NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

NISZ-TKASZ
külső félre delegált autentikációra vonatkozó követelmények
(KDA-TKASZ)

Verziószám	1.1
Hatályba lépés dátuma	2020.10.11.
Dokumentum besorolása	nyilvános

Dátum:
2020.10.12
12:05:16 +02'00'

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
0.9	2018.07.25	Kiinduló változat	Polysys Kft.		
0.91b	2018.08.13	Delegált hitelesítési modellek logikai leírása	NISZ Zrt.		
0.93	2020.07.09	NISZ-TKASZ szabályzatok 0.93 verziójával összhangban átdolgozott változat	Polysys Kft.		
0.94	2020.07.28.	NISZ információbiztonsági terült (EIBI) által támasztott követelményekkel való kiegészítés	Németh Ágota		
1.0	2020.07.31	Első induló változat	Németh Ágota	Kővári Ferenc	Adorján István
1.1	2020.09.10	NMHH észrevételei alapján módosítva	Németh Ágota	Kővári Ferenc	Adorján István

Tartalomjegyzék

1 BEVEZETÉS

A NISZ-TKASZ a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban: Szolgáltató) gépi interfészes kapcsolaton elérhető, tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatása.

A 84/2012. (IV. 21.) Korm. rendelet 4. § több olyan, elektronikus dokumentumok hitelesítésére irányuló, a Kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatást (továbbiakban: SZEÜSZ) és központi elektronikus ügyintézési szolgáltatást (továbbiakban: KEÜSZ) határoz meg, melyeknél az elektronikus aláírások és bélyegzők létrehozásához szükséges, a vonatkozó nemzetközi szabvány által meghatározott kriptográfiai művelet (a továbbiakban Kriptográfiai Művelet) elvégzése bizalmi szolgáltatásban tárolt magánkulcsok felhasználásával is történhet:

h) központi dokumentumhitelesítési ügynök (továbbiakban: KDÜ);

k) Kormányzati Elektronikus Aláíró WEB-szolgáltatás (továbbiakban: KEASZ-WS).

A NISZ-TKASZ szolgáltatást (továbbiakban: Szolgáltatás) a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., mint a jogszabályban kijelölt kormányzati hitelesítés-szolgáltató, az előző bekezdésben meghatározott SZEÜSZ/KEÜSZ-ökhöz (továbbiakban együttesen: TK-EÜSZ) kapcsolódóan nyújtja a vele szerződéses viszonyban levő Előfizetők számára.

A Szolgáltatást az E-ügyintézési tv. 1. § 17. pontjában megnevezett, elektronikus ügyintézést biztosító szervek valamint egyéb állami, közfeladatot ellátó szervek vehetik igénybe. A Szolgáltatásban használt, elektronikus aláírás/bélyegző létrehozásához használt adatokat (magánkulcsokat) Szolgáltató az erre a célra szolgáló, elkülönített HSM komponensben (továbbiakban: TKASZ-HSM) tárolja. A Szolgáltatást az Előfizető egy adott informatikai rendszerében (továbbiakban: Szakrendszer), az adott TK-EÜSZ interfész specifikációja (továbbiakban: Interfész Specifikáció) szerint megvalósított gépi interfészen keresztül veheti igénybe. A Szolgáltatás igénybevétele során a Felhasználó (Aláíró vagy Bélyegző Létrehozó) a hozzá rendelt magánkulcsát távolról tudja aktiválni, így a Szakrendszeren keresztül képes az elektronikus aláírás/bélyegző létrehozásához szükséges Kriptográfiai Művelet végrehajtására, a magánkulcshoz kapcsolódó minősített tanúsítvány felhasználásával.

A NISZ-TKASZ szolgáltatás önállóan nem, csak a TK-EÜSZ-höz integrált módon vehető igénybe.

A TK-EÜSZ révén a Felhasználó a minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírások és bélyegzők létrehozása során a NISZ-TKASZ szolgáltatást használja a

Kriptográfiai Művelet elvégzésére, a kiszámított aláírás értéknek (azaz a hitelesítendő dokumentum(ok) lenyomatának a magánkulccsal és a megfelelő kriptográfiai algoritmusokkal történő titkosításával előállított digitális jelsorozatnak) az elektronikus aláírás vagy bélyegző formátumban történő elhelyezésére.

Így a Szolgáltatásban tárolt kulcsaik és a Szakrendszerük felhasználásával a Felhasználók a 137/2016. (VI. 13.) Korm. rendeletben (illetve a 1506/2015/EU rendelet mellékletében) meghatározott, alábbi technikai specifikációknak megfelelő elektronikus bélyegzőket, illetve aláírásokat hozhatnak létre:

- XAdES alapprofil: ETSI TS 103 171 v.2.1.1
- PAdES alapprofil: ETSI TS 103 172 v.2.2.2
- Aláírás-, illetve bélyegzőkonténer alapprofil: ETSI TS 103 174 v.2.2.1

A NISZ-TKASZ szolgáltatáshoz kapcsolódóan az Előfizető igénybe veszi a Kormányzati hitelesítés-szolgáltató minősített elektronikus aláírási/bélyegző tanúsítvány szolgáltatását és minősített időbélyegzés szolgáltatását is.

A Szolgáltatás felhasználásával minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás/bélyegző hozható létre, minősített elektronikus aláírás/bélyegző nem hozható létre.

A NISZ-TKASZ az eIDAS 3. cikk 16. pontja értelmében bizalmi szolgáltatásnak minősül.

Szolgáltató a NISZ-TKASZ szolgáltatást nem minősített bizalmi szolgáltatásként valósítja meg és nyújtja Előfizetők számára.

1.1 Áttekintés

- A NISZ-TKASZ szolgáltatásra vonatkozó követelményeket az alábbi nemzetközi szabványok és jogszabályok határozzák meg:
- **TS 119 431-1**: Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev
- **EN 419 241-1**: Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements
- **ETSI TS 119 312**: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites („AlgoPaper”)

- NIST Special Publication SP-800-63B Digital Identity Guidelines - Authentication and Lifecycle Management
- **910/2014/EU**: Az Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban: eIDAS)
- **2015/1502/EU**: A BIZOTTSÁG (EU) 2015/1502 végrehajtási rendelete (2018. 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
- **2015. évi CCXXII. törvény** az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- **451/2016. (XII. 16.) Korm. rendelet** az elektronikus ügyintézés részletszabályairól
- **84/2012. (IV. 21**.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- **137/2016 (VI. 13.) Korm. rendelet** az elektronikus ügyintézés céljára felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről

A NISZ-TKASZ szolgáltatás keretében az elektronikus aláírás és elektronikus bélyegző létrehozását a Bélyegző Létrehozó (elektronikus bélyegző esetén), illetve az Aláíró (elektronikus aláírás esetén) csak és kizárólag az Alany sikeres azonosítását és jogosultságának ellenőrzését követően végezheti.

