MICROSEC
Számítástechnikai Fejlesztő zrt.

Az e-akta formátum specifikációja

Azonosító:	1.3.6.1.4.1.21528.2.1.1.28.1.5
Verzió:	1.5
Státusz:	jóváhagyott
Dátum:	2015. február 20.
Kezelési mód:	Nyilvános

Microsec Számítástechnikai Fejlesztő zrt.
1031 Budapest, Záhony u. 7.

Változáskövetés

Verzió	**A változás leírása**	**Dátum**	**Készítette**
1.0	Első változat	2008. július 1.	Dr. Berta István Zsolt, Tóth Szilveszter
1.1	XML séma hivatkozás javítva	2009. július 22.	Dr. Berta István Zsolt, Tóth Szilveszter
1.2	XAdES verzió váltás, elavult elemek kivétele, pontosítások	2011. február 4.	Endrődi Csilla
1.3	Frissítés	2011. november 17.	Endrődi Csilla
1.4	Frissítés	2013. augusztus 6.	Endrődi Csilla
1.5	Pontosítások: - XAdES v1.4.2-es elemek bevétele, - Minta sémadefiníciós állomány (eszigno30.xsd) és a szöveges specifikáció eltérésének értelmezése, - Pontosítások az egyes elemek használatával kapcsolatban, - További metaadatok használatának engedélyezése, - Speciális célú e-akta sémák meghatározása (4. fejezet), - Kivételek (5. fejezet).	2015. február 20.	Endrődi Csilla, Réti Kornél, Tóth Szilveszter

Tartalomjegyzék

1. Bevezetés

Az **elektronikus akta** (e-akta) elnevezés alatt az Közigazgatási és Igazságügyi Minisztérium részére az elektronikus cégeljárás kapcsán a Microsec zrt. által kifejlesztett olyan fájlformátumot értünk, amely dokumentumokat, és a dokumentumokon elektronikus aláírásokat és időbélyegeket tartalmaz. A dokumentumokon elhelyezett aláírások szabványos, az ETSI által kidolgozott ETSI TS 101 903 (XAdES) specifikáció v1.2.2, v1.3.2 vagy v1.4.2 verziójának megfelelő ún. XAdES aláírások lehetnek.

Jelen specifikáció nem tesz megkötéseket a XAdES aláírásokkal kapcsolatban, hanem azt írja le, hogy egy XML fájlban (az ún. **e-aktában**) hogyan helyezhetőek el dokumentumok, illetve hogyan helyezhetőek el XAdES formátumú aláírások ezen dokumentumokon, illetve a rajtuk elhelyezett aláírásokon. A gyakorlati alkalmazásokban általában nem elengedő a dokumentumokat önmagukban aláírni, hanem különféle metaadatokat is kell csatolni hozzájuk. Az e-akta specifikáció a Dublin Core Metadata Initiative által meghatározott, szabványos formátumú metaadatok csatolását támogatja, de más metaadatok csatolására is van lehetőség.

Magyarországon az e-akta formátum de facto szabvánnyá vált, számos felhasználói közösség, illetve alkalmazás e-akta formátumú elektronikusan aláírt dokumentumokat kezel.

1.1. Hivatkozott dokumentumok

- 2001. évi XXXV. törvény az elektronikus aláírásról
- ETSI TS 101 903 V1.2.2. (2004-04): XML Advanced Electronic Signatures (XAdES)
- ETSI TS 101 903 v1.3.2 (2006-03): XML Advanced Electronic Signatures (XAdES)
- ETSI TS 101 903 v1.4.2 (2010-12): XML Advanced Electronic Signatures (XAdES)
- Dublin Core Metadata Initiative (DCMI) Metadata Terms
- XML Signature Syntax and Processing (Second Edition) – XMLDSIG

1.2. Elérhetőség

A specifikáció aktuális változata a http://www.e-szigno.hu/?lap=eakta30 címen érhető el.

2. Az e-akta formátum rövid bemutatása

Az e-akta egy **XML fájl**, amelyben a bináris elemek (pl. dokumentumok, tanúsítványok) base64 kódolással szerepelnek. Egy e-aktában ***dokumentumok*** helyezkedhetnek el, amelyekhez Dublin Core szerinti ***metaadatok*** kapcsolódhatnak, és a dokumentumokon XAdES ***aláírások*** vagy ***időbélyegek*** lehetnek. Az aláírás vagy időbélyeg vagy csak egyetlen dokumentumhoz, vagy pedig az aktában lévő összes dokumentumhoz kapcsolódik (ez utóbbi esetben ***keretaláírásnak*** vagy ***keretidőbélyegnek*** is nevezzük). A keretaláírások (és keretidőbélyegek) az aktában lévő összes dokumentumon, valamint a dokumentumokon lévő (nem keret-) aláírásokon és időbélyegeken helyezkednek el.

Például, egy e-akta a következő struktúrát követheti:

```
<es:Dossier ... >
<es:DossierProfile>...</es:DossierProfile>
<es:Documents>
  <es:Document>                                <!-- egy beillesztett dokumentum -->
    <es:DocumentProfile>...</es:DocumentProfile>
    <ds:Object>...</ds:Object>                 <!-- a dokumentum base64 kódolással -->
    <ds:Signature>...</ds:Signature>           <!-- aláírás a dokumentumon -->
    <es:TimeStamp>...</es:TimeStamp>           <!-- időbélyeg a dokumentumon -->
  </es:Document>
  <ds:Signature>...</ds:Signature>             <!-- keretaláírás -->
  <es:TimeStamp>...</es:TimeStamp>             <!-- keretidőbélyeg -->
</es:Documents>
```

Az automatizált feldolgozhatóság érdekében minden e-akta rendelkezik valamilyen ***sémával***, amely az e-aktában lévő adatokkal kapcsolatban tartalmazhat megkötéseket. Az alapértelmezett séma csak azt mondja meg, hogy a dokumentumoknak, aláírásoknak, időbélyegeknek és leíró adatoknak milyen sorrendben, struktúrában kell szerepelniük. De egy séma például megkötheti, hogy a sémának megfelelő e-aktákban kizárólag meghatározott számú dokumentum szerepelhet, valamint megkötéseket tartalmazhat a dokumentumok címére, formátumára, illetve a hozzájuk kapcsolódó adatelemekre is. Az e-akta sémája (amely egyben egy XML séma) alapján automatizmus is könnyen tudja ellenőrizni, hogy egy e-akta teljesíti-e ezen követelményeket. Például, ellenőrizni lehet, hogy egy aláírt beadvány tartalmazza-e a szükséges mellékleteket, illetve az automatizmus is könnyen meg tudja különböztetni a beadványhoz csatolt egyes dokumentumokat egymástól (pl. meg tudja állapítani, hogy melyik dokumentum a beadvány, és melyik a csatolt melléklet). A speciális célú sémákkal kapcsolatban lásd a 4. fejezetet.

