MICROSEC

Számítástechnikai Fejlesztő zrt.

Végrehajtási Iratok Elektronikus Kézbesítési Rendszere (VIEKR)

Státusz:	munkaverzió
Verzió:	0.94
Dátum:	2012. szeptember 2.
Kezelési mód:	Nyilvános

Microsec Számítástechnikai Fejlesztő zrt.

1031 Budapest, Záhony u. 7.

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
0.7	Első változat	2012. március 7.	Szabóné Endrődi Csilla
0.8	Pontosítások, példák szerepeltetése	2012. március 28.	Szabóné Endrődi Csilla
0.9	Közlemény fogalmának bevezetése, Értesítés fogalmának pontosítása, KüldeményAzonosító helyett Azonosító használata; Küldemény, tértivevény, feladóvevény állapotaina kpontosítása VHKIR kliens funkcióinak pontosítása	2012. április 1.	Szabóné Endrődi Csilla
0.91	„VHKIR kommunikációs modul” elnevezés bevezetése A VHKIR rövidítés magyarázata	2012. április 24.	Szabóné Endrődi Csilla
0.92	Küldemény „letöltött” állapot helyett „kézbesített” használata Az „E-mail kézbesítési állapotok” megszüntetése Az 5. fejezet új címet kapott	2012. május 21.	Szabóné Endrődi Csilla
0.93	Kommunikációs modul funkcióinak pontosítása	2012. július 2.	Szabóné Endrődi Csilla
0.94	A VHKIR rövidítés VIEKR-re való átírása; Az alap URL megadása; A lehetséges szervezet típusok felsorolása	2012. szeptember 2.	Szabóné Endrődi Csilla

Tartalomjegyzék

1. Bevezetés

A dokumentum a magyar önálló bírósági végrehajtók és a végrehajtási ügyekben velük hivatalos kapcsolatban álló felek közötti elektronikus kommunikáció leírását tartalmazza.

Az informatikai rendszer elsődleges célja, hogy a Magyar Bírósági Végrehajtói Kamarával kapcsolatban álló felek és az eljárásban részt vevő egyéb személyek a végrehajtási eljárások során az egyes végrehajtókkal elektronikus okirati formában legyenek képesek kommunikálni. Az üzenetközvetítő rendszerben az elektronikus okiratok hitelességét a 2001. évi XXXV. törvény (továbbiakban: Eat.) szerinti elektronikus aláírás és időbélyeg biztosítja, bizalmasságukat pedig a felek részére történő tanúsítvány alapú titkosítás valósítja meg. A kézbesítési rendszer megfelel a 2011. december 13-án módosított, a bírósági végrehajtásról szóló 1994. évi LIII. törvényben (továbbiakban: Vht.) foglalt követelményeknek a végrehajtási iratok elektronikus kézbesítésével kapcsolatban.

A végrehajtók és a végrehajtást kérők közötti elektronikus kommunikáció megvalósítására 2011-ben létrehozásra került rendszer a Végrehajtást Kérők Informatikai Rendszere (VHKIR). Jelen rendszer ennek továbbfejlesztése, amely a Kamara döntése alapján a törvényben nevesített „Végrehajtási Iratok Elektronikus Kézbesítési Rendszere”, amelynek rövidítése VIEKR (de a VHKIR rövidítés még egyes helyeken előfordulhat).

1.1. Dokumentum hatóköre

Jelen dokumentum hivatott meghatározni, hogy az egyes végrehajtók és a velük kapcsolatban álló felek között az elektronikus kommunikáció milyen csatornán, milyen formában történik milyen peremfeltételek mellett. A dokumentum továbbá meghatározza, hogy az üzenetközvetítő rendszerhez csatlakozó feleknek milyen infrastrukturális feltételeknek kell megfelelniük, hogy sikeresen részt vehessenek a folyamatban.

A kommunikáció közbenső szereplője a Magyar Bírósági Végrehajtói Kamara által üzemeltetett központi szolgáltató szerver (későbbiekben: Központi szerver).

1.2. Hivatkozott dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

A bírósági végrehajtásról szóló 1994. évi LIII. törvény

Felhasználási szabályzat

VIEKR üzenetformátum specifikáció

VHKIR kommunikációs modul leírása

Microsec Megbízható üzenettovábbító szerver interfészének leírása

2. Fogalmak

Üzenet: A „VIEKR üzenetformátum specifikáció” című dokumentumban meghatározott, a hivatkozott XML sémának megfelelő XML dokumentum, amely tartalmilag alkalmas arra, hogy a végrehajtási ügyekkel kapcsolatban kérdéseket illetve válaszokat tartalmazzon. Egy üzenethez tartozhat egy vagy akár több, kötött formátumú csatolmány is, amelyeket a rendszer együttesen (egyazon e-aktában) továbbít az XML dokumentummal.

Aláírt üzenet: Olyan *üzenet*, amit feladója elektronikus aláírással látott el. Egy ilyen aláírás legalább XAdES-T típusú kell legyen, azaz minősített időbélyeget is kell tartalmazzon.

Titkosított üzenet: Olyan *aláírt üzenet*, amit feladója titkosított a címzett(ek) számára.

Küldemény: Az üzenetközvetítő rendszerben továbbítható adategység, amely a titkosított üzenetnek a továbbításhoz szükséges információkkal (meghatározott metaadatokkal) kiegészített változata.

Feladóvevény: A Központi szerver által elektronikusan aláírt, időbélyegzett, szabványos elismervény arról, hogy továbbításra átvette a hivatkozott e-aktát.

Tértivevény: A címzett által elektronikusan aláírt, időbélyegzett, szabványos elismervény arról, hogy a címzett átvette a hivatkozott e-aktát.

Hibajelentés: Hibajelentés XML-t tartalmazó küldemény. Hibajelentést kell küldeni akkor, ha egy átvett küldemény kititkosítása során, vagy a benne található XML informatikai ellenőrzése során hiba merül fel. A hibajelentés típusú küldeményben a metaadatok között található hivatkozás az eredeti küldeményre.

Közlemény: A rendszerben továbbított adategységek (küldemény, hibajelentés, feladóvevény és tértivevény) összefoglaló neve.

Értesítés: Az értesítés a küldemény meghatározott (meta)adatait tartalmazó XML struktúra. Az üzenetközvetítő rendszer egy értesítést tesz elérhetővé a címzett számára, amennyiben számára új küldemény érkezett. A címzett szoftvere az értesítés segítségével tudja elkészíteni a tértivevényt.

Központi szerver: Az üzenetközvetítő rendszer megbízható üzenettovábbító egysége.

Szervezet: A Központi szerverre regisztrált szervezetek (végrehajtói irodák, pénzintézetek, illetve egyéb, a végrehajtókkal hivatalos kapcsolatban álló szervezetek), akik jogosultak küldemények küldésére és fogadására. Egy regisztrált szervezethez tartozhat több, saját tanúsítványokkal rendelkező felhasználó (akár automata) is, akik egyenértékűen tudják kezelni a szervezet által kapott vagy küldött küldeményeket. Az üzenetküldő rendszerben a feladók és címzettek mindig a szervezetek.

Felhasználó: A Központi szerverre regisztrált felhasználók, akik rendelkeznek egy aláíró és egy titkosító tanúsítvánnyal, valamint egy authentikációs tanúsítvánnyal vagy felhasználónév/jelszó párossal. A rendszer üzenetküldő funkcionalitását akkor tudják használni, ha szervezethez vannak rendelve.

Kliens oldal: A rendszer felhasználóinak (feladók és címzettek) informatikai környezete, amely küldemények beküldése és fogadása céljából csatlakozik a Központi szerverhez.

VHKIR kommunikációs modul: A kliens oldalon megvalósítandó szoftvermodul, amely összekapcsolja a kliensek saját informatikai rendszerét az üzenetküldő rendszerrel.

Feladás dátuma: A küldemény feladásának dátuma a feladóvevényben szereplő időpont.

Átvétel dátuma: A küldemény átvételének dátuma a tértivevényben szereplő időpont.

VHKIR: Végrehajtást Kérők Informatikai Rendszere

VIEKR: Végrehajtási Iratok Elektronikus Kézbesítési Rendszere

3. A rendszer általános bemutatása

3.1. Üzenet előállítása és feldolgozása

A végrehajtók és a velük kapcsolatban álló felek rendszerei egymással **XML formátumú üzeneteken** keresztül kommunikálnak.

Az elküldendő üzenet XML-t a küldő félnek kell előállítania saját informatikai környezetében. (Ez történhet úgy, hogy az ügyintéző a saját gépén futó programjában megadja a kért adatokat, de automatizmus is készítheti egy adatbázis alapján.)

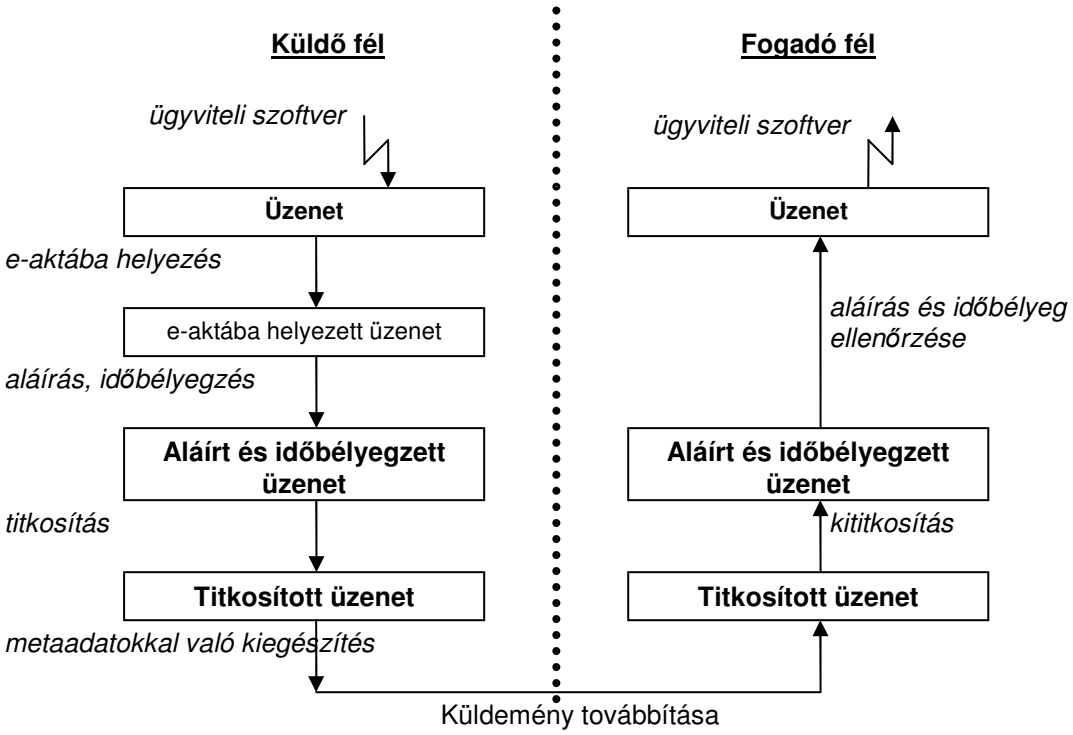
A válaszként kapott üzenet XML feldolgozása szintén a felhasználó rendszerének feladata. A gépi adatfeldolgozás elősegítése érdekében a küldhető XML-ek köre szabályozott.

A VIEKR rendszerben a Felhasználási Szabályzatnak megfelelően csak a „VIEKR üzenetformátum specifikáció” című dokumentumban meghatározott formátumú XML állományok küldhetőek[12]. Egy üzenethez egy vagy több, kötött formátumú csatolmány is tartozhat, amelyeket a rendszer együttesen továbbít az XML dokumentummal.

3.2. Küldemény előállítása és feldolgozása

A küldő fél által előállított XML üzenetet be kell helyezni egy e-aktába, amelyet **időbélyeges aláírással** kell ellátni. Ezt követően **titkosítani** kell a címzett(ek) számára. Az így létrejött e-aktát (címzési információkkal kiegészítve) kell elküldeni a rendszer segítségével a fogadó félnek.

A fogadó oldal a kapott e-aktát kititkosítja, ellenőrzi az aláírását. Ezt követően feldolgozza az e-aktában szereplő XML állományt. Amennyiben választ kell rá küldenie, akkor összeállítja a választ szintén XML formátumban, és az előbbivel egyező módon csomagolja és visszajuttatja azt az eredeti feladónak.



