

# Végrehajtási Iratok Elektronikus Kézbesítési Rendszere (VIEKR)

<b>Státusz:</b>	jóváhagyott verzió
<b>Verzió:</b>	1.0
<b>Dátum:</b>	2013. január 15.
<b>Kezelési mód:</b>	Nyilvános

## 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 állapotainak pontosítása; 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 „kézbizított” használata; Az „E-mail kézbizítési 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
1.0	A feltöltött tértivevényt a feladó ellenőrzés után átveheti (3.4., 4.7, 5.1.3); Küldemények kézbizítési státuszai fejezet (3.5); Authentikáció tanúsítvány alapján (3.6); A rendszerben használható tanúsítványok (3.11); Típus, üzenettípus pontosítása (4.6); „Tértivevényezés alatt” állapot bevezetése (4.7); Tértivevény záradéka nem kötelező (4.8); Speciális keresési URL-ek bevezetése (5., 6.); A VHKIR kommunikációs modul változásainak bevezetése (5.2.); A szerver túlzott terhelését előidéző felhasználási mód (3.12); VHKIR kommunikációs modul leírásának rövidítése (5.2);	2013. január 15.	Szabóné Endrődi Csilla

# Tartalomjegyzék

<b>1.</b>	<b>Bevezetés .....</b>	<b>4</b>
1.1.	Dokumentum hatóköre .....	4
1.2.	Hivatkozott dokumentumok .....	4
<b>2.</b>	<b>Fogalmak .....</b>	<b>5</b>
<b>3.</b>	<b>A rendszer általános bemutatása.....</b>	<b>6</b>
3.1.	Üzenet előállítás és feldolgozása .....	6
3.2.	Küldemény előállítás és feldolgozása.....	6
3.3.	Megbízható üzenettovábbítás .....	7
3.4.	A kommunikáció folyamata.....	7
3.5.	Küldemények kézbesítési státuszai .....	8
3.6.	Címzés: szervezetek és felhasználók.....	8
3.7.	Titkosító tanúsítványok központi nyilvántartása .....	8
3.8.	Kézbizítési vélelem beállta .....	9
3.9.	Küldemények és bizonyítékelemek megőrzése .....	9
3.10.	Üzenetsémák központi nyilvántartása .....	9
3.11.	A rendszerben használható tanúsítványok .....	9
3.12.	A szerver túlzott terhelését előidéző felhasználási mód.....	9
<b>4.</b>	<b>A rendszer működésének részletes bemutatása.....</b>	<b>10</b>
4.1.	REST .....	10
4.2.	Felhasználók és szervezetek azonosítása.....	10
4.3.	Szervezetek típusa .....	11
4.4.	Közlemények azonosítása.....	11
4.5.	Címzés .....	11
4.6.	Típus, üzenettípus.....	12
4.7.	Adatfeldolgozás, küldemény állapotok.....	12
4.8.	A kézbesítési adategységek áttekintése.....	13
<b>5.</b>	<b>A rendszerben részt vevő felek feladatai a kommunikáció során .....</b>	<b>15</b>
<b>5.1.</b>	<b>Az üzenetküldéssel kapcsolatos alapfunkciók áttekintése .....</b>	<b>15</b>
5.1.1.	Küldemény összeállítása .....	15
5.1.2.	Feladóvevény fogadása.....	15
5.1.3.	Tértivevény fogadása.....	16
5.1.4.	Hibajelentés fogadása .....	16
5.1.5.	Értesítés fogadása .....	16
5.1.6.	Tértivevény összeállítása.....	17
5.1.7.	Küldemény fogadása .....	17
5.1.8.	Hibajelentés küldése .....	17
5.1.9.	Hibás küldemények listájának lekérése.....	17
<b>5.2.</b>	<b>VHKIR kommunikációs modul .....</b>	<b>18</b>
<b>6.</b>	<b>A Központi szerver interfészének áttekintése .....</b>	<b>19</b>
6.1.1.	A szolgáltatások .....	19
<b>MELLÉKLETEK .....</b>		<b>22</b>
1.	Példa e-akta .....	22
2.	Példa tértivevény .....	23

## 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 kézbiztosítási rendszer megfelel a 2011. december 13-án módosított, a bírósági végrehajtásról szóló 1994. évi LIII. törvényben (továbbiakban: Vht.) foglalt követelményeknek a végrehajtási iratok elektronikus kézbiztosításával 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 Kézbiztosítási Rendszere”, amelynek rövidítése VIEKR (de a VHKIR rövidítés a rendszerben 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

Végrehajtási Iratok Elektronikus Kézbiztosítási Rendszerének Felhasználási Szabályzata

VIEKR üzenetformátum specifikáció

VHKIR kommunikációs modul leírása

Microsec Megbízható üzenet továbbító 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 elektronikus aláírt, időbélyegzett, szabványos elismervény arról, hogy továbbításra átvette a hivatkozott e-aktát.