Az e-akta kiterjesztése **.es3**, átvételi elismervény esetén **.et3** (korábban használt kiterjesztések: .eak, .etv).

A továbbiakban az e-akta formátum specifikációját adjuk meg szöveges formában. Elérhetővé teszünk egy minta sémadefiníciót is, azonban felhívjuk a figyelmet arra, hogy **az irányadó mindig a szöveges leírás**. A minta xsd állomány bizonyos esetekben megengedőbb feltételeket tartalmaz a specifikációban rögzítettekhez képest, ugyanis egyrészt nem minden követelmény írható le formálisan, másrészt a visszafelé való kompatibilitás fenntartása érdekében az xsd állomány opcionálisan tartalmazza a korábban használt, de már nem támogatott elemeket is (amelyek használatát jelen specifikáció már nem engedélyezi). A minta xsd állomány bizonyos más esetekben szigorúbb feltételeket tartalmaz a specifikációban rögzítettekhez képest, ezzel a javasolt alkalmazási módot illusztrálja. A szövegben jelezzük, ha ettől eltérő XML tartalom is engedélyezett egy e-aktában.

A továbbiakban minden szöveges állítás kötelező követelményt fogalmaz meg, ahol nem, ott egyértelműen jelöljük, hogy opcionális követelményről van szó.

3. Az e-akta (es:Dossier) felépítése

Az e-akta egy XML fájl, amelynek gyökere egy `es:Dossier` elem, amely az e-aktában használt névtereket is definiálja (a metaadatokra vonatkozó névtereket nem kötelező itt definiálni). Az e-akta specifikáció a következő névterekre támaszkodik:

- XML Schema namespace:
  `xmlns:xs="http://www.w3.org/2001/XMLSchema"`
- XML Schema instance namespace:
  `xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
- Az XMLDSIG specifikáció névtere:
  `xmlns:ds="http://www.w3.org/2000/09/xmldsig#"`
- A XAdES v1.2.2. specifikáció névtere:
  `xmlns:xades="http://uri.etsi.org/01903/v1.2.2#"`
- A XAdES v1.3.2. specifikáció névtere:
  `xmlns:xades132="http://uri.etsi.org/01903/v1.3.2#"`
- A XAdES v1.4.2. specifikáció által használt névterek:
  `xmlns:xades141="http://uri.etsi.org/01903/v1.4.1#"`
  `xmlns:xades132="http://uri.etsi.org/01903/v1.3.2#"`

Az e-akta sémájának névtere, a továbbiakban: *e-szignó névtér*. Az **„alapértelmezett" sémájú** e-akták esetén az e-szignó névtér:

```
xmlns:es=https://www.microsec.hu/ds/e-szigno30#
```

Más sémájú e-aktákhoz más névtér tartozik. A speciális célú sémákkal kapcsolatban lásd a 4. fejezetet.

A továbbiakban az egyes névtereket a fenti prefixekkel jelöljük. Az e-szignó névtér – amelyet az **`es` prefixszel** jelölünk – kitüntetett szereppel bír, ez határozza meg az e-akta sémáját. Az e-akta sémája lehet a fenti „alapértelmezett" séma, amelyhez a fenti névtér tartozik. Ha az e-akta más sémával rendelkezik, akkor az adott sémához más e-szignó névtér tartozik. A továbbiakban az alapértelmezett sémának megfelelő e-aktákat mutatjuk be, de e-akták más sémákkal is rendelkezhetnek. Minden e-akta séma meg kell, hogy feleljen a fenti, alapértelmezett sémának megfelelő struktúrának, de ezen túl további megkötéseket tehet az e-aktában elhelyezkedő dokumentumok számára és nevére, valamint további elemeket definiálhat a `/es:Dossier/es:DossierProfile` és a `/es:Dossier/es:Documents/es:Document/es:DocumentProfile` elemek alá. (Ezek az e-akta, illetve a dokumentum további, a Dublin Core specifikációban nem definiált metaadatait tartalmazhatják.)

Az `es:Dossier` ezen túl hivatkozást kell, hogy tartalmazzon az adott e-akta névteret leíró XML séma helyére (URL), pl. alapértelmezett esetben:

```
xsi:schemaLocation="https://www.microsec.hu/ds/e-szigno30#
https://www.microsec.hu/ds/e-szigno30.xsd"
```

A gyökér elem a következő elemeket tartalmazhatja: `es:DossierProfile`, `es:Documents`, `ds:Signature`, `es:TimeStamp`.

Az `es:DossierProfile` és `es:Documents` elemekből egy-egy darabnak kell szerepelnie ebben a sorrendben. Ezek után következhet tetszőleges számú (0 vagy több) `ds:Signature` vagy `es:TimeStamp` elem (vagy akár mindkettő) tetszőleges sorrendben (akár váltakozva is).

Megjegyzés: Korábban az `es:Dossier` elemnek volt `AckEmail` és `Location` attribútuma, de ezek már nem használatosak.