1. ábra: Teendők üzenet küldés illetve fogadás esetén

[1] A dokumentáció tartalmazza a korábbi pénzintézeti megkeresések rendszerében használt megkereséseket és valaszokat is.

[2] A meghatározott formátumhoz tartozó XML sémákat a kamara a VHKIR üzenetformátum specifikációban megadott központi helyen közzé teszi.

3.3. Megbízható üzenettovábbítás

A küldemények címzetthez való eljuttatása a **Központi szerveren** keresztül történik. A Központi szerver egy megbízható üzenettovábbító egység, amely **átveszi**, és a küldemény fogadásáig (illetve meghatározott időtartamig) **tárolja** a küldeményeket. A hozzá feltöltött küldemények átvételét **feladóvevények** készítésével igazolja, illetve a címzett féltől kikényszerített **tértivevény** visszajuttatásával nyújt bizonyítékot a küldemény címzett által történő átvételéről. A küldemények **kézbesítési státusza** bármikor lekérdezhető.

A rendszeren keresztül küldött üzenetek tartalmát a szerver semmilyen módon nem tudja megismerni az alkalmazott **titkosítási** eljárásnak köszönhetően. A felek az üzenetek hitelességéről és készítésük időpontjáról az **elektronikus aláírás** és **időbélyeg** ellenőrzése révén szerezhetnek bizonyságot.

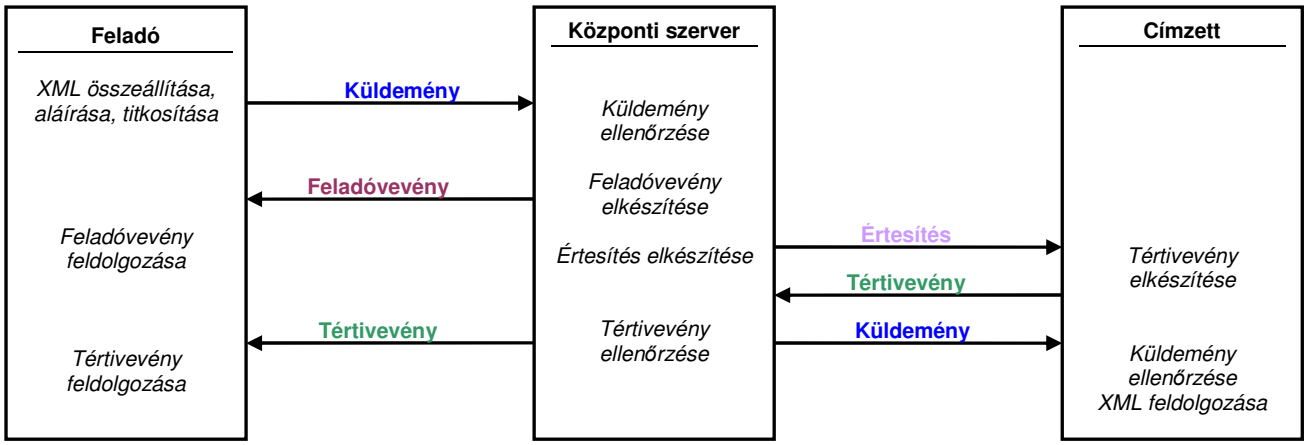
3.4. A kommunikáció folyamata

Az alábbiakban részletezzük a kommunikációs folyamat során szükséges lépéseket:

1. A feladó előállítja a küldendő XML állományt, e-aktába helyezi, időbélyeges aláírással látja el, és titkosítja az e-aktát a címzett(ek) részére.
2. A feladó megküldi az előállított küldeményt a Központi szervernek.
3. A Központi szerver ellenőrzi a beérkezett küldeményt (valóban titkosított e-akta-e, és hogy a megfelelően lett-e titkosítva). Helyes küldemény esetén a továbbításra történő átvételről aláírt és időbélyegzett feladóvevényt ad a feladónak, hibás küldemény esetén elutasítja a továbbítást.
4. Helyes küldemény esetén a Központi szerver egy értesítést teszt elérhetővé a címzett számára.
5. A címzett szoftvere letölti az új értesítést, ami alapján elkészíti a tértivevényt és visszajuttatja a Központi szervernek. A szerver ellenőrzi a tértivevényt.
6. Helyes tértivevény beérkezése esetén a szerver elérhetővé teszi a címzett számára a küldeményt. A címzett szoftvere letölti az új küldeményt.
7. A címzett szoftvere a letöltött küldeményt kititkosítja, megvizsgálja, hogy van-e aláírás az e-aktában, elvégzi az e-aktában elhelyezett aláírás ellenőrzését, ellenőrzi a kapott XML állományt formai szempontból. Amennyiben helyes küldeményt kapott, az XML állomány tartalmát feldolgozza (pl. betölti az ügyviteli szoftver adatbázisába).
8. Amennyiben hibás küldeményt kapott, akkor előállít egy hibajelentést, és a Központi szerveren keresztül eljuttatja a feladó részére. A hibajelentés kézbesítése ugyanúgy történik, mint a küldeményeké.
9. Miután a címzett letöltötte a küldeményt, a Központi szerver elérhetővé teszi a feladó számára a címzett által készített tértivevényt.

A címzett a beérkezett üzenetre küldendő válaszát – amennyiben szükséges – egy új küldemény formájában tudja eljuttatni a feladónak. Az előzmény üzenet azonosítóját, illetve minden további azonosítót (pl. ügy azonosítók a feladó illetve címzett rendszerében) a legbelső XML állomány tartalmazza (lásd: VHKIR üzenetformátum specifikáció).

A következő ábra szemléletesen bemutatja a fent ismertetett folyamatot.



2. ábra: A küldemény továbbítás folyamata

A feladóvevény jelentése: „A hivatkozott küldemény megfelel a továbbítás kritériumainak, a küldeményt a szerver továbbításra átvette.” A küldemény **feladásának időpontja** a feladóvevény aláírásának időpontja.

A tértivevény jelentése: „A hivatkozott küldeményt adott szervezet nevében átvettem.” A küldemény **kézbesítésének időpontja** a tértivevény aláírásának időpontja.

Az alkalmazott titkosítási eljárás miatt a szerver a küldemények belsejében utazó XML üzeneten nem tud formátumellenőrzést végezni. Ezért ha abban van hiba, az csak a fogadó félnél, a titkosítás feloldását követően fog kiderülni. Ebben az esetben a fogadó fél egy hibajelentésben tájékoztatja erről a feladó felet. A hibajelentés XML az informatikai ellenőrzés eredményét tartalmazza formálisan, ez automatizmus által elkészíthető. A hibajelentés XML-t a fogadó fél ugyanúgy „csomagolja” (aláírja, titkosítja, metaadatokkal látja el), mint bármely más üzenet XML-t, de a metaadatok között szerepelteti a hivatkozott küldemény azonosítóját, és a normál küldeményekkel megegyező módon továbbítja a Központi szerver felé. Ez egyben azt is jelenti, hogy a hibajelentésről is kap feladóvevényt és tértivevényt. Hibajelentésre azonban nem lehet hibajelentéssel válaszolni (ezt a rendszer figyeli).

A VIEKR rendszerben egy küldemény küldhető egyszerre **több címzettnek** is. Ekkor is egy feladóvevény, de természetesen több tértivevény érkezik rá.

3.5. Küldemények kézbesítési státuszai

A Központi szervertől bármikor lekérdezhetőek a beküldött küldemények kézbesítési státuszával kapcsolatos információk. A legfontosabb alapadatok (feladás dátuma, kézbesítés dátuma, feldolgozási állapot, kézbesítési állapot, hibajelentés) mellett a kapott adatok alapján elérhetőek a küldeményhez tartozó feladóvevény, tértivevény(ek) és hibajelentés(ek) is.

3.6. Címzés: szervezetek és felhasználók

A VIEKR rendszerben az üzenettovábbítás **szervezetek** között történik, azaz a feladó és a címzett mindig egy szervezet. Egy szervezetnek lehet több felhasználója, akik a szervezet küldeményeit egyenrangúan tudják kezelni.

Továbbá, egy felhasználó tartozhat több szervezethez is. Ekkor a felhasználó az összes szervezetének küldeményeit (és minden kapcsolódó adategységet) kezelhet[3].

Az üzenetközvetítő rendszert csak regisztrált szervezetek regisztrált felhasználói használhatják[4]. A felhasználók vagy a megadott authentikációs tanúsítvány alapján, vagy a felhasználónév/jelszó alapján végzett azonosítást követően használhatják a rendszert.

Előfordulhat (pl. a pénzintézeti megkeresések esetében), hogy egy feladó egy adott küldeményt egyszerre több címzett szervezetnek is el kíván küldeni. A VIEKR-ben is van erre lehetőség, ekkor a küldemény metaadatai között az összes címzett szervezet azonosítóját meg kell adni.

3.7. Titkosító tanúsítványok központi nyilvántartása

A VIEKR rendszerben a küldemények titkosított formában tartalmazzák az üzeneteket. A titkosítást úgy kell elvégezni, hogy azt a címzett szervezet(ek) minden felhasználója, valamint a feladó szervezet minden felhasználója fel tudja oldani (és senki más). Ennek érdekében a titkosítást el kell végezni a címzett szervezet(ek) és a feladó szervezet minden felhasználójának számára[5]. Ehhez titkosításkor ismerni kell a két (több) szervezet aktuális felhasználóinak aktuális titkosító tanúsítványait.

[3] Az egyes szervezetek küldeményeinek elkülönítését ekkor a felhasználó rendszerében kell megoldani. A szerverrel való kommunikációban lehetőség van arra, hogy egyszerre csak egy megadott szervezethez kapcsolódó adatokat kérjük le.

[4] A regisztráció a Vht-ban megfogalmazott feltételek szerint történik, a részleteket a rendszer „Szolgáltatási szabályzat” című dokumentuma tartalmazza.

[5] PKI alapú titkosítást alkalmazunk: az üzenet először kódolásra kerül egy egyedi szimmetrikus kulccsal, majd csak ez a kulcs kerül kódolásra a címzett szervezet és a feladó szervezet minden felhasználójának számára, az ő titkosító tanúsítványukban szereplő nyilvános kulccsal.

A Központi szerver nyilvántartja a regisztrált felhasználóinak aktuális titkosító tanúsítványait. Annak érdekében, hogy az üzenet titkosításakor mindig a megfelelő tanúsítványok kerüljenek felhasználásra, azokat a küldemény elkészítésekor a felhasználó szoftvermodul egyezteti a szerverrel.

3.8. Kézbesítési vélelem beállta

A Vht. szerint a kézbesítési vélelem akkor is beáll, ha a címzett a feladást követően ötödik munkanap elteltével sem veszi át a küldeményt (nem ad rá tértivevényt). Azaz, a küldemény legkésőbb a feladást követő 6. munkanapon kézbesítettnek minősül.

Ha a kézbesítési vélelem azáltal következett be, hogy öt munkanapon belül a címzett nem vette át a küldeményt, akkor ennek tényét a Központi szerver rögzíti egy aláírt nyilatkozatban, és ezt tértivevényként visszajuttatja az eredeti feladónak és a címzettnek, valamint a küldeményt elektronikus levélben kiküldi a címzett szervezetnek a regisztrációkor megadott e-mail címére.

3.9. Küldemények és bizonyítékelemek megőrzése

A Vht-nak megfelelően a rendszer a feladóvevényeket és tértivevényeket, valamint a küldemények metaadatait 10 évig megőrzi. Szintén a törvényi előírásoknak megfelelően, a küldeményt a kézbesítés beálltát követően 30 nappal törli a rendszerből.

3.10. Üzenetsémák központi nyilvántartása

A VIEKR rendszerben csak a „VIEKR üzenetformátum specifikáció” című dokumentumban meghatározott formátumú XML állományok küldhetőek – ide tartozik a pénzintézeti megkeresések rendszerében használt megkeresés és válasz is. A meghatározott formátumokhoz tartozó XML sémákat a kamara a dokumentációban megadott központi helyen közzé teszi.

A feltételnek való megfelelés érdekében a felhasználók szoftvermoduljának elküldés előtt ellenőrizniük kell, hogy az összeállított üzenet XML megfelel-e az aktuális XML sémának. Fel kell készülni arra, hogy a sémák adott esetben módosításra kerülhetnek, illetve idővel újabbak kerülnek bevezetésre. A Központi szerver nyilvántartja az aktuálisan használható sémákat a megfelelő verzióban, így a felhasználó szoftvermodulja szinkronizálhatja saját adatbázisát.