**Tértivevény:** A címzett által elektronikus 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 kitérítéskor, 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 üzenet továbbító egysége.

**Szervezet:** A Központi szerverre regisztrált szervezetek (végrehajtói irodák, pénzügyi intézetek, 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 autentikációs tanúsítvánnyal vagy felhasználónév/jelszó párossal. A rendszer üzenetküldő funkcionálisát 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 Kézbizítési 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.)

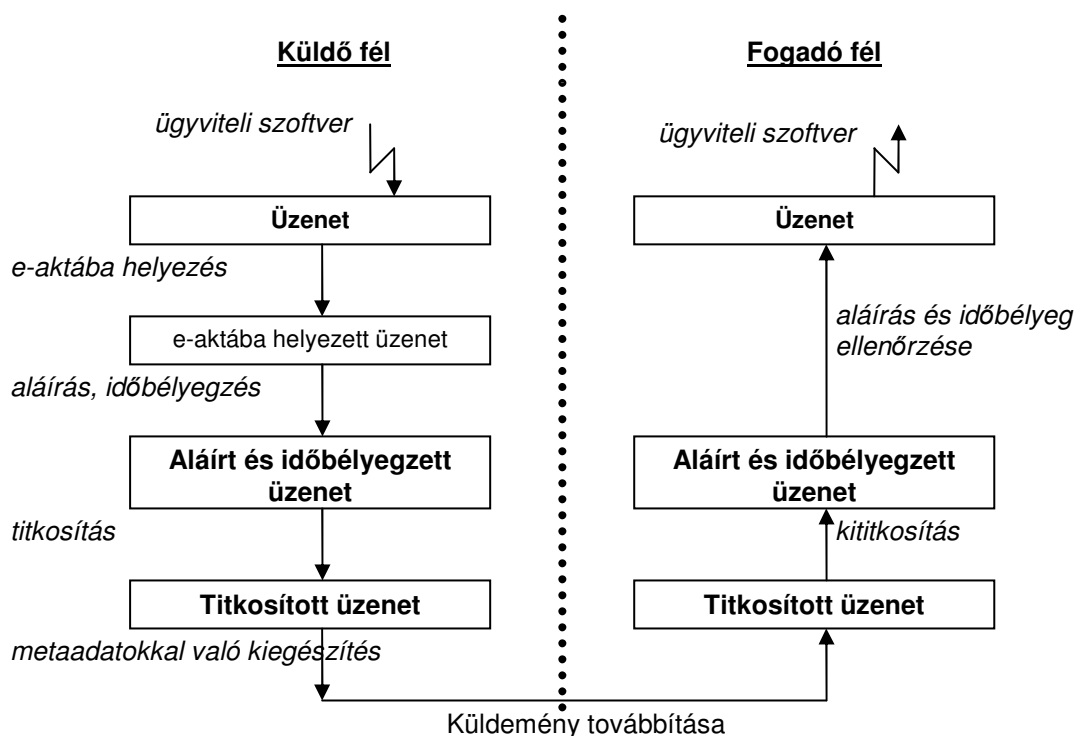
A válaszként kapott üzenet XML feldolgozása szintén a felhasználó rendszerének feladata. A gépi adatfeldolgozás elősegítése érdekében a küldhető XML-ek köre szabályozott.

A VIEKR rendszerben csak a „VIEKR üzenetformátum specifikáció” című dokumentumban meghatározott formátumú XML állományok küldhetőek<sup>12</sup>. 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 (címezési információkkal kiegészítve) kell elküldeni a rendszer segítségével a fogadó félnek.

A fogadó oldal a kapott e-aktát ktitkosítja, 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

<sup>1</sup> A dokumentáció tartalmazza a korábbi pénzügyi megkeresések rendszerében használt megkereséseket és válaszokat is.

<sup>2</sup> A meghatározott formátumhoz tartozó XML sémákat a kamara a VIEKR üzenetformátum specifikációban megadott központi helyen közzé teszi.

### 3.3. Megbízható üzenettovábbítás

A küldemények címzethez 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. Adott küldemény **kézbizítási 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 bizonyosságot.