Jelen fejezet alfejezetei azon struktúrát határozzák meg, ahogy az e-aktában további elemek helyezkedhetnek el. Amennyiben egy fejezet címe mellett

- **kérdőjel (?)** szerepel, úgy az adott helyen 0 vagy 1 példányban szerepelhet az adott elem (így opcionális).
- **csillag (*)** szerepel, úgy az adott helyen 0 vagy több példányban szerepelhet az adott elem (így opcionális).
- **pluszjel (+)** szerepel, úgy az adott helyen 1 vagy több példányban szerepelhet az adott elem.
- a fenti jelek **egyike sem** szerepel, úgy az adott helyen pontosan 1 példányban szerepelhet az adott elem.

3.1. es:DossierProfile

Az e-akta adatait tartalmazza.

Az `es:DossierProfile` elemnek két attribútuma van: `Id` (kötelező, típusa: xs:ID) és `OBJREF` (nem kötelező, típusa: string). Az `Id` attribútum tartalmazza az elem azonosítóját (amivel hivatkozni lehet rá, pl. a keretaláírásban). Az `OBJREF` attribútum az `/es:Dossier/es:Documents` elem `Id` attribútumára hivatkozik.

Amennyiben az e-aktán keretaláírás vagy keretidőbélyeg helyezkedik el, ezek az `es:DossierProfile` elem integritását is védik.

3.1.1. es:Title

Az e-akta címe, típusa `string`.

3.1.2. es:E-category (?)

Annak meghatározása, hogy az e-akta egyszerű e-akta vagy átvételi elismervény. Típusa `string`. A következő értékekkel rendelkezhet:

- „electronic dossier”: e-akta;
- „electronic acknowledgement”: átvételi elismervény;
- „elektronikus akta”: e-akta, már nem használatos;
- „elektronikus átvételi elismervény”: átvételi elismervény, már nem használatos.

3.1.3. es:CreationDate

Az e-akta létrehozásának időpontja. Típusa `xs:dateTime`.

3.1.4. es:Metadata (?)

Az e-akta Dublin Core szerinti metaadatait tartalmazhatja. A szükséges névtereket itt, az `es:Metadata` elemben kell definiálni. Az `es:Metadata` kötelezően rendelkezik egy `Custom` nevű attribútummal, amelynek értéke „true”. (Ez az elem a minta xsd állományban nem jelenik meg.)

Ezen kívül az `es:DossierProfile` elem további metaadatokat is tartalmazhat (amelyekre például a séma tehet megkötéseket). Ezek esetében az XML elem neve jelenti a metaadat elnevezését, annak egyszerű szöveges tartalma pedig a metaadat értékét. Minden ilyen további metaadat elem kötelezően rendelkezik egy `Custom` nevű attribútummal, amelynek értéke „true”. (Ez a lehetőség a minta xsd állományban egy `xs:any` elem formájában jelenik meg.)

3.2. es:Documents

Az `es:Documents` az e-aktában lévő dokumentumokat tartalmazza. A dokumentumokhoz kapcsolható egyéb adatokról lásd a következő alfejezetet. Az `es:Documents` kizárólag `Id` attribútummal rendelkezik (kötelező, típusa: `xs:ID`).

Amennyiben az e-aktán keretaláírás vagy keretidőbélyeg helyezkedik el, ezek védik az `es:Documents` elem integritását.

3.2.1. es:Document (*)

Az aktában minden egyes dokumentumhoz pontosan egy `es:Document` elem tartozik. Ezen elem tartalmazza magát a dokumentumot, és – ha vannak – a dokumentumhoz tartozó metaadatokat, a dokumentumon lévő aláírásokat és ellenjegyzéseket (azaz a keretaláírásokat nem), valamint időbélyegeket (a keretidőbélyegeket nem). Az aláíráshoz kapcsolódó információkról lásd a 3.2.1.3. `ds:Signature` (*) alfejezetet.

3.2.1.1. es:DocumentProfile

A dokumentum profilját, azaz metaadatait (pl. címét), és a dokumentum megjelenítéséhez szükséges információkat tartalmazza.

Már nem támogatott, de korábban használt elemek az **`es:UsedDispApplication`**, az **`es:SourceLocation`** és az **`es:MimeChecked`** (ezek a sémadefinícióban opcionálisként szerepelnek).

Az `es:DocumentProfile` elemnek két attribútuma van: `Id` (kötelező, típusa: `xs:ID`) és `OBJREF` (nem kötelező, típusa: `string`). Az `Id` attribútum tartalmazza a dokumentum-profil azonosítóját (amivel pl. az aláírások hivatkozhatnak rá). Az `OBJREF` attribútum hivatkozik arra a dokumentumra (`../ds:Object`), aminek a profilja ez az elem. (Mind a `ds:Object` helyére, mind a referenciára vonatkozó követelménynek teljesülnie kell.)

Amennyiben a dokumentumon aláírás vagy időbélyeg helyezkedik el, ezek védik az `es:DocumentProfile` elem integritását.

3.2.1.1.1 es:Title

A dokumentum címe, típusa `string`.

3.2.1.1.2 es:E-category (?)

Annak meghatározása, hogy a szóban forgó dokumentum milyen kategóriába sorolható. Típusa `string`. A következő értékekkel rendelkezhet:

- „electronic data”
- „electronic document”
- „electronic record”
- „elektronikus adat”
- „elektronikus dokumentum”
- „elektronikus irat”
- „electronic profile”
- „elektronikus adatlap”

Ennek a leíró adatnak a használata idővel gyakorlatilag értelmét vesztette; jelenleg – automatikus kitöltés esetén – mindig **„electronic data”** értéket kap. Az elektronikus adat, dokumentum és irat (data, document és record) szerinti kategorizálás eredetileg az elektronikus aláírásról szóló törvényből származik, de ezen megkülönböztetés a törvény 2004. évi módosításával megszűnt.

A magyar nyelvű elnevezések már nem használatosak, azok csak az e-akta specifikáció korábbi verzióival való kompatibilitás végett szerepelnek a sémában.

Az „electronic profile” és az "electronic adatlap" értékek szintén nem használatosak már, a specifikáció korábbi verzióival való kompatibilitás végett szerepelnek a sémában.

3.2.1.1.3 es:CreationDate

Dátum, annak a dátuma, amikor a felhasználó beillesztette a dokumentumot az e-aktába, `xs:dateTime` formátumban.

