eSign Day 2023

Attribútum tanúsítványok

2022/06/30

Miről szól ez az előadás?

- Rövid bevezető
  - Mi az attribútum, mi az attribútum tanúsítvány, jogi háttér
- Az attribútum ETSI szabványok jelenlegi állása
  - A legutolsó változat alapján a tanúsítvány lehetséges tartalma
- Az attribútum tanúsítványok használata a gyakorlatban
  - A legutolsó változat alapján a tanúsítvány lehetséges tartalma

Alapfogalmak 1.

Attribútum

- Latin eredetű szó (attributum), amelynek jelentése: mellérendel, neki tulajdonít.
- Magyarul egy entitás tulajdonságait jelenti.

Attribútum igazolás (attribute attestation)

- Az eIDAS2 tervezi bevezetni az attribútum igazolást, mint jogi fogalmat.
- Többféle protokoll is használható.
  - Ezek közül egy metódus az X.509 attribútum tanúsítvány.
- Ez tulajdonképpen egy a CA által adott formátumban aláírt dokumentum, amely a kapcsolódó entitás valamely tulajdonságát igazolja, és amit a CA engedélyezett.

Alapfogalmak 2.

Attribútum-tanúsítvány

- Gyorsan változó adatokat, bár elméletben lehetséges, de nem érdemes aláíró tanúsítványba foglalni.
  - Az ilyen adatok igazolására való az attribútum tanúsítvány.
- Az RFC 5755 definiálja.
- A CA ebben az igazolást az adott tulajdonságról ad, melyet kiállítás előtt ellenőriz.
- Nincs benne nyilvános kulcs, a CA aláírását kell ellenőrizni a hitelesség megállapításához.
- Az attribútum tanúsítvány aláíró tanúsítványhoz kötött a holder mezőn keresztül.
- Az ETSI TS 119472 az RFC 5755-öt Extenension-ökkel egészíti ki, annak megfelel.

```
AttributeCertificate ::= SEQUENCE {
  acinfo               AttributeCertificateInfo,
  signatureAlgorithm   AlgorithmIdentifier,
  signatureValue       BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
  version                 AttCertVersion, -- version is v2
  holder                  Holder,
  issuer                  AttCertIssuer,
  signature               AlgorithmIdentifier,
  serialNumber            CertificateSerialNumber,
  attrCertValidityPeriod  AttCertValidityPeriod,
  attributes              SEQUENCE OF Attribute,
  issuerUniqueID          UniqueIdentifier OPTIONAL,
  extensions              Extensions OPTIONAL
}
```

Jogi háttér

Eüt. (2015. évi CCXXII. Törvény)

- A kormányzati szereplők számára lehetővé teszi a szerepkörök (beosztás) igazolását
  - Ez, habár csak a szerepkör, de attribútum tanúsítvány kiadás

eIDAS2 Attribútum igazolás (attribute attestation)

- Megteremti a jogi hátteret.
- A következő adatok lesznek várhatóan igazolhatók attribútum igazolással.
  - Cím; Kor; Nem; Házassági állapot; Család összetétel
  - Nemzetiség vagy állampolgárság
  - Oktatási kvalifikációk, címek és licencek; Professzionális kvalifikációk, címek és licencek
  - Engedélyek és licencek
  - Pénzügyi és vállalati adatok

Attribútum szabványok 1. - ETSI TS 119471

Az új szabvány tervezetek:

- ETSI TS 119471 Attribútum szolgáltatókra vonatkozó előírások
  - Az eIDAS2 szövegét vették alapul a szabvány megfogalmazásához.
  - Az ETSI 319411-1 és 319411-2 (tanúsítvány kiadókra vonatkozó) szabványok attribútum szolgáltatásra vonatkozó megfelelője.
  - Jól kidolgozott, sok változás már nem várható. (V0.0.5 (2023-04) Stabil draft a legutolsó verzió)
  - Struktúrájában az ETSI 319 401-et követi.
    (Ez szerintem hiba volt, az ETSI 319 411-X szabványokból kellett volna kiindulni.)
  - Követelmények tekintetében a az ETSI 319 401-et hivatkozza bőségesen.

