A BIZOTTSÁG (EU) 2015/1502 VÉGREHAJTÁSI RENDELETE

(2015. szeptember 8.)

az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó minimális technikai specifikációknak és eljárásoknak a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 8. cikkének (3) bekezdése szerint történő megállapításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletre [1] és különösen annak 8. cikke (3) bekezdésére,

mivel:

(1) A 910/2014/EU rendelet 8. cikke előírja, hogy a 9. cikk (1) bekezdése szerint bejelentett elektronikus azonosítási rendszereknek meg kell határozniuk a keretükben kibocsátott elektronikus azonosító eszközök „alacsony”, „jelentős” és „magas” biztonsági szintjeit.

(2) A minimális technikai specifikációk, szabványok és eljárások meghatározása elengedhetetlen ahhoz, hogy egységesen legyenek értelmezve a biztonsági szintek részletei, valamint a bejelentett elektronikus azonosítási rendszerek nemzeti biztonsági szintjeinek a 8. cikk szerinti biztonsági szinteknek való megfeleltetésekor biztosítva legyen az átjárhatóság, ahogy azt a 910/2014/EU rendelet 12. cikke (4) bekezdésének b) pontja előírja.

(3) Az ebben a végrehajtási aktusban megállapított specifikációkhoz és eljárásokhoz – az elektronikus azonosító eszközök biztonsági szintjeinek területén rendelkezésre álló legfontosabb nemzetközi szabványként – az ISO/IEC 29115 nemzetközi szabványt vettük figyelembe. A 910/2014/EU rendelet tartalma azonban eltér ettől a nemzetközi szabványtól, különösen a személyazonosítási és személyazonosság-ellenőrzési követelmények, valamint a tagállamok személyazonosságra vonatkozó előírásai és az ugyanilyen célú meglévő uniós eszközök közötti eltérések figyelembevétele tekintetében. Tehát a melléklet, bár ezen a nemzetközi szabványon alapul, nem hivatkozhat az ISO/IEC 29115 szabvány semmilyen konkrét elemére.

(4) E rendelet a célra legmegfelelőbbnek bizonyuló, eredményalapú megközelítés alapján került kidolgozásra, ami a kifejezések és fogalmak meghatározásában is tükröződik. A fogalommeghatározások figyelembe veszik a 910/2014/EU rendeletnek az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó célkitűzését. Ezért az e végrehajtási aktusban megállapított specifikációk és eljárások kialakításakor a legmesszebbmenőkig figyelembe kell venni a nagyszabású STORK kísérleti projektet, és ezen belül a projekt keretében kidolgozott előírásokat, valamint az ISO/IEC 29115 definícióit és fogalmait.

(5) Attól függően, hogy milyen kontextusban szükséges a személyazonosság bizonyítékának egy aspektusát ellenőrizni, a hiteles források többfélék lehetnek, így többek között nyilvántartások, dokumentumok, szervek. A hiteles források még hasonló kontextus esetén is eltérőek lehetnek az egyes tagállamokban.

(6) A személyazonosítási és személyazonosság-ellenőrzési követelményeknek figyelembe kell venniük a különféle rendszereket és gyakorlatokat, eközben azonban kellően biztonságosnak kell lenniük ahhoz, hogy megteremtsék a szükséges bizalmat. Az elektronikus azonosító eszközök kibocsátásától eltérő célra korábban alkalmazott eljárások elfogadását tehát függővé kell tenni annak igazolásától, hogy az eljárások megfelelnek az adott biztonsági szintre előírt követelményeknek.

[1] HL L 257., 2014.8.28., 73. o.

(7) Általában alkalmazásra kerülnek bizonyos hitelesítési tényezők, így például megosztott titkok, fizikai eszközök és fizikai attribútumok. Ösztönözni kell azonban a nagyobb számú hitelesítési tényező – különösen különféle kategóriákba tartozó tényezők – alkalmazását a hitelesítési folyamat biztonságának növelése céljából.

(8) E rendelet nem érintheti a jogi személyek képviseleti jogát. A mellékletnek azonban követelményeket kell megfogalmaznia a természetes és jogi személyek elektronikus azonosító eszközeinek összekapcsolására vonatkozólag.

(9) Fel kell ismerni az információbiztonsági és szolgáltatásirányítási rendszerek, valamint az elismert módszerek használatának és a szabványokba – így például az ISO/IEC 27000 és az ISO/IEC 20000 sorozatba – beépített elvek alkalmazásának fontosságát.

(10) A biztonsági szintekkel kapcsolatos helyes tagállami gyakorlatokat is figyelembe kell venni.

(11) A nemzetközi szabványokon alapuló informatikai biztonsági tanúsítás fontos eszköz annak ellenőrzésére, hogy a termékek biztonsági szempontból megfelelnek-e e végrehajtási aktus követelményeinek.