3.2.1.1.4 es:Format

A dokumentum formátumára vonatkozó információt tartalmaz.

Ha a dokumentum tömörítve került beillesztésre, akkor ez az elem tartalmazza a tömörítés előtti formátumot; egyébként megegyezik a `xades132:SignedProperties` elemben található `xades132:DataObjectFormat` elem tartalmával.

3.2.1.1.4.1 es:MIME-Type

A dokumentum mime típusát adja meg. Attribútumai:

- `type`: a mime főtípus (pl. text),
- `subtype`: a mime altípus (pl. html),
- `extension`: a fájl kiterjesztése (pl. html), opcionális,
- `charset`: a fájlban használt karakterkészlet (pl. utf-8), opcionális.

3.2.1.1.5 es:SourceSize

A `../../ds:Object` dokumentum forrásának mérete. A `sizeValue` attribútum (típusa: `xs:integer`) a byte-okban vett méretet tartalmazza, a `sizeUnit` attribútum értéke kötelezően „B”, ami azt jelenti, hogy a méretet byte-okban kell érteni.

3.2.1.1.6 es:BaseTransform

Megadja, hogy milyen transzformációk során jött létre a beillesztett forrásdokumentumból a `../../ds:Object` elemben lévő base64 kódolt dokumentum. Minden `es:Transform` gyermeke egy-egy transzformációt jelent. Az e-akta specifikáció jelen verziója szerint a következő három transzformáció szerepelhet itt, kizárólag a következő sorrendben:

- zip: zip tömörítés (elhagyható),
- encrypt: S/MIME szerinti titkosítás (elhagyható),
- base64: base64 kódolás (kötelező).

3.2.1.1.6.1 es:Transform (+)

Egy transzformációt ad meg, egy `Algorithm` nevű kötelező attribútummal rendelkezhet (típusa: `string`), amely kizárólag az előző pontban szereplő értékeket veheti fel.

3.2.1.1.7 es:RecipientCertificateList (?)

Titkosított dokumentum esetén megadható, hogy a titkosítás milyen nyilvános kulcsokkal történt. Ezen elem minden egyes gyermeke egy-egy titkosító tanúsítványt sorol fel.

3.2.1.1.7.1 es:RecipientCertificate (+)

Egy base64 kódolású tanúsítványt tartalmaz. Az ezen tanúsítványhoz tartozó magánkulcs segítségével az `../../../ds:Object` elemben lévő dokumentum visszafejthető.

3.2.1.1.8 es:Metadata (?)

A dokumentum Dublin Core szerinti metaadatait tartalmazhatja. A szükséges névtereket itt, az `es:Metadata` elemben kell definiálni. Az `es:Metadata` kötelezően rendelkezik egy `Custom` nevű attribútummal, amelynek értéke „true”. (Ez az elem a minta xsd állományban is látható.)

Ezen kívül az `es:DocumentProfile` elem további metaadatokat is tartalmazhat (amelyekre például a séma tehet megkötéseket). Ezek esetében az XML elem neve jelenti a metaadat elnevezését, annak egyszerű szöveges tartalma pedig a metaadat értékét. Minden ilyen további metaadat elem kötelezően rendelkezik egy `Custom` nevű attribútummal, amelynek értéke „true”. (Ez a lehetőség a minta xsd állományban nem jelenik meg, ennek ellenére engedélyezett.)

3.2.1.2. ds:Object

A beillesztett dokumentumot tartalmazza, base64 kódolással.

Megjegyzés: Az e-akta formátum szerint a base64 kódolás akkor is kötelező, ha a beillesztett dokumentum egy TXT vagy egy XML fájl.

A `ds:Object` elemnek egy kötelező attribútuma van: `Id` (típusa: `xs:ID`), ami az elem egyedi azonosítója.

Az XMLDSIG szerint a `ds:Object` elemnek van két további opcionális attribútuma is: `MimeType` (típusa: `string`) és `Encoding` (típusa: `xs:anyURI`), de ezeket az e-aktában nem használjuk.

Amennyiben a dokumentumon aláírás vagy időbélyeg helyezkedik el, ezek védik az `ds:Object` elem integritását. Ld. még az `es:Document/ds:Signature` és az `es:Document/es:TimeStamp` elemek leírását.

3.2.1.3. ds:Signature (*)

Ezen elem (leszármazottaival együtt) egy XAdES formátumú elektronikus aláírást tartalmaz, amelynek szerkezetét a XAdES és az XMLDSIG specifikációk írják le. Jelen specifikációnak nem célja a `ds:Signature` elemeinek részletes ismertetése, így csak olyan mértékben tárgyaljuk a `ds:Signature` tartalmát, amennyire az az e-akta formátumból eredő megszorítások alkalmazásához szükséges. Az e-akta formátum az aláírással kapcsolatban nem tesz megkötéseket (így az aláírás megfelelhet más ETSI TS 101 903 alapú specifikációknak), az e-akta formátum megszorításai arra vonatkoznak, hogy az aláírás hogyan kapcsolódik az XML fájl többi részéhez, illetve mely részeihez kapcsolódhat.

Megjegyzések:

1. Az ETSI TS 101 903 (XAdES), illetve az XMLDSIG specifikáció nem köti meg, hogy az XML fájlban hol helyezkedhet el `ds:Signature` elem, és nem a `ds:Signature` elem helye, hanem a `ds:Signature/ds:SignedInfo` elem tartalma határozza meg, hogy az `ds:Signature` beli aláírás mire vonatkozik.

   A fentieken túl az e-akta azt is megköti, hogy az XML fájlban hol szerepelhetnek a `ds:Signature` elemek, illetve a `ds:Signature` elem helye meghatározza, hogy az aláírás mire vonatkozik. (A `es:Document/ds:Signature` azt jelenti, hogy az aláírás az adott dokumentumra vonatkozik, míg a `/es:Dossier/ds:Signature` azt jelenti, hogy az aláírás keretaláírás, tehát az e-aktára - és így többek között a benne lévő összes dokumentumra - vonatkozik.) Az e-akta formátum ezen további megszorításokkal jelentős segítséget nyújt az aktát feldolgozó aláírás-ellenőrző alkalmazás számára.

