eIDAS kriptográfiai követelmények

Szabó Áron

MELASZ szakmai nap
Budapest
2016-01-12

eIDAS Technical Specification v1.0

eIDAS

Az eIDAS Technical Specification v1.0 dokumentumhalmaz 2015. november 26-án került ki nyilvánosan.

- eIDAS – Interoperability Architecture
- eIDAS - SAML Attribute Profile
- eIDAS – SAML Message Format
- eIDAS – Cryptographic requirements for the Interoperability Framework

https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10

A dokumentumhalmaz az EU tagállamok által üzemeltetendő átjárók (SAML protokollon alapuló PEPS - SSO/IdP - rendszerek) követelményeit határozzák meg. A negyedik dokumentum azonban érinti a hitelesítés-szolgáltatókat (CA) is, illetve később általánossá válhatnak, ami miatt minden elektronikus aláíráshoz és rejtjelezéshez kapcsolódó alkalmazást felül kellhet vizsgálni!

SSL/TLS

Az eIDAS – Cryptographic requirements for the Interoperability Framework egyik része az SSL/TLS protokollt és azok implementációit érintő biztonsági feltételekről szól.

[...] the eIDAS node MUST use TLS 1.2. [...] TLS 1.1 MAY be used [...] eIDAS nodes MUST only use cipher suites that provide perfect forward secrecy.

https://joinup.ec.europa.eu/sites/default/files/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf

	Key agreement and authentication mechanisms		*Encryption*	*Mode of operation*	*Hash*
TLS_	ECDHE_ECDSA_	WITH_	AES_128_	CBC_ GCM_	SHA256
			AES_256_	CBC_ GCM_	SHA384
	ECDHE_RSA_	WITH_	AES_128_	CBC_ GCM_	SHA256
			AES_256_	CBC_ GCM_	SHA384
	DHE_RSA_	WITH_	AES_128_	CBC_ GCM_	SHA256
			AES_256_	CBC_	SHA256
				GCM_	SHA384

SSL/TLS

Az eIDAS – Cryptographic requirements for the Interoperability Framework egyik része az SSL/TLS protokollt és azok implementációit érintő biztonsági feltételekről szól.

[...] SHA-2 [...] to be used, eIDAS nodes SHALL use this hash function for signatures within the handshake (and not SHA-1). [...] TLS compression SHOULD NOT be used. The heartbeat extension SHOULD NOT be used. [...] eIDAS nodes SHOULD support and use the Enc-then-MAC extension [...] Session Renegotiation SHOULD NOT be used.

https://joinup.ec.europa.eu/sites/default/files/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf

SSL/TLS

Az eIDAS – Cryptographic requirements for the Interoperability Framework egyik része az SSL/TLS protokollt és azok implementációit érintő biztonsági feltételekről szól.

2009-11-04: renegotiation attack
SSLv3.0 – TLSv1.2 verziók érintettek
ClientHello esetén végződtetni kell mindig
IETF RFC 5746 javítja

2011-09-23: BEAST
SSLv3.0 – TLSv1.0 verzió érintett
CBC sérülékenység
TLSv1.1 verzió javítja

2012-09-13: CRIME
SSLv3.0 – TLSv1.2 verziók érintettek
TLS-szintű tömörítés esetén adatszivárgás
TLS-szintű tömörítés kikapcsolása javítja

SSL/TLS

Az eIDAS – Cryptographic requirements for the Interoperability Framework egyik része az SSL/TLS protokollt és azok implementációit érintő biztonsági feltételekről szól.

2013-08-01: BREACH
SSLv3.0 – TLSv1.2 verziók érintettek
HTTP-szintű tömörítés esetén adatszivárgás
HTTP-szintű tömörítés kikapcsolása javítja

2013-02-04: Lucky 13
SSLv3.0 – TLSv1.2 verziók érintettek
időalapú padding oracle alapján adatszivárgás

2013-03-12: RC4
SSLv3.0 – TLSv1.2 verziók érintettek
kulcsfolyam felfedése azonos üzeneteknél
AES használata javítja

SSL/TLS

Az eIDAS – Cryptographic requirements for the Interoperability Framework egyik része az SSL/TLS protokollt és azok implementációit érintő biztonsági feltételekről szól.