Az Alanyok azonosítása az alábbiak szerint történik:

1) Bélyegző Létrehozó esetén: - A NISZ-TKASZ szolgáltatás használatára az Előfizető és a Szolgáltató szolgáltatási szerződést köt egymással (TKASZ Szolgáltatási Szerződés). Ezzel egyidejűleg, a NISZ GovCA az Előfizető számára autentikációs tanúsítványt (Előfizető Autentikációs Tanúsítványa) ad ki. Előfizető (illetve az által működtetett Szakrendszer) a gépi interfészen, a HTTPS kapcsolat felépítéséhez ezen autentikációs tanúsítványt, illetve az ahhoz kapcsolódó magánkulcsot kell, használja. Így az Előfizető azonosítása a HTTPS protokoll által biztosított, kliens autentikáció keretében történik meg.

A Szakrendszer az Interfész Specifikációnak megfelelően összeállított kérésben Előfizető elektronikus bélyegzés célú tanúsítványát kell szerepeltesse.

2) Aláíró esetén: - Első lépésben megtörténik az Aláíró azonosítása, az adott Előfizető szervezetén belül használt Autentikációs Folyamat keretében. Az Aláíró tanúsítványának megszerzése az Azonosítási Szolgáltatásban megvalósított nyilvántartásból (pl. X.500 kompatibilis könyvtárszolgáltatási szoftverből, LDAP protokoll használatával), az Aláíróhoz kapcsolt aláírói tanúsítványának lekérdezésével kell történjen. A Szakrendszer az Interfész Specifikációnak megfelelően összeállított kérésben az így megszerzett aláírói tanúsítványt kell szerepeltesse. Majd második lépésben megtörténik az Előfizető, illetve az általa működtetett Szakrendszer azonosítása az 1) pontban leírt módon.

Az Alanyok jogosultságának ellenőrzése az alábbiak szerint történik:

A) Bélyegző Létrehozó esetén: a HTTPS protokoll által biztosított, kliens autentikációhoz használt tanúsítvány alapján történik meg Előfizető jogosultságának elbírálása.

B) Aláíró esetén: az A) pont szerinti sikeres ellenőrzést követően, ellenőrzésre kerül, hogy az Interfész Specifikációnak megfelelően a kérésben megadott aláírói tanúsítvány alanya adott Előfizetőhöz tartozik-e, valamint az Előfizetőhöz tartozó Aláíró rendelkezik-e megfelelő jogosultsággal a kért elektronikus aláírás létrehozására.

A sikeres azonosítást és jogosultság ellenőrzést követően, az Interfész Specifikációnak megfelelően összeállított kérésben szereplő aláírói tanúsítvány alapján kerül a TKASZ-HSM-ben tárolt magánkulcs kiválasztásra, és annak használatával az Aláíró, illetve Bélyegző Létrehozó által kerül az I Aláírás Érték létrehozásra.

A TS 119 431-1 szabvány lehetőséget nyújt arra, hogy a NISZ-TKASZ szolgáltatásban az Aláírók azonosítását ne a Szolgáltató, hanem külső fél végezze, ügynevezett „delegált autentikáció” keretében.

Jelen dokumentum a külső fél által az Aláírók azonosítására (az Autentikációs Folyamatra) vonatkozó biztonsági követelményeket határozza meg.

1.2 Fogalmak, rövidítések és hivatkozások

1.2.1 Fogalmak

A jelen szabályzatban használt fogalmak értelmezése megegyezik a Szolgáltatásokra vonatkozó szabványokban és jogszabályokban (1.1 fejezet) szereplő meghatározásokkal.

Az ezen felül alkalmazott fogalmak meghatározása az alábbiakban olvasható.

Alany: A tanúsítványban a bizalmi szolgáltató által igazolt azonosságú vagy tulajdonságú természetes személy vagy jogi személy, illetve közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet. Jelen dokumentumban az Alany kifejezés elektronikus aláírás célú tanúsítvány esetén az Aláírót, elektronikus bélyegzés célú tanúsítvány esetén a Bélyegző Létrehozót jelenti. A tanúsítványokat a NISZ GovCA minősített bizalmi szolgáltatása bocsátja ki az Alanyok számára.

Aláírás Érték: A Felhasználó (Aláíró, vagy Bélyegző Létrehozó) által, a TKASZ-HSM modulban tárolt magánkulcsának felhasználásával, távolról aktivált és végrehajtott Kriptográfiai Művelet eredménye, azaz az aláírandó dokumentum(ok) lenyomatának a magánkulccsal történő titkosításával előállított digitális jelsorozat. Jelen dokumentum fogalomrendszerében az Aláírás Érték az elektronikus aláírásban, illetve elektronikus bélyegzőben elhelyezett aláírás értéket (az AdES szabványokban a `SignatureValue`) értelemszerűen, egyaránt jelenti.

Aláíró: Az elektronikus aláírás célú tanúsítvány alanya - a természetes személy - aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hoz létre. Jelen dokumentum fogalomrendszerében az Aláíró az Előfizetővel kapcsolatban álló természetes személyt (képviseleti joggal rendelkező vagy cégjegyzésre jogosult személyt, vagy Előfizető szervezete által foglalkoztatott személyt) jelenti.

Autentikációs Folyamat: az Aláírók azonosítását végző folyamat, amely meg kell feleljen az ezen dokumentumban szereplő biztonsági és műszaki követelményeknek. Az Autentikációs Folyamat sikeressége előfeltétele az Aláíró TKASZ-HSM modulban tárolt magánkulcsa távolról történő aktiválásának, és így az elektronikus aláírás Aláíró által távolról történő létrehozásának

Bélyegző Létrehozó: az elektronikus bélyegzés célú tanúsítvány alanya - a jogi személy, illetve közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet (vagy annak valamely szervezeti egysége) -, amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hoz létre

CHSM: az SCDev (TKASZ-HSM) felhőalapú műszaki megvalósításában elhelyezett olyan, kizárólag csak a Szolgáltatás nyújtásához használt kriptográfiai modul (hardver elem), amely:

- olyan megbízható rendszer, melynek értékelése az MSZ/ISO/IEC 15408 szerint, illetve azzal egyenértékű biztonsági kritériumok szerint - az AVA_VAN.5 garancia összetevővel kiegészítve - 4-es vagy magasabb értékelési garancia szinten történt meg;
- vagy megfelel az ISO/IEC 19790 követelményeinek; vagy

- megfelel a FIPS 140-2 3-a, illetve annál magasabb szintű követelményeknek.