AZ ATTRIBÚTUM SZOLGÁLTATÓRA VONATKOZÓ KÖVETELMÉNYEK A TANÚSÍTVÁNYKIADÓKRA VONATKOZÓ SZINTE MEGEGYEZNEK.

Attribútum szabványok 2. - ETSI TS 119472

Az új szabvány tervezetek:

- ETSI 119472 Az attribútum „kódolására” vonatkozó előírások
  - Több adatformátum is támogatásra kerül.
    - W3C Verifiable credentials
    - X509 Attribútum tanúsítvány
  - Erős küzdést követően várható, hogy lesz egységes uniós kódolása az attribútumoknak.
    - Fontos, hogy az egyik szolgáltató által kiadott attribútumok a más szolgáltató által is értelmezhetőek legyenek.
    - Fontos, hogy a soknyelvűség problémája is kezelésre kerüljön.
  - Az eIDAS2 szövegét vették alapul a szabvány megfogalmazásához.
  - Az eIDAS2 még nem végleges, várható még változás. V0.0.4 (2022-09) Early draft

Az ETSI TS 119472 komponensei 1.

component name	jelentés	kötelezőség	tanúsítvány mező	megjegyzés
Az attribútum attestációk kontextus adatai				
Context information	Az attribútum attestációnak meg kell határoznia a kontextust	kötelező	version := V2 (1)	X.509 AC esetén a version V2 (1) tekintett kontextus meghatározásának.
Attributes Attestation type information	Az attribútum attestációnak jeleznie kell magáról, hogy attribútum attestáció.	kötelező	-	Magával az attribútum tanúsítvánnyal az attestáció teljesül.
Az attribútum attestációk alapvető adatai				
identifier component	Az attribútum tanúsítványt egyedileg azonosítja	kötelező	serialNumber	A serialNumber egyedi azonosító.
issuer component	Egyértelműen azonosítania kell az attestáció kibocsátóját.	kötelező	issuer	Az issuer azonosítása az issuer mezővel történik.
subject component	Egyértelműen azonosítania kell az attestáció alanyát.	kötelező	holder	A holder mező tartalmáva a subject.
issuedAt component	A kibocsátás időpontja.	X.509 AC esetén nem értelmezett.	-	-
validityPeriod component	Az érvényesség időtartama.	kötelező	attrCertValidityPeriod (notBefore/notAfter)	
qualified component	Minősítettség jelzése	minősített szolgáltató esetén kötelező	qaaCompliance (qcCompliance)	A qcCompliance mező jelzi a minősítettségét az attribútumnak.

Az ETSI TS 119472 komponensei 2.

component name	jelentés	kötelezőség	tanúsítvány mező	megjegyzés
Az attribútum attestációk használatát befolyásoló komponensek				
aud component	Azt tartalmazza, hogy kinek a részére készül az adott attestáció.	opcionális	id-ce-targetInformation	-
oneTimeUse component	Ha tartalmazza ezt a komponenst, akkor ez csak egyszer használható.	opcionális / nem biztos, hogy tartósan marad	még nem meghatározott	Ha oneTimeUse akkor a tanúsítványban nem szerepelhet id-ce-cRLDistributionPoints extension, ellenben szerepelnie kell az id-ce- noRevAvail extension-nek
evidence component	Az extension tartalmazza azt, hogy milyen bizonyíták alapján került kiállításra az attestáció.	opcionális / nem biztos, hogy tartósan marad	még nem meghatározott	-
attestationStatusService component	Az X.509 AC-nak tartalmaznia kell referenciát vagy OCSP vagy CRL vagy mindkét szolgáltatásra, vagy jeleznie kell, hogy nincs visszavonási információ	kötelező	id-ce-authorityInfoAccess/ accessMethod := id-ad-ocsp és/vagy id-ce-cRLDistributionPoints VAGY id-ce-noRevAvail	-
attestationRefreshService component	Ha tartalmazza ezt a komponenst, akkor innen szerezhető be friss attestáció.	opcionális / nem biztos, hogy tartósan marad	még nem meghatározott	problematikus: "consent of the person" nem valósul meg, ha alanytól függetlenül kérhető frissítés
verificationSchema component	Ellenőrzési séma.	X.509 AC esetén nem értelmezett.	-	-
encodingSchema component	Kódolási séma.	X.509 AC esetén nem értelmezett.	-	-
attributeGroups component	Attribútumok csoportosítására szolgálna	opcionális / nem biztos, hogy tartósan marad	még nem meghatározott	-