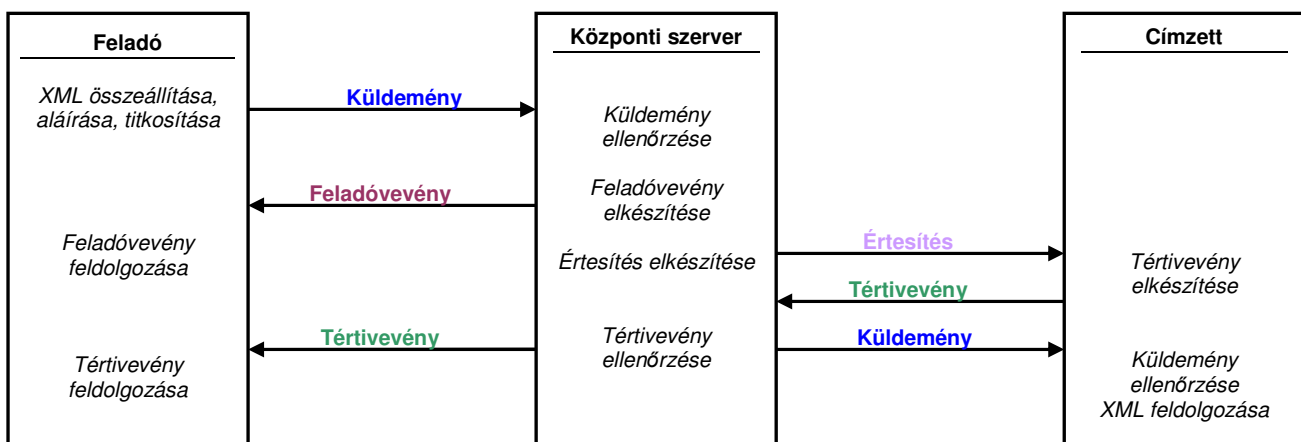
### 3.4. A kommunikáció folyamata

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 tesz 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 kézbizítása ugyanúgy történik, mint a küldeményké.
9. 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 legelső XML állomány tartalmazza (lásd: VIEKR 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 **kézbizítésének 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 is 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 figyelni).

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

### 3.5. Küldemények kézbizítési státuszai

Egy adott küldemény kézbizítési állapota nyomon követhető a rendszerben. A kézbizítéshez kapcsolódó minden fontos adat letölthető (pl. feladás dátuma, kézbizítés dátuma, feldolgozási állapot, kézbizítési állapot), a kapott adatok alapján elérhetőek a küldeményhez tartozó feladóvevény és tértivevény(ek) is.

Ez a funkció alapvetően nyomozásra, hibakeresésre szolgál, a rendes üzenetküldési folyamatnak nem képezi részét.

Egy adott szervezet csak az által beküldött, vagy neki küldött küldemények kézbizítési állapotát tekintheti meg.

### 3.6. Címzés: szervezetek és felhasználók

A VIEKR rendszerben az üzenet továbbítás **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 adataegységet) kezelheti<sup>3</sup>.

Az üzenetközvetítő rendszert csak regisztrált szervezetek regisztrált felhasználói használhatják<sup>4</sup>. A felhasználók a megadott autentikációs tanúsítvány alapján használhatják a rendszert.

Előfordulhat (pl. a pénzügyi 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<sup>5</sup>. Ehhez titkosításkor ismerni kell a két (több) szervezet aktuális felhasználóinak aktuális titkosító tanúsítványait.

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.

<sup>3</sup> Az egyes szervezetek küldeményeinek elkülönítését ekkor a felhasználó rendszerében kell megoldani. A szerverrel való kommunikációban meg kell adni, hogy aktuálisan mely szervezethez tartozó adatokat kívánja lekérni.

<sup>4</sup> A regisztráció a Vht-ban megfogalmazott feltételek szerint történik, a részleteket a rendszer „Felhasználási szabályzat” című dokumentuma tartalmazza.

<sup>5</sup> 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.



### **3.8. Kézbizítési vélelem beállta**

A Vht. szerint a kézbizítési 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 kézbizítottnek minősül.

Ha a kézbizítési 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 („vélelem”) 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 kézbizítés beálltát követően 30 nappal<sup>6</sup> törli a rendszerből.

### **3.10. Üzenetsémák központi nyilvántartása**

A VIEKR rendszerben csak a „VIEKR üzenetformátum specifikáció” című dokumentumban meghatározott formátumú XML állományok küldhetők – ide tartozik a pénzügyi 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.