Delegált Autentikáció: az {Sz4} EN 419 241-1 szabvány lehetővé teszi, hogy az Autentikációs Folyamatot külső fél végezze és meghatározza az erre vonatkozó műszaki és biztonsági követelményeket. A Delegált Autentikáció folyamatábráját az {Sz3} TS 119 431-1 szabvány 4.4 fejezete tartalmazza. Szolgáltató a TKASZ Szolgáltatási Szerződés megkötését megelőzően ellenőrzi, hogy a külső fél maradéktalanul teljesíti a számára meghatározott, jelen dokumentumban szereplő valamennyi műszaki és biztonsági követelményt.

Előfizető: a Szolgáltatóval kapcsolatban álló jogi személy, illetve közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet, amely megrendeli a Szolgáltatótól a NISZ-TKASZ szolgáltatást, jellemzően a tárolt magánkulccsal a kriptográfiai műveletek elvégzését – a TK-EÜSZ elektronikus aláírások vagy bélyegzők létrehozása során - az általa megnevezett Felhasználók számára

Előfizető Autentikációs Tanúsítványa: a TK-EÜSZ Csatlakozási Kérelem benyújtását és Szolgáltató általi befogadását követően, a TKASZ Szolgáltatási Szerződés megkötésekor vagy azt megelőzően, Előfizető számára kiadott autentikációs tanúsítvány, amelyet a HTTPS protokoll szerinti kliens PKI autentikációra használ

Interfész Specifikáció: NISZ-TKASZ szolgáltatást kiközvetítő TK-EÜSZ-re vonatkozó műszaki dokumentáció, amely meghatározza, hogy az Előfizető által működtetett Szakrendszer milyen módon kapcsolódhat a TK-EÜSZ, illetve a NISZ-TKASZ szolgáltatáshoz, abból célból, hogy a Felhasználók (Aláírók és Bélyegző Létrehozók) a tárolt magánkulcsukkal távolról elektronikus aláírásokat/bélyegzőket hozzanak létre

Felhasználó: az Előfizető szervezetével kapcsolatban álló (pl. munkaviszonyban) természetes személy (Aláíró), valamint Előfizető szervezete, vagy annak valamely szervezeti egysége, vagy Előfizető, mint jogi személy (Bélyegző Létrehozó), aki/amely a NISZ-TKASZ szolgáltatást a TK-EÜSZ közvetítésével használja

Kriptográfiai Művelet: az elektronikus aláírás/bélyegző létrehozásához szükséges, az RFC 8017 szabvány által meghatározott kriptográfiai műveletek összessége, amely kiszámítja az Aláírás Értéket (a hitelesítendő dokumentum(ok) lenyomatának a Felhasználó TKASZ-HSM-ben tárolt magánkulcsával történő titkosításával előállított digitális jelsorozatot). A Kriptográfiai Műveletet a Felhasználó távolról hajtja végre, azt követően, hogy a Szolgáltatásban tárolt magánkulcsát aktiválta**.**

NETHSM: az SCDev (TKASZ-HSM) nem felhőalapú műszaki megvalósításában, a Szolgáltató saját informatikai rendszereinek belső hálózatában elhelyezett, kizárólag csak a Szolgáltatás nyújtásához használt hálózati kriptográfiai modul (hardver elem), amely:

- olyan megbízható rendszer, melynek értékelése az MSZ/ISO/IEC 15408 szerint, illetve azzal egyenértékű biztonsági kritériumok szerint - az AVA_VAN.5 garancia összetevővel kiegészítve - 4-es vagy magasabb értékelési garancia szinten történt meg;
- vagy megfelel az ISO/IEC 19790 követelményeinek; vagy
- megfelel a FIPS 140-2 3-as, illetve annál magasabb szintű követelményeknek.

NISZ-TKASZ: a bizalmi szolgáltatás keretében tárolt magánkulcsokkal a Kriptográfiai Műveletet elvégző szolgáltatás, melynek eredményét a TK-EÜSZ közvetíti a Felhasználók felé

SCDev: a TS 119 431-1 szabvány 3.1 fejezetében definiált fogalom, azaz olyan konfigurált szoftver és hardver elemek összessége, melynek működési célja a tárolt magánkulcs felhasználásával az Aláírás Érték kiszámítása (a Kriptográfiai Művelet végrehajtásával)

Szakrendszer: Előfizető által működtetett informatikai rendszer, amely az Interfész Specifikáció szerint megvalósított gépi interfészen keresztül, a TK-EÜSZ közvetítésével kapcsolódik a NISZ-TKASZ rendszerhez, és amellyel a Bélyegző Létrehozók, illetve az Aláírók a tárolt magánkulcsukkal végzendő Kriptográfiai Műveletet kezdeményeznek.

TK-EÜSZ: a 84/2012. Korm. rendelet 4. §-ban meghatározott, olyan, elektronikus dokumentumok hitelesítésére irányuló, a Kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatás (SZEÜSZ) vagy központi elektronikus ügyintézési szolgáltatás (KEÜSZ), melyeknél az elektronikus aláírások és bélyegzők létrehozásához szükséges Kriptográfiai Műveletek elvégzése bizalmi szolgáltatásban tárolt magánkulcsok felhasználásával is történhet

TK-EÜSZ Csatlakozási Kérelem: Előfizető által a TK-EÜSZ igénybevételéhez benyújtott csatlakozási kérelem űrlap.

TKASZ-HSM: a Szolgáltatásban működtetett SCDev, melyet a Felhasználók távoli elektronikus aláírás/bélyegző létrehozó eszközként, távolról használnak az Aláírás Érték kiszámítására irányuló Kriptográfiai Művelet elvégzésére. A „TKASZ-HSM” jelölés a CHSM-t és a NETHSM-t együttesen jelenti. Egy Felhasználó valamely magánkulcsa vagy a CHSM-ben, vagy a NETHSM-ben kerül tárolásra. A Szolgáltatásra vonatkozó szabályzatok közösen, „TKASZ-HSM” jelöléssel tárgyalják azokat a követelményeket és előírásokat, melyek a CHSM-re és NETHSM-re azonosan vonatkoznak. Azok a fejezetek, melyek a CHSM-re és NETHSM-re vonatkozó, de eltérő, nem azonos követelményeket vagy előírásokat tárgyalnak, „[CHSM]” és „[NETHSM]” mintával jelölt

külön-külön bekezdéseket tartalmaznak, melyek értelemszerűen vagy csak a CHSM-re, vagy csak a NETHSM-re vonatkoznak

TKASZ Szolgáltatási Szerződés: Előfizető és Szolgáltató között, a NISZ-TKASZ igénybevételére megkötött szolgáltatási szerződés