4. A rendszer működésének részletes bemutatása

4.1. REST

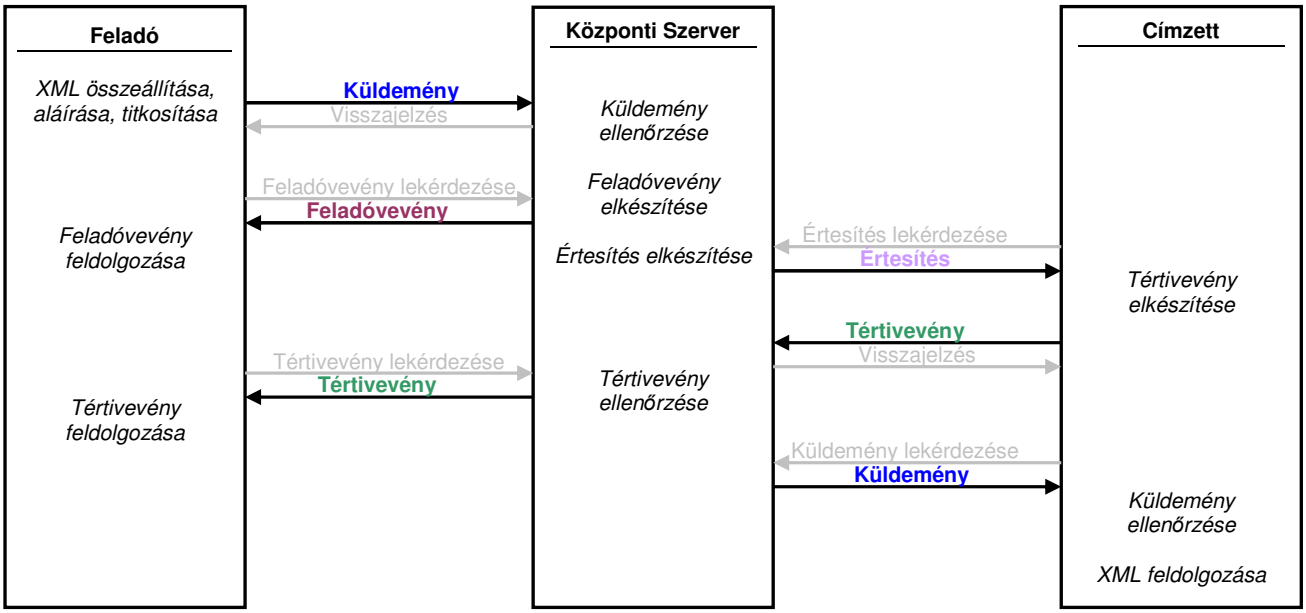
A Központi szerver funkciói **HTTP protokollon** keresztül érhetőek el **SSL felett** az RFC1945 és az RFC2616 ajánlások szerint. A szolgáltatásokat a **Representational State Transfer** (REST)[6] alapelveinek megfelelően nyújtja.

Ez azt jelenti, hogy a szerver az általa kezelt entitásokat (pl. küldemények, feladóvevények, tértivevények) adott URL-en keresztül teszi elérhetővé, és a HTTP protokoll metódusaival lehet rajtuk műveleteket végezni (pl. listázni, adott elemet letölteni, új elemet feltölteni, módosítani, törölni).

A VIEKR rendszer esetében az alap URL: *https://viekr.mbvk.hu/viekr/rest/*

A REST-nek alapelveinek megfelelően a kommunikációban mindig a **kliens oldal az aktív** (kezdeményező), azaz nem csak az egyes entitások feltöltését, hanem letöltését (törlését, módosítását) is a kommunikáló felek szoftvereinek kell indítaniuk.

Az alábbi ábra szemlélteti ennek megfelelően a küldemény továbbítás tényleges folyamatát.



3. ábra A küldemény továbbítás folyamata

Az ábrán a dupla nyilak egyetlen HTTP kapcsolatot jelölnek.

4.2. Felhasználók és szervezetek azonosítása

A VIEKR rendszerben a feladók és címzettek szervezetek. Minden regisztrált szervezetnek van egy, a rendszerben egyedi **SzervezetID**-ja, ami egy szám[7], pl. „9”. Továbbá minden szervezetnek létezik egy **SzervezetAzonositoja** is, amely lehet egy beszédes elnevezés, akár egy már létező cím is[8], de a feltétel itt is az, hogy a rendszerben egyedinek kell lennie.

Hasonlóan, a felhasználók is rendelkeznek **FelhasznaloID**-val és **FelhasznaloAzonositoval** is.

A címzés során az azonosítókat (a beszédes elnevezéseket) használjuk.

[6] Bővebb információ: http://en.wikipedia.org/wiki/Representational_State_Transfer

[7] Ez a későbbiekben kiegészítésre kerülhet a rendszerre jellemző adattal, amely globálisan egyedivé teszi, pl. „9@viekr.mbvk.hu”.

[8] Például a végrehajtói irodák esetében a „VHI”, a pénzintézetek esetében a „PI” előtagok használva, pl. „VHI-0098” ill. „PI-116”.

4.3. Szervezetek típusa

A szerverre felvett szervezeteket típusokba soroljuk annak érdekében, hogy könnyebben lehessen közöttük keresni.

A VIEKR-ben a vonatkozó végrehajtási rendeletnek megfelelően felvehető felek:

- a Magyar Bírósági Végrehajtói Kamara,
- a végrehajtók,
- a végrehajtói törvény által kötelezettek (jelenleg a pénzintézetek)
- a megbízotti tevékenységet hivatásszerűen ellátó megánszemélyek és szervezetek,
- egyéb magánszemélyek és szervezetek

lehetnek.

Ennek megfelelően egy regisztrált szervezet típusa jelenleg „KAMARA", „VEGREHAJTO", „PENZINTEZET", „HIV_MEGH_MAGANSZEMELY", „HIV_MEGH_SZERVEZET", „EGYEB_FEL_MAGANSZEMELY" illetve „EGYEB_FEL_SZERVEZET" lehet.

4.4. Közlemények azonosítása

A rendszerben minden továbbított adategység (küldemény, tértivevény, feladóvevény és hibajelentés) rendelkezik egy **globálisan egyedi azonosítóval**.

A küldemények, tértivevények és hibajelentések azonosítóját a felhasználó rendszere generálja (annak érdekében, hogy bele lehessen írni a küldemény metaadatai közé), a feladóvevény azonosítóját a szerver hozza létre.

Az azonosító formátuma a következő:

VIEKR-[SZERVEZET-ID].[FELHASZNÁLÓ-ID].[DÁTUMIDŐ].[SORSZÁM]
Pl.: VIEKR-41413.41483.20101216080000.01

A **SzervezetID** a szervezet regisztrációkor kapott egyedi ID (lásd a 4.2 fejezetet)[9].

A **FelhasznaloID** a felhasználó regisztrációkor kapott egyedi ID (lásd a 4.2 fejezetet).

A **dátumidő** a küldemény generálásának időpontja YYYYMMDDHHMMSS formátumban, ahol kötelezően UTC időt kell használni.

A **sorszám** egy kétjegyű szám, amelyet a feladó szoftvere generál (arra az esetre, ha egy másodperc alatt több küldemény is készülne).

A generált azonosítót a burkoló e-aktában az **Azonosito** metaadatban kell elhelyezni.

Egy adott küldemény azonosítója szerepelni fog a küldemény továbbításhoz tartozó minden entitásban (küldemény, feladóvevény, tértivevény, hibajelentés), azaz végigkíséri a küldési folyamatot. A feladóvevény, tértivevény és hibajelentés esetében a hivatkozott küldemény azonosító az **ElozmenyAzonosító** metaadatban szerepel (hiszen azoknak is saját azonosítójuk van).

4.5. Címzés

A továbbítandó adategységek (küldemény, tértivevény, feladóvevény és hibajelentés) burkoló e-aktájának metaadatai között szerepelnek továbbá a **CimzettSzervezetAzonosito** és **FeladoSzervezetAzonosito** metaadatok. A címzés ezek alapján történik[10].

A FeladoSzervezetAzonosito elembe a küldő felhasználó szervezetének azonosítóját kell beírni[11]. A CimzettSzervezetAzonosito elembe a megcímzett szervezet azonosítója kerül, itt vesszővel elválasztva **több címzett is megadható**!

[9] Amennyiben a felhasználó több szervezethez tartozik, akkor annak a szervezetnek az ID-ját kell használni, akinek a nevében éppen eljár.

[10] Annak érdekében, hogy a feladó és címzett kiléte az üzenet kicsomagolása után is ismert legyen, ezen azonosítókat a belső, érdemi üzenetben is szerepeltetni kell (lásd: VIEKR üzenetformátum specifikáció).

4.6. Típus, üzenettípus

A továbbítandó adategységek (küldemény, tértivevény, feladóvevény és hibajelentés) burkoló e-aktájában szerepel továbbá az adott adategység típusára vonatkozó információ.

A **Tipus** metaadat értéke lehet „küldemény", „feladóvevény" és „tértivevény". Az **UzenetTipus** metaadat tartalma utal arra, hogy az e-akta belsejében milyen jellegű üzenet XML található, így értéke „küldemény" esetében lehet pl. „pénzintézeti megkeresés" vagy „hibajelentés". „Tértivevény" esetében az az információ kerül ide, hogy a tértivevényt a címzett állította-e ki, vagy a szerver nyilatkozik a kézbesítési vélelem beálltáról.

4.7. Adatfeldolgozás, küldemény állapotok

A szerver a hozzá feltöltött küldeményeket és tértivevényeket **aszinkron módon** dolgozza fel. Ez azt jelenti, hogy a feltöltést követően csak a letárolhatósághoz kapcsolódó alapkövetelményeket ellenőrzi (van-e, és egyedi-e a küldemény azonosítója), a további ellenőrzést saját belső ütemezése szerint végzi el.

Adott **küldemény feldolgozási állapotát**, valamint **kézbesítési állapotát** a szerver nyilvántartja, ez az állapot a küldemény azonosító alapján lekérdezhető.

Egy küldemény **feldolgozási állapota** (F) a következő lehet:

1. Iktatott: Feldolgozásra vár.

2. Feldolgozás alatt: A feldolgozás folyamatban.

3. Feldolgozott: Sikeresen feldolgoztuk a küldeményt.

4. Feldolgozatlan: Nem sikerült feldolgozni belső hiba miatt, még újra próbálja a szerver.

5. Feldolgozhatatlan: Nem sikerült feldolgozni belső hiba miatt, és a szerver már nem próbálja újra.

A 3. állapot esetében a feldolgozás eredménye a **Státuszkód** illetve **Státusz leírás** adatokból derül ki.

Egy küldemény **kézbesítési állapota** (K) a következő lehet:

1. Tértivevényre vár: A küldemény adatait tartalmazó értesítés elérhető, az alapján el kell készíteni és bekűldeni a tértivevényt.

2. Letölthető: A küldeményre adott tértivevény ellenőrizve és jó, a küldemény letölthető

3. Kézbesített: A küldeményt letöltötték

Hasonlóan a **tértivevények** is rendelkeznek állapotokkal. A tértivevény **feldolgozási állapotai** megegyeznek a küldemény feldolgozási állapotaival. A **letöltési állapotok** annyiban különböznek, hogy a feladó a küldeményre visszaküldött tértivevényt akkor veheti át, ha magát a küldeményt a címzett már letöltötte; ezért a „Tértivevényre vár" állapot helyett az „Iktatott" állapotot használjuk.

A **feladóvevényeket** a Központi szerver generálja, így azoknak csak egyféle **feldolgozási állapota** van („Feldolgozott"), **letöltési állapotai** pedig „Letölthető" és „Kézbesített" lehetnek.

A küldemények, tértivevények és feladóvevények állapotai a szervertől lekérdezhetőek.

Adott felhasználó (szoftvere) a neki küldött illetve általa küldött küldemények állapotának ismeretében tudja meghatározni, hogy milyen adategységekkel mik a teendői. Ezek a következők:

A) Ha van **általa küldött**, **„Feldolgozott" feldolgozási állapotú, 2.0.1 státuszkódú** küldemény, amelynek a feladóvevényét még nem töltöttük le, akkor annak feladóvevényét le kell tölteni.