### **3.11. A rendszerben használható tanúsítványok**

A VIEKR rendszerben minden felhasználónak pontosan három tanúsítvánnyal kell rendelkeznie: egy aláíróival, egy titkosítóval és egy autentikációval. Legalább fokozott biztonságú tanúsítványok használata kötelező. Mindhárom tanúsítványban szerepelnie kell a tulajdonos adatai között<sup>7</sup> a tulajdonos globálisan egyedi azonosítójának, amelyet az adott hitelesítés szolgáltató osztott ki számára. Az egy felhasználóhoz rendelt tanúsítványok esetében ezeknek egyezniük kell. Ez a regisztrációs folyamat során ellenőrzésre kerül.

### **3.12. A szerver túlzott terhelését előidéző felhasználási mód**

Amennyiben valamely felhasználó vagy rendszere bármilyen hibából eredően, szándékosan vagy véletlenül indokolatlanul nagy, a szolgáltatások normál elérhetőségét veszélyeztető terhelést ró a szerverre, akkor a VIEKR rendszer védelme érdekében az adott felhasználó illetve szervezete hozzáférése korlátozásra kerülhet.

---

<sup>6</sup> Ez – a kézbizítési vélelem miatt – legkésőbb a feladást követő 35. napot jelenti.

<sup>7</sup> A Subject DN-ban a SERIALNUMBER mezőben.

## 4. A rendszer működésének részletes bemutatása

### 4.1. REST

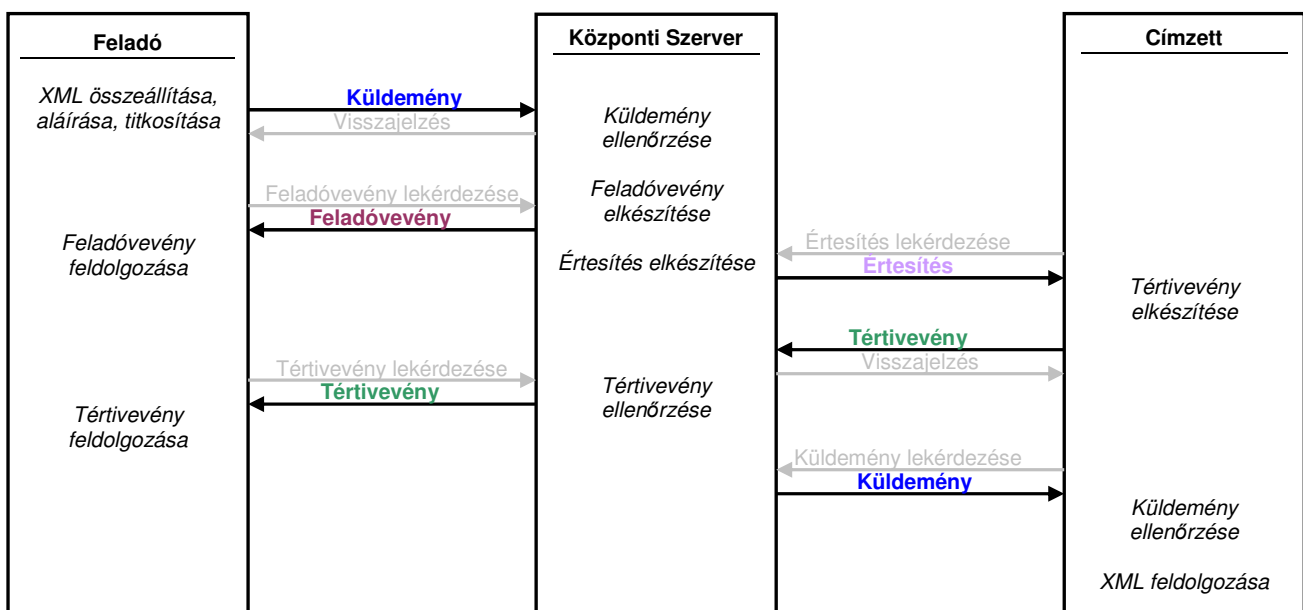
A Központi szerver funkciói **HTTP protokollon** keresztül érhetőek el **SSL felett** az RFC1945 és az RFC2616 ajánlások szerint. A szolgáltatásokat a **Representational State Transfer (REST)**<sup>8</sup> alapelveinek megfelelően nyújtja.

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 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<sup>9</sup>, pl. „9”. Továbbá minden szervezetnek létezik egy **SzervezetAzonosítója** is, amely lehet egy beszédes elnevezés, akár egy már létező cím is<sup>10</sup>, de a feltétel itt is az, hogy a rendszerben egyedinek kell lennie.

Hasonlóan, a felhasználók is rendelkeznek **FelhasználóID**-val és **FelhasználóAzonosítóval** is.