1.2.2 Rövidítések

AdES	Advanced Electronic Signature / Seal	fokozott biztonságú elektronikus aláírás vagy bélyegző, formátuma lehet PAdES (PDF aláírási formátum) vagy XAdES (XML aláírási formátum)
CHSM	Cloud HSM	felhő HSM
EIAD	az Egységes Infrastruktúra Active Directory szolgáltatása	
eDirectory	X.500-kompatibilis könyvtárszolgáltatási szoftver	
HSM	Hardware Security Module	hardver biztonsági modul, kriptográfiai eszköz
HTTPS	HyperText Transfer Protocol Secure	biztonságos hipertext átviteli protokoll
KDÜ	a 84/2012. Korm. rendelet 4. § h) pontjában meghatározott központi dokumentumhitelesítési ügynök	
KEASZ-WS	a 84/2012. Korm. rendelet 4. § k) pontjában meghatározott a Kormányzati Elektronikus Aláíró WEB-szolgáltatást megvalósító részszolgáltatás	
LSCP	Lightweight SSASC Policy	„könnyűsúlyú”, szerver oldali aláírási szolgáltatást megvalósító összetevőre vonatkozó szabályzat
NETHSM	Network HSM	hálózati HSM
PAdES	PDF Advanced Electronic Signature	PDF aláírási formátum
QSCD	Qualified Signature/Seal Creation	az eIDAS II. mellékletének megfelelő,

	Device	minősített aláírást/bélyegzőt létrehozó eszköz
SCAL	Sole Control Assurance Level	kizárólagos irányítás biztosítási szintje
SCAL1	Sole Control Assurance Level 1	kizárólagos irányítás 1-es biztosítási szintje
SSA	Server Signing Application	szerver oldali aláírás létrehozó alkalmazás
SSASC	Server Signing Application Service Component	szerver oldali aláírási szolgáltatást megvalósító összetevő, amellyel az Aláíró vagy Bélyegző Létrehozó a TKASZ-HSM-ben tárolt magánkulcsa felhasználásával kiszámíttatja az Aláírás Értéket
SSASP	Server Signing Application Service Provider	a szerver oldali aláírási szolgáltatást megvalósító összetevőt működtető bizalmi szolgáltató
SIC	Signer's Interaction Component	aláíró közreműködését kiváltó összetevő
SZEÜSZ	szabályozott elektronikus ügyintézési szolgáltatás	
TKASZ	tárolt kulcsos aláírás szolgáltatás	
UTC	Coordinated Universal Time	koordinált univerzális idő
XAdES	XML Advanced Electronic Signature	XML aláírási formátum

1.2.3 Hivatkozások

1.2.4 Jogszabályi hivatkozások

Az 1.1 fejezet tartalmazza.

1.2.4.1 Szabványok és műszaki technikai specifikációk

Az 1.1 fejezet tartalmazza.

1.2.4.2 Hivatkozott dokumentumok

BR-NISZ-TKASZ	NISZ-TKASZ Bizalmi Szolgáltatási Rend tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatáshoz
BSZ-NISZ-TKASZ	NISZ-TKASZ Bizalmi Szolgáltatási Szabályzat tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatáshoz
ISPEC-TK-EÜSZ	NISZ-TKASZ szolgáltatást kiközvetítő TK-EÜSZ-nek a hozzá történő kapcsolódás megvalósítását részletező dokumentációja (Interfész Specifikáció)

1.3 A NISZ-TKASZ bizalmi szolgáltatás biztonsági szintje

Mivel a NISZ-TKASZ bizalmi szolgáltatást a Szolgáltató nem minősített bizalmi szolgáltatásként nyújtja, az erre vonatkozó BR-NISZ-TKASZ bizalmi szolgáltatási rendjében a minősített bizalmi szolgáltatáshoz képest alacsonyabb biztonsági szintet határozott meg:

- a NISZ-TKASZ bizalmi szolgáltatási rend a TS 119 431-1 szabvány 4.3.2 fejezete szerinti LSCP (Lightweight SSASC Policy) szintet vállalja fel.

Mivel a NISZ-TKASZ szolgáltatás felhasználásával minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírások, illetve bélyegzők kerülnek létrehozásra a TKASZ-HSM-ben tárolt magánkulcsok felhasználásával, az Aláírók azonosítására, illetve az aláírási művelet aktiválására vonatkozóan Szolgáltató a minősített elektronikus aláírásra/bélyegzőre vonatkozó biztonsági szinthez képest alacsonyabb biztonsági szintet határozott meg:

- a NISZ-TKASZ szolgáltatás keretében az Aláírók, illetve a Bélyegző Létrehozók azonosítása, jogosultságának ellenőrzése, és az aláírási művelet aktiválására vonatkozó biztonsági szint az EN 419 241-1 szabvány 5.4 fejezete szerint SCAL1 (Sole Control Assurance Level 1).

Az SCAL1 definíciója az alábbi:

- az SCDev-ben tárolt magánkulcsokat az Aláíró kizárólagos irányítására vonatkozóan alacsony bizalmi szinttel használják;
- a felhatalmazott Aláíró az SSA (Server Signing Application) általi hitelesítése után használhatja az SCDev-ben tárolt magánkulcsát.

Az alábbi ábra szemlélteti a tárolt kulcsos aláírás és bélyegző elhelyezés szolgáltatás logikai architektúráját az SCAL1 szintre vonatkozóan (lásd EN 419 241-1, 5.13.2 fejezetében):