B) Ha van **általa küldött**, **„Kézbesített" kézbesítési állapotú** küldemény, akkor annak tértivevényét le kell tölteni.

C) Ha van **neki címzett**, **„Tértivevényre vár" kézbesítési állapotú** küldemény, akkor le kell töltenie az értesítést és tértivevényt kell adnia.

D) Ha van **neki címzett**, **„Letölthető" kézbesítési állapotú** küldemény, akkor azt le kell töltenie.

E) Ha van **általa küldött**, **„Feldolgozott" feldolgozási állapotú, nem 2.0.1 státuszkódú** küldemény, akkor a státuszkód és státuszleírás alapján meg kell határozni a hiba okát, majd a probléma orvoslását követően újra kell küldeni a küldeményt.

---

[11] Ha a felhasználó több szervezethez is tartozik, akkor annak a szervezetnek az azonosítóját kell megadni, amelyiknek a nevében eljár.

A többi esetben a felhasználónak nincs teendője.

Az **F5**-ös állapotban a Központi szerver operátorának kell orvosolnia a hibát. A **K1**-es állapotból legkésőbb 5 munkanap elteltével átkerül a küldemény a **K2**-es állapotba.

A hibajelentés a küldeménnyel azonos módon kerül letöltésre, ezért ezt külön nem emeltük ki.

Természetesen a felhasználó a kézbesítési státuszinformációk lekérdezésével bármikor információt kaphat egy adott küldemény kézbesítési státuszáról.

4.8. A kézbesítési adategységek áttekintése

A rendszerben továbbított adategységek a **küldemény**, **feladóvevény** és a **tértivevény**.

A **hibajelentés** egy speciális küldemény, amely előre meghatározott XML formátumban tartalmazza a tapasztalt hiba leírását. A címzett készíti, amennyiben az átvett küldeményben található üzenet formátumhibás, vagy az aláírás nem megfelelő.

A **„vélelem”** egy speciális – záradékkal ellátott – tértivevény, amelyben a szerver igazolja a kézbesítés tényét. Egy küldemény vonatkozásában a kézbesítési vélelem akkor is beáll, ha azt a címzett 5 munkanap alatt nem veszi át; ekkor a címzett helyett a szerver készíti el a tértivevényt.

Az **értesítés** a küldemény fontosabb adatait tartalmazó, XML formátumú kivonat, amely alapján a küldeményre vonatkozó tértivevény elkészíthető.

A következő táblázatban áttekintjük a kézbesítési adategységek fontosabb jellemzőit.

		Küldemény	Hibajelentés	Feladóvevény	Tértivevény	„Vélelem”	Értesítés
Formátum		Titkosított e-aktát tartalmazó e-akta, metaadatokkal. Kiterjesztése .es3.	Titkosított e-aktát tartalmazó e-akta, metaadatokkal. Kiterjesztése .es3. Egy speciális küldemény.	Tértivevény formátumú e-akta, metaadatokkal. Kiterjesztése .et3.	Tértivevény formátumú e-akta, metaadatokkal és záradékkal. Kiterjesztése .et3.	Tértivevény formátumú e-akta, metaadatokkal és záradékkal. Kiterjesztése .et3. Egy speciális tértivevény.	Egy adott küldemény metaadatait tartalmazó XML struktúra.
Ki állítja elő?		Felhasználó.	Felhasználó Automatikusan generálható.	Központi szerver	Felhasználó	Központi szerver	Központi szerver
Honnan lehet letölteni?		***https://viekr.mbvk.hu/viekr/rest/kuldemenyek***	***https://viekr.mbvk.hu/viekr/rest/kuldemenyek***	***https://viekr.mbvk.hu/viekr/rest/feladovevenyek***	***https://viekr.mbvk.hu/viekr/rest/tertivevenyek***	***https://viekr.mbvk.hu/viekr/rest/tertivevenyek***	***https://viekr.mbvk.hu/viekr/rest/kuldemenyek***
METAADATOK	**Azonosito**	Felhasználó állítja elő a megadott szabályok alapján. Mindig újat kell előállítani.	Felhasználó állítja elő a megadott szabályok alapján. Mindig újat kell előállítani.	Központi szerver elő a megadott szabályok alapján. Mindig újat kell előállítani.	Felhasználó állítja elő a megadott szabályok alapján. Mindig újat kell előállítani.	Központi szerver állítja elő a megadott szabályok alapján. Mindig újat kell előállítani.	Nem értelmezett.
	ElozmenyAzonosito	NINCS	A hivatkozott küldemény Azonositoja	A hivatkozott küldemény Azonositoja	A hivatkozott küldemény Azonositoja	A hivatkozott küldemény Azonositoja	Nem értelmezett.
	CimzettSzervezet	Egy vagy több szervezetazonosító szerepelhet itt.	Egy szervezetazonosító szerepelhet itt.	Egy szervezetazonosító szerepelhet itt.	Egy szervezetazonosító szerepelhet itt.	Az eredeti feladó, valamint az összes eredeti címzett szervezet azonosítója szerepel itt, akiknél a kézbesítési vélelem beálltára vonatkozik.	Nem értelmezett.
	FeladoSzervezet	Egy szervezetazonosító szerepelhet itt.	Egy szervezetazonosító szerepelhet itt.	A Központi szerver azonosítója szerepel itt.	Egy szervezetazonosító szerepelhet itt.	A Központi szerver azonosítója szerepel itt.	Nem értelmezett.
	Tipus	küldemény	küldemény	feladóvevény	tértivevény	tértivevény	Nem értelmezett.

	Uzenettpus	Pl. pénzintézeti megkeresés	hibajelentés	NINCS	NINCS	vélelem	Nem értelmezett.
Záradék		NINCS	NINCS	NINCS	Címzett által kiállított nyilatkozat. Tartalmazza a szervezet azonosítóját.	Azon szervezetek azonosítóját tartalmazza, akiknél a kézbesítési vélelem beálltáról szól.	Nem értelmezett.

1. táblázat A kézbesítési adategységek áttekintése

5. A rendszerben részt vevő felek feladatai a kommunikáció során

Ahhoz, hogy egy felhasználó használni tudja az üzenettovábbító rendszert, szüksége van egy olyan szoftverre, amely segítségével el tudja végezni az előzőekben ismertetett feladatokat (üzenet előállítása, aláírása, titkosítása, küldemény előállítása, beküldése, feladóvevény letöltése és ellenőrzése, tértivevény letöltése és ellenőrzése, értesítés letöltése és tértivevény készítése, küldemény átvétele, aláírás ellenőrzése, XML formátumának ellenőrzése, hibajelentés készítése, kézbesítési státuszinformációk lekérdezése, tanúsítványok szinkronizálása, sémák szinkronizálása).

Az alábbiakban áttekintjük az üzenetküldéssel kapcsolatos alapfeladatok a következő rendszerezés szerint:

Küldési folyamat részeként:

1. Küldemény összeállítása
2. Feladóvevény fogadása
3. Tértivevény fogadása
4. Hibajelentés fogadása

Fogadási folyama részeként:

5. Értesítés fogadása
6. Tértivevény összeállítása
7. Küldemény fogadása
8. Hibajelentés összeállítása

5.1. Az üzenetküldéssel kapcsolatos alapfunkciók áttekintése

5.1.1. Küldemény összeállítása

Ennek során a feladó (szoftvere segítségével) összeállítja az XML formátumú üzenetet[12], beilleszti ezt egy e-aktába és aláírja[13], valamint időbélyegzi. Ezután beszerzi a címzett és a feladó szervezetekhez tartozó felhasználók titkosító tanúsítványait a Központi szervertől, és titkosítja számukra az e-aktát. A titkosítást minden visszakapott tanúsítvánnyal el kell végezni, kivéve a lejárt vagy visszavont tanúsítványokkal történő titkosítást.

Ezt követően a titkosított e-aktából a feladó elkészíti a küldeményt, ami az e-aktában a metaadatok megadását jelenti. Az adatokat a burkoló e-akta metaadataiban kell megadni. A következő metaadatokat kell megadni: **Azonosito**, **CimzettSzervezetAzonosito**, **FeladoSzervezetAzonosito**, **Tipus**, **UzenetTipus**; a 4. fejezetben ismertetett szabályok szerint.

Ezután be kell jelentkezni a Központi szerverre (felhasználó authentikáció), és az elkészített küldeményt a következő URL-en keresztül kell feltölteni: ***https://viekr.mbvk.hu/viekr/rest/kuldemenyek.***

A küldemény feltöltésekor a szerver a letárolhatóság és visszakereshetőség feltételeit ellenőrzi (szerepel-e benne globálisan egyedi Azonosito), az érdemi ellenőrzés később történik meg. Amennyiben az ellenőrzés sikeresen zárul, a szerver elkészíti a feladóvevényt, amelyet majd később le kell tölteni; valamint a küldeményről értesítést tesz elérhetővé a címzett(ek) számra. Ha az ellenőrzés eredményeképpen kiderül, hogy valamilyen probléma van a küldeménnyel, akkor nem készül feladóvevény: A küldemény ekkor is feldolgozott állapotba kerül, a hiba kódja és a leírása a státuszkódból és státuszleírásból derül ki. Időnként ellenőrizni kell, hogy van-e ilyen küldemény (lásd: 5.1.9. fejezet).

5.1.2. Feladóvevény fogadása

A szerver a feldolgozási folyamat során ellenőrzi a feltöltött küldeményt annak tekintetében, hogy titkosított e-akta-e, hogy szerepel-e benne minden szükséges metaadat, hogy a címzésben megadott szervezet felhasználóinak titkosítva van-e, illetve hogy ha a küldemény hibajelentés, akkor létező illetve a címzettnek küldött küldeményre érkezett-e (hibajelentésre nem lehet hibajelentést küldeni). Ha az ellenőrzés sikeresen zárul, akkor a szerver elkészíti a feladóvevényt.

[12] A formátumát ellenőrizni kell a Központi szerverről beszerzett séma alapján.
[13] Keretaláírást készít rá.

Azaz, ha van olyan, a felhasználó által feltöltött küldemény, amely „feldolgozott” állapotban van, és a státusza 2.0.1 (azaz az ellenőrzés sikeresen zárult) – ezek listája lekérdezhető a szervertől –, akkor letölthető annak feladóvevénye a ***https://viekr.mbvk.hu/viekr/rest/feladovevenyek*** címről.

Egy felhasználó csak az ő szervezete számára küldött feladóvevényeket éri el[14].

A feladóvevény egy aláírt és időbélyeggel ellátott igazolás a szervertől arról, hogy az adott azonosítójú küldeményt adott időpontban kézbesítésre átvette.

A feladó ellenőrzi a letöltött feladóvevény aláírását, a megfelelő üzenetküldési folyamathoz kapcsolja illetve feldolgozza a benne szereplő adatokat.

A küldemény feladásának hivatalos dátuma a feladóvevényben szereplő időpont.

5.1.3. Tértivevény fogadása

Amennyiben a címzett átvette a küldeményt, akkor a küldemény letöltési állapota „kézbesített” állapotba kerül, és a feladó számára elérhetővé válik a címzett által adott tértivevény.

Azaz, ha van olyan, a felhasználó által feltöltött küldemény, amely „kézbesített” állapotban van – ezek listája lekérdezhető a szervertől –, akkor letölthető az arra, a címzett által adott tértivevény a ***https://viekr.mbvk.hu/viekr/rest/tertivevenyek*** címről.

Egy felhasználó csak az ő szervezete számára küldött (illetve a szervezete által készített) tértivevényeket éri el[15].

Amennyiben a kézbesítési vélelem azáltal állt be, hogy a címzett 5 munkanap elteltével sem adott tértivevényt, akkor a következő munkanapon a Központi szerver készíti el a tértivevényt, amely hasonló módon letölthető az eredeti feladó számára. Az ilyen módon kiállított tértivevény metaadatai között szereplő FeladoSzervezetAzonosito a szerver azonosítója lesz, és az Uzenettipus metaadatban is szerepel, hogy ez a szerver által kiállított tértivevény („velelem”). A tértivevény záradékában szerepel azon szervezet(ek) azonosítója, akiknél a kézbesítési vélelem beálltáról szól.

Amennyiben az eredeti üzenetnek több címzettje volt, akkor az eredeti feladó természetesen több tértivevényt fog visszakapni.