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

<sup>8</sup> Bővebb információ: [http://en.wikipedia.org/wiki/Representational\\_State\\_Transfer](http://en.wikipedia.org/wiki/Representational_State_Transfer)

<sup>9</sup> Ez a későbbiekben kiegészítésre kerülhet a rendszerre jellemző adattal, amely globálisan egyedivé teszi, pl. „9@viekr.mbvk.hu”.

<sup>10</sup> Például a végrehajtói irodák esetében a „VHI”, a pénzügyes 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 pénzügyintézetek),
- a megbízotti tevékenységet hivatásszerűen ellátó magánszemélyek 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 és feladóvevény) rendelkezik egy **globálisan egyedi azonosítóval**.

A küldemények (köztük a hibajelentések) és tértivevények 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)<sup>11</sup>.

A **FelhasználóID** 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 **ElozmenyAzonosito** metaadatban szerepel (hiszen azoknak is saját azonosítójuk van).

### 4.5. Címzés

A továbbítandó adategységek (küldemény, tértivevény és feladóvevény) burkoló e-aktájának metaadatai között szerepelnek továbbá a **CimzettSzervezetAzonosito** és **FeladoSzervezetAzonosito** metaadatok. A címzés ezek alapján történik<sup>12</sup>.

A FeladoSzervezetAzonosito elembe a küldő felhasználó szervezetének azonosítóját kell beírni<sup>13</sup>. A CimzettSzervezetAzonosito elembe a megcímezett szervezet azonosítója kerül, itt vesszővel elválasztva **több címzett is megadható!**

<sup>11</sup> Amennyiben a felhasználó több szervezethez tartozik, akkor annak a szervezetnek az ID-ját kell használni, akinek a nevében éppen eljár.

<sup>12</sup> 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).

<sup>13</sup> Ha a felhasználó több szervezethez is tartozik, akkor annak a szervezetnek az azonosítóját kell megadni, amelyiknek a nevében eljár.

## 4.6. Típus, üzenettípus

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

A **Típus** metaadat értéke lehet „KULDEMENY”, „FELADOVEVENY” és „TERTIVEVENY”<sup>14</sup>. Az **UzenetTípus** metaadat tartalma utal arra, hogy az e-akta belsejében milyen jellegű üzenet XML található, így értéke „KULDEMENY” típusú közlemény esetében lehet pl. „vegrehajto\_bank” vagy „hibajelentes”. Tértivevény esetében az üzenettípus csak akkor kerül kitöltésre, ha a tértivevény a szerver nyilatkozata a kézbizítási vélelem beálltáról. Ekkor ennek értéke „velelem”.

## 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 **kézbizítási állapotát** a szerver nyilvántartja, ez az állapot a küldemény azonosító alapján lekérdezhető.

Egy küldemény **feldolgozási állapota** (F) a következő lehet<sup>15</sup>:

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 **Státusz kód** illetve **Státusz leírás** adatokból derül ki.

Egy küldemény **kézbizítási állapota** (K) a következő lehet<sup>16</sup>:

1. **Tértivevényre vár:** A küldemény adatait tartalmazó értesítés elérhető, az alapján el kell készíteni és beküldeni a tértivevényt.
2. **Tértivevényezés alatt:** A küldeményhez tértivevény érkezett, de az még nem került feldolgozásra.
3. **Letölthető:** A küldeményre adott tértivevény ellenőrizve és jó, a küldemény letölthető.
4. **Kézbizített:** A küldeményt letöltötték.

Hasonlóan a **tértivevények** is rendelkeznek állapotokkal. A tértivevény **feldolgozási állapotai** megegyeznek a küldemény feldolgozási állapotaival. A **kézbizítási állapotok** közül azonban csak a „Letölthető” és „Kézbizített” állapotokat használjuk.

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

A küldemények, tértivevények és feladóvevények állapotai a szervertől lekérdezhetőek.

Adott felhasználónak (szoftverének) a következő esetekben van teendője:

- 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**, „**Letölthető**” vagy „**Kézbizített**” **kézbizítási állapotú** küldemény, amelynek a tértivevényét még nem töltöttük le, akkor annak tértivevényét le kell tölteni.
- C) Ha van **neki címzett**, „**Tértivevényre vár**” **kézbizítási állapotú** küldemény, akkor le kell töltenie az értesítést és tértivevényt kell adnia.
- D) Ha van **neki címzett**, „**Letölthető**” **kézbizítási állapotú** küldemény, amelyet még nem töltöttünk le, 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.

<sup>14</sup> A hibajelentés típusa „küldemény”.