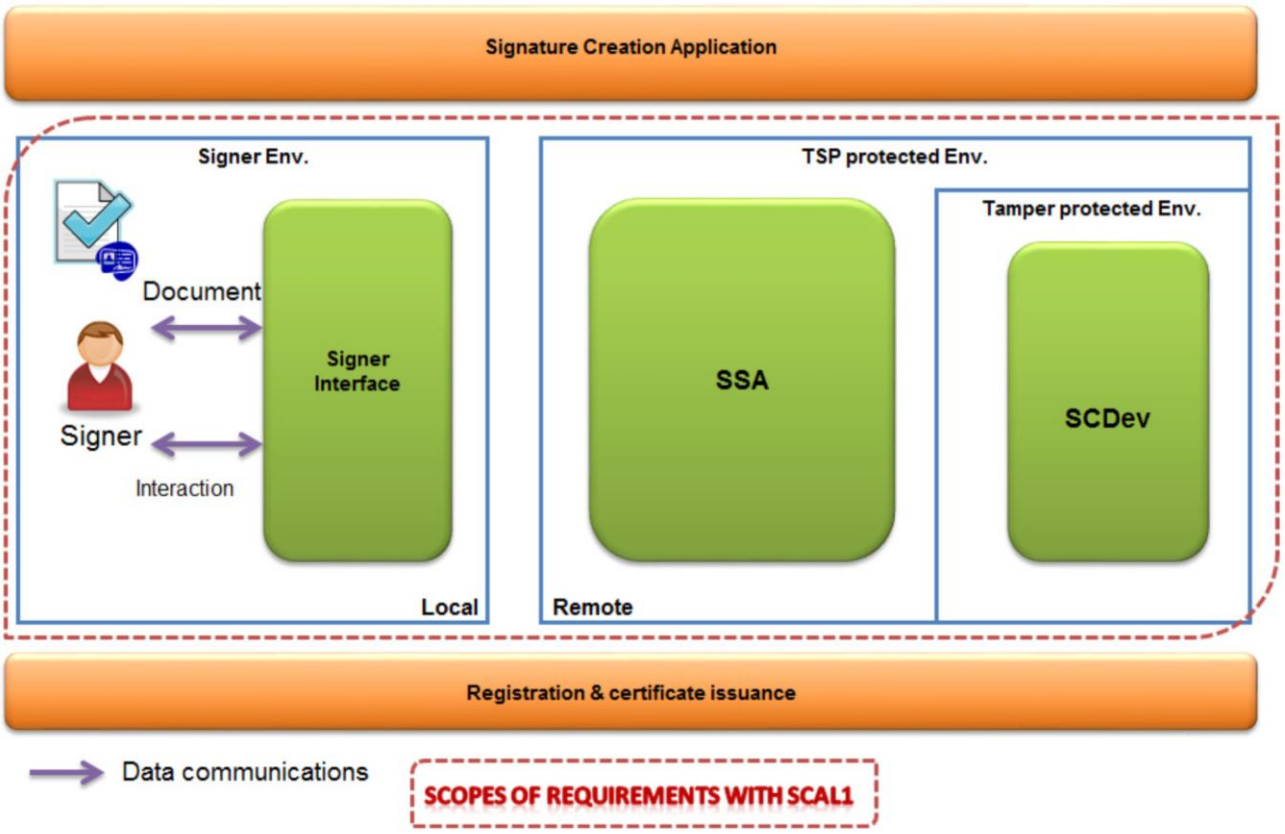

Figure 1 — Scope of requirements

Az EN 419 241-1 szabvány 5.7.4 fejezete kifejezetten lehetővé teszi a bizalmi szolgáltató számára, hogy az Aláíró azonosítását külső fél, delegált autentikáció keretében végezze.

A NISZ-TKASZ szolgáltatásban a Bélyegző Létrehozók (Előfizetők) azonosítását a Szolgáltató által működtetett informatikai rendszer végzi, míg az Aláírók azonosítását egy külső fél, delegált autentikáció keretében (Autentikációs Folyamat) végzi el.

1.3.1 Aláírási művelet aktiválása

Az EN 419 241-1 szabvány 5.13.3.2 fejezete adja meg a Kriptográfiai Műveletre vonatkozó előírásokat az SCAL1 szintre vonatkozóan:

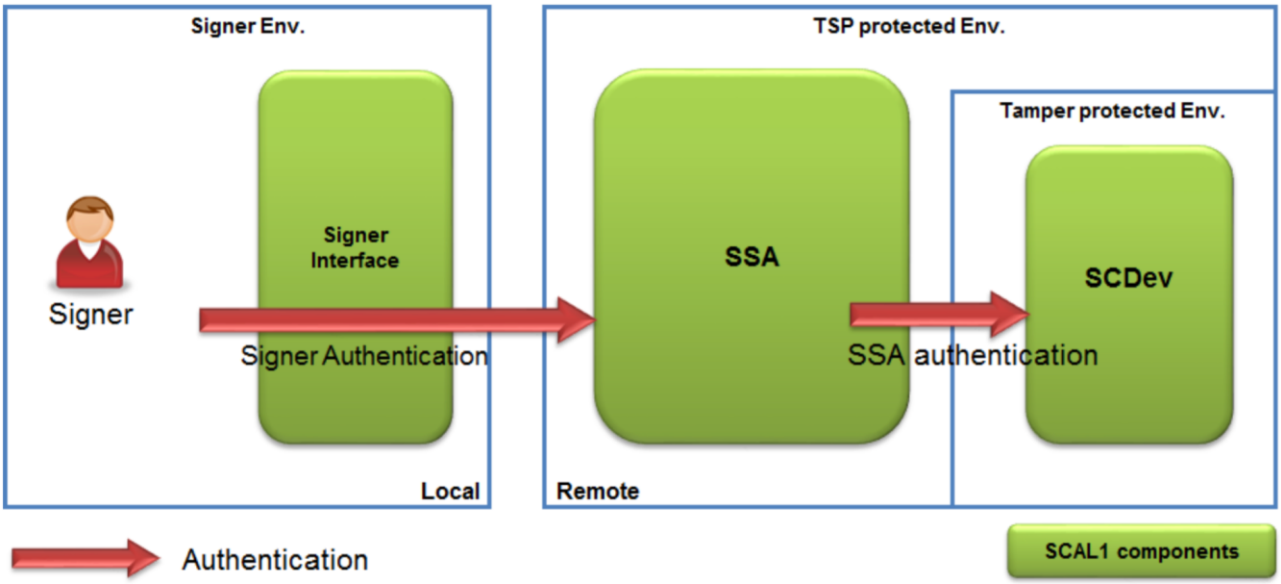

Figure 2 —Signature activation system with SCAL1

A magánkulcs bizalmasságát és integritását a TKASZ-HSM (amely CC EAL4+ vagy FIPS 140-2, 3-as szintű tanúsítással rendelkezik) biztosítja.

Az Aláíró azonosítását az Autentikációs Folyamat, a Bélyegző Létrehozók (Előfizető) azonosítását az SSA (Server Signing Application) végzi el, a sikeres azonosítást és jogosultság ellenőrzést követően a TKASZ-HSM-ben tárolt, a Felhasználóhoz vagy Bélyegző Létrehozóhoz kapcsolt magánkulcs használatát az SSA engedélyezi, egy bizonyos időtartamra, vagy meghatározott számú aláírásra vonatkozóan.

1.4 Autentikációs Folyamat megvalósulási lehetőségei

Az előző fejezetekben leírtak szerint Szolgáltató a NISZ-TKASZ szolgáltatás megvalósítása során igénybe vehet külső feleket a delegált autentikáció megvalósítására. Ebben az esetben a Szolgáltató teljes körűen felelős a külső fél tevékenységéért, és biztosítania kell, hogy a külső fél teljesítse a jelen dokumentumban megadott, vonatkozó biztonsági követelményeket, továbbá bizonyítékot kell szolgáltatnia az alkalmazandó biztonsági követelmények teljesüléséről.