Az ETSI TS 119472 komponensei 3.

component name	jelentés	kötelezőség	tanúsítvány mező	megjegyzés
Attribútum metaadat				
attributes component	A tanúsítani kívánt attribútum, JSON vagy ASN.1 formában kódolva.	kötelező	Attributes	Ez esetben az attribútum JSON formában kerül be a tanúsítványba. Ez esetben az attribútum a szokásos ASN.1 formában kerül be a tanúsítványba.
selectiveDisclosure component	Nem definiált X.509 AC esetén	Nem definiált X.509 AC esetén	Nem definiált X.509 AC esetén	A selectiveDisclosure X.509 AC esetén atomi (egy attribútumot tartalmazó) X.509 AC tanúsítványokkal valósítható meg.
Autentikusság				
signature component	A kiadó aláírása, amely bizonyítja a forrást, és védi az autentikusságot.	kötelező	Az aláírás az X.509 AC tanúsítványon.	-

Attribútum tanúsítvány struktúra 1.

Az Attribútum tanúsítvány struktúrája az eIDAS2 alatt

- Az ETSI TS 119472 kompatibilis az RFC 5755-tel.
- Az új Extension-ök az RFC 5280-ben és az ETSI EN 319412-5-ben már definiált Extension-ök.
- Kötelező extension-ök
  - visszavonási információk vagy annak hiánya:
    - id-ce-cRLDistributionPoints (RFC 5280) és/vagy id-ad-ocsp (RFC 5280)
    - ha egyik előző pontból sem szerepel akkor id-ce-noRevAvail (RFC 5755)
- Opcionális extension-ök
  - az attribútum címzettje, azaz akinek a felhasználása engedélyezett
    id-ce-targetInformation (RFC 5755)
  - a minősítettség jelzése
    id-etsi-qcs-QcCompliance (ETSI EN 319412-5)
- EU szintű egységes attribútum szótár nem került definiálásra, majd határidőt kap.

```
AttributeCertificate ::= SEQUENCE {
  acinfo               AttributeCertificateInfo,
  signatureAlgorithm   AlgorithmIdentifier,
  signatureValue       BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
  version                 AttCertVersion, -- version is v2
  holder                  Holder,
  issuer                  AttCertIssuer,
  signature               AlgorithmIdentifier,
  serialNumber            CertificateSerialNumber,
  attrCertValidityPeriod  AttCertValidityPeriod,
  attributes              SEQUENCE OF Attribute,
  issuerUniqueID          UniqueIdentifier OPTIONAL,
  extensions              Extensions OPTIONAL
}
```

Attribútum tanúsítvány struktúra 2.

Módosítási, javítási lehetőségek az ETSI TS 119472 szabványban

- Az kiadói tanúsítvány elérhetősége kimaradt.
  id-ad-caIssuers (RFC 5280)

  mert az eDIAS 2 szerint ez kötelező tartalom:

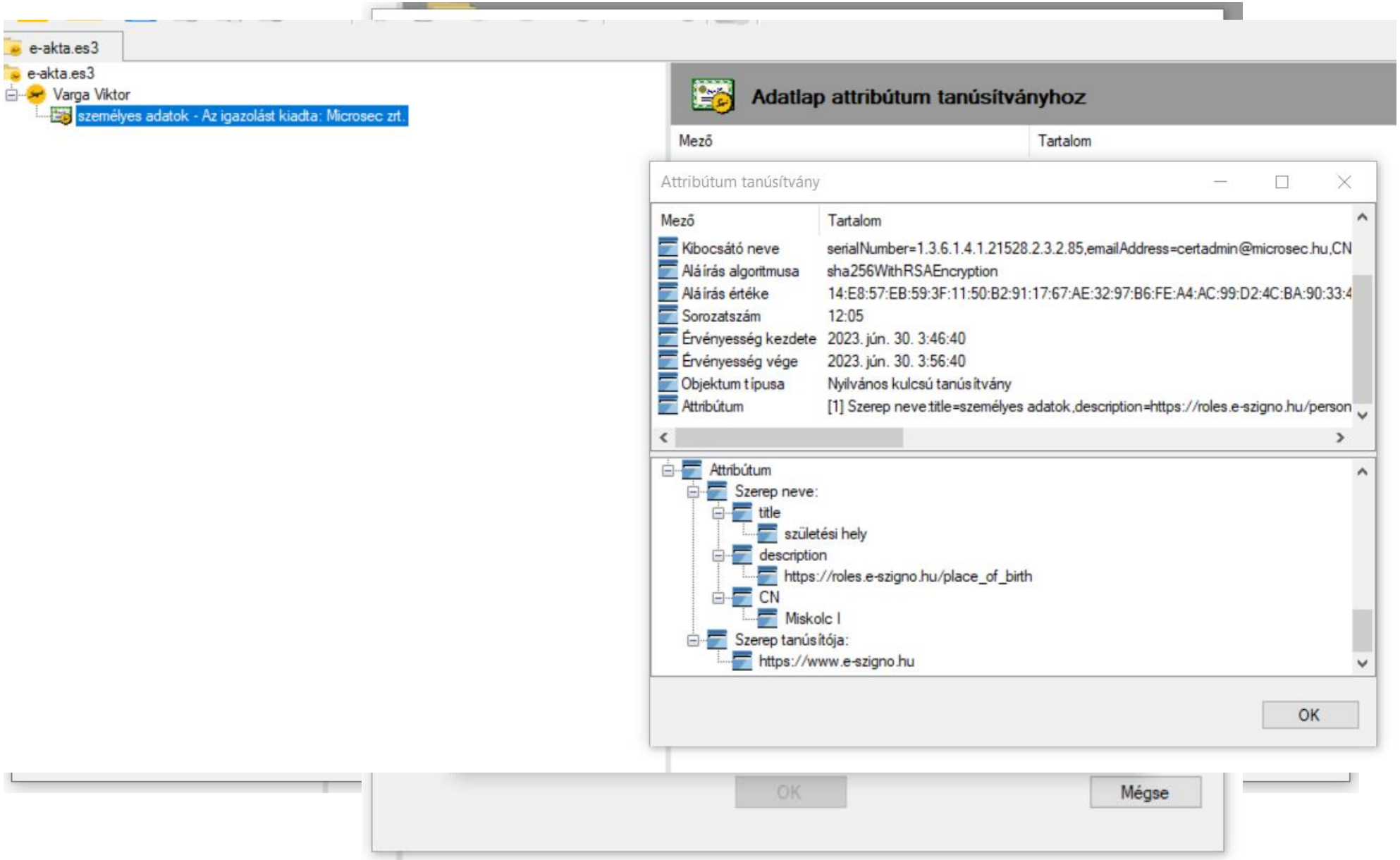
  "the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (f) is available free of charge;„

- További qcStatements-ek (ETSI EN 319412-5) lehetnének értelmezhetőek erre a szolgáltatásra:
  - id-etsi-qcs-QcPDS
  - qcs-QcRetentionPeriod
  - id-etsi-qcs-QcType (ha definiálásra kerül az attribútumnak is típus azonosító)
- EU attribútum szótár felállítása lenne szükséges

```
AttributeCertificate ::= SEQUENCE {
  acinfo               AttributeCertificateInfo,
  signatureAlgorithm   AlgorithmIdentifier,
  signatureValue       BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
  version                 AttCertVersion, -- version is v2
  holder                  Holder,
  issuer                  AttCertIssuer,
  signature               AlgorithmIdentifier,
  serialNumber            CertificateSerialNumber,
  attrCertValidityPeriod  AttCertValidityPeriod,
  attributes              SEQUENCE OF Attribute,
  issuerUniqueID          UniqueIdentifier OPTIONAL,
  extensions              Extensions OPTIONAL
}
```

A gyakorlat az sokkal egyszerűbb



MICROSEC

Kérdések, hozzászólások

Kapcsolat

Contact

VARGA VIKTOR
CA SERVICE MANAGER

Microsec zrt. | 1033 Budapest, Ángel Sanz Briz út 13.
varga.viktor@microsec.hu
microsec.hu