<sup>15</sup> Az állapot pontos elnevezését a Microsec Megbízható üzenettovábbító szerver interfészének leírása tartalmazza.

<sup>16</sup> Az állapot pontos elnevezését a Microsec Megbízható üzenettovábbító szerver interfészének leírása tartalmazza.

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 **K3**-es állapotba.

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

#### 4.8. A kézbizítési 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, pl. amennyiben az átvett küldeményben található üzenet formátumhibás, vagy az aláírás nem megfelelő.

A „**vélelem**” egy speciális – záradékkal ellátott – tértivevény, amelyben a szerver igazolja a kézbizítés tényét. Erre akkor kerül sor, ha a címzett 5 munkanap alatt nem veszi át a küldeményt. Ekkor beáll a kézbizítési vélelem, és a címzett helyett a szerver készíti el a tértivevényt.

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

A következő táblázatban áttekintjük a kézbizítési adategységek fontosabb jellemzőit.

	Küldemény	Hibajelentés	Feladóvevény	Tértivevény	„Vélelem”	Értesítés	
<b>Formátum</b>	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.	
<b>Ki állítja elő?</b>	Felhasználó	Felhasználó Automatikusan generálható.	Központi szerver	Felhasználó	Központi szerver	Központi szerver	
<b>Honnan lehet letölteni?</b>	<a href="https://viekr.mbv.k.hu/viekr/rest/kuldemenyek/{azonosito}.es3">https://viekr.mbv.k.hu/viekr/rest/kuldemenyek/{azonosito}.es3</a>	<a href="https://viekr.mbv.k.hu/viekr/rest/kuldemenyek/{azonosito}.es3">https://viekr.mbv.k.hu/viekr/rest/kuldemenyek/{azonosito}.es3</a>	<a href="https://viekr.mbv.k.hu/viekr/rest/feladovevenyek/{azonosito}.et3">https://viekr.mbv.k.hu/viekr/rest/feladovevenyek/{azonosito}.et3</a>	<a href="https://viekr.mbv.k.hu/viekr/rest/tertivevenyek/{azonosito}.et3">https://viekr.mbv.k.hu/viekr/rest/tertivevenyek/{azonosito}.et3</a>	<a href="https://viekr.mbv.k.hu/viekr/rest/tertivevenyek/{azonosito}.et3">https://viekr.mbv.k.hu/viekr/rest/tertivevenyek/{azonosito}.et3</a>	<a href="https://viekr.mbv.k.hu/viekr/rest/kuldemenyek/{azonosito}.xml">https://viekr.mbv.k.hu/viekr/rest/kuldemenyek/{azonosito}.xml</a>	
<b>METAADATOK</b>	<b>Azonosito</b>	Felhasználó állítja 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.	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.
	<b>ElozmenyAzonosito</b>	NINCS	A hivatkozott küldemény Azonositoja	A hivatkozott küldemény Azonositoja	A hivatkozott küldemény Azonositoja	A hivatkozott küldemény Azonositoja	Nem értelmezett.
	<b>CimzettSzervezet</b>	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 kézbizítési vélelem beálltára vonatkozik.	Nem értelmezett.
	<b>FeladoSzervezet</b>	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.
	<b>Tipus</b>	küldemény	küldemény	feladóvevény	tértivevény	tértivevény	Nem értelmezett.
	<b>Uzenettpus</b>	Pl. pénzügyi megkeresés	hibajelentés	NINCS	NINCS	vélelem	Nem értelmezett.

Záradék	NINCS	NINCS	NINCS	NEM KÖTELEZŐ. Ha van, akkor a címzett által kiállított nyilatkozat., amely tartalmazza a szervezete azonosítóját.	Azon szervezetek azonosítóját tartalmazza, akiknél a kézbizítási vélelem beálltáról szól.	Nem értelmezett.
---------	-------	-------	-------	--	---	------------------

**1. táblázat A kézbizítási 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 előállítás, aláírása, titkosítása, küldemény előállítás, 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 alapfeladatokat a következő rendszerezés szerint:

### Küldési folyamat részeként:

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

### Fogadási folyamata 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<sup>17</sup>, beilleszti ezt egy e-aktába és időbélyeges aláírást készít rá<sup>18</sup>. Ezután beszerzi a címzett és a feladó szervezetekhez tartozó felhasználók titkosító tanúsítványait a Központi szerverről, 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: **Azonosító**, **CímzettSzervezetAzonosító**, **FeladóSzervezetAzonosító**, **Tipus**, **ÜzenetTipus**; a 4. fejezetben ismertetett szabályok szerint.