1.4.1 eIDAS 6. cikk (1) bekezdése szerinti elektronikus azonosító eszköz használatával

Amennyiben az Autentikációs Folyamat olyan elektronikus azonosító eszközt alkalmaz, amelynek eIDAS 9. cikke szerinti bejelentése, vagy megfelelőségértékelése szerint legalább „alacsony” biztonsági szinttel rendelkezik, akkor úgy kell tekinteni, hogy az autentikációs folyamat teljesíti a

TS 119 431-1 szabvány 6.2.2 fejezetében előírt, a külső fél által végzett azonosításra vonatkozó követelményeket.

1.4.2 NISZ-TKASZ szolgáltatója által hitelesnek tekintett, X.500 szabványcsaládra épülő címtárszolgáltatás használatával

Jelenleg a NISz Zrt. által üzemeltetett rendszerekben is használatos címtár szolgáltatások megbízható gyártók jól dokumentált termékei. Ennek megfelelően az alap termékre vonatkozóan egyaránt dokumentálva van a rendszer kialakításhoz szükséges tervezés, az implementálás és a megszűntetés folyamata is. Ez a dokumentáltsági szint lehetővé teszi az előírások és ajánlások szerinti kialakítás lehetőségét. Így ezen címtárak használatával biztosítható, hogy:

- a címtárban lehessen tárolni a tanúsítványt,
- egy felhasználónak maximum 1 db tanúsítványa lehessen a címtárban tárolva,
- a tanúsítvány címtárból történő kiolvasása csak a kérés elküldésekor történjen meg,
- a címtár használatát érintő folyamatok és kommunikáció a címtár házirendjében bekonfigurálható módon:
    - ismeret alapú azonosítással,
    - titkosítva,
    - limitált titkosítási munkamenet idővel,
    - naplózva történjen,
- a felhasználó és a tanúsítvány összerendelésének sértetlenségét csak privilegizált felhasználó nevében futó folyamat törheti meg,
- az ajánlásoknak megfelelő címtár architektúra kialakítása esetén rendkívül magas rendelkezésre-állás érhető el a címtár attribútumokra, így a tanúsítványokra is.
- a megfelelő, akár többszintű jogosultsági rendszer is kialakítható legyen.

A Szolgáltató jelenleg két olyan gyártói címtár implementációt fogad el hitelesnek a delegált autentikációs eljárás alapjául, melyet az ügyfelei is használnak címtárszolgáltatásként:

- A Microsoft cég Active Directory-nak (AD) nevezett címtár megoldásának EIAD nevű implementációs példányát;

- A Novell Netware cég eDirectory-nak nevezett címtár megoldásának eDirectory nevű implementációs példányát, vagy egyéb Novel Netware címtárat, ami gyártói támogatással rendelkezik,

1.4.3 Szakrendszer által

Amennyiben az Előfizető által működtetett informatikai rendszer (Szakrendszer) nem a jelen fejezet megelőző alfejezeteiben említett autentikációs megoldást használja az Aláírók azonosítására, akkor a jelen dokumentumban foglalt biztonsági követelményeket magának a Szakrendszernek kell teljesítenie. A biztonsági követelmények teljesülését Szolgáltatónak a csatlakozást megelőzően vizsgálnia és értékelnie kell. A NISZ-TKASZ szolgáltatást a Szakrendszer csak azt követően veheti igénybe, hogy Szolgáltató meggyőződött a vonatkozó biztonsági követelmények maradéktalan teljesítéséről.

2 DELEGÁLT AZONOSÍTÁSRA VONATKOZÓ SZABÁLYZÓ-RENDSZER

Jelen fejezet megadja a külső fél által végzett, delegált autentikációra vonatkozó biztonsági követelményeket.

Minden egyes biztonsági követelménynél egy-egy táblázatban megadásra kerül a szabvány (vagy jogszabály) hivatkozása és a követelmény egyedi azonosítója. Az egyes szabványokat, illetve jogszabályokat a táblázat fejlécében eltérő háttér színek jelzik.

A szabványokból származó követelmények esetében, a táblázat tartalmazza az eredeti angol nyelvű szöveget (*dőlt szedéssel*), annak jelen dokumentum fogalomrendszerére testreszabott, magyar nyelvű fordítását és a külső fél számára megfontolandó alkalmazási megjegyzéseket.

A 2015/1502/EU végrehajtási aktusból származó követelmények esetében, a táblázat csak a vonatkozó, „alacsony” biztonsági szinthez tartozó, a joganyagból származó, hivatalos angol, illetve magyar nyelvű szöveget tartalmazza (*dőlt szedéssel*).

2.1 Aláírói kulcs és az Aláírót azonosító eszköz összekapcsolása

TS 119 431-1	**BIN-6.2.2-03**
The SSASP shall link signing keys with the appropriate signer's authentication means reference.	
Szolgáltatónak (a delegált autentikációt végző külső félnek) össze kell kapcsolnia az aláíró kulcsokat a megfelelő, Aláírót azonosító eszközzel.	
Alkalmazási megjegyzés: a felhasználók nyilvántartásának tartalmaznia kell az adott Aláíró számára kibocsátott, minősített, elektronikus aláírás célú tanúsítványt. Az Interfész Specifikációnak megfelelően összeállított kérésben csak és kizárólag az Aláíró sikeres azonosítását követően, az ezen nyilvántartásból kiolvasott, aláírói tanúsítványt szabad szerepeltetni, mivel a NISZ-TKASZ-ban e tanúsítvány alapján történik az Aláíró magánkulcsának kiválasztása. A tanúsítvány éles használatát a használatba vételkor minden Aláírónak tesztelnie szükséges. A delegált autentikációt végző külső félnek ellenőriznie szükséges, hogy minden Aláíró kizárólag a saját tanúsítványához, kulcsához fér hozzá.	

2.2 Aláíró személyazonossága egyező a számára kiadott tanúsítvány Alanyával

TS 119 431-1	BIN-6.2.2-05
The SSASP shall ensure that the identity linked to the authentication means reference is the same as the one linked to the subject of the associated certificate.	
Szolgáltatónak (a delegált autentikációt végző külső félnek) biztosítania kell, hogy az azonosító eszközhöz rendelt személyazonosság azonos legyen a kapcsolódó aláírói tanúsítvány Alanyának személyazonosságával.	
Alkalmazási megjegyzés: megfelelő műszaki és/vagy eljárási óvintézkedésekkel biztosítani kell, hogy az Aláírók nyilvántartása minden egyes Aláíró vonatkozásában a számára kibocsátott, megfelelő, minősített, elektronikus aláírás célú tanúsítványt tartalmazza (és nem más tanúsítványt).	