   Az e-akta formátum szerint a `ds:Signature` elem helye és a `ds:Signature/ds:SignedInfo` elemben szereplő referenciák együttesen határozzák meg, hogy az aláírás mire vonatkozik, mindkét követelményrendszernek külön-külön is teljesülnie kell. (Az e-akta formátum ezen túl arra is tartalmaz megkötéseket, hogy a `ds:Signature/ds:SignedInfo` referenciái milyen esetekben mire hivatkozhatnak.)

   A hivatkozások minden esetben Id alapú lokális XML fragment URI-k formájában kell, hogy szerepeljenek a ds:Reference elemek URI attribútumában.

2. A `ds:Reference/ds:Transforms/ds:Transform` elemek Algorithm attribútumában a következő (kanonizációs) transzformációk engedélyezettek:
   - `http://www.w3.org/TR/2001/REC-xml-c14n-20010315`
   - `http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments`
   - `http://www.w3.org/2001/10/xml-exc-c14n#`
   - `http://www.w3.org/2001/10/xml-exc-c14n#WithComments`
   - `http://www.w3.org/2006/12/xml-c14n11`
   - `http://www.w3.org/2006/12/xml-c14n11#WithComments`

   A `ds:Object` elemekre történő hivatkozás esetén a base64 transzformáció is megengedett, sőt, alapértelmezetten alkalmazandó:
   - `http://www.w3.org/2000/09/xmldsig#base64`
3. A `ds:Signature` és az `es:TimeStamp` elemek tetszőleges sorrendben szerepelhetnek.

3.2.1.3.1 ds:SignedInfo

Ezen elem azt írja le, hogy az aláírás mely más elemekre vonatkozik, felépítését az XMLDSIG specifikáció határozza meg. Az e-akta formátum szerint az `es:Document/ds:Signature/ds:SignedInfo` a következő elemekre hivatkozik:

- Az aláírt dokumentumra, azaz a befoglaló `es:Document` `ds:Object` elemére.
- Az aláírás profiljára, azaz a befoglaló `ds:Signature` `ds:Object` elemében található `es:SignatureProfile` elemre.
- Az aláírt dokumentum profiljára, azaz a befoglaló `es:Document` `es:DocumentProfile` elemére.
- A XAdES specifikáció szerinti aláírt információkra, azaz a befoglaló `ds:Signature` `ds:Object/QualifyingProperties/SignedProperties` elemére.
- Ellenjegyzés esetén az ellenjegyzett aláírások (tehát az adott dokumentumon lévő összes előző aláírás) `ds:SignatureValue` elemére és az adott dokumentumon lévő összes előző időbélyeget reprezentáló `es:TimeStamp` elemre.

3.2.1.3.2 ds:SignatureValue

Az aláírás értéke az XMLDSIG specifikáció szerint.

3.2.1.3.3 ds:KeyInfo

Az aláíráshoz használt kulcspárról tartalmaz információt, jellemzően egy X.509 tanúsítvány szerepel benne. Felépítését az XMLDSIG specifikáció határozza meg.

3.2.1.3.4 ds:Object

Az aláírás profilját tartalmazó aláírt objektum, kötelező `Id` attribútummal (típusa: `xs:ID`) rendelkezik.

Az XMLDSIG szerint a ds:Object elemnek van két további opcionális attribútuma is: MimeType (típusa: string) és Encoding (típusa: xs:anyURI), de ezeket az e-aktában nem használjuk.

3.2.1.3.4.1 es:SignatureProfile

Az aláírás profilját fejti ki. A következő attribútumokat tartalmazza:

- **Id:** egyedi azonosító; kötelező, típusa: xs:ID;
- **OBJREF:** hivatkozás az adott (ős) dokumentum ../../../../ds:Object Id attribútumára, típusa string;
- **SIGREF:** hivatkozás az adott (ős) aláírás ds:Signature Id attribútumára, típusa string;
- **SIGREFLIST:** azon URI-k space-szel elválasztott listája, amelyekre az aláírás vonatkozik (ugyanezen lista szerepel az ős aláírás ds:Signature/ds:SignedInfo elemében). Aláírás esetén itt szerepel a hivatkozás a dokumentumra (ez megegyezik az OBJREF értékével), a dokumentum profiljára (es:DocumentProfile), magára a szóban forgó aláírás profilra (es:SignatureProfile), valamint a XAdES ajánlás által definiált xades:SignedProperties (vagy xades132:SignedProperties) elemre. Amennyiben az aláírás ellenjegyzés, akkor a listában szerepel továbbá hivatkozás az ellenjegyzett aláírások ds:SignatureValue elemeire is. A SIGREFLIST attribútum opcionális. Típusa string.

3.2.1.3.4.1.1 es:SignerName

Az aláíró neve, az aláíró tanúsítványának Subject DN / common name mezeje szerint. Típusa string.

3.2.1.3.4.1.2 es:SDPresented (?)

Értéke „true” vagy „false” lehet, azt mondja meg, hogy az aláírás-létrehozó alkalmazás szerint az aláíró megtekintette-e egy biztonságos megjelenítővel az aláírni kívánt dokumentumot.

Egy opcionális attribútuma van, melynek neve server, értéke pedig „true” vagy „false” lehet.

3.2.1.3.4.1.3 es:Type

Típusa string, az aláírás típusát adja meg. A következő értékeket veheti fel:

- „signature”: dokumentumon vagy aktán elhelyezett aláírásról (tehát nem ellenjegyzésről) van szó
- „countersignature”: ellenjegyzésről van szó
- „aláírás”: már nem használatos
- „ellenjegyzés”: már nem használatos

A magyar elnevezések már nem használatosak, az e-akta formátum korábbi verzióival való kompatibilitás miatt szerepelnek a sémában.

3.2.1.3.4.1.4 es:Generator

Azt adja meg, hogy az aláírás milyen programmal illetve eszközzel lett létrehozva.