2014-10-14: POODLE
SSLv3.0 verzió érintett
CBC sérülékenység
TLSv1.0 javítja

2015-05-20: weakDH, Logjam
SSLv3.0 - TLSv1.2 verziók érintettek
Diffie-Hellman paraméterek gyengítése
SSLCipherSuite módosítása, böngésző frissítése javítja

SAML

```
3.1     General requirements
3.1.1   Hash functions

        MUST be supported:
        SHA-2                                          256

        MAY be supported:
        -

3.2     XML Encryption with SAML
3.2.1   Content Encryption

        MUST be supported:
        http://www.w3.org/2009/xmlenc11#aes128-gcm
        http://www.w3.org/2009/xmlenc11#aes256-gcm

        MAY be supported:
        http://www.w3.org/2009/xmlenc11#aes192-gcm

3.2     XML Encryption with SAML
3.2.2   Key Encryption
3.2.2.1 Methods for key transport

        MUST be supported:
        http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p 3072
        http://www.w3.org/2009/xmlenc11#rsa-oaep        3072

        MAY be supported:
        -
```

SAML

```
3.2     XML Encryption with SAML
3.2.2   Key Encryption
3.2.2.2 Methods for key agreement

        MUST be supported:
        http://www.w3.org/2009/xmlenc11#ECDH-ES         256
        http://www.w3.org/2001/04/xmlenc#kw-aes128      128
        http://www.w3.org/2001/04/xmlenc#kw-aes256      256

        MAY be supported:
        -

3.3     Signatures for SAML and SAML Metadata
3.3.1   Signature Algorithms

        MUST be supported:
        RSASSA-PSS                                      3072
        ECDSA                                           256

        MAY be supported:
        -
```

SAML lenyomatképzés (dokumentum)

3.1 General requirements
3.1.1 Hash functions

sha-2
SHA-256 is required in the future

sha-2
SHA-256 is used recently

Az eIDAS – Cryptographic requirements for the Interoperability Framework követelménye nem jelent változást a jelenlegi helyzethez képest, mivel 2012. január 1. után kiadott tanúsítványoknál, illetve létrehozott aláírásoknál SHA-1 már nem használható, csak az SHA-2 családba tartozó SHA-256.

SAML rejtjelezés (dokumentum)

3.2 XML Encryption with SAML
3.2.1 Content Encryption

aes256-gcm
no padding is needed
unique counter + random nonce

aes256-cbc
padding is needed (padding oracle attack?)
random IV (CWE-329 - unique?)

Az eIDAS – Cryptographic requirements for the Interoperability Framework követelménye jelent változást a jelenlegi helyzethez képest, mivel bár jogi szabályozás nincs rá, de elterjedten a CBC módban alkalmazzák az AES algoritmust.

CBC
The IV need not be secret, but it must be unpredictable [...]. For the CBC and CFB modes, the IVs must be unpredictable.

http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SAML rejtjelezés (dokumentum)

CTR

The sequence of counters must have the property that each block in the sequence is different from every other block. [...] The specification of the CTR mode requires a unique counter block for each plaintext block that is ever encrypted under a given key, across all messages.

http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

GCM

The mode of operation that uses GCM as a stand-alone message authentication code is denoted as GMAC. [...] The IV need not be random, as it must be with CBC mode; a sequential IV value is sufficient. [...] The counter format and increment function that are used matches that in the proposed IPsec ESP Counter Mode standard [19]. [...] [19] R. Housley, Using AES Counter Mode With IPsec ESP.