2.3 Azonosító eszköz külső fél általi szolgáltatása

TS 119 431-1	BIN-6.2.2-06
The signer's authentication means reference may be provided by an authorized (external) party.	
Az Aláíró azonosító eszközét az autentikációs folyamatban egy felhatalmazott (külső) fél is szolgáltathatja.	
Alkalmazási megjegyzés: ez teszi lehetővé pl. az eSzemélyi és más, a Központi Azonosítási Ügynökön keresztül elérhető azonosítási szolgáltatás elektronikus azonosítás célú felhasználását az autentikációs folyamatban.	

2.4 Aláíró nyilvántartásba vétele

TS 119 431-1	BIN-6.2.2-07
If all or part of the authentication process is delegated to an external party the SSASP shall ensure the external party meets the requirements specified in BIN-6.2.2-01.	
Amennyiben az azonosítási folyamat egészét vagy egy részét külső fél végzi (delegált autentikáció keretében), akkor teljesíteni kell a BIN-6.2.2-01 követelményt.	

Alkalmazási megjegyzés: lásd a 2015/1502/EU, 2.1 követelményt

TS 119 431-1	**BIN-6.2.2-01**
Clause SRC_SA.1.1 of CEN EN 419 241-1, specifying enrolment, shall apply.	
Az EN 419 241-1 szabvány, SRC_SA.1.1, nyilvántartásba vételre vonatkozó követelményét kell alkalmazni.	
Alkalmazási megjegyzés: lásd a 2015/1502/EU, 2.1 követelményt.	

EN 419 241-1	**SRC-SA.1.1**
The enrolment of the signer SHALL be as specified in (EU) 2015/1502 Clause 2.1, for assurance level low or higher. *The electronic identification means characteristics and design SHALL be as specified as specified in (EU) 2015/1502 Clause 2.2.1, for assurance level low or higher.* *The authentication mechanism SHALL be as specified in (EU) 2015/1502 Clause 2.3.1, for assurance level low or higher.*	
Az Aláíró nyilvántartásba vételét a 2015/1502/EU melléklet 2.1 pontjában leírtaknak megfelelően, az alacsony vagy annál magasabb biztonsági szinthez előírtak szerint kell elvégezni. Az elektronikus azonosító eszköz jellemzői és kialakítása meg kell feleljen a 2015/1502/EU melléklet 2.2.1 pontjában, az alacsony vagy annál magasabb biztonsági szinthez előírtaknak. A hitelesítési mechanizmus meg kell feleljen a 2015/1502/EU melléklet 2.3.1 pontjában, az alacsony vagy annál magasabb biztonsági szinthez előírtaknak.	
Alkalmazási megjegyzés: lásd a 2015/1502/EU, 2.1 követelményt	

2015/1502/EU	2.1

2.1 Enrolment

2.1.1 Application and registration

1. *Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.*
2. *Ensure the applicant is aware of recommended security precautions related to the electronic identification means.*
3. *Collect the relevant identity data required for identity proofing and verification.*

2.1.2 Identity proofing and verification (natural person)

1. *The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.*
2. *The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.*
3. *It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.*

2.1 Nyilvántartásba vétel

2.1.1 Igénylés és regisztráció

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.*

2.1.2 Személyazonosítás és személyazonosság-ellenőrzés (természetes személy esetén)

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 magának tulajdonító személy valóban az a személy.*
Alkalmazási megjegyzés: az azonosító eszköz igénylésekor az igénylőt tájékoztatni kell a 2.1.1 pontban említett ismeretekről, valamint össze kell gyűjteni a személyazonosság ellenőrzéséhez szükséges adatokat. Aláíró nyilvántartásba vétele előtt a személyazonosság megállapításához használt adatok helyességét ellenőrizni kell.

2015/1502/EU	**2.2.1**
2.2 Electronic identification means management 1. The electronic identification means utilises at least one authentication factor. 2. The electronic identification means is designer so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.	
2.2 Az elektronikus azonosító eszközök irányítása *2.2.1 Az elektronikus azonosító eszközök jellemzői és kialakítása* 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.*	
Alkalmazási megjegyzés: a „hitelesítési tényező” fogalmának leírását a 2015/1502/EU végrehajtási határozat Melléklete tartalmazza. *„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*.

Az előírás szerint, elégséges csak egy hitelesítési tényező használata, pl. ismeretalapú (pl. név/jelszó) alapú azonosítás. Ezzel kapcsolatban be kell tartani a jelszó alapú azonosítással kapcsolatos, általános biztonsági óvintézkedéseket.

A jelszavak bizalmasságának fenntartásához a mértékadó dokumentumok alapján (pl. lásd NIST SP-800-63B 5.1.1.2 fejezet) megfelelő hash algoritmus, sózás (minimum 32 bit) és megfelelő számú iteráció (minimum 10000) alkalmazása elengedhetetlen.

A lenyomatképző algoritmus kiválasztásánál az „ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites” (AlgoPaper) nemzetközi ajánlást szükséges figyelembe venni.

2015/1502/EU	**2.3.1**

2.3.1 Authentication mechanism

1. *The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.*
2. *Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.*
3. *The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.*

2.3.1 Hitelesítési mechanizmus

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 találgatás, lehallgatás, vagy a kommunikáció visszajátszása, illetve manipulálása egy közepes-alapszintű támadási potenciállal rendelkező támadó meghiúsítja a hitelesítési mechanizmust.*
Alkalmazási megjegyzés: biztosítani kell az autentikációs kiszolgáló hitelességét, a felhasználói név/jelszó helyességének ellenőrzését. Továbbá biztosítani kell az Aláírók nyilvántartásának védelmét a megsemmisülés és veszélyeztetés ellen. Az autentikációs eljárás során olyan biztonsági óvintézkedéseket kell alkalmazni a felhasználói adatok védelme érdekében, amelyek az említett támadási lehetőségek egy közepes-alapszintű támadási potenciállal rendelkező támadó általi kihasználásának lehetőségét minimalizálja.

2.5 Az Aláíró és az azonosítási hivatkozása közötti kapcsolat sértetlensége

TS 119 431-1	**BIN-6.2.2-10**
The SSASP shall protect the integrity of links between signer's signing key and its authentication reference.	
Szolgáltatónak (a delegált autentikációt végző külső félnek) meg kell védenie az aláíró magánkulcsának és az azonosítási hivatkozás közötti kapcsolat sértetlenségét.	
Alkalmazási megjegyzés: biztosítani kell az Aláírók Felhasználók nyilvántartásában az egyes Felhasználók és a számukra kibocsátott minősített, elektronikus aláírás célú tanúsítvány közötti összerendelés sértetlenségét. Pl. X.500 szabványnak megfelelő címtár használata esetén ez a követelmény teljesül.	

2.6 Aláírási művelet aktiválása

TS 119 431-1	**SIG-6.3.1-01**
Clause SRC_SA.1.2 of CEN EN 419 241-1, specifying authentication, shall apply.	