(12) A 910/2014/EU rendelet 48. cikkében említett bizottság az elnöke által kitűzött határidőn belül nem nyilvánított véleményt,

ELFOGADTA EZT A RENDELETET:

1. cikk

(1) A valamely bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszközökre vonatkozó „alacsony”, „jelentős” és „magas” biztonsági szinteket a mellékletben megállapított specifikációkra és eljárásokra való hivatkozással kell meghatározni.

(2) A valamely bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszközök biztonsági szintjének meghatározásához a mellékletben megállapított specifikációkat és eljárásokat kell alkalmazni, az alábbi elemek megbízhatóságának és minőségének meghatározása útján:

a) nyilvántartásba vétel, ahogy az a 910/2014/EU rendelet 8. cikke (3) bekezdésének a) pontja értelmében e rendelet mellékletének 2.1. pontjában szerepel;

b) az elektronikus azonosító eszközök irányítása, ahogy az a 910/2014/EU rendelet 8. cikke (3) bekezdésének b) és f) pontja értelmében e rendelet mellékletének 2.2. pontjában szerepel;

c) hitelesítés, ahogy az a 910/2014/EU rendelet 8. cikke (3) bekezdésének c) pontja értelmében e rendelet mellékletének 2.3. pontjában szerepel;

d) irányítás és szervezés, ahogy az a 910/2014/EU rendelet 8. cikke (3) bekezdésének d) és e) pontja értelmében e rendelet mellékletének 2.4. pontjában szerepel.

(3) Amennyiben a valamely bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszköz megfelel egy magasabb biztonsági szintnél felsorolt követelménynek, azt kell feltételezni, hogy egy alacsonyabb biztonsági szint ezzel egyenértékű követelményének is megfelel.

(4) Hacsak a melléklet vonatkozó részében másképp nem szerepel, a valamely bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszköznek az adott biztonsági szintre vonatkozóan a mellékletben felsorolt összes elemet teljesítenie kell ahhoz, hogy megfeleljen az igényelt biztonsági szintnek.

2. cikk

Ez a rendelet az *Európai Unió Hivatalos Lapjá*ban való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2015. szeptember 8-án.

a Bizottság részéről
az elnök
Jean-Claude JUNCKER

MELLÉKLET

Technikai specifikációk és eljárások a bejelentett elektronikus azonosítási rendszerek keretében kibocsátott elektronikus azonosító eszközök „alacsony”, „jelentős” és „magas” biztonsági szintjeihez

1. **Alkalmazandó fogalommeghatározások**

E melléklet alkalmazásában:

1. „hiteles forrás”: formájától függetlenül bármely megbízható forrás, amely a személyazonosság igazolásához felhasználható pontos adatokat, információkat és/vagy bizonyítékokat szolgáltat;

2. „hitelesítési tényező”: olyan tényező, amely bizonyítottan egy személyhez kapcsolódik, és amely az alábbi kategóriák valamelyikébe tartozik:

   a) „birtoklásalapú hitelesítési tényező”: olyan hitelesítési tényező, amelynél az alanynak igazolnia kell, hogy a birtokában van;

   b) „ismeretalapú hitelesítési tényező”: olyan hitelesítési tényező, amelynél az alanynak igazolnia kell, hogy ismeri;

   c) „inherens hitelesítési tényező”: olyan hitelesítési tényező, amelynek alapja egy természetes személy valamely fizikai attribútuma, és amelynél az alanynak igazolnia kell, hogy rendelkezik az adott fizikai attribútummal;

3. „dinamikus hitelesítés”: olyan elektronikus folyamat, amely kriptográfia vagy egyéb technikák alkalmazásával kérésre elektronikus igazolást készít arról, hogy az azonosító adatok az alany ellenőrzése alatt állnak vagy birtokában vannak, és amely az alany és az alany személyazonosságát igazoló rendszer közötti minden egyes hitelesítéskor változik;

4. „információbiztonsági irányítórendszer”: olyan folyamatok és eljárások összessége, amelyek kialakításának célja, hogy az információbiztonsági kockázatokat elfogadható szinten tartsa;

2. **Technikai specifikációk és eljárások**

Az e mellékletben megállapított technikai specifikációk és eljárások elemeit kell használni annak meghatározására, hogy hogyan kell alkalmazni a 910/2014/EU rendelet 8. cikkének követelményeit és kritériumait a bejelentett elektronikus azonosítási rendszer keretében kibocsátott elektronikus azonosító eszközökre.