http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf

SAML rejtjelezés (dokumentum)

```
3.2     XML Encryption with SAML
3.2.2   Key Encryption
3.2.2.1 Methods for key transport

RSAES-OAEP
1. EME-OAEP encoding
2. RSA encryption
3. Output the ciphertext C.

RSAES-OAEP
1. EME-OAEP encoding

   lHash      = Hash(L)
   PS         = 00 .. 00
   DB         = lHash || PS || 01 || M
   seed       = PRNG(0..MAX)
   maskLen    = k - hLen - 1
   dbMask     = MGF(seed, maskLen)
   MGF(seed, maskLen) {
    //Hash()  = SHA-1 (default)
    for (i = 0; ceil(maskLen/hLen)-1; i++) {
     C        = I2OSP (i, 4)
     dbMask   = dbMask || Hash(seed || C)
    }
   }
   maskedDB   = DB xor dbMask
   maskLen    = hLen
   seedMask   = MGF(maskedDB, maskLen)
   MGF(maskedDB, maskLen) {
    //Hash()  = SHA-1 (default)
    for (i = 0; ceil(maskLen/hLen)-1; i++) {
     C        = I2OSP (i, 4)
     dbMask   = dbMask || Hash(maskedDB || C)
    }
   }
   maskedSeed = seed xor seedMask
   EM         = 00 || maskedSeed || maskedDB
```

```
RSAES-PKCS1-v1_5
1. EME-PKCS1-v1_5 encoding
2. RSA encryption
3. Output the ciphertext C.

RSAES-PKCS1-v1_5
1. EME-PKCS1-v1_5 encoding

   PS = FF .. FF

   EM = 00 || 02 || PS || 00 || M
```

SAML rejtjelezés (dokumentum)

Az eIDAS – Cryptographic requirements for the Interoperability Framework követelménye jelent változást a jelenlegi helyzethez képest, mivel bár jogi szabályozás nincs rá, de elterjedten a RSAES-PKCS1-v1_5 módban alkalmazzák az RSA algoritmust.

Daniel Bleichenbacher [...] chosen ciphertext attack [...]. If the oracle says that c' is PKCS conforming, then the attacker knows that the first two bytes of ms are 00 and 02. [...] By collecting several such pieces of information, we can eventually derive m.

http://link.springer.com/content/pdf/10.1007%2FBFb0055716.pdf

RSA Version 1.5 [...] REQUIRED [...] Support of this algorithm for transporting other keys is OPTIONAL. RSA-OAEP is RECOMMENDED for the transport of AES keys. [...] RSA-OAEP [...] REQUIRED

http://www.w3.org/TR/xmlenc-core/

SAML rejtjelezés (dokumentum)

```
3.2     XML Encryption with SAML
3.2.2   Key Encryption
3.2.2.2 Methods for key agreement

ECDH-ES

        MUST be supported:
        SHA-1                                       160
        SHA-2                                       256

        MAY be supported:
        SHA-2                                       384
        SHA-2                                       512

        MUST be supported:
        http://www.w3.org/2009/xmlenc11#ConcatKDF

        MAY be supported:
        http://www.w3.org/2009/xmlenc11#pbkdf2
        ...

        MUST be supported:
        NIST Curve P-256

        MAY be supported:
        NIST Curve P-384
        NIST Curve P-521

AESKW

        MUST be supported:
        AES-128                                     128
        AES-256                                     256

        MAY be supported:
        -
```

SAML rejtjelezés (dokumentum)

Az eIDAS – Cryptographic requirements for the Interoperability Framework követelménye jelent változást a jelenlegi helyzethez képest, mivel bár jogi szabályozás nincs rá, de elterjedten a RSAES-PKCS1-v1_5 módban alkalmazzák az RSA algoritmust (a szimmetrikus megoldások helyett is).

Diffie-Hellman Key Values [...] OPTIONAL [...] Diffie-Hellman Key Agreement [...] OPTIONAL [...] AES KeyWrap [...] Implementation of wrapping 128 bit keys REQUIRED. [...] Implementation of wrapping 256 bit keys REQUIRED.

http://www.w3.org/TR/xmlenc-core/

SAML rejtjelezés (dokumentum)

Az előírt "http://www.w3.org/2009/xmlenc11#ECDH-ES" algoritmus kevés library által támogatott.

A "http://www.w3.org/2009/xmlenc11#ConcatKDF" esetében a "shared secret" értékéből származtatott, elvárt hosszúságú (AES-256 esetén 256 bit) "DerivedKeyingMaterial" az egyedi és növekvő "counter", a "shared secret" és egyéb paraméterek összefűzött értékei "keydatalen/hashlen" értékszer lenyomatolva (pl. 256 bites SHA-2 esetén pontosan egy lenyomat darabka szükséges AES-256 256 bites kulcsához), majd ezen Hash[i] darabok összefűzve és szükség szerint csonkolva.