Az EN 419 241-1 szabvány, SRC_SA.1.2, az Aláíró azonosításra vonatkozó követelményét kell alkalmazni.

EN 419 241-1	**SRC-SA.1.2**
SSA SHALL require each signer to be successfully identified and authenticated before allowing any actions that can impact the sole control of any signing key.	
Az SSA-nak (a delegált autentikációt végző külső félnek) meg kell követelnie, hogy minden egyes Aláíró sikeresen azonosítva és hitelesítve legyen bármely olyan műveletet megelőzően, amelynek kihatása van valamely aláíró kulcs kizárólagos irányítására.	
Alkalmazási megjegyzés: biztosítani kell, hogy az Interfész Specifikációnak megfelelően összeállított kérés csak és kizárólag az Aláíró sikeres azonosítását követően kerülhet beküldésre a TK-EÜSZ felé, továbbá a kérésben minden esetben az azonosított Aláíró számára kibocsátott, az Aláírók nyilvántartásából kiolvasott, aláírói tanúsítványt kell szerepeltetni, mivel a NISZ-TKASZ-ban e tanúsítvány alapján történik az Aláíró magánkulcsának kiválasztása.	

TS 119 431-1	**SIG-6.3.1-08**
Signing keys shall be usable in only those cases for which the signer's consent has been obtained.	
Az aláíró kulcsokat csak azokban az esetekben lehet használni, amelyekhez az Aláíró beleegyezését megszerezték.	
Alkalmazási megjegyzés: - a Szakrendszernek biztosítania kell, hogy az aláírási művelet kiváltása (az Interfész Specifikációnak megfelelően összeállított kérés beküldése TK-EÜSZ felé) csak és kizárólag az Aláíró tudtával és beleegyezésével történhessen meg.	

3 A Szolgáltató által az azonosítási rendszerrel szemben meghatározott információbiztonsági követelmények

A Szolgáltató részéről elvárás, hogy tárolt kulcsos aláíró szolgáltatás igénybe vétele esetén a delegált autentikációt megvalósító rendszer és a hozzá kapcsolódó folyamatok a biztonsági követelmények legalább olyan szigorúak legyenek, mint amelyeket a NISZ Zrt. a saját azonosítási rendszereivel, a kapcsolódó folyamatokkal, az üzemeltető személyzettel kapcsolatban alkalmaz.

A Központi Azonosítási Ügynökön keresztül elérhető azonosítás, vagy eSzemélyi, mint eIDAS Rendelet szerinti legalább „alacsony" biztonsági szintű azonosító eszköz esetén elégséges a választott megoldás megjelölése.

Ha egyéb rendszer kerül alkalmazásra a delegált autentikációhoz, akkor a követelmények teljesülését és azok folyamatos meglétének biztosítását részletesen igazolni szükséges, amelyre a legmegfelelőbb a külső auditor által tanúsított és folyamatosan felülvizsgált releváns nemzetközi minősítés megléte.

3.1 A delegált autentikációs megoldás megfelelősége

Címtár alkalmazása esetén annak megadása szükséges, ha a szervezet a NISZ Zrt. által üzemeltetett címtárat vesz igénybe. Nem a NISZ Zrt. által üzemeltetett címtár esetén az Előfizető nyilatkozata arról, hogy a delegált autentikációra alkalmazni kívánt megoldás az adott Szolgáltatás csatlakozási követelményeiben meghatározott, gyártói támogatású címtárat alkalmaz.

3.2 A delegált autentikációs megoldás védelmének megfelelősége

Az Előfizetőnek a rendszer illesztése előtt – amennyiben a kiszolgáló pontokat nem NISZ Zrt. biztosítja – a Szolgáltató (NISZ Zrt.) szakemberei felé be kell mutatni, hogy a delegált autentikációt megvalósító hálózati alapszolgáltatást biztosító kiszolgáló pontokat a 41/2015 (VII. 15.) BM rendelet módszertana szerint milyen relevánsan értelmezhető adminisztratív, fizikai, logikai védelmi kontrollokkal látta el.

A kiszolgáló pontokra relevánsan értelmezhető kontrolloknak legalább olyan szintű védelmet kell megvalósítaniuk, amelyet az az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényhez kapcsolódó 41/2015 (VII. 15.) BM rendelet a KEASZ-KEASZ WS rendszer biztonsági osztályának megfelelően előír. KEASZ-KEASZ WS rendszer biztonsági osztálya: 3.

3.3 A delegált autentikációs megoldás konfigurációjának megfelelősége

Címtár esetén annak megadása szükséges, ha a szervezet a NISZ Zrt. által üzemeltetett címtárat vesz igénybe. Nem a NISZ Zrt. által üzemeltetett címtár, és/vagy a szakrendszer saját azonosítási megoldása esetén az Előfizető nyilatkozata arról, hogy a vonatkozó címtárrendszerében, és/vagy szakrendszerében kizárólag rendszergazdai jogosultsággal lehetséges az aláírókulcshoz kapcsolódó certificate attribútumot írni, a szakrendszeri felhasználóhoz a tanúsítványt (a felhasználói profilban) hozzárendelni. Az Előfizető felelőssége, hogy az aláíró/bélyegző tanúsítványokat manipulálhatatlan módon lehessen felhasználni. Az Előfizető nyilatkozata szükséges annak elfogadásáról, hogy a Szolgáltató (NISZ Zrt.) szakemberei a konfigurációt ellenőrizhetik.

3.4 A delegált autentikációs megoldás folyamatainak megfelelősége

Címtár esetén annak megadása szükséges, ha a szervezet a NISZ Zrt. által üzemeltetett címtárat vesz igénybe. Nem a NISZ Zrt. által üzemeltetett címtár, és/vagy a szakrendszer saját azonosítási megoldása esetén annak megadása, hogy az Előfizető rendelkezik ISO 27 001 és ISO 20 000 tanúsítással, amelynek hatóköre a szóban forgó címtárszolgáltatást, vagy a szakrendszer saját azonosítási megoldását is lefedi. Tanúsítványok hiányában annak tételes bemutatása, hogy a folyamatok az ISO 27 001 és ISO 20 000 szabványok követelményeinek megfelelnek.

3.5 Az emberi erőforrás megfelelősége

Címtár esetén annak megadása szükséges, ha a szervezet a NISZ Zrt. által üzemeltetett címtárat vesz igénybe. Nem a NISZ Zrt. által üzemeltetett címtár, és/vagy a szakrendszer saját azonosítási megoldása esetén az Előfizető nyilatkozata arról, hogy az érintett címtárszolgáltatáshoz, és/vagy a szakrendszer saját azonosítási megoldásához hozzáféréssel rendelkező adminisztrátorai kockázatokat nem feltáró nemzetbiztonsági átvilágítással rendelkeznek.