A tértivevény egy aláírt és időbélyeggel ellátott igazolás a címzettől (szervertől) arról, hogy az adott azonosítójú küldeményt adott időpontban adott szervezet nevében átvette (kézbesítettnek minősül).

Az eredeti küldemény feladója a tértivevény letöltését követően ellenőrzi a tértivevény aláírását, a megfelelő üzenetküldési folyamathoz kapcsolja illetve feldolgozza a benne szereplő adatokat.

A küldemény kézbesítésének hivatalos dátuma a tértivevényben szereplő időpont.

5.1.4. Hibajelentés fogadása

A hibajelentés átvétele a küldemény átvételével megegyező módon történik (lásd később).

Ha az eredeti küldemény feladója hibajelentést kap, akkor annak letöltését követően kititkosítja, ellenőrzi rajta az aláírást és feldolgozza a benne szereplő adatokat. Ha hibát észlel, akkor annak megoldását más csatornára kell terelni; hibajelentésre nem küldhető újabb hibajelentés.

5.1.5. Értesítés fogadása

Sikeres küldemény átvétel esetén a Központi szerver elérhetővé teszi a címzett(ek) számára az új küldemény fontosabb adatait a ***https://viekr.mbvk.hu/viekr/rest/kuldemenyek*** címen (ekkor maga a küldemény még nem elérhető!), XML formátumban.

Ez azt jelenti, hogy ha van olyan, a felhasználónak címzett küldemény, amely „tértivevényre vár” állapotban van – ezek listája lekérdezhető a szervertől –, akkor letöltheti a tértivevény készítéséhez szükséges adatokat tartalmazó értesítést a ***https://viekr.mbvk.hu/viekr/rest/kuldemenyek*** címről.

Egy felhasználó csak az ő szervezetének címzett értesítéseket éri el[16].

[14] Amennyiben egy felhasználó több szervezethez tartozik, akkor a lekérdezés során megadhatja, hogy mely szervezet adatait kéri.
[15] Amennyiben egy felhasználó több szervezethez tartozik, akkor a lekérdezés során megadhatja, hogy mely szervezet adatait kéri.
[16] Amennyiben egy felhasználó több szervezethez tartozik, akkor a lekérdezés során megadhatja, hogy mely szervezet adatait kéri.

5.1.6. Tértivevény összeállítása

Az előző lépésben átvett értesítés alapján a felhasználó szoftvere segítségével elkészíti a tértivevényt (ennek során időbélyeges aláírást kell készítenie; a tértivevény záradékában szerepeltetnie kell az átvevő szervezet azonosítóját; a metaadatokat helyesen kell kitölteni a burkoló e-aktában).

Az elkészített tértivevényt fel kell tölteni a Központi szerverre a ***https://viekr.mbvk.hu/viekr/rest/tertivevenyek*** címre.

A tértivevény feltöltésekor a szerver a letárolhatóság és visszakereshetőség feltételeit ellenőrzi (szerepel-e benne a globálisan egyedi Azonosito), az érdemi ellenőrzés később történik meg. Amennyiben az ellenőrzés sikeresen zárul, a szerver elérhetővé teszi a felhasználó számára a megfelelő küldeményt, valamint elérhetővé teszi az eredeti feladó számára a beküldött tértivevényt. Ha az ellenőrzés eredménye szerint a tértivevény nem volt megfelelő, akkor az adott küldemény állapota nem fog változni, azaz marad „tértivevényre vár" állapotban, és újra tértivevényt kell rá adni.

Ugyanarra a küldeményre csak az első helyes tértivevényt veszi át a szerver. Ha a kézbesítési vélelem beállt, akkor a szerver már nem fogad el tértivevényt.

A küldemény átvételének hivatalos dátuma az első helyes tértivevényben szereplő időpont.

5.1.7. Küldemény fogadása

Ha a címzett sikeresen feltöltötte a tértivevényt, és az ellenőrzés eredménye is jó volt, akkor a küldemény „letölthető" állapotba kerül és elérhetővé válik a címzett számára. Ezeket a címzett a ***https://viekr.mbvk.hu/viekr/rest/kuldemenyek*** címről tudja letölteni. Az ilyen küldemények listája a szervertől lekérdezhető.

Egy felhasználó csak az ő szervezetének küldött és tértivevényezett (illetve a szervezet általa küldött) küldeményeket éri el[17].

A letöltött küldeményt a címzett kititkosítja, ellenőrzi rajta az aláírást és formai ellenőrzést végez a kapott XML-en. Ha bármilyen hibát észlel, akkor erről hibajelentés formájában értesíti a feladó felet. Ha a kapott üzenet értelmezhető, akkor elkészíti az arra adandó választ, és az üzenetküldő rendszer segítségével új küldeményként eljuttatja azt a küldemény feladójának.

5.1.8. Hibajelentés küldése

Ha a címzett által átvett küldemény formai ellenőrzése során valamilyen hibára derül fény, erről egy hibajelentésben lehet értesíteni a feladót. A hibajelentés formáját tekintve egy új küldemény (új Azonosito értéket kap), de szerepel benne hivatkozás az eredeti küldeményre (ElozmenyAzonosito metaadatban). A hibajelentés küldésének folyamata megegyezik a küldemény küldésével, annyi különbséggel, hogy hibajelentésre nem lehet hibajelentést küldeni (ezt a szerver ellenőrzi).

A hibajelentés XML generálható automatikusan.

5.1.9. Hibás küldemények listájának lekérése

A feladó által feltöltött küldemények ellenőrzését a szerver saját ütemezése szerint végzi el. Amennyiben az ellenőrzés eredményeképpen kiderül, hogy valamilyen probléma van a küldeménnyel, akkor nem készül feladóvevény. A küldemény ekkor is feldolgozott állapotba kerül, a hiba kódja és a leírása a státuszkódból és státuszleírásból derül ki.

Emiatt időnként ellenőrizni kell, hogy van-e ilyen küldemény, azaz le kell kérdezni a szervertől azon küldemények listáját, amelyeket a felhasználó töltött fel, „feldolgozott" állapotban vannak és státuszuk nem 2.0.1. A státuszleírás részletesebb információt is tartalmazhat a hiba okáról. Ezeket a küldeményeket a hiba kijavítását követően újra kell küldeni (új Azonosito megadásával!).

[17] Amennyiben egy felhasználó több szervezethez tartozik, akkor a lekérdezés során megadhatja, hogy mely szervezet adatait kéri.

5.2. VHKIR kommunikációs modul

Az ismertetett feladatokat ellátó szoftvermodul többféleképpen is megvalósítható, attól függően, hogy a VIEKR-hez csatlakozni kívánó szervezet milyen informatikai rendszerre rendelkezik, azzal milyen mértékben és módon kívánja integrálni az üzenetküldő funkcionalitást, hogy milyen mértékben kíván automatizmusokat bevezetni, az üzenetküldő funkcionalitások mellett milyen támogató funkciókat kíván nyújtani stb. (A PKI műveletek végzéséhez szükség van a felhasználó titkosító, authentikációs és aláírói tanúsítványaira, valamint magánkulcsainak használatára.)

A VIEKR szerver szabványos interfészen szolgálja ki az erőforrás-kéréseket (a részleteket lásd a VIEKR központi szerver interfészének leírása című dokumentációban). A jelen dokumentumban (és a hivatkozott dokumentumokban) foglalt követelmények teljesítése esetén a rendszerhez bármilyen szoftverrel lehetséges csatlakozni.

Ugyanakkor a rendszerhez való csatlakozás elősegítése érdekében kifejlesztésre került egy ún. **VHKIR kommunikációs modul**, amely megvalósítja a kommunikációhoz szükséges funkciókat.

A következőkben mintaként felsoroljuk a VHKIR kommunikációs modulban megvalósított funkciókat.

1. Szervezetek listájának letöltése

Bemenet:

- a lista xml fájl mentési útvonala

Kimenet:

- a szervezetek adatait tartalmazó lista XML formátumban
- OK vagy hibaüzenet

Feladata:

- Letölti az összes szervezet aktuális adatait tartalmazó XML listát a megadott nevű fájlba.

2. Küldemény (hibajelentés) beküldése

Bemenet:

- üzenet XML (vagy a hibajelentés XML)
- meta-adatok (üzenettípus, címzett szervezetek azonosítói, opcionális: előzmény-azonosító)
- küldemény mentési helyének megadása (lokális könyvtárhivatkozás)

Opcionális bemenet:

- csatolt iratok (PDF dokumentumok)
- aláírt (rejtjelezetlen) küldemény mentési könyvtára (lokális könyvtárhivatkozás)
- feldolgozatlan küldemények mentési könyvtára (ha meg van adva, akkor a bemeneti adatok ellenőrzése után elment egy feldolgozatlan e-aktát, amelynek a további feldolgozását a „félbehagyottak folytatása”, vagy az „összes beérkező küldemény átvétele” műveletek esetén automatikusan folytatni tud)
- eredmény XML mentési helye (lokális fájlhivatkozás)

Kimenet:

- Eredmény XML
- OK vagy hibaüzenet

Feladata:

- a küldeménynek azonosító generálása;
- az üzenet XML formális ellenőrzése, esetleges hiba jelzése;
- a megadott XML e-aktába helyezése, aláírása, időbélyegzése;
- a feladó és a kiválasztott címzett szervezetekhez tartozó titkosító tanúsítványok beszerzése;
- az aláírt e-akta titkosítása;
- az aláírt és a titkosított e-akták meta-adatokkal való ellátása (a feladó szervezet azonosítója konfigurációs beállításból töltődik ki);
- küldemény feltöltése a központi szerverre, esetleges hibaüzenetek lekezelése.

3. Tértivevények beküldése

Bemenet:

- tértivevények mentési helyének megadása (lokális könyvtár hivatkozás)

Opcionális bemenet:

- az előzmény küldemények azonosítóinak listája
- eredmény XML mentési helye (lokális fájlhivatkozás)

Kimenet:

- Eredmény XML
- OK vagy hibaüzenet

Feladata:

- Ha nincs megadva küldemény-azonosító lista, akkor beszerzi azoknak a küldeményeknek az azonosítóit, amelyek a kérdező szervezete számára érkeztek (szervezet azonosító a konfigurációból derül ki), és „Tértivevényre vár" kézbesítési állapotban vannak; a továbbiakban ezzel az azonosító listával dolgozik.
- Minden egyes küldemény azonosítóhoz:
  - a hozzá tartozó értesítés (a küldemény meta-adatai és lenyomata) letöltése;
  - az értesítés alapján a tértivevény elkészítése (ennek részeként időbélyeges aláírás készítés; a záradékba bele kell írni a szervezet azonosítóját, amely a konfigurációban van megadva)
  - a tértivevény feltöltése, esetleges hibaüzenetek jelzése

4. Feladóvevények letöltése

Bemenet:

- feladóvevények mentési helyének megadása (lokális könyvtárhivatkozás)

Opcionális bemenet:

- az előzmény küldemények azonosítóinak listája
- eredmény XML mentési helye (lokális fájlhivatkozás)

Kimenet:

- a letöltött feladóvevények a fájlrendszerben
- Eredmény XML
- OK vagy hibaüzenet

Feladata:

- Ha nincs megadva küldemény-azonosító lista, akkor beszerzi azoknak a küldeményeknek az azonosítóit, amelyet a kérdező szervezete töltött fel (a szervezet-azonosító a konfigurációból derül ki), „Feldolgozott" kézbesítési állapotban vannak, és a státuszuk 2.0.1. Ezzel az azonosító listával dolgozik tovább.
- Minden egyes előzmény küldemény azonosítóhoz:
  - az adott előzmény-azonosítóhoz tartozó feladóvevény letöltése,
  - ellenőrzése, esetleges hibaüzenetek lekezelése
  - fájlrendszerbe mentése

5. Küldemények (hibajelentések) letöltése

Bemenet:

- a titkosított küldemények mentési helye (lokális könyvtárhivatkozás)
- nyers XML-ek mentési könyvtára (lokális könyvtárhivatkozás)

Opcionális bemenet:

- a letöltendő küldemények (hibajelentések) azonosítóinak listája
- aláírt (rejtjelezetlen) küldemények mentési könyvtára (lokális könyvtárhivatkozás)
- nyers csatolmányok (PDF-ek) mentési könyvtára (lokális könyvtárhivatkozás; ha nincs megadva, a csatolmányok az üzenet XML-ek mellé kerülnek)
- feldolgozatlan küldemények mentési könyvtára (Amennyiben olyan problémába ütközik a feldolgozás során a program, ami vélhetőleg nem a küldő fél hibája, félbehagyja a feldolgozást, és feldolgozatlan küldeményként menti el a bejövő titkosított e-aktát. A feldolgozás a „félbehagyottak folytatása", vagy az „összes beérkező küldemény átvétele" műveletek esetében automatikusan folytatódik. Ha meg van adva erre a célra egy könyvtár, azt használja, különben a titkosított küldemények közé menti a félbehagyottakat is.)
- hibás küldemények mentési könyvtára (Amennyiben olyan problémába ütközik a program, ami vélhetőleg nem a küldő fél hibája, ellenben nem tudta azt automatikusan megoldani, hibás küldeményként menti el a titkosított e-aktát. Ha meg van adva erre a célra külön könyvtár, oda teszi, különben a feldolgozatlan küldemények mellé menti ezeket a hibás küldeményeket.)
- automatikus hibajelentés küldésének tiltása (Amennyiben a kapcsolót megadjuk, feladóoldali hibák esetén nem küld a program automatikusan hibajelentést, csak elkészíti a hibajelentés XML fájlt, amit a nyers XML-ek közé ment el. Az eltárolt fájlra az eredmény XML hivatkozik, azzal hibajelentés utólag is előállítható.)
- eredmény XML mentési helye (lokális fájlhivatkozás)

Kimenet:

- a letöltött küldemények (opcionálisan az aláírt, rejtjelezetlen e-akták is) a fájlrendszerben
- a letöltött küldemények kicsomagolt dokumentumai a fájlrendszerben
- esetleges hibajelentések fájljai (hibajelentés XML, a kiküldött/kiküldendő titkosított, esetleg csak aláírt hibajelentés e-akták) a fájlrendszerben
- eredmény XML
- OK vagy hibaüzenet

Feladata:

- Ha nincs megadva küldemény-azonosító lista, akkor beszerzi azoknak a küldeményeknek az azonosítóit, amelyet a kérdező szervezete számára küldtek (szervezet-azonosító a konfigurációból derül ki), és „Letölthető" kézbesítési állapotban vannak. Ezzel az azonosító listával dolgozik tovább.
- Minden egyes küldemény azonosítóhoz:
  - az azonosítóhoz tartozó titkosított küldemény letöltése;
  - a letöltött küldemény ellenőrzése, esetleges hibajelentések lekezelése;
  - a titkosított küldemény fájlrendszerbe mentése;
  - a küldemény titkosításának visszafejtése, az esetleges hibák lekezelése (feldolgozatlan küldemény);
  - az aláírások ellenőrzése, az esetleges hibaüzenetek lekezelése (hibajelentés küldése, feldolgozatlan küldemény);
  - a küldemény dokumentumainak fájlrendszerbe mentése
  - az üzenet XML-ek (hibajelentés XML-ek) formai ellenőrzése;
  - küldő oldali hibák esetén (kivéve, ha a küldemény maga hibajelentés volt) hibajelentés XML elkészítése, és amennyiben nincs tiltva, beküldése a 2. funkcióval;
  - címzett oldali feldolgozási probléma esetén feldolgozatlan fájl mentése;
  - az eredmény XML-ben minden egyes sikeresen vagy sikertelenül feldolgozott, letöltött küldeményről, ill. az előkészített vagy kiküldött hibajelentésekről egyaránt 1-1 bejegyzés készítése.

6. Tértivevények letöltése

Bemenet:

- tértivevények mentési helyének megadása (lokális könyvtárhivatkozás)

Opcionális bemenet:

- az előzmény küldemények azonosítóinak listája
- eredmény XML mentési helye (lokális fájlhivatkozás)

Kimenet:

- a letöltött tértivevények a fájlrendszerben
- Eredmény XML
- OK vagy hibaüzenet

Feladata:

- Ha nincs megadva küldemény-azonosító lista, akkor beszerzi azoknak a küldeményeknek az azonosítóit, amelyet a kérdező szervezete töltött fel (a szervezet-azonosító a konfigurációból derül ki), és „Letöltött" kézbesítési állapotban vannak. Ezzel az azonosító listával dolgozik tovább.
- Minden egyes előzmény küldemény azonosítóhoz:
  - az adott előzmény-azonosítóhoz tartozó tértivevény letöltése,
  - ellenőrzése, esetleges hibaüzenetek lekezelése
  - fájlrendszerbe mentése

7. Beküldött hibás küldemények státuszának letöltése

Opcionális bemenet:

- az ellenőrzendő küldemények azonosítóinak listája
- eredmény XML mentési helye (lokális fájlhivatkozás)

Kimenet:

- az eredmény XML-ben jelennek meg azok a lekérdezett kimenő küldemények, amelyeket a szerver feldolgozott és hibásnak talált
- OK vagy hibaüzenet

Feladata:

- Beszerzi azoknak a küldeményeknek (ha megadtak azonosító listát, csak ezeket a küldeményeket ellenőrzi) az adatait és hibakódjait, amelyeket a kérdező szervezete töltött fel (szervezet-azonosító a konfigurációból derül ki), „Feldolgozott" kézbesítési állapotban vannak, és a státuszuk nem 2.0.1.

8. Státuszinformációk lekérdezése

Bemenet:

- a státusz XML mentési helye (lokális fájlhivatkozás)

Opcionális bemenet:

- küldemény-azonosítóik listája
- maximális találati darabszám
- csak a letölthető küldemények listázása
- adott dátumtól kezdődő listázás

Kimenet:

- A feltételeknek megfelelő küldemény-továbbításhoz tartozó státuszinformációk XML-je
- OK vagy hibaüzenet

Feladata:

- a megadott feltételeknek megfelelő küldemény-továbbításokhoz tartozó státuszinformációk lekérése, a válasz fájlrendszerbe történő mentése, az esetleges hibaüzenetek kezelése

9. Félbehagyott feldolgozások folytatása

Bemenet:

- a titkosított küldemények mentési helye (lokális könyvtárhivatkozás)
- nyers XML-ek mentési könyvtára (lokális könyvtárhivatkozás)

Opcionális bemenet:

- aláírt (rejtjelezetlen) küldemények mentési könyvtára (lokális könyvtárhivatkozás)
- nyers csatolmányok (PDF-ek) mentési könyvtára (lokális könyvtárhivatkozás; ha nincs megadva, a csatolmányok az üzenet XML-ek mellé kerülnek)
- feldolgozatlan küldemények mentési könyvtára (Amennyiben olyan problémába ütközik a feldolgozás során a program, ami vélhetőleg nem a küldő fél hibája, félbehagyja a feldolgozást, és feldolgozatlan küldeményként menti el a bejövő titkosított e-aktát. A feldolgozás a „félbehagyottak folytatása", vagy az „összes beérkező küldemény átvétele" műveletek esetében automatikusan folytatódik. Ha meg van adva erre a célra egy könyvtár, azt használja, különben a titkosított küldemények közé menti a félbehagyottakat is.)
- hibás küldemények mentési könyvtára (Amennyiben olyan problémába ütközik a program, ami vélhetőleg nem a küldő fél hibája, ellenben nem tudta azt automatikusan megoldani, hibás küldeményként menti el a titkosított e-aktát. Ha meg van adva erre a célra külön könyvtár, oda teszi, különben a feldolgozatlan küldemények mellé menti ezeket a hibás küldeményeket.)
- automatikus hibajelentés küldésének tiltása (Amennyiben a kapcsolót megadjuk, feladóoldali hibák esetén nem küld a program automatikusan hibajelentést, csak elkészíti a hibajelentés XML fájlt, amit a nyers XML-ek közé ment el. Az eltárolt fájlra az eredmény XML hivatkozik, azzal hibajelentés utólag is előállítható.)
- a félbehagyott bejövő, ill. kimenő irányú küldemények feldolgozásának tiltása (a kapcsolók egyikének megadásával lehetséges csak a kimenő, ill. csak a bejövő félbehagyott küldemények feldolgozása)
- eredmény XML mentési helye (lokális fájlhivatkozás)

Kimenet:

- a letöltött küldemények (opcionálisan az aláírt, rejtjelezetlen e-akták is) a fájlrendszerben
- a letöltött küldemények kicsomagolt dokumentumai a fájlrendszerben
- esetleges hibajelentések fájljai (hibajelentés XML, a kiküldött/kiküldendő titkosított, esetleg csak aláírt hibajelentés e-akták) a fájlrendszerben
- eredmény XML
- OK vagy hibaüzenet

Feladata:

- A 2. ill. 5. funkciók által félbehagyott küldemények feldolgozásának folytatása az ott leírt módokon. Az elvégzett műveletekről az eredmény XML ad tájékoztatást.
- A félbehagyott kimenő küldeményeket aláírja, rejtjelezi és kiküldi.
- A félbehagyott bejövő küldemények titkosítását visszafejti, aláírásait ellenőrzi, tartalmukat kicsomagolja, és a fájlrendszerbe elmenti.
- Sikeres feldolgozás után automatikusan törli a feldolgozatlan küldemény e-aktát (a megfelelő titkosított, ill. aláírt küldemény könyvtárakban lesz ez után megtalálható az állomány).

10. Összes beérkező közlemény átvétele

Bemenet:

- a titkosított küldemények mentési helye (lokális könyvtárhivatkozás)
- nyers XML-ek mentési könyvtára (lokális könyvtárhivatkozás)
- feladóvevények mentési helyének megadása (lokális könyvtárhivatkozás)
- tértivevények mentési helyének megadása (lokális könyvtárhivatkozás)

Opcionális bemenet:

- a letöltendő küldemények (hibajelentések) azonosítóinak listája
- aláírt (rejtjelezetlen) küldemények mentési könyvtára (lokális könyvtárhivatkozás)
- nyers csatolmányok (PDF-ek) mentési könyvtára (lokális könyvtárhivatkozás; ha nincs megadva, a csatolmányok az üzenet XML-ek mellé kerülnek)
- feldolgozatlan küldemények mentési könyvtára (Amennyiben olyan problémába ütközik a feldolgozás során a program, ami vélhetőleg nem a küldő fél hibája, félbehagyja a feldolgozást, és feldolgozatlan küldeményként menti el a bejövő titkosított e-aktát. A feldolgozás a „félbehagyottak folytatása", vagy az „összes beérkező küldemény átvétele" műveletek esetében automatikusan folytatódik. Ha meg van adva erre a célra egy könyvtár, azt használja, különben a titkosított küldemények közé menti a félbehagyottakat is.)
- hibás küldemények mentési könyvtára (Amennyiben olyan problémába ütközik a program, ami vélhetőleg nem a küldő fél hibája, ellenben nem tudta azt automatikusan megoldani, hibás küldeményként menti el a titkosított e-aktát. Ha meg van adva erre a célra külön könyvtár, oda teszi, különben a feldolgozatlan küldemények mellé menti ezeket a hibás küldeményeket.)
- automatikus hibajelentés küldésének tiltása (Amennyiben a kapcsolót megadjuk, feladóoldali hibák esetén nem küld a program automatikusan hibajelentést, csak elkészíti a hibajelentés XML fájlt, amit a nyers XML-ek közé ment el. Az eltárolt fájlra az eredmény XML hivatkozik, azzal hibajelentés utólag is előállítható.)
- eredmény XML mentési helye (lokális fájlhivatkozás)

Kimenet:

- a letöltött küldemények (opcionálisan az aláírt, rejtjelezetlen e-akták is) a fájlrendszerben
- a letöltött feladóvevények a fájlrendszerben
- a letöltött küldemények kicsomagolt dokumentumai a fájlrendszerben
- a letöltött tértivevények a fájlrendszerben
- esetleges hibajelentések fájljai (hibajelentés XML, a kiküldött/kiküldendő titkosított, esetleg csak aláírt hibajelentés e-akták) a fájlrendszerben
- eredmény XML
- OK vagy hibaüzenet

Feladata:

- Elvégzi a 3., 4., 5., 6., 7. és 9. funkciók feladatait. Ha küldemény-azonosítók megadásra kerülnek, akkor a listát megkapják az egyes részfunkciók.
    - A tértivevényre váró értesítésekre a tértivevények elkészítése, feltöltése.
    - A kérdező szervezete által beküldött küldeményekhez tartozó, elkészült és még át nem vett feladóvevények átvétele.
    - A kérdező szervezetének címzett, már tértivevénnyel visszaigazolt küldeményeket letölti, titkosításukat visszafejti, aláírásait ellenőrzi, tartalmukat kicsomagolja, és a fájlrendszerbe elmenti.
    - A kérdező szervezete által küldött küldeményekhez tartozó, már beküldött és még át nem vett tértivevények átvétele.
    - A kérdező szervezete által beküldött, a szerver által feldolgozott, de hibásnak talált küldeményeket lekérdezi.
    - A félbehagyott kimenő küldeményeket aláírja, rejtjelezi és kiküldi.
    - A félbehagyott bejövő küldemények titkosítását visszafejti, aláírásait ellenőrzi, tartalmukat kicsomagolja, és a fájlrendszerbe elmenti.