3.2.1.3.4.1.4.1 es:Program

Az aláírás-létrehozó alkalmazás neve és verziószáma. Két kötelező attribútuma van, mindkettő string. A `name` az alkalmazás nevét, a `version` a verziószámát adja meg.

Példa:

```
<es:Program name="e-Szigno" type="3.1.28.0"/>
```

3.2.1.3.4.1.4.2 es:Device (?)

Az aláírás-létrehozó eszköz neve és típusa. A `name` kötelező attribútum, az eszköz nevét adja meg. A `type` opcionális attribútum. Mindkét attribútum `string`.

Példa:

```
<es:Device name="OpenSSL 0.9.8c" type=""/>
```

3.2.1.3.4.1.5 es:Comment (?)

Az aláíró aláíráskor megjegyzést (vagy pl. záradékot) fűzhet az aláíráshoz, e megjegyzés az aláírás szerepét határozhatja meg. A megjegyzés jellemzően egy csatolt dokumentum. Az `es:Comment` rendelkezhet egy `Type` nevű attribútummal, amely a megjegyzés típusát adja meg. A `Type` a következő értékeket veheti fel:

- „clause” vagy „záradék”
- „gloss” vagy „széljegyzet”
- „comment” vagy „megjegyzés”
- „opinion” vagy „vélemény”

3.2.1.3.4.1.5.1 es:Document (?)

A megjegyzés, mint dokumentum. Felépítését a 3.2.1. fejezet írja le (`/es:Dossier/es:Documents/es:Document`). Az egyetlen lényeges különbség, hogy ezen a dokumentumon nem lehet sem aláírás, sem időbélyeg.

Megjegyzés: E megszorítás a sémában nem jelenik meg.

3.2.1.3.4.1.6 es:SigPolChecked (?)

Megadható, hogy az aláírás-létrehozó alkalmazás ellenőrizte, hogy az aláírás valóban egy adott elektronikus aláírási szabályzat szerint készült-e. Az elem „true” vagy „false” értékeket vehet fel, és opcionális.

3.2.1.3.4.1.7 es:CustomData (?)

Az aláírás tetszőleges metaadatait tartalmazhatja (amelyekre például a séma tehet megkötéseket). A szükséges névtereket itt, az `es:CustomData` elemben kell definiálni.

3.2.1.3.5 ds:Object

Az aláíráson belüli objektum, amely a XAdES kiterjesztéseket tartalmazza.

A `ds:Object` elemnek egy kötelező attribútuma van: `Id` (típusa: `xs:ID`), ami az elem egyedi azonosítója.

Az XMLDSIG szerint a `ds:Object` elemnek van két további opcionális attribútuma is: `MimeType` (típusa: `string`) és `Encoding` (típusa: `xs:anyURI`), de ezeket az e-aktában nem használjuk.

3.2.1.3.5.1 xades:QualifyingProperties vagy xades132:QualifyingProperties

Felépítését, tartalmát a XAdES specifikáció határozza meg.

3.2.1.3.5.1.1 xades:SignedProperties vagy xades132:SignedProperties

Aláírt elemek a XAdES szerint.

A befoglaló `ds:Signature` elem a `ds:SignedInfo` elemében meghivatkozza ezt az elemet is aláírt tartalomként.

3.2.1.3.5.1.2 xades:UnsignedProperties vagy xades132:UnsignedProperties

Nem aláírt elemek a XAdES szerint (pl. az aláírásra kerülő időbélyeg, stb).

3.2.1.4. es:TimeStamp (*)

A szülő `es:Document` elemen elhelyezett XAdES időbélyeget tartalmaz, a típusa a XAdES által definiált `xades:TimeStampType`. Az időbélyeg a következő elemekre hivatkozik `xades:Include` elemekben szereplő lokális XML fragment URI-kkal:

- Az adott dokumentumra, azaz a befoglaló `es:Document ds:Object` elemére.
- Az adott dokumentum profiljára, azaz a befoglaló `es:Document es:DocumentProfile` elemére.

3.3. ds:Signature (*)

Az aktán lévő keretaláírások. Felépítésükben megegyeznek a `//es:Document/ds:Signature` elemmel, egyedüli különbség, hogy keretaláírás esetén a `ds:SignedInfo` elemben lévő referenciák máshova mutatnak. Az `es:Dossier/ds:Signature/ds:SignedInfo` elem a következő elemekre hivatkozik:

- `/es:Dossier/es:Documents` elemre – az aktában lévő összes dokumentumra, és rajtuk minden aláírásra.
- Az aláírás profiljára, azaz az adott `ds:Signature` elemen belül lévő `ds:Object`-ben lévő `es:SignatureProfile` elemre.
- Az e-akta profiljára, azaz az `/es:Dossier/es:DossierProfile` elemre.
- A XAdES szerinti aláírt információkra, azaz az adott `ds:Signature` elemen belül lévő `ds:Object`-ben lévő `QualifyingProperties`-ben lévő `SignedProperties` elemre.

- Ellenjegyzés esetén az ellenjegyzett aláírások (az összes, `es:Dossier` elem alatt található, az adott aláírást megelőző aláírás) `ds:SignatureValue` elemeire illetve az összes előző, `es:Dossier` alatt található `es:TimeStamp` elemre.

A dokumentumon lévő aláírásnál lévő `ds:Signature` elemnél tett, `ds:Reference`-ekre és `es:Transform`-okra vonatkozó megjegyzések itt is érvényesek.

A `ds:Signature` és az `es:TimeStamp` elemek tetszőleges sorrendben szerepelhetnek.

3.4. es:TimeStamp (*)

Az e-aktán elhelyezett keretidőbélyeget tartalmaz, a típusa `xades:TimeStampType`. Az időbélyeg a következő elemekre hivatkozik `xades:Include` elemekben szereplő lokális XML fragment URI-kkal:

- Az e-aktában lévő összes dokumentumra, azaz az `/es:Dossier/es:Documents` elemre.
- Az e-akta profiljára, azaz az `/es:Dossier/es:DocumentProfile` elemre.