A "http://www.w3.org/2001/04/xmlenc#kw-aes256" algoritmus az adatot rejtjelező kulcs nyílt változata és a kulcsot rejtjelező kulcs (a "shared secret" értékéből származtatott "DerivedKeyingMaterial", mint a KEK, "key-encryption key") alapján létrehozza az adatot rejtjelező kulcs rejtjelezett változatát (AES esetében szimmetrikus kulccsal).

SAML aláírás (dokumentum, tanúsítvány)

```
3.3     Signatures for SAML and SAML Metadata
3.3.1   Signature Algorithms
```

```
RSASSA-PSS
1. EMSA-PSS encoding
2. RSA signature
3. Output the signature S.
```

```
RSASSA-PSS
1. EMSA-PSS encoding
   EMSA-PSS-ENCODE (M, emBits)

   mHash      = Hash(M)
   salt       = PRNG(0..MAX)
   8iZO       = 00 .. 00
   M'         = 8iZO || mHash || salt
   H          = Hash(M')

   PS         = 00 .. 00
   DB         = PS || 01 || salt
   maskLen    = emLen - hLen - 1
   dbMask     = MGF(H, maskLen)
   MGF(H, maskLen) {
    //Hash()  = SHA-1 (default)
    for (i = 0; ceil(maskLen/hLen)-1; i++) {
     C        = I2OSP (i, 4)
     dbMask   = dbMask || Hash(H || C)
    }
   }
   maskedDB   = DB xor dbMask
   EM         = maskedDB || H || bc
```

```
RSASSA-PSS
randomness is not critical to security
uniqueness is not critical to security
```

```
RSASSA-PKCS1-v1_5
1. EMSA-PKCS1-v1_5 encoding
2. RSA signature
3. Output the signature S.
```

```
RSASSA-PKCS1-v1_5
1. EMSA-PKCS1-v1_5 encoding
   EMSA-PKCS1-v1_5-ENCODE (M, emLen)

   H = Hash(M)
   T = DigestInfo
       DigestInfo ::= SEQUENCE {
        digestAlgorithm AlgorithmIdentifier,
        digest          OCTET STRING
       }
   PS = FF .. FF

   EM = 00 || 01 || PS || 00 || T
```

```
ECDSA
randomness is critical to security
uniqueness is critical to security
```

SAML aláírás (dokumentum, tanúsítvány)

Az eIDAS – Cryptographic requirements for the Interoperability Framework követelménye jelent változást a jelenlegi helyzethez képest, mivel a jogszabályok által közvetve meghivatkozott műszaki leírás alapján a RSASSA-PKCS1-v1_5 módban alkalmazzák az RSA algoritmust.

RSASSA-PKCS-v1_5

The expression "RSA algorithm" as used in this specification refers to the RSASSA-PKCS1-v1_5 algorithm described in RFC 2437 [PKCS1]. [...] The SignatureValue content for an RSA signature is the base64 [MIME] encoding of the octet string computed as per RFC 2437 [PKCS1, section 8.1.1: Signature generation for the RSASSA-PKCS1-v1_5 signature scheme].

http://www.w3.org/TR/xmldsig-core/
https://tools.ietf.org/html/rfc3275

SAML aláírás (dokumentum, tanúsítvány)

ECDSA

Az eIDAS az alábbi elliptikus görbék támogatását várja el:

- BrainpoolP256r1
- BrainpoolP384r1
- BrainpoolP512r1
- NIST Curve P-256
- NIST Curve P-384
- NIST Curve P-521

De mit mond ezekről Daniel J. Bernstein és csapata? Biztonságosak?

		Parameters:			ECDLP security:				ECC security:			
Curve	Safe?	field	equation	base	rho	transfer	disc	rigid	ladder	twist	complete	ind
Anomalous	False	True✓	True✓	True✓	True✓	False	False	True✓	False	False	False	False
M-221	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
E-222	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
NIST P-224	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False	False
Curve1174	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Curve25519	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
BN(2,254)	False	True✓	True✓	True✓	True✓	False	False	True✓	False	False	False	False
brainpoolP256t1	False	True✓	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False
ANSSI FRP256v1	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False	False
NIST P-256	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	True✓	False	False
secp256k1	False	True✓	True✓	True✓	True✓	True✓	False	True✓	False	True✓	False	False
E-382	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
M-383	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Curve383187	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
brainpoolP384t1	False	True✓	True✓	True✓	True✓	True✓	True✓	True✓	False	True✓	False	False
NIST P-384	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	True✓	False	False
Curve41417	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Ed448-Goldilocks	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
M-511	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
E-521	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓

http://safecurves.cr.yp.to/

SAML aláírás (dokumentum, tanúsítvány)

