

Telepítési dokumentáció

e-Szignó Hitelesítő Szerver (EHSZ)

Tomcat

Dokumentum verzió: 1.3

2021. 08. 24.



Tartalomjegyzék

1	Bevezetés	9
2	Fizikai rendszerterv	9
2.1	Architektúra	9
2.2	EHSZ minta konfigurációja	9
2.3	Architektúra terv	9
2.4	Belépés a rendszerbe	10
3	Az EHSZ architektúra leírás	10
3.1	Az EHSZ felépítése	11
3.1.1	Rest interfész	11
3.1.2	MQ interfész	11
4	Adatmodell és entitás specifikáció	11
4.1	Adatbázis	11
4.1.1	Adatbázis méretezés	12
4.1.2	Adatszerkezet	12
4.2	Adatbázis létrehozás Pl.: PostgreSQL-en	12
4.3	Adatbázis létrehozása Liquibase segítségével	13
5	Részletes interfész leírás	13
5.1	EHSZ webservice interfész funkciók	13
5.1.1	Szerver XML válasz formátumának leírása	14
5.1.2	ASiC_sign	14
5.1.3	ASiC_validate	15
5.1.4	ASiC_extension	16
5.1.5	ASiC_addarchivetimestamp	17
5.1.6	XAdES_sign	18
5.1.7	Add_archive_timestamp	20
5.1.8	XAdES_validate	21
5.1.9	Info	22
5.1.10	Encrypt	23
5.1.11	Decrypt	24
5.1.12	Pades_sign	25
5.1.13	Pades_validate	27
5.1.14	Pades_extension	28
5.1.15	Pades_addarchivetimestamp	29
5.1.16	Create_acknowledgement	30
5.1.17	Check_acknowledgement	31
5.1.18	XAdES_extension	32

5.1.19	Esign	34
5.1.19.1	Esign_pdfsign	38
5.1.19.2	Esign_xadessign	39
5.1.19.3	ESign_asicsign.....	40
5.1.19.4	Esign_signhash	42
5.1.19.5	Esign_downloadsignedfile.....	42
5.1.20	RemoteSign_PAdES	43
5.1.21	RemoteSign_PAdES_Status	44
5.1.22	RemoteSign_PAdES_Multiple	45
5.1.23	RemoteSign_PAdES_Status_Multiple.....	47
5.1.24	RemoteSign_XAdES.....	48
5.1.25	RemoteSign_XAdES_Staus	49
5.1.26	RemoteSign_ASIC	50
5.1.27	RemoteSign_ASIC_Staus.....	52
5.2	ESignProxy Callback funkció	53
5.3	Szerver PKI MQ interfész funkciók	53
5.3.1	XAdES_sign.....	54
5.3.2	XAdES_validate.....	54
5.3.3	Encrypt.....	55
5.3.4	Decrypt.....	55
5.3.5	Pades_sign.....	55
5.3.6	Pades_validate.....	56
5.3.7	Create_acknowledgement	56
5.3.8	Check_acknowledgement	57
5.4	EHSZ teszt oldalak	57
5.4.1	Regisztrációs információk	57
5.5	Monitor funkciók leírása	57
6	Konfiguráció	57
6.1	Szerver konfigurációs fájlok.....	57
6.1.1	A szerver tulajdonságai (ServerContext)	57
6.1.1.1	A szerver dedikált könyvtárai és fájljai.....	58
6.1.1.1.1	eszigno_cert_auth_dir - azonosítási tanúsítványokat tartalmazó könyvtár útvonal	58
6.1.1.1.2	eszigno_dir - e-Szignó telepítési könyvtár útvonala	58
6.1.1.1.3	eszigno_work_dir - e-Szignó munkakönyvtár útvonala	58
6.1.1.1.4	eszigno_intermediate_cert_dir - Köztes tanúsítványok könyvtárának útvonala	58
6.1.1.1.5	eszigno_trusted_cert_dir - Megbízható tanúsítványok könyvtárának útvonala	58