4. Speciális célú sémák

Az e-akta formátum ideális formátum az elektronikus ügyintézés támogatására, hiszen a segítségével összefogottan kezelhetőek az adott ügyhöz tartozó iratok. Speciális felhasználási területek esetében szükség lehet arra, hogy egy e-akta belső felépítésére vonatkozóan további megkötéseket tegyünk. Például megköthető, hogy az e-aktában kizárólag meghatározott számú dokumentum szerepelhet, vagy megkötéseket tartalmazhat a dokumentumok címére, formátumára, illetve a hozzájuk kapcsolódó adatelemekre is.

Jelenleg is több ilyen speciális, az alap struktúrának megfelelő, de többlet követelményeket tartalmazó séma van forgalomban. Ezek mindegyike saját névtérrel rendelkezik, de definíció szerint ezeket is e-aktának nevezzük.

A speciális sémás e-aktákban az `es:` prefixet kell a séma saját névteréhez rendelni (amely az eddigiekben bemutatott Alapértelmezett séma esetében a `https://www.microsec.hu/ds/e-szigno30#` értéket kapja). Specializált sémás e-aktában tehát mindegyik, a fentiekben `es:` prefixszel bemutatott elem a séma saját névterébe kerül.

A speciális sémák és névtereik a következők:

Séma neve	**XML névtér**
Beszámoló	`http://www.e-cegjegyzek.hu/2006/beszamolo#`
Beszámoló 2008	`http://www.e-cegjegyzek.hu/2008/beszamolo#`
Céginformáció kérés	`http://www.e-cegjegyzek.hu/2006/ceginformacio_keres#`
Cégtörvényességi ügy	`http://www.e-cegjegyzek.hu/2014/cegtorvenyessegi#`
e-Cégeljárás	`http://www.e-cegjegyzek.hu/2006/e-cegeljaras#`
e-Cégeljárás 2007	`http://www.e-cegjegyzek.hu/2007/e-cegeljaras#`
e-Cégeljárás 2009	`http://www.e-cegjegyzek.hu/2009/e-cegeljaras#`
e-Cégeljárás 2012	`http://www.e-cegjegyzek.hu/2012/e-cegeljaras#`
e-Cégeljárás 2014	`http://www.e-cegjegyzek.hu/2014/e-cegeljaras#`
Értékbecslő	`http://schema.e-szigno.hu/schema/raiffeisen_ertekbecslo2012#`
Irattár 2013	`http://schema.e-szigno.hu/schema/msc_irattar2013#`
Kérelmek	`http://www.e-cegjegyzek.hu/2005/kerelmek#`
Közjegyzői 2008	`http://www.e-szigno.hu/2008/kozjegyzo2008`
Közjegyzői 2009	`http://www.e-szigno.hu/2009/kozjegyzo20090119#`
Közjegyzői 2010	`http://www.e-szigno.hu/2010/kozjegyzo20100101#`
Mérleg	`http://www.e-cegjegyzek.hu/2005/merleg#`
OCCSZ	`http://www.e-cegjegyzek.hu/2005/occsz#`

5. Kivételek

Kivételes esetben e-aktának tekintjük az olyan állományokat is, amelyek megfelelnek a jelen specifikációnak azzal az eltéréssel, hogy a `/es:Dossier/es:Documents` elemen belül tartalmaznak egy vagy több olyan `es:Document` elemet, amely kizárólag egy üres `ds:Object` elemet foglal magában. (Ez a minta xsd szerint nem felelne meg, mivel hiányzik belőle az `es:DocumentProfile` elem.)

Továbbá szintén e-aktának tekintjük az olyan állományokat is, amelyek a fenti leírás szerint már nem használatos, de korábban használt attribútumokat (pl. `AckEmail`, `Location`) vagy elemeket (pl. `es:UsedDispApplication`, `es:SourceLocation`, `es:MimeChecked`) tartalmaznak, vagy valamelyik elem tartalma a rá vonatkozó felsorolásban már nem használatosként megjelölt értékek egyike.

Az e-akta kezelő alkalmazásnak az ilyen állományok megjelenítését célszerű támogatnia, azonban új e-akta létrehozáskor a 3. fejezetben leírt követelményeknek szigorúan megfelelő állományt kell készítenie.