11. Bizonyítékelemek ellenőrzése

Bemenet:

- Tértivevény vagy feladóvevény állomány
- a küldemény állomány, amelyről a bizonyítékot kiállították

Kimenet:

- OK vagy hibaüzenet

Feladata:

- Ellenőrzi, a megadott tértivevény (feladóvevény) aláírását, és hogy a megadott küldeményhez tartozik-e.

A részleteket a „VHKIR kommunikációs modul leírása” című dokumentáció tartalmazza.

6. A Központi szerver interfészének áttekintése

A következőkben rövid áttekintést nyújtunk a Központi szerveren elérhető szolgáltatásokról.

A kliens oldali szoftvernek ezeket a szolgáltatásokat kell megfelelő sorrendben és megfelelő paraméterekkel meghívnia a feladatai megvalósításához. Jelen fejezet ismerete csak azok számára szükséges, akik maguk kívánnak szoftvert fejleszteni a VIEKR eléréséhez.

6.1.1. A szolgáltatások

A REST alapelveinek megfelelően az üzenetküldő rendszerben megjelenő entitásokat erőforrásokként kezeli a szerver.

Ezek az erőforrások a következők:

1. **Küldemény**
2. **Feladóvevény**
3. **Tértivevény**
4. **Kézbesítési státusz**
5. **Szervezet**
6. **Felhasználó**
7. **Munkatárs kapcsolat**
8. **Tanúsítvány**
9. **Séma**

Az erőforrásokat URL-lel lehet azonosítani. Például a küldeményeket a ***https://viekr.mbvk.hu/viekr/rest/kuldemenyek*** URL-en keresztül lehet elérni. Minden erőforrás rendelkezik egy egyedi azonosítóval, amelyen keresztül hivatkozható. Így egy adott küldemény elérése a ***https://viekr.mbvk.hu/viekr/rest/kuldemenyek/{id}*** URL-en keresztül történik.

Az erőforrásokat a HTTP protokoll metódusaival lehet menedzselni. **GET** metódussal lehet lekérdezni, **POST** metódussal lehet feltölteni, létrehozni, **PUT** metódussal lehet módosítani, és **DELETE** metódussal lehet törölni erőforrásokat (amelyekre értelmezettek illetve engedélyezettek ezek a műveletek).

Az erőforrásoknak többféle megjelenési formája lehet. Minden entitás lekérhető **XML** vagy **json** formátumban (ekkor az adataikat kapjuk vissza), illetve speciális entitások lekérhetőek a „saját” formátumukban (az e-akta típusú entitások e-akta formátumban[18], a tanúsítványok PEM formátumban). A hívás során vagy a HTTP protokoll **Accept** fejlécében kell megadni a válaszban várt formátumot, vagy az URL-ben kell megadni a várt kiterjesztést (pl. ***https://viekr.mbvk.hu/viekr/rest/kuldemenyek.xml*** vagy ***https://viekr.mbvk.hu/viekr/rest/kuldemenyek/2.es3***).

A válasz

Az erőforrások kezelésének kimenetét **HTTP státuszkódokkal** írjuk le.

A leggyakoribb HTTP státuszüzenetek a következők:

- HTTP 200: OK – A kérés sikeresen fel lett dolgozva
- HTTP 201: Created – A kérés sikeresen fel lett dolgozva, az adott erőforrás a szerveren elkészült.
- HTTP 400: Bad Request – A kérésben hiba volt (pontos leírás ilyenkor a válasz státuszüzenetben van)
- HTTP 401: Authentication Required – Az erőforrást csak belépés után lehet elérni
- HTTP 403: Forbidden – A belépett felhasználó az erőforrást nem érheti el
- HTTP 404: Not Found – Nincs ilyen erőforrás
- HTTP 405: Method Not Allowed – Az erőforráson nem lehet ilyen műveletet végrehajtani
- HTTP 406: Not Acceptable – Olyan formátumban kértük a választ, amit a szerver nem tud előállítani
- HTTP 5**: Szerver oldali hiba

[18] Az e-akta formátum hivatalos specifikációja elérhető a http://srv.e-szigno.hu/menu/index.php?lap=eakta címen. E-akta típusú entitás a küldemény, a feladóvevény, az értesítés és a tértivevény. Utóbbi három speciális e-akta.

Ha nincs hiba (HTTP 200 vagy 202), akkor a válasz a kért entitást tartalmazza (módosításnál illetve létrehozásnál a szerveren létrejött friss adatokat tartalmazó XML a válasz, törlésnél üres a válasz).

Ha valamilyen hiba lépett fel (HTTP 4** vagy 5**), akkor a válasz tartalmazhatja a hiba okát részletesebben leíró **hibakódot**.

A HTTP 4**-os státuszkód esetén adott hibakódok a következők lehetnek:

Hibakód	**Jelentése**
4.0.001	Hiba az ellenőrzés során (ValidationException)
4.0.002	Hiányzik a felhasználó aláírói tanúsítványa (MissingSignerCertificateException)
4.0.003	A felhasználónak több aláíró tanúsítvány van (MultipleSignerCertificateException)
4.0.004	Hiányzik a titkosító tanúsítvány (MissingEncryptorCertificateException)
4.0.005	Több titkosító tanúsítvány található (MultipleEncryptorCertificateException)
4.0.006	Hibás tanúsítvány (InvalidCertificateException)
4.0.007	Tanúsítvány konvertálási hiba (CertificateConversionException)
4.0.008	Hibás kulcshasználat beállítás a tanúsítványban (KeyUsageException)
4.0.009	Hiba az e-akta megnyitásakor (EDossierOpenException)
4.0.010	Nem sikerült kinyerni az e-akta tartalmát (EDocumentExtractException)
4.0.011	Hiányzó dokumentum (MissingEDocumentException)
4.0.012	Több dokumentum található az e-aktában (MultipleEDocumentException)
4.0.013	Hiányzó küldemény azonosító (MissingKuldemenyAzonositoException)
4.0.014	Hibás formátumú küldemény azonosító (KuldemenyAzonositoFormatException)
4.0.015	Hiányzik a feladó szervezet azonosítója (SenderOrganizationIdMissmatchException)
4.0.016	Az adott szervezet nevében a felhasználó nem küldhet küldeményt (SenderUserIdMissmatchException)
4.0.017	Nem létező feladó szervezet (SenderOrganizationNotFoundException)
4.0.018	Nem létező címzett szervezet (RecipientOrganizationNotFoundException)
4.0.019	A megadott küldemény azonosítóval már van érkeztetett küldemény (DuplicatedKuldemenyException)
4.0.020	Nem sikerült kinyerni a dokumentum titkosító tanúsítványait (EncryptorCertificateExtractException)
4.0.021	Nincs titkosítva minden címzett számára (NotEncryptedForAllRecipientException)
4.0.022	Nincs titkosítva minden feladó számára (NotEncryptedForAllSenderException)
4.0.023	Nincs küldemény a megadott azonosítóhoz (MissingKuldemenyException)
4.0.024	Több küldemény is található a megadott azonosítóhoz (MultipleKuldemenyException)
4.0.025	Hiba a tértivevény ellenőrzése közben (TertivevenyValidationException)
4.0.026	Hibás formátumú előzmény azonosító (ElozmenyAzonositoFormatException)
4.0.027	A tértivevény már létezik (TertivevenyAlreadyExistsException)
4.0.028	A „elozmenyAzonosito” előzményazonosítóhoz már van érkeztetett hibajelentés (DuplicatedHibajelentesException)
4.0.029	(SignerCertificateExtractException)
4.0.030	Nem sikerült az aláírást kinyerni a tértivevényből (ESignatureExtractException)
4.0.999	Ismeretlen hibás kérés (UnknownBadRequestException)
4.3.001	Hiányzó tértivevény (MissingTertivevenyException)

A fenti lista általánosságban tartalmazza az egyes hibakódokat és jelentésüket. Az egyes szolgáltatások igénybe vétele során ezek közül azok a hibakódok fordulhatnak elő, amelyeknek az adott esetben értelme van. Ezért az egyes szolgáltatások bemutatásánál a lehetséges hibakódokat és azok pontos jelentését külön megadjuk.

Szolgáltatások felsorolása

A Központi szerver által biztosított funkciók, erőforrásonkénti csoportosításban a következők:

Küldemények

1. **Küldemény feltöltése**
2. **Keresés a küldemények között (listázás)**
3. **Adott küldemény (értesítés) letöltése**

Feladóvevények

4. **Keresés a feladóvevények között (listázás)**
5. **Adott feladóvevény letöltése**

Tértivevény

6. **Keresés a tértivevények között (listázás)**
7. **Tértivevény feltöltése**
8. **Adott tértivevény letöltése**

Kézbesítési státusz

9. **Keresés a kézbesítési státuszok között (listázás)**
10. **Adott küldeményhez tartozó kézbesítési státusz letöltése**

Szervezet

11. **Keresés a szervezetek között (listázás)**
12. **Adott szervezet adatainak lekérdezése**
13. **Adott szervezet adatinak módosítása**

Felhasználó

14. **Keresés a felhasználók között (listázás)**
15. **Adott felhasználó adatainak lekérdezése**
16. **Adott felhasználó adatinak módosítása**

Munkatárs kapcsolat

17. **Új munkatárs kapcsolat létrehozása**
18. **Keresés a munkatárs kapcsolatok között (listázás)**
19. **Adott munkatárs kapcsolat letöltése**
20. **Adott munkatárs kapcsolat adatainak módosítása**
21. **Adott munkatárs kapcsolat törlése**

Tanúsítvány

22. **Új tanúsítvány feltöltése**
23. **Keresés a tanúsítványok között (listázás)**
24. **Adott tanúsítvány letöltése**
25. **Tanúsítvány cseréje**

Séma

26. **Új séma feltöltése**
27. **Keresés a sémák között (listázás)**
28. **Adott séma letöltése**
29. **Séma cseréje**

A felsorolt funkciók részletes leírását a VIEKR Központi szerver interfészének leírása című dokumentáció tartalmazza.