6.1.1.1.6	eszigno_ocsp_trusted_cert_dir - OCSP tanúsítványok könyvtárának útvonala	58
6.1.1.1.7	eszigno_signer_trusted_cert_dir - Aláírás ellenőrzésekor megbízhatónak elfogadott gyökértanúsítványok könyvtárának útvonala	58
6.1.1.1.8	eszigno_tsa_trusted_cert_dir - Időbélyeg tanúsítványok könyvtárának útvonala	59
6.1.1.1.9	eszigno_ssl_trusted_cert_dir - SSL tanúsítványok könyvtárának útvonala	59
6.1.1.1.10	server_upload_dir - A szerver feltöltési könyvtárának útvonala	59
6.1.1.1.11	eszigno_reg_file_path - e-Szignó regisztrációs fájl elérési útja	59
6.1.1.2	e-Szignó naplózás	59
6.1.1.2.1	eszigno_log_dir - Az e-Szignó napló könyvtárának útvonala	59
6.1.1.2.2	eszigno_log_level - Az e-Szignó naplózási szintje	59
6.1.1.2.3	eszigno_log_max_size - e-Szignó naplómérete	59
6.1.1.3	Proxy beállítások	59
6.1.1.3.1	eszigno_proxy_host - e-Szignó proxy host beállítása	60
6.1.1.3.2	eszigno_proxy_port - e-Szignó proxy port beállítása	60
6.1.1.3.3	eszigno_proxy_user - e-Szignó proxy felhasználó	60
6.1.1.3.4	eszigno_proxy_password - e-Szignó proxy felhasználó jelszava	60
6.1.1.3.5	eszigno_proxy_exception_list - e-Szignó proxy kivétel lista	60
6.1.1.4	e-Szignó futási módok	60
6.1.1.4.1	eszigno_run_mode - e-Szignó futási mód	60
6.1.1.4.2	daemon_port - e-Szignó daemon port	60
6.1.1.4.3	daemon_children_number - e-Szignó daemon gyereke száma	60
6.1.1.5	e-Szignó egyéb beállítások	60
6.1.1.5.1	eszigno_digest_algorithm - e-Szignó lenyomatképző algoritmus	60
6.1.1.5.2	eszigno_sdk_password - e-Szignó SDK jelszó	61
6.1.1.5.3	eszigno_time_out_millisec - e-Szignó kapcsolódási timeout	61
6.1.1.5.4	eszigno_xades_version - aláírásoknál használt XAdES verzió	61
6.1.1.5.5	verbose - e-Szignó verbose mód	61
6.1.1.6	ESign szerver beállítások	61
6.1.1.6.1	esign_proxy_mode - ESignProxy-n történő állapotváltozás nyomonkövetése	61
6.1.1.6.2	esign_max_thread_num - várakozó szálak maximális száma	61
6.1.1.7	Dokumentum törlési beállítások	61
6.1.1.7.1	delete_poll_second - A fájlok életkorának ellenőrzési periódusa	61
6.1.1.7.2	delete_period_second - A fájlok maximális életkora	62
6.1.1.8	Adatbázis elérés	62
6.1.1.8.1	db_resource_jndi_name - Adatbázis elérés	62
6.1.1.9	MQ beállítások (MQWorkerContext)	62
6.1.1.9.1	Queue manager csoport	62