6. Alapértelmezett e-akta XML séma minta

```
<?xml version="1.0" encoding="ISO-8859-2"?>
<schema targetNamespace="https://www.microsec.hu/ds/e-szigno30#"
xmlns:es="https://www.microsec.hu/ds/e-szigno30#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xades="http://uri.etsi.org/01903/v1.2.2#"
xmlns:mireg="http://mireg.org/schema/1.0/"
xmlns="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="xmldsig-core-schema.xsd"/>
  <import namespace="http://uri.etsi.org/01903/v1.2.2#"
schemaLocation="XAdES.xsd"/>
  <import namespace="http://uri.etsi.org/01903/v1.3.2#" schemaLocation="XAdES-
1.3.2.xsd"/>
  <import namespace="http://mireg.org/schema/1.0/"
schemaLocation="metadata.xsd"/>
  <element name="Dossier">
    <complexType>
      <sequence>
        <element name="DossierProfile">
          <complexType>
            <sequence>
              <element name="Title" type="string"/>
              <element name="E-category" minOccurs="0">
                <simpleType>
                  <restriction base="string">
                    <enumeration value="electronic dossier"/>
                    <enumeration value="electronic acknowledgement"/>
                    <enumeration value="elektronikus akta"/>
                    <enumeration value="elektronikus átvételi elismervény"/>
                  </restriction>
                </simpleType>
              </element>
              <element name="CreationDate" type="dateTime"/>
              <any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
            </sequence>
            <attribute name="Id" type="ID" use="required"/>
            <attribute name="OBJREF" type="string"/>
          </complexType>
        </element>
        <element name="Documents">
          <complexType>
            <sequence>
              <element ref="es:Document" minOccurs="0" maxOccurs="unbounded"/>
            </sequence>
            <attribute name="Id" use="required">
              <simpleType>
                <restriction base="ID">
                  <enumeration value="Object0"/>
                </restriction>
              </simpleType>
            </attribute>
          </complexType>
        </element>
        <choice minOccurs="0" maxOccurs="unbounded">
          <element ref="ds:Signature"/>
          <element name="TimeStamp" type="xades:TimeStampType"/>
        </choice>
      </sequence>
      <attribute name="AckEmail">
```

```
      <simpleType>
        <restriction base="string">
          <pattern value="([^@]+@[^\.]+\..+)?"/>
        </restriction>
      </simpleType>
    </attribute>
    <attribute name="Location" type="string"/>
  </complexType>
</element>
<element name="Document">
  <complexType>
    <sequence>
      <element name="DocumentProfile">
        <complexType>
          <sequence>
            <element name="Title" type="string"/>
            <element name="E-category" minOccurs="0">
              <simpleType>
                <restriction base="string">
                  <enumeration value="electronic data"/>
                  <enumeration value="electronic document"/>
                  <enumeration value="electronic record"/>
                  <enumeration value="elektronikus adat"/>
                  <enumeration value="elektronikus dokumentum"/>
                  <enumeration value="elektronikus irat"/>
                  <enumeration value="electronic profile"/>
                  <enumeration value="elektronikus adatlap"/>
                </restriction>
              </simpleType>
            </element>
            <element name="CreationDate" type="dateTime"/>
            <element name="Format">
              <complexType>
                <sequence>
                  <element name="MIME-Type">
                    <complexType>
                      <attribute name="type"/>
                      <attribute name="subtype"/>
                      <attribute name="extension"/>
                      <attribute name="charSet"/>
                    </complexType>
                  </element>
                </sequence>
              </complexType>
            </element>
            <element name="UsedDispApplication" minOccurs="0">
              <complexType>
                <attribute name="name"/>
                <attribute name="version"/>
              </complexType>
            </element>
            <element name="MimeChecked" minOccurs="0">
              <complexType>
                <simpleContent>
                  <extension base="boolean">
                    <attribute name="executed" type="boolean"/>
                  </extension>
                </simpleContent>
              </complexType>
            </element>
            <element name="SourceLocation" type="string" minOccurs="0"/>
            <element name="SourceSize">
              <complexType>
```

```
            <attribute name="sizeValue" type="integer"/>
            <attribute name="sizeUnit" fixed="B"/>
          </complexType>
        </element>
        <element name="BaseTransform">
          <complexType>
            <sequence maxOccurs="unbounded">
              <element name="Transform">
                <complexType>
                  <attribute name="Algorithm">
                    <simpleType>
                      <restriction base="string">
                        <enumeration value="zip"/>
                        <enumeration value="encrypt"/>
                        <enumeration value="base64"/>
                      </restriction>
                    </simpleType>
                  </attribute>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
        <element name="RecipientCertificateList" minOccurs="0">
          <complexType>
            <sequence>
              <element name="RecipientCertificate" maxOccurs="unbounded"/>
            </sequence>
          </complexType>
        </element>
        <element name="Metadata" minOccurs="0">
          <complexType>
            <sequence>
              <element ref="mireg:metadata"/>
            </sequence>
            <attribute name="Custom" type="boolean" fixed="true"/>
          </complexType>
        </element>
      </sequence>
      <attribute name="Id" type="ID" use="required"/>
      <attribute name="OBJREF" type="string"/>
    </complexType>
  </element>
  <element ref="ds:Object"/>
  <choice minOccurs="0" maxOccurs="unbounded">
    <element ref="ds:Signature"/>
    <element name="TimeStamp" type="xades:TimeStampType"/>
  </choice>
 </sequence>
</complexType>
</element>
<element name="SignatureProfile">
  <complexType>
    <sequence>
      <element name="SignerName" type="string"/>
      <element name="SDPresented" minOccurs="0">
        <complexType>
          <simpleContent>
            <extension base="boolean">
              <attribute name="server" type="boolean"/>
            </extension>
          </simpleContent>
        </complexType>
```

```
        </element>
        <element name="Type">
          <simpleType>
            <restriction base="string">
              <enumeration value="signature"/>
              <enumeration value="countersignature"/>
              <enumeration value="aláírás"/>
              <enumeration value="ellenjegyzés"/>
            </restriction>
          </simpleType>
        </element>
        <element name="Generator">
          <complexType>
            <sequence>
              <element name="Program">
                <complexType>
                  <attribute name="name"/>
                  <attribute name="version"/>
                </complexType>
              </element>
              <element name="Device" minOccurs="0">
                <complexType>
                  <attribute name="name"/>
                  <attribute name="type"/>
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
        <element name="Comment" minOccurs="0">
          <complexType mixed="true">
            <sequence>
              <element ref="es:Document" minOccurs="0"/>
            </sequence>
            <attribute name="Type">
              <simpleType>
                <restriction base="string">
                  <enumeration value="clause"/>
                  <enumeration value="gloss"/>
                  <enumeration value="comment"/>
                  <enumeration value="opinion"/>
                  <enumeration value="záradék"/>
                  <enumeration value="széljegyzet"/>
                  <enumeration value="megjegyzés"/>
                  <enumeration value="vélemény"/>
                </restriction>
              </simpleType>
            </attribute>
          </complexType>
        </element>
        <element name="SigPolChecked" type="boolean" minOccurs="0"/>
        <element name="CustomData" minOccurs="0">
          <complexType>
            <sequence>
              <any namespace="##any" minOccurs="0" maxOccurs="unbounded"
processContents="lax"/>
            </sequence>
          </complexType>
        </element>
      </sequence>
      <attribute name="Id" type="ID" use="required"/>
      <attribute name="OBJREF" type="string"/>
      <attribute name="SIGREF" type="string"/>
```

```
      <attribute name="SIGREFLIST" type="string"/>
    </complexType>
  </element>
  <element name="Metadata">
    <complexType>
      <sequence>
        <element ref="mireg:metadata"/>
      </sequence>
      <attribute name="Custom" type="boolean" fixed="true"/>
    </complexType>
  </element>
</schema>
```