Ezután be kell jelentkezni a Központi szerverre (ekkor megtörténik a felhasználó autentikáció), 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 Azonosító), 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) számára. 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 státuskódból 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.

---

<sup>17</sup> A formátumát ellenőrizni kell a Központi szerverről beszerzett séma alapján.

<sup>18</sup> 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), akkor letölthető annak feladóvevénye.

A letölthető feladóvevények listáját a <https://viekr.mbvk.hu/viekr/rest/feladovevények/bejovo/letoltendo> címen lehet elérni, míg egy adott feladóvevényt a <https://viekr.mbvk.hu/viekr/rest/feladovevények/{azonosito}> címről lehet letölteni.

Egy felhasználó csak az ő szervezete számára küldött feladóvevényeket éri el<sup>19</sup>.

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 helyes tértivevényt adott egy neki küldött küldeményre, akkor a feladó számára elérhetővé válik a címzett által adott tértivevény.

Azaz, ha van olyan, a felhasználó által feltöltött küldemény, amely „letölthető” vagy „kézbizított” állapotban van, akkor letölthető az arra, a címzett által adott tértivevény. A letölthető tértivevények listáját a <https://viekr.mbvk.hu/viekr/rest/tertivevenyek/bejovo/letoltendo> címről lehet letölteni, míg egy adott tértivevényt a <https://viekr.mbvk.hu/viekr/rest/tertivevenyek/{azonosito}> címről lehet letölteni.

Egy felhasználó csak az ő szervezetének küldött (illetve a szervezete által készített) tértivevényeket éri el<sup>20</sup>.

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 címzettjei között, valamint a 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 (kézbizítottnek 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: 5.1.7. fejezet).

Ha az eredeti küldemény feladója hibajelentést kap, akkor annak letöltését követően kititkosítja, ellenőrzi rajta az aláírást és feldolgozza a benne szereplő adatokat, azaz intézkedik a hibajelentésben jelzett hiba megszüntetése érdekében. Ha a hibajelentés feldolgozása közben hibát észlel, akkor annak megoldását más csatornára kell terelni<sup>21</sup>; 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/bejovo/tertivevenyezendo> 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, akkor letöltheti a tértivevény készítéséhez szükséges adatokat tartalmazó értesítést a <https://viekr.mbvk.hu/viekr/rest/kuldemenyek/bejovo/tertivevenyezendo> címről.

Egy felhasználó csak az ő szervezetének címzett küldemények értesítéseit éri el<sup>22</sup>.

<sup>19</sup> Listázáskor a lekérdezés során kötelezően meg kell adni, hogy mely szervezet adatait kéri.

<sup>20</sup> Listázáskor a lekérdezés során kötelezően meg kell adni, hogy mely szervezet adatait kéri.

<sup>21</sup> A szerveren a szervezetek adatai között elérhetőek az Általános kapcsolattartó illetve a Technikai kapcsolattartó adatai.

<sup>22</sup> A lekérdezés során kötelezően meg kell adni, 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 szerepeltetheti 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/tertivevények>** címre.

A tértivevény feltöltésekor a szerver a letárolhatóság és visszakereshetőség feltételeit ellenőrzi (szerepel-e benne a globálisan egyedi Azonosító), 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. Ezek listáját a címzett a **<https://viekr.mbvk.hu/viekr/rest/kuldemenyek/bejovo/letoltendo>** címről tudja letölteni, míg egy adott küldeményt a **<https://viekr.mbvk.hu/viekr/rest/kuldemenyek/bejovo/letoltendo/azonositoAlapjan?{azonosito}>** címről lehet letölteni.

Egy felhasználó csak az ő szervezetének küldött és tértivevényezett (illetve a szervezet általa küldött) küldeményeket éri el<sup>23</sup>.

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 feladót. 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 Azonosító 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 státuszleírásból 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. Ezek listája a következő címen érhető el: **<https://pelda.pel.da/pelda/rest/kuldemenyek/kimeno/hibas>**.

A státuszleírás részletesebb információt is tartalmazhat a hiba okáról.

A hiba javítását követően a korábbi hibás küldemények tartalmát egy új (már helyes) küldeményben újra el kell küldeni (új Azonosító megadásával!).

Egy felhasználó csak az ő szervezete által küldött hibás küldeményeket éri el<sup>21</sup>.

---

<sup>23</sup> A lekérdezés során meg kell adni, 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, autentikációs és aláírói tanúsítványaira, valamint magánkulcsainak használatára.

A VIEKR szerver szabványos interfészen szolgálja ki az erőforrás-kéréseket (a részleteket lásd a Microsec Megbízható üzenettovábbító 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.