6.1.1.9.2	Globális MQ beállítások	63
6.1.1.10	Tárolt kulcsú aláírás szolgáltatás (TKSZ)	63
6.1.1.10.1	remote_sign_session_dir – Session könyvtár	63
6.1.1.10.2	clean_poll_remote_sign_session_dir_second – Ideiglenes fájlok vizsgálata ideje	64
6.1.1.10.3	clean_period_remote_sign_session_dir_second – Ideiglenes fájlok élettartama	64
6.1.1.11	Bizalmi listák kezelése (EU TSL)	64
6.1.1.11.1	tsl_usage_mode – TSL használat módja	64
6.1.1.11.2	tsl_cache_dir – TSL munkakönyvtár	64
6.1.1.11.3	tsl_service_info_usage – TSL használatot segítő Microsec szolgáltatás használata	64
6.1.1.11.4	tsl_root_url – Gyökér TSL elérési URL-je	64
6.1.1.11.5	tsl_trusted_cert_dir – TSL megbízható tanúsítványok könyvtára	64
6.1.1.12	Szerver konfiguráció MQ használatával	65
6.1.1.13	Szerver konfiguráció MQ nélkül	68
6.1.2	Technikai felhasználói profilok (UserProfile)	71
6.1.2.1	Átvételi elismervény beállításai	71
6.1.2.1.1	acknowledgement_version – átvételi elismervény verziója	71
6.1.2.2	Titkosítás visszafejtése	71
6.1.2.2.1	decryptor_key – A profil tulajdonosának magánkulcsa	71
6.1.2.2.2	decryptor_password – visszafejtő magánkulcs jelszava	71
6.1.2.3	Az ESign protokoll beállításai	71
6.1.2.3.1	esign_use – ESign szolgáltatás ki-be kapcsolása	71
6.1.2.3.2	esign_auth_http_username – Authentikáció az ESignProxy szerveren	71
6.1.2.3.3	esign_auth_http_password – Authentikáció az ESignProxy szerveren	71
6.1.2.3.4	esign_use_pkcs7 – Kérelem aláírás	71
6.1.2.3.5	esign_server_url – ESignProxy szerver gyökér URL-je	72
6.1.2.3.6	esign_spname – Kiszolgáló rendszer neve	72
6.1.2.3.7	esign_message – üzenet	72
6.1.2.3.8	esign_image_format – QR kód képformátuma	72
6.1.2.3.9	esign_poll_delay_sec – Két pollozás közti idő	72
6.1.2.3.10	esign_poll_timeout_sec – teljes lekérés időtúllépése	72
6.1.2.4	Időbélyeg szerver beállítások	72
6.1.2.4.1	esigno_timestamp_provider_host – Időbélyeg szolgáltató host	72
6.1.2.4.2	esigno_timestamp_url_list – Időbélyeg URL-ek	72
6.1.2.4.3	esigno_auth_http_username – Időbélyeg hosztra felhasználói név	72
6.1.2.4.4	esigno_auth_http_password – Időbélyeg hosztra jelszó	72
6.1.2.4.5	esigno_auth_key – Időbélyeg hosztra autentikációs tanúsítvány	73

6.1.2.4.6	esizigno_auth_key_password – Az autentikáció tanúsítvány jelszava	73
6.1.2.5	Általános aláírási beállítások	73
6.1.2.5.1	esizigno_signer_key_form – aláíró kulcs formátuma	73
6.1.2.5.2	ignore_keyusage – Aláírói kulcshasználat megkövetelése	73
6.1.2.5.3	ocsp_url_list – e-Szignó dedikált OCSP URL-jei	73
6.1.2.5.4	revocation_checking_mode – Tanúsítvány visszavonási állapot ellenőrzés módja	73
6.1.2.5.5	server_cert_validation – Szerver tanúsítvány ellenőrzés	73
6.1.2.5.6	validate_ocsp_responder – OCSP válaszadó visszavonási állapot ellenőrzés	73
6.1.2.5.7	wait_for_grace_period – Csak megbízható időpont utáni OCSP/CRL-t fogadjon el	74
6.1.2.5.8	use_ocsp_cache – e-Szignó OCSP cache	74
6.1.2.5.9	xades_type – AdES típus beállítása	74
6.1.2.5.10	signer_key – A profilhoz tartozó aláírói magánkulcs	74
6.1.2.5.11	signer_password – Az aláírói magánkulcs jelszava	74
6.1.2.6	PDF (PAdES) aláírás	74
6.1.2.6.1	pdfsig_img_visible – Látható legyen-e az aláírás	74
6.1.2.6.2	pdfsig_adjust – Egymást elfedő aláírások eltolása	74
6.1.2.6.3	pdfsig_align – Látható aláírás igazítása a megadott sarokba	74
6.1.2.6.4	pdfsig_img – Látható aláírás képének útvonala	75
6.1.2.6.5	pdfsig_resize – Új méret[%]	75
6.1.2.6.6	pdfsig_resize_mode – Az átméretezés módja	75
6.1.2.6.7	pdfsig_padding_x – Vízszintes behúzás[%]	75
6.1.2.6.8	pdfsig_padding_y – Függőleges behúzás[%]	75
6.1.2.6.9	pdfsig_page – Az oldal száma	75
6.1.2.6.10	pdfsig_title_visible – Az aláírás feliratának megjelenítése	75
6.1.2.6.11	pdfsig_title_align – Az aláírás felirata	75
6.1.2.6.12	pdfsig_title_align – A szöveg igazításának módja	76
6.1.2.6.13	pdfsig_title_fontsize – A szöveg betűmérete	76
6.1.2.6.14	pdfsig_title_padding_x – Vízszintes margó	