint: A svéd eID-kibocsátónak oly módon kell biztosítania az e-személyazonosító okmányt, hogy az igazolja a hatósági nyilvántartásban szereplő elérhetőségeket, illetve az elektronikus eljárással kapcsolatban rögzített adatokat a K5.13 2. szint szerint.

3. szint: Az a svéd eID-kibocsátó, amely a K5.11 3. szintnek, a K5.12 3. szintnek vagy a K5.13 3. szintnek megfelelő elektronikus eljárással bocsát ki elektronikus személyazonosítót, új kibocsátás esetén külön, biztonsági szempontból a rendelkezésre bocsátástól függetlenül biztosítja, hogy a felhasználót tájékoztassák arról, hogy az elektronikus személyazonosító dokumentumot átadták, vagy más intézkedésekkel azonos szintű ellenőrzést biztosít arra vonatkozóan, hogy a személyt a rendelkezésre bocsátáskor figyelmeztetik a személyazonosság-lopás kockázatára.

4. szint: Az a svéd eID-kibocsátó, amely a K5.12. szakasz 4. szintjének megfelelő elektronikus eljáráson keresztül bocsát ki elektronikus személyazonosítót, új kibocsátás esetén biztonsági szempontból a rendelkezésre bocsátástól függetlenül biztosítja, hogy a felhasználót tájékoztassák az ilyen eID-okmány átadásáról.

K6.7 A személyes látogatás során történő rendelkezésre bocsátás:

A svéd eID-kibocsátó a személyes látogatás során és a K5.10. pont szerinti személyazonosság-ellenőrzést követően aláírással ellátott átvételi elismervény ellenében rendelkezésre bocsátja az elektronikus személyazonosító okmányt, továbbá külön, a hivatalos nyilvántartásban szereplő elérhetőségek vagy más, ezzel egyenértékű hitelességgel rendelkező információk alapján, biztonsági szempontból a rendelkezésre bocsátástól függetlenül átadja azt a részt, amelyet a felhasználónak az eID aktiválásához használnia kell.

Letiltási szolgáltatás

K6.8 A svéd elektronikus személyazonosítók kibocsátóinak gondoskodniuk kell egy olyan, a felhasználó számára könnyen elérhető letiltási szolgáltatásról, amellyel az elektronikus személyazonosítóját letilthatja.

K6.9 A svéd elektronikus azonosítók kibocsátói haladéktalanul és biztonságosan feldolgozzák és végrehajtják a letiltási kérelmeket, és intézkedéseket hoznak a letiltási szolgáltatással való rendszeres visszaélés vagy más olyan szándékos cselekmények megakadályozására, amelyek az elektronikus azonosító okmányok széles körű letiltásához vezetnek, így biztosítva, hogy a felhasználók elektronikus azonosítói szükség esetén rendelkezésre álljanak

7. A birtokosok elektronikus személyazonosságának ellenőrzése

K7.1 A svéd elektronikus személyazonosítók kibocsátóinak gondoskodniuk kell arról, hogy a birtokos személyazonosságának ellenőrzésekor megbízható ellenőrzésekre kerítsenek sort az elektronikus személyazonosító okmány hitelességével és érvényességével kapcsolatban.

K7.2 A svéd elektronikus személyazonosítók kibocsátóinak gondoskodniuk kell arról, hogy a birtokosok elektronikus személyazonosságának ellenőrzése során technikai biztonsági ellenőrzéseket is elvégezzenek, hogy ily módon valószínűtlen legyen, hogy harmadik felek találgatás, lehallgatás, visszajátszás vagy a folyamat manipulálása révén megsérthessék a védelmi mechanizmusokat.

8. Személyazonosító igazolványok kiállítása

A svéd e-személyazonosítók azon kibocsátóinak, akik az e-szolgáltatások számára nyújtanak személyazonosító igazolványok kiállítására irányuló szolgáltatást, szintén meg kell felelniük e szakasz rendelkezéseinek.

K8.1 A svéd elektronikus személyazonosítók kibocsátóinak gondoskodniuk kell arról, hogy a személyazonosító igazolványok kiállítására irányuló szolgáltatás könnyen elérhető legyen, és hogy a személyazonosító igazolványok kiállítását a 7. szakasz rendelkezéseivel összhangban megbízható azonosítás előzze meg.

4. szint: Az igazolványoknak hivatkozniuk kell a kibocsátó által ellenőrzött kriptográfiai kulcsanyagra, amely a birtokos kizárólagos tulajdonát képezi.

K8.2 A benyújtott személyazonosító igazolványok csak addig érvényesek, amíg az ahhoz szükséges, hogy a felhasználó a kért e-szolgáltatáshoz hozzáférhessen, és védetteknek kell lenniük annak érdekében, hogy az információkat csak a tervezett címzett tudja elolvasni, és hogy az igazolványok címzettjei a tanúsítványok hitelességét ellenőrizhessék.

K8.3 A svéd elektronikus személyazonosítók kibocsátói – figyelembe véve a tanúsítási szolgáltatással való visszaélés kockázatát – korlátozzák azt az időtartamot, amelyen belül egy adott birtokos számára több egymást követő személyazonosító igazolvány is kiállítható, még azelőtt, hogy a birtokosát a 7. szakasz rendelkezéseivel összhangban újra azonosítanák.