### **VHKIR kommunikációs modul funkciói:**

- 1. Szervezetek listájának letöltése**
- 2. Küldemény (hibajelentés) beküldése**
- 3. Tértivevények beküldése**
- 4. Feladóvevények letöltése**
- 5. Küldemények (hibajelentések) letöltése**
- 6. Tértivevények letöltése**
- 7. Beküldött hibás küldemények státuszának letöltése**
- 8. Státuszinformációk lekérdezése**
- 9. Félbehagyott feldolgozások folytatása**
- 10. Összes beérkező közlemény átvétele**
- 11. Bizonyítékelemek ellenőrzése**

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. Kézbizítási státusz
5. Szervezet
6. Tanúsítvány
7. Séma

Az erőforrásokat URL-lel lehet azonosítani. Például a bejövő letöltendő küldeményeket a **<https://viekr.mbvk.hu/viekr/rest/kuldemenyek/bejovo/letoltendo>** 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** formátumban (ekkor az adataikat kapjuk vissza), illetve speciális entitások lekérhetőek a „saját” formátumukban (az e-akta típusú entitások e-akta formátumban<sup>24</sup>, 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/bejovo/letoltendo.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 202: Accepted – A kérés sikeres volt. A küldeményt a szerveren aszinkron feldolgozásra átvette.
- 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

Ha nincs hiba (HTTP 200 vagy 201), 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**.

---

<sup>24</sup> 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 és a tértivevény. Utóbbi kettő speciális e-akta.

A HTTP 4\*\*-os státusz kód esetén adott hibakódok a következők lehetnek:

<b>Hibakód</b>	<b>Jelentése</b>
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 kulcsfelhasználás 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 (SenderOrganizationIdMismatchException)
4.0.016	Az adott szervezet nevében a felhasználó nem küldhet küldeményt (SenderUserIdMismatchException)
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 az általános felhasználók számára biztosított funkciók, erőforrásonkénti csoportosításban a következők:

### **Küldemények**

1. Küldemény feltöltése
2. Bejövő tértivevényezendő küldemények listája
3. Bejövő tértivevényezendő küldemények listája azonosító alapján
4. Bejövő letöltendő küldemények listája
5. Bejövő letöltendő küldemények listája azonosító alapján
6. Kimenő hibás küldemények listája
7. Kimenő hibás küldemények listája azonosító alapján
8. Adott küldemény letöltése

### **Feladóvevények**

9. Bejövő letöltendő feladóvevények listája
10. Bejövő letöltendő feladóvevények listája előzményazonosító alapján
11. Bejövő feladóvevények listája előzményazonosító alapján
12. Adott feladóvevény letöltése

### **Tértivevény**

13. Bejövő letöltendő tértivevények listája
14. Bejövő letöltendő tértivevények listája előzményazonosító alapján
15. Bejövő tértivevények listája előzményazonosító alapján
16. Tértivevény feltöltése
17. Adott tértivevény letöltése

### **Kézbizítási státusz**

18. Adott küldeményhez tartozó kézbizítási státusz letöltése

### **Szervezet**

19. Szervezetek listája
20. Adott szervezet adatainak lekérdezése

### **Tanúsítvány**

21. Új tanúsítvány feltöltése
22. Érvényes titkosító tanúsítványok listája
23. Adott tanúsítvány letöltése

### **Séma**

24. Sémák listája
25. Adott séma letöltése

A felsorolt funkciók részletes leírását a Microsec Megbízható üzenettovábbító 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/xmlsig#"
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 törtívény

```

<?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="P01fe31b7c-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="#P01fe31b7c-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>APf6hcZ0WpssDMXpZn10LEndC60=</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/xmlsig#sha1"/>
  <ds:DigestValue>oPdemB13IK1dAeeavuCTVzqH2mQ=</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 #P01fe31b7c-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/xmlsig#sha1"/>
              <ds:DigestValue>2BBHOXQuJwJOHCnSMRFmto+RSOE=

```



```

        </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/xmlsig#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>16283945475445056955051130376
0376565328</ds:X509SerialNumber>
          </IssuerSerial>
        </Cert>
        <Cert URI="#EC20893052-5952-11e0-b609-86b0f8800d63">
          <CertDigest>
            <ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
            <ds:DigestValue>g9GDrL9oT70N41vgpsnex3dwHmU=
            </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>374371239611423716322982027
43087162653</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>yyyxbkCLfbbueDsfdwk1LuVrrRg=
        </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>2248377330113881489465712
17034242358565</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>

```