2.1. *Nyilvántartásba vétel*

2.1.1. Igénylés és regisztráció

Biztonsági szint	Szükséges elemek
Alacsony	1. Annak biztosítása, hogy az igénylő ismeri az elektronikus azonosító eszköz használatával kapcsolatos feltételeket. 2. Annak biztosítása, hogy az igénylő ismeri az elektronikus azonosító eszköz használatával kapcsolatban ajánlott biztonsági óvintézkedéseket. 3. A személyazonosításhoz és a személyazonosság-ellenőrzéshez szükséges vonatkozó személyazonossági adatok összegyűjtése.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.1.2. Személyazonosítás és személyazonosság-ellenőrzés (természetes személy esetén)

Biztonsági szint	Szükséges elemek
Alacsony	1. Feltételezhető, hogy a személy birtokában van egy azon tagállam által elismert bizonyítéknak, ahol az elektronikus azonosító eszköz igénylése történik, és e bizonyíték igazolja az állítólagos személyazonosságot. 2. Feltételezhető, hogy a bizonyíték valódi, vagy hogy egy hiteles forrás szerint létezik, és a bizonyíték megalapozottnak tűnik. 3. Hiteles forrás számára ismert, hogy az állítólagos személyazonosság létezik, és feltételezhető, hogy a személyazonosságot magáénak tulajdonító személy valóban az a személy.
Jelentős	Az alacsony szint, továbbá teljesíteni kell az 1–4. pontban felsorolt alternatívák egyikét: 1. Beigazolódott, hogy a személy birtokában van egy azon tagállam által elismert bizonyítéknak, ahol az elektronikus azonosító eszköz igénylése történik, és e bizonyíték igazolja az állítólagos személyazonosságot és ellenőrzésre kerül, hogy a bizonyíték valódi-e; vagy egy hiteles forrás szerint létezik-e és egy valós személyhez kapcsolható-e és lépéseket tettek annak a kockázatnak a minimalizálására, hogy a személy azonossága esetleg nem egyezik meg az állítólagos személyazonossággal, figyelembe véve például az elveszett, ellopott, felfüggesztett, visszavont vagy lejárt érvényességű bizonyítékok kockázatát; vagy 2. A regisztrációs eljárás során bemutatásra kerül egy személyazonossági okirat abban a tagállamban, ahol az okiratot kiadták, és úgy tűnik, hogy az okirat az azt bemutató személyhez tartozik és lépéseket tettek annak a kockázatnak a minimalizálására, hogy a személy azonossága esetleg nem egyezik meg az állítólagos személyazonossággal, figyelembe véve például az elveszett, ellopott, felfüggesztett, visszavont vagy lejárt érvényességű okiratok kockázatát; vagy 3. Amennyiben egy közigazgatási vagy magánszervezet által ugyanabban a tagállamban korábban elektronikus azonosító eszközök kibocsátásától eltérő célra használt eljárások egyenértékű biztonságot nyújtanak, mint a 2.1.2. pontban a jelentős biztonsági szintnél megállapítottak, akkor a regisztrációért felelős szervezetnek nem kell megismételnie azokat a korábbi eljárásokat, feltéve, hogy az egyenértékű biztonságot egy, a 765/2008/EK európai parlamenti és tanácsi rendelet [1] 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezet, vagy azzal egyenértékű szervezet megerősíti; vagy 4. Amennyiben jelentős vagy magas biztonsági szintű, érvényes bejelentett elektronikus azonosító eszköz alapján és a személyazonosító adatok esetleges megváltozásában rejlő kockázatokat figyelembe véve bocsátottak ki elektronikus azonosító eszközt, akkor nem szükséges megismételni a személyazonosítási és személyazonosság-ellenőrzési folyamatokat. Amennyiben az alapként szolgáló elektronikus azonosító eszközt nem jelentették be, akkor a jelentős vagy magas biztonsági szintet egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezetnek, vagy azzal egyenértékű szervezetnek meg kell erősítenie.