EdDSA

For example, deterministic nonces were proposed in 1997, are integrated into modern signature mechanisms such as EdDSA, and would have prevented the 2010 Sony PlayStation ECDSA security disaster.

http://safecurves.cr.yp.to/

EdDSA

2. Does not require the use of a unique random number for each signature.

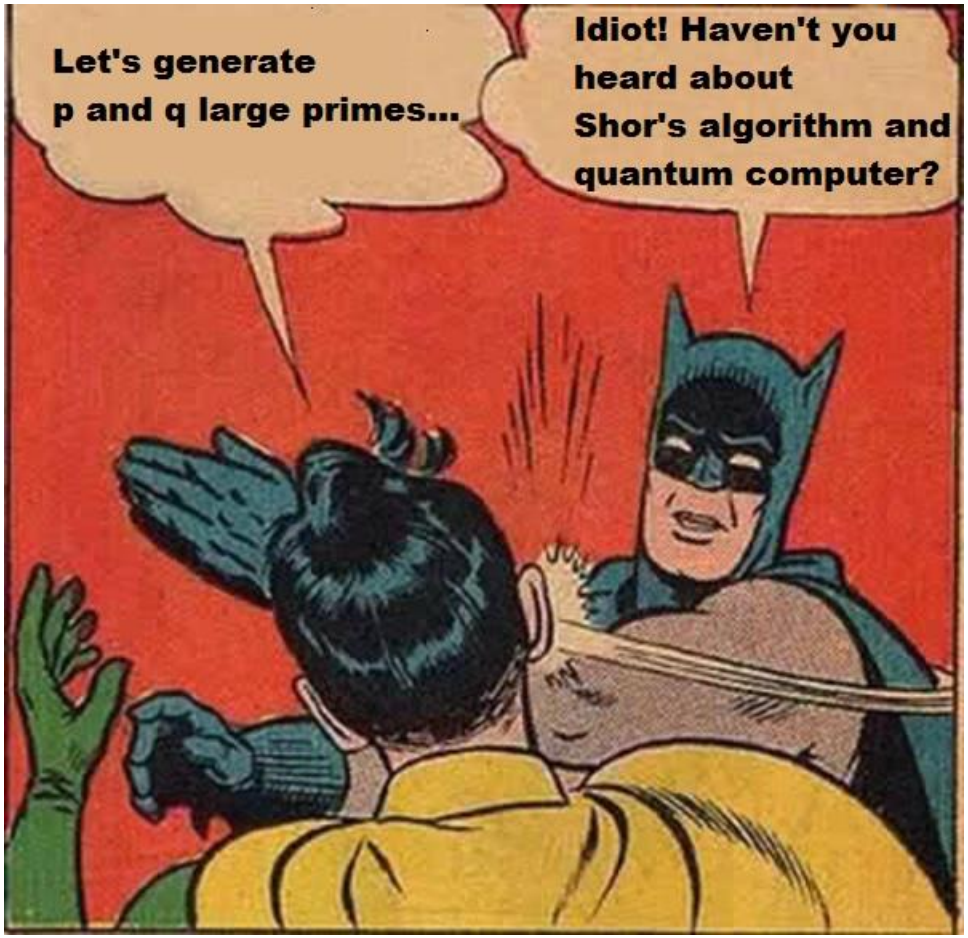
https://tools.ietf.org/html/draft-irtf-cfrg-eddsa-00

RSASSA-PSS

However, the randomness is not critical to security. In situations where random generation is not possible, a fixed value or a sequence number could be employed instead [...].

https://tools.ietf.org/html/rfc3447

PQCRYPTO???



Post-Quantum Cryptography for Long-Term Security (2015-09-07)

http://pqcrypto.eu.org/docs/initial-recommendations.pdf

Köszönöm a figyelmet!

MELASZ

Magyar Elektronikus Aláírás Szövetség