MELLÉKLETEK

1. Példa e-akta

Az e-akta formátum hivatalos specifikációja elérhető a ***http://srv.e-szigno.hu/menu/index.php?lap=eakta*** címen.

```
<?xml version="1.0" encoding="UTF-8" ?>
<es:Dossier xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns="http://uri.etsi.org/01903/v1.2.2#"
xmlns:es="https://www.microsec.hu/ds/e-szigno30#"
xsi:schemaLocation="https://www.microsec.hu/ds/e-szigno30#
https://www.microsec.hu/ds/e-szigno30.xsd">
  <es:DossierProfile Id="PObject0" OBJREF="Object0">
    <es:Title>es3cli_cryptdossier_4197841204047461310.es3</es:Title>
    <es:E-category>electronic dossier</es:E-category>
    <es:CreationDate>2011-03-28T11:06:46Z</es:CreationDate>
    <es:KuldemenyAzonosito Custom="true" displayname="Küldemény
azonosító">1.1.20110328110635.01</es:KuldemenyAzonosito>
    <es:CimzettSzervezetId Custom="true" displayname="Címzett szervezet
id">2</es:CimzettSzervezetId>
  </es:DossierProfile>
  <es:Documents Id="Object0">
    <es:Document>
      <es:DocumentProfile Id="PO10282cc5-2eb4-44b7-8119-b28ce0b85200"
OBJREF="O10282cc5-2eb4-44b7-8119-b28ce0b85200">
        <es:Title>Encrypted e-dossier</es:Title>
        <es:E-category>electronic record</es:E-category>
        <es:CreationDate>2011-03-28T11:06:55Z</es:CreationDate>
        <es:Format>
          <es:MIME-Type type="application" subtype="eszigno3" extension="es3"
/>
        </es:Format>
        <es:MimeChecked executed="true">true</es:MimeChecked>
        <es:SourceSize sizeValue="25421" sizeUnit="B" />
        <es:BaseTransform>
          <es:Transform Algorithm="zip" />
          <es:Transform Algorithm="encrypt" />
           <es:Transform Algorithm="base64" />
        </es:BaseTransform>
        <es:RecipientCertificateList>
        <es:RecipientCertificate>MI..</es:RecipientCertificate>
        <es:RecipientCertificate>MI..</es:RecipientCertificate>
        <es:RecipientCertificate>MI..</es:RecipientCertificate>
        <es:RecipientCertificate>MI..</es:RecipientCertificate>
        </es:RecipientCertificateList>
      </es:DocumentProfile>
      <ds:Object Id="O10282cc5-2eb4-44b7-8119-b28ce0b85200">MI ..</ds:Object>
    </es:Document>
  </es:Documents>
</es:Dossier>
```

2. Példa tértivevény

```
<?xml version="1.0" encoding="UTF-8"?>
<es:Dossier xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns="http://uri.etsi.org/01903/v1.2.2#"
xmlns:es="https://www.microsec.hu/ds/e-szigno30#"
xsi:schemaLocation="https://www.microsec.hu/ds/e-szigno30#
https://www.microsec.hu/ds/e-szigno30.xsd">
  <es:DossierProfile Id="PObject0" OBJREF="Object0">
    <es:Title>Acknowledgement</es:Title>
    <es:E-category>electronic acknowledgement</es:E-category>
    <es:CreationDate>2011-03-28T15:43:27Z</es:CreationDate>
    <es:CimzettSzervezetId Custom="true" displayname="Címzett szervezet
id">2</es:CimzettSzervezetId>
    <es:KuldemenyAzonosito Custom="true" displayname="Küldemény
azonosító">1.1.20110328110635.01</es:KuldemenyAzonosito>
  </es:DossierProfile>
  <es:Documents Id="Object0">
    <es:Document>
      <es:DocumentProfile Id="PO1fe31b7c-5952-11e0-b609-86b0f8800d63"
OBJREF="O1fe31b7c-5952-11e0-b609-86b0f8800d63">
        <es:Title>acknowledgement.xml</es:Title>
        <es:E-category>electronic document</es:E-category>
        <es:CreationDate>2011-03-28T15:43:27Z</es:CreationDate>
        <es:Format>
          <es:MIME-Type type="text" subtype="xml" extension="xml"/>
        </es:Format>
        <es:MimeChecked executed="true">true</es:MimeChecked>
        <es:SourceSize sizeValue="767" sizeUnit="B"/>
        <es:BaseTransform>
          <es:Transform Algorithm="zip"/>
          <es:Transform Algorithm="base64"/>
        </es:BaseTransform>
      </es:DocumentProfile>
      <ds:Object Id="O1fe31b7c-5952-11e0-b609-86b0f8800d63">..</ds:Object>
      <ds:Signature Id="S1fe33a62-5952-11e0-b609-86b0f8800d63">
        <ds:SignedInfo Id="SIS1fe33a62-5952-11e0-b609-86b0f8800d63">
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-
xml-c14n-20010315"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/>
        <ds:Reference Id="R1fe33d00-5952-11e0-b609-86b0f8800d63"
URI="#O1fe31b7c-5952-11e0-b609-86b0f8800d63">
          <ds:Transforms>
            <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#base64"/>
          </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>x2wUe8PBOePDuyCI8HNr5EI/UnY=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference Id="R1fe33e72-5952-11e0-b609-86b0f8800d63"
URI="#PS1fe33a62-5952-11e0-b609-86b0f8800d63">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
          </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>7oHVgK871RnCIzKK2z45K79xmgU=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference Id="R1fe33f94-5952-11e0-b609-86b0f8800d63"
URI="#PO1fe31b7c-5952-11e0-b609-86b0f8800d63">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
```

```
          </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>APf6hcZ0WpssDMXpZn1OLEndC60=</ds:DigestValue>
        </ds:Reference>
        <ds:Reference Id="R1fe340ac-5952-11e0-b609-86b0f8800d63"
URI="#XS1fe33a62-5952-11e0-b609-86b0f8800d63"
Type="http://uri.etsi.org/01903/v1.2.2#SignedProperties">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
          </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <ds:DigestValue>oPdemBl3IK1dAeeavuCTvZqH2mQ=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue Id="VS1fe33a62-5952-11e0-b609-
86b0f8800d63">Mp..</ds:SignatureValue>
      <ds:KeyInfo Id="KS1fe33a62-5952-11e0-b609-86b0f8800d63">
        <ds:X509Data>
          <ds:X509Certificate>MI..</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
      <ds:Object Id="O1S1fe33a62-5952-11e0-b609-86b0f8800d63">
        <es:SignatureProfile Id="PS1fe33a62-5952-11e0-b609-86b0f8800d63"
OBJREF="O1fe31b7c-5952-11e0-b609-86b0f8800d63" SIGREF="S1fe33a62-5952-11e0-
b609-86b0f8800d63" SIGREFLIST="#O1fe31b7c-5952-11e0-b609-86b0f8800d63
#PS1fe33a62-5952-11e0-b609-86b0f8800d63 #PO1fe31b7c-5952-11e0-b609-
86b0f8800d63 #XS1fe33a62-5952-11e0-b609-86b0f8800d63">
          <es:SignerName>Teszt Magyar Bírósági Végrehajtói
Kamara</es:SignerName>
          <es:SDPresented server="true">false</es:SDPresented>
          <es:Type>signature</es:Type>
          <es:Generator>
            <es:Program name="e-Szigno" version="3.2.2.25"/>
            <es:Device name="OpenSSL 0.9.8c 05 Sep 2006" type=""/>
          </es:Generator>
          <es:Comment>
            <es:Document>
              <es:DocumentProfile Id="PCDS1fe33a62-5952-11e0-b609-
86b0f8800d63" OBJREF="CDS1fe33a62-5952-11e0-b609-86b0f8800d63">
                <es:Title>feladoveveny_zaradek_5619072535745123300.xml
                </es:Title>
                <es:E-category>electronic data</es:E-category>
                <es:CreationDate>2011-03-28T15:43:27Z</es:CreationDate>
                <es:Format>
                  <es:MIME-Type type="application" subtype="octet-stream"
extension="xml"/>
                </es:Format>
                <es:MimeChecked executed="false">false</es:MimeChecked>
                <es:SourceSize sizeValue="370" sizeUnit="B"/>
                <es:BaseTransform>
                  <es:Transform Algorithm="zip"/>
                  <es:Transform Algorithm="base64"/>
                </es:BaseTransform>
              </es:DocumentProfile>
            <ds:Object Id="CDS1fe33a62-5952-11e0-b609-
86b0f8800d63">UE..</ds:Object>
            </es:Document>
          </es:Comment>
        </es:SignatureProfile></ds:Object>
        <ds:Object Id="O2S1fe33a62-5952-11e0-b609-86b0f8800d63">
          <QualifyingProperties Target="#S1fe33a62-5952-11e0-b609-
86b0f8800d63" Id="QPS1fe33a62-5952-11e0-b609-86b0f8800d63">
            <SignedProperties Id="XS1fe33a62-5952-11e0-b609-86b0f8800d63">
              <SignedSignatureProperties>
                <SigningTime>2011-03-28T15:43:27Z</SigningTime>
```

```
                <SigningCertificate>
                  <Cert>
                    <CertDigest>
                      <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                      <ds:DigestValue>2BBHOxQuJwJOHCnSMRFmto+RS0E=
                      </ds:DigestValue>
                    </CertDigest>
                    <IssuerSerial>
                      <ds:X509IssuerName>CN=e-Szigno Teszt CA1,OU=e-Szigno
CA,O=Microsec Ltd.,L=Budapest,C=HU</ds:X509IssuerName>
                      <ds:X509SerialNumber>3266</ds:X509SerialNumber>
                    </IssuerSerial>
                  </Cert>
                </SigningCertificate>
                <SignaturePolicyIdentifier>
                  <SignaturePolicyImplied/>
                </SignaturePolicyIdentifier>
              </SignedSignatureProperties>
              <SignedDataObjectProperties>
                <DataObjectFormat ObjectReference="#R1fe33d00-5952-11e0-b609-
86b0f8800d63">
                  <MimeType>application/zip</MimeType>
                </DataObjectFormat>
                <DataObjectFormat ObjectReference="#R1fe33e72-5952-11e0-b609-
86b0f8800d63">
                  <MimeType>text/xml</MimeType>
                </DataObjectFormat>
                <DataObjectFormat ObjectReference="#R1fe33f94-5952-11e0-b609-
86b0f8800d63">
                  <MimeType>text/xml</MimeType>
                </DataObjectFormat>
                <DataObjectFormat ObjectReference="#R1fe340ac-5952-11e0-b609-
86b0f8800d63">
                  <MimeType>text/xml</MimeType>
                </DataObjectFormat>
              </SignedDataObjectProperties>
            </SignedProperties>
            <UnsignedProperties>
              <UnsignedSignatureProperties>
                <SignatureTimeStamp Id="T206d290c-5952-11e0-b609-
86b0f8800d63">
                <Include URI="#VS1fe33a62-5952-11e0-b609-86b0f8800d63"/>
                <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                <EncapsulatedTimeStamp Id="ET206d290c-5952-11e0-b609-
86b0f8800d63">..</EncapsulatedTimeStamp>
                </SignatureTimeStamp>
                <CompleteCertificateRefs Id="CCR20895bd6-5952-11e0-b609-
86b0f8800d63">
                  <CertRefs>
                    <Cert URI="#EC208920c6-5952-11e0-b609-86b0f8800d63">
                      <CertDigest>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>VfwniyJGiDxLGh5bineCSxfZhHE=</ds:DigestValue>
                      </CertDigest>
                      <IssuerSerial>
                        <ds:X509IssuerName>CN=Microsec e-Szigno Teszt Root
CA,OU=e-Szigno CA,O=Microsec Ltd.,L=Budapest,C=HU</ds:X509IssuerName>
                        <ds:X509SerialNumber>162839454754450569550511303760
0376565328</ds:X509SerialNumber>
                    </IssuerSerial>
                    </Cert>
                    <Cert URI="#EC20893052-5952-11e0-b609-86b0f8800d63">
                      <CertDigest>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```
                        <ds:DigestValue>g9GDrL9oT7ON4lvgpsnex3dwHmU=
                        </ds:DigestValue>
                      </CertDigest>
                      <IssuerSerial>
                        <ds:X509IssuerName>CN=Microsec e-Szigno Teszt Root
CA,OU=e-Szigno CA,O=Microsec Ltd.,L=Budapest,C=HU</ds:X509IssuerName>
                      <ds:X509SerialNumber>37437123961142371632298202743087162653</ds:X509SerialNumber>
                      </IssuerSerial>
                    </Cert>
                    <Cert URI="#EC20ba1852-5952-11e0-b609-86b0f8800d63">
                      <CertDigest>
                        <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>yyyxbkcLfbbueDsfdwklLuVrrRg=
                        </ds:DigestValue>
                      </CertDigest>
                      <IssuerSerial>
                        <ds:X509IssuerName>CN=Microsec e-Szigno Teszt Root
CA,OU=e-Szigno CA,O=Microsec Ltd.,L=Budapest,C=HU</ds:X509IssuerName>
                        <ds:X509SerialNumber>22483773301138814894657121703424235856 5</ds:X509SerialNumber>
                      </IssuerSerial>
                    </Cert>
                  </CertRefs>
                </CompleteCertificateRefs>
                <CertificateValues Id="CV20893322-5952-11e0-b609-
86b0f8800d63">
                  <EncapsulatedX509Certificate Id="EC208920c6-5952-11e0-b609-
86b0f8800d63">MI.. </EncapsulatedX509Certificate>
                  <EncapsulatedX509Certificate Id="EC20893052-5952-11e0-b609-
86b0f8800d63">MI.. </EncapsulatedX509Certificate>
                  <EncapsulatedX509Certificate Id="EC20ba1852-5952-11e0-b609-
86b0f8800d63">MI..</EncapsulatedX509Certificate>
                </CertificateValues>
              </UnsignedSignatureProperties>
            </UnsignedProperties>
          </QualifyingProperties>
        </ds:Object>
      </ds:Signature>
    </es:Document>
  </es:Documents>
</es:Dossier>
```