Biztonsági szint	Szükséges elemek
Magas	Vagy az 1., vagy a 2. pont szerinti követelményeket kell teljesíteni: 1. A jelentős szint, továbbá teljesíteni kell az a–c) pontban felsorolt alternatívák egyikét: a) Ha beigazolódott, hogy a személy birtokában van egy azon tagállam által elismert fényképes vagy biometriai azonosító bizonyítéknak, ahol az elektronikus azonosító eszköz igénylése történik, és a bizonyíték igazolja az állítólagos személyazonosságot, akkor a bizonyíték ellenőrzésre kerül, hogy megállapítsák, hogy érvényes-e egy hiteles forrás szerint; és egy hiteles forrással a személy egy vagy több fizikai tulajdonságát összehasonlítva az igénylőt azonosították az állítólagos személyazonossággal; vagy b) Amennyiben egy közigazgatási vagy magánszervezet által ugyanabban a tagállamban korábban elektronikus azonosító eszközök kibocsátásától eltérő célra használt eljárások egyenértékű biztonságot nyújtanak, mint a 2.1.2. pontban a magas biztonsági szintnél megállapítottak, akkor a regisztrációért felelős szervezetnek nem kell megismételnie azokat a korábbi eljárásokat, feltéve, hogy az egyenértékű biztonságot egy, a 765/2008/EK 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezet, vagy azzal egyenértékű szervezet megerősíti; és lépéseket tesznek annak igazolására, hogy a korábbi eljárások eredményei továbbra is érvényesek; vagy c) Amennyiben magas biztonsági szintű, érvényes bejelentett elektronikus azonosító eszköz alapján és a személyazonosító adatok esetleges megváltozásában rejlő kockázatokat figyelembe véve bocsátottak ki elektronikus azonosító eszközt, akkor nem szükséges megismételni a személyazonosítási és személyazonosság-ellenőrzési folyamatokat. Amennyiben az alapként szolgáló elektronikus azonosító eszközt nem jelentették be, akkor a magas biztonsági szintet egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezetnek, vagy azzal egyenértékű szervezetnek meg kell erősítenie és lépéseket tesznek annak igazolására, hogy egy bejelentett elektronikus azonosító eszköz e korábbi kibocsátási eljárásának eredményei továbbra is érvényesek. VAGY 2. Amennyiben az igénylő nem mutat be semmilyen elismert fényképes vagy biometriai azonosító bizonyítékot, akkor pontosan ugyanazokat az eljárásokat kell alkalmazni, mint amelyeket a regisztrációért felelős szervezet szerinti tagállamban nemzeti szinten alkalmaznak ilyen elismert fényképes vagy biometriai azonosító bizonyítékok megszerzéséhez.

([1]) Az Európai Parlament és a Tanács 2008. július 9-i 765/2008/EK rendelete a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről (HL L 218., 2008.8.13., 30. o.).

2.1.3. Személyazonosítás és személyazonosság-ellenőrzés (jogi személy esetén)

Biztonsági szint	Szükséges elemek
Alacsony	1. A jogi személy állítólagos személyazonossága egy azon tagállam által elismert bizonyíték alapján kerül igazolásra, ahol az elektronikus azonosító eszköz igénylése történik.

Biztonsági szint	Szükséges elemek
	2. A bizonyíték érvényesnek tűnik, és feltételezhető, hogy valódi, illetve hogy egy olyan hiteles forrás szerint létezik, amelybe a jogi személy önkéntes alapon kerül felvételre, és a felvételt a jogi személy és a hiteles forrás közötti megállapodás szabályozza. 3. A jogi személynek egy hiteles forrás szerint sem olyan a státusa, amely meggátolná abban, hogy az adott jogi személyként eljárjon.
Jelentős	Az alacsony szint, továbbá teljesíteni kell az 1–3. pontban felsorolt alternatívák egyikét: 1. A jogi személy állítólagos személyazonossága egy azon tagállam által elismert bizonyíték alapján kerül igazolásra, ahol az elektronikus azonosító eszköz igénylése történik, amely bizonyíték magában foglalja a jogi személy nevét, jogi formáját és regisztrációs számát (ha van) és a bizonyíték ellenőrzésre kerül annak megállapítására, hogy valódi-e, vagy hogy létezik-e egy olyan hiteles forrás szerint, amelybe a jogi személynek kötelezően be kell kerülnie ahhoz, hogy ágazatában működhessen és lépéseket tettek azon kockázat minimalizálására, hogy a jogi személy azonossága esetleg nem egyezik meg az állítólagos személyazonossággal, figyelembe véve például az elveszett, ellopott, felfüggesztett, visszavont vagy lejárt érvényességű okiratok kockázatát; vagy 2. Amennyiben egy közigazgatási vagy magánszervezet által ugyanabban a tagállamban korábban elektronikus azonosító eszközök kibocsátásától eltérő célra használt eljárások egyenértékű biztonságot nyújtanak, mint a 2.1.3. pontban a jelentős biztonsági szintnél megállapítottak, akkor a regisztrációért felelős szervezetnek nem kell megismételnie azokat a korábbi eljárásokat, feltéve, hogy az egyenértékű biztonságot egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezet, vagy azzal egyenértékű szervezet megerősíti; vagy 3. Amennyiben jelentős vagy magas biztonsági szintű, érvényes bejelentett elektronikus azonosító eszköz alapján bocsátottak ki elektronikus azonosító eszközt, nem szükséges megismételni a személyazonosítási és személyazonosság-ellenőrzési folyamatokat. Amennyiben az alapként szolgáló elektronikus azonosító eszközt nem jelentették be, akkor a jelentős vagy magas biztonsági szintet egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezetnek, vagy azzal egyenértékű szervezetnek kell megerősítenie.
Magas	A jelentős szint, továbbá teljesíteni kell az 1–3. pontban felsorolt alternatívák egyikét: 1. A jogi személy állítólagos személyazonossága egy azon tagállam által elismert bizonyíték alapján kerül igazolásra, ahol az elektronikus azonosító eszköz igénylése történik, amely bizonyíték magában foglalja a jogi személy nevét, jogi formáját és legalább egy egyedi azonosítót, ami a jogi személyt nemzeti kontextusban azonosítja és ellenőrzésre kerül, hogy a bizonyíték egy hiteles forrás szerint érvényes-e; vagy

Biztonsági szint	Szükséges elemek
	2. Amennyiben egy közigazgatási vagy magánszervezet által ugyanabban a tagállamban korábban elektronikus azonosító eszközök kibocsátásától eltérő célra használt eljárások egyenértékű biztonságot nyújtanak, mint a 2.1.3. pontban a magas biztonsági szintnél megállapítottak, akkor a regisztrációért felelős szervezetnek nem kell megismételnie azokat a korábbi eljárásokat, feltéve, hogy az egyenértékű biztonságot egy, a 765/2008/EK rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezet, vagy azzal egyenértékű szervezet megerősíti és lépéseket tesznek annak igazolására, hogy az említett korábbi eljárás eredményei továbbra is érvényesek; vagy 3. Amennyiben magas biztonsági szintű, érvényes bejelentett elektronikus azonosító eszköz alapján bocsátottak ki elektronikus azonosító eszközt, nem szükséges megismételni a személyazonosítási és személyazonosság-ellenőrzési folyamatokat. Amennyiben az alapként szolgáló elektronikus azonosító eszközt nem jelentették be, akkor a magas biztonsági szintet egy, a 765/2008/EK európai parlamenti és tanácsi rendelet 2. cikkének 13. pontja szerinti megfelelőségértékelő szervezetnek, vagy azzal egyenértékű szervezetnek kell megerősítenie és lépéseket tesznek annak igazolására, hogy egy bejelentett elektronikus azonosító eszköz e korábbi kibocsátási eljárásának eredményei továbbra is érvényesek.

2.1.4. Természetes és jogi személyek elektronikus azonosító eszközeinek egymáshoz rendelése

Egy természetes személy elektronikus azonosító eszközének és egy jogi személy elektronikus azonosító eszközének egymáshoz rendelésére megfelelő esetben az alábbi feltételek vonatkoznak:

1. Meg kell lennie a lehetőségnek az egymáshoz rendelés felfüggesztésére és/vagy visszavonására. Az egymáshoz rendelés életciklusának (pl. aktiválás, felfüggesztés, megújítás, visszavonás) kezelése nemzeti szinten elismert eljárások szerint történik.

2. Az a természetes személy, akinek elektronikus azonosító eszköze hozzá van rendelve a jogi személy elektronikus azonosító eszközéhez, nemzeti szinten elismert eljárások alapján más természetes személyre ruházhatja át az egymáshoz rendelés gyakorlását. Az átruházó természetes személy azonban felelősségre vonható marad.

3. Az egymáshoz rendelés az alábbi módon történik:

Biztonsági szint	Szükséges elemek
Alacsony	1. Ellenőrzésre került, hogy a jogi személy nevében eljáró természetes személy személyazonosságának igazolása alacsony vagy afeletti szinten történt. 2. Az egymáshoz rendelés nemzeti szinten elismert eljárások alapján történt. 3. A természetes személynek egy hiteles forrás szerint sem olyan a státusa, amely meggátolná a személyt abban, hogy a jogi személy nevében eljárjon.
Jelentős	Az alacsony szint 3. pontja, továbbá: 1. Ellenőrzésre került, hogy a jogi személy nevében eljáró természetes személy személyazonosságának igazolása jelentős vagy magas szinten történt.

Biztonsági szint	Szükséges elemek
	2. Az egymáshoz rendelés nemzeti szinten elismert eljárások alapján történt, és ennek eredményeként egy hiteles forrás regisztrálta az egymáshoz rendelést. 3. Az egymáshoz rendelés hiteles forrásból származó információk alapján került ellenőrzésre.
Magas	Az alacsony szint 3. pontja és a jelentős szint 2. pontja, továbbá: 1. Ellenőrzésre került, hogy a jogi személy nevében eljáró természetes személy személyazonosságának igazolása magas szinten történt. 2. Az egymáshoz rendelés ellenőrzése egy, a jogi személyhez nemzeti kontextusban tartozó egyedi azonosító alapján, és hiteles forrásból származó, a természetes személyt egyedileg azonosító információk alapján történt.

2.2. *Az elektronikus azonosító eszközök irányítása*

2.2.1. Az elektronikus azonosító eszközök jellemzői és kialakítása

Biztonsági szint	Szükséges elemek
Alacsony	1. Az elektronikus azonosító eszköz legalább egy hitelesítési tényezőt alkalmaz. 2. Az elektronikus azonosító eszköz úgy van kialakítva, hogy a kibocsátó ésszerű lépéseket tesz annak ellenőrzésére, hogy az eszközt kizárólag annak a személynek az ellenőrzése alatt vagy birtokában használják-e, akihez az eszköz tartozik.
Jelentős	1. Az elektronikus azonosító eszköz legalább két, különböző kategóriába tartozó hitelesítési tényezőt alkalmaz. 2. Az elektronikus azonosító eszköz úgy van kialakítva, hogy feltételezhető, hogy csak annak a személynek az ellenőrzése alatt vagy birtokában használják, akihez az eszköz tartozik.
Magas	A jelentős szint, továbbá: 1. Az elektronikus azonosító eszköz védelmet nyújt a másolással és manipulációval, valamint a nagy támadási potenciálú támadókkal szemben. 2. Az elektronikus azonosító eszköz úgy van kialakítva, hogy az a személy, akihez az eszköz tartozik, bizonyosan meg tudja védeni az eszközt attól, hogy mások használják.

2.2.2. Kibocsátás, átadás és aktiválás

Biztonsági szint	Szükséges elemek
Alacsony	A kibocsátást követően az elektronikus azonosító eszköz átadása egy olyan mechanizmus révén történik, amellyel feltételezhetően csak a célszemélyt érik el.
Jelentős	A kibocsátást követően az elektronikus azonosító eszköz átadása egy olyan mechanizmus révén történik, amellyel az átadás feltételezhetően csak annak a személynek a birtokába történik, akihez az eszköz tartozik.
Magas	Az aktiválási folyamat ellenőrzi, hogy az elektronikus azonosító eszköz átadása csak annak a személynek a birtokába történt, akihez az tartozik.

2.2.3. Felfüggesztés, visszavonás és újraaktiválás

Biztonsági szint	Szükséges elemek
Alacsony	1. Az elektronikus azonosító eszközt rövid időn belül és hatékony módon fel lehet függeszteni és/vagy vissza lehet vonni. 2. Meghozták az illetéktelen felfüggesztés, visszavonás és/vagy újraaktiválás megakadályozásához szükséges intézkedéseket. 3. Újraaktiválásra csak akkor kerülhet sor, ha a felfüggesztés vagy visszavonás előtt érvényes biztonsági követelmények továbbra is teljesülnek.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.2.4. Megújítás és csere

Biztonsági szint	Szükséges elemek
Alacsony	A személyazonosító adatok esetleges megváltozásában rejlő kockázatokat figyelembe véve a megújításnak vagy cserének ugyanazoknak a biztonsági követelményeknek kell megfelelnie, mint a kiindulási személyazonosításnak és személyazonosság-ellenőrzésnek, vagy egy azonos vagy magasabb biztonsági szintű, érvényes elektronikus azonosító eszközön kell alapulnia.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Az alacsony szint, továbbá: Ha a megújítás vagy csere érvényes elektronikus azonosító eszköz alapján történik, a személyazonossági adatokat egy hiteles forrásban ellenőrizni kell.

2.3. *Hitelesítés*

E pontban a hitelesítési mechanizmus alkalmazásához kapcsolódó veszélyekre összpontosítunk, és felsoroljuk az egyes biztonsági szintek követelményeit. E pont alkalmazásában úgy kell értelmezni, hogy az ellenőrzéseknek arányban kell állniuk az adott szinthez tartozó kockázatokkal.

2.3.1. Hitelesítési mechanizmus

Az alábbi táblázatban biztonsági szintenként adjuk meg az azon hitelesítési mechanizmusra vonatkozó követelményeket, amelynek keretében a természetes vagy jogi személy az elektronikus azonosító eszközzel személyazonosságát igazolja az igénybe vevő fél számára.

Biztonsági szint	Szükséges elemek
Alacsony	1. A személyazonossági adatok kiadása előtt megbízható módon ellenőrzésre kerül az elektronikus azonosító eszköz és annak érvényessége. 2. Amennyiben a személyazonossági adatokat a hitelesítési mechanizmus részeként tárolják, ott biztosítva van, hogy ez az információ ne vesszen el és ne legyen veszélyeztetve, ideértve az offline analízist. 3. A hitelesítési mechanizmus biztonsági ellenőrzéseket végez az elektronikus azonosító eszközök ellenőrzéséhez azért, hogy ily módon minimálisra csökkentse annak valószínűségét, hogy olyan módszerekkel, mint a találgatás, a lehallgatás, vagy a kommunikáció visszajátszása, illetve manipulálása egy közepes-alapszintű támadási potenciállal rendelkező támadó meghiúsítja a hitelesítési mechanizmust.

Biztonsági szint	Szükséges elemek
Jelentős	Az alacsony szint, továbbá: 1. A személyazonossági adatok kiadása előtt megbízható módon, dinamikus hitelesítés révén ellenőrzésre kerül az elektronikus azonosító eszköz és annak érvényessége. 2. A hitelesítési mechanizmus biztonsági ellenőrzéseket végez az elektronikus azonosító eszközök ellenőrzéséhez azért, hogy ily módon minimálisra csökkentse annak valószínűségét, hogy olyan módszerekkel, mint a találgatás, a lehallgatás, vagy a kommunikáció visszajátszása, illetve manipulálása egy mérsékelt támadási potenciálú támadó meghiúsítja a hitelesítési mechanizmust.
Magas	A jelentős szint, valamint: A hitelesítési mechanizmus biztonsági ellenőrzéseket végez az elektronikus azonosító eszközök ellenőrzéséhez azért, hogy ily módon minimálisra csökkentse annak valószínűségét, hogy olyan módszerekkel, mint a találgatás, a lehallgatás, vagy a kommunikáció visszajátszása, illetve manipulálása egy magas támadási potenciálú támadó meghiúsítja a hitelesítési mechanizmust.

2.4. *Irányítás és szervezés*

A határokon átnyúló elektronikus azonosításhoz kapcsolódó szolgáltatásokat nyújtó összes résztvevőnek („szolgáltató") dokumentált információbiztonság-irányítási gyakorlatokat, politikákat, kockázatkezelési módszereket és egyéb elismert ellenőrzéseket kell alkalmaznia, hogy biztosítékkal szolgáljanak az adott tagállamban az elektronikus azonosítási rendszerekért felelős megfelelő irányító szervek számára arról, hogy hatékony gyakorlatokat alkalmaznak. A 2.4. pontban úgy kell értelmezni, hogy az összes követelménynek/elemnek arányban kell állnia az adott szinthez tartozó kockázatokkal.

2.4.1. Általános rendelkezések

Biztonsági szint	Szükséges elemek
Alacsony	1. Az e rendelet hatálya alá tartozó bármilyen operatív szolgáltatást nyújtó szolgáltatók közigazgatási hatóságok vagy valamely tagállam nemzeti törvényei által ilyenként elismert jogi személyek, amelyek kialakított szervezettel rendelkeznek, és a szolgáltatások nyújtása szempontjából releváns valamennyi részük teljes mértékben működőképes. 2. A szolgáltatók a szolgáltatás működtetésével és nyújtásával kapcsolatban rájuk vonatkozó összes törvényi követelménynek megfelelnek, ideértve a kért információk típusára, a személyazonosság igazolásának módjára, valamint arra vonatkozó követelményeket, hogy milyen információk őrizhetők meg és mennyi ideig. 3. A szolgáltatók bizonyítani tudják, hogy képesek vállalni a károkozási felelősség kockázatát, továbbá elegendő anyagi eszközzel rendelkeznek a folyamatos működéshez és a szolgáltatások nyújtásához. 4. A szolgáltatók felelősséggel tartoznak a más szervezethez kiszervezett valamennyi kötelezettség teljesítéséért, valamint a rendszer előírásainak oly módon történő betartásáért, mintha maguk végezték volna el a feladatokat. 5. A nem a nemzeti törvények alapján létrehozott elektronikus azonosítási rendszerek esetében hatékony lezárási terv szükséges. Ennek a tervnek tartalmaznia kell a szolgáltatás rendezett befejezését vagy más szolgáltató általi folytatását, az illetékes hatóságok és a végfelhasználók tájékoztatásának módját, valamint azt, hogy a rendszer előírásaival összhangban hogyan kell az eltárolt adatokat megvédeni, megőrizni vagy megsemmisíteni.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.4.2. Értesítések közzététele és felhasználói tájékoztatás

Biztonsági szint	Szükséges elemek
Alacsony	1. A szolgáltatás meghatározásának közzététele, amelyben szerepel az összes alkalmazandó feltétel és díj, a használatra vonatkozó összes korlátozást is ideértve. A szolgáltatás meghatározásának tartalmaznia kell az adatvédelmi szabályokat is. 2. Megfelelő szabályokat és eljárásokat kell bevezetni annak érdekében, hogy a szolgáltatás felhasználói kellő időben és megbízható módon értesüljenek magának a szolgáltatásnak a meghatározását vagy az alkalmazandó feltételeket és az adott szolgáltatásra vonatkozó adatvédelmi szabályokat érintő bármely változásról. 3. Megfelelő szabályokat és eljárásokat kell bevezetni, amelyek alapján teljes körű és pontos válaszok adhatók a tájékoztatáskérésekre.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.4.3. Információbiztonsági irányítás

Biztonsági szint	Szükséges elemek
Alacsony	Az információbiztonsági kockázatok kezelésére és ellenőrzésére hatékony információbiztonsági irányítórendszer áll rendelkezésre.
Jelentős	Az alacsony szint, továbbá: Az információbiztonsági irányítórendszer az információbiztonsági kockázatok kezelése és ellenőrzése során bevált normákhoz vagy elvekhez igazodik.
Magas	Ugyanaz, mint a jelentős szintnél.

2.4.4. Nyilvántartás

Biztonsági szint	Szükséges elemek
Alacsony	1. A vonatkozó információk rögzítése és tárolása hatékony nyilvántartás-kezelő rendszer alkalmazásával, az adatvédelemmel és az adatmegőrzéssel kapcsolatos alkalmazandó jogszabályokat és helyes gyakorlatot is figyelembe véve. 2. Az eltárolt adatok megőrzése, ameddig a nemzeti törvények vagy más nemzeti adminisztratív rendelkezések megengedik, és védelme, ameddig azok a biztonság megsértéseinek auditálása vagy vizsgálata, továbbá megőrzés céljára szükségesek, amelyet követően az eltárolt adatokat biztonságosan meg kell semmisíteni.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.4.5. Létesítmények és személyzet

Az alábbi táblázat az esetleges olyan alvállalkozók létesítményeire és személyzetére vonatkozó követelményeket ismerteti, akik e rendelet hatálya alá tartozó feladatokat végeznek. Az egyes követelmények betartásának arányosnak kell lennie a nyújtott biztonsági szinthez kapcsolódó kockázatok szintjével.

Biztonsági szint	Szükséges elemek
Alacsony	1. Olyan eljárások megléte, amelyek biztosítják, hogy a személyzet és az alvállalkozók az általuk elvégzendő feladatokhoz szükséges képességek tekintetében kellő képzettséggel, szakképzettséggel és tapasztalattal rendelkeznek. 2. Elegendő személyzet és alvállalkozó megléte a szolgáltatásnak a saját előírásai és eljárásai szerinti működtetéséhez és erőforrásokkal való ellátásához. 3. A szolgáltatás nyújtásához használt létesítményeket folyamatosan felügyelik és védik a környezeti események, illetéktelen hozzáférés és más tényezők okozta károk ellen, amelyek befolyással lehetnek a szolgáltatás biztonságára. 4. A szolgáltatás nyújtásához használt létesítmények biztosítják, hogy kizárólag a személyzet vagy az alvállalkozók juthassanak be a személyes, kriptográfiás vagy egyéb bizalmas információkat tároló vagy feldolgozó területekre.
Jelentős	Ugyanaz, mint az alacsony szintnél.
Magas	Ugyanaz, mint az alacsony szintnél.

2.4.6. Technikai ellenőrzések

Biztonsági szint	Szükséges elemek
Alacsony	1. Arányos technikai ellenőrzések megléte a szolgáltatások biztonságát, valamint a feldolgozott információk bizalmas jellegét, sértetlenségét és rendelkezésre állását veszélyeztető kockázatok kezelésére. 2. A személyes vagy érzékeny információk cseréjéhez használt elektronikus kommunikációs csatornák védve vannak a lehallgatás, manipuláció és visszajátszás ellen. 3. Az érzékeny kriptográfiai anyagokhoz való hozzáférés, amennyiben elektronikus azonosító eszközök kibocsátásához és hitelesítéshez használják, kizárólag a szigorúan hozzáférést igénylő szerepekre és alkalmazásokra korlátozódik. Biztosítani kell, hogy az ilyen anyagokat ne tárolják hosszabb ideig egyszerű szöveg formájában. 4. Vannak olyan eljárások, amelyek biztosítják, hogy az idő előrehaladtával ne csökkenjen a biztonság mértéke, és hogy megfelelő megoldások álljanak rendelkezésre a kockázati szintek változásaira, a biztonsági eseményekre és a biztonság megsértéseire vonatkozóan. 5. A személyes, kriptográfiás vagy egyéb bizalmas információkat tartalmazó összes adathordozót biztonságos módon tárolják, szállítják és ártalmatlanítják.
Jelentős	Ugyanaz, mint az alacsony szintnél, valamint: Bizalmas kriptográfiai anyagok, amennyiben azokat elektronikus azonosító eszközök kibocsátásához és hitelesítéshez használják, a manipuláció ellen védettek.
Magas	Ugyanaz, mint a jelentős szintnél.

2.4.7. Megfelelőség és audit

Biztonsági szint	Szükséges elemek
Alacsony	Olyan rendszeres belső auditok elvégzése, amelyek a szolgáltatás nyújtásával kapcsolatos összes részre kiterjednek és biztosítják a vonatkozó előírások betartását.

Biztonsági szint	Szükséges elemek
Jelentős	Olyan rendszeres független belső vagy külső auditok elvégzése, amelyek a szolgáltatás nyújtásával kapcsolatos összes részre kiterjednek és biztosítják a vonatkozó előírások betartását.
Magas	1. Olyan rendszeres független külső auditok elvégzése, amelyek a szolgáltatás nyújtásával kapcsolatos összes részre kiterjednek és biztosítják a vonatkozó előírások betartását. 2. Amennyiben egy rendszert közvetlenül egy kormányzati szerv irányít, akkor a rendszer auditálása a nemzeti jogszabályokkal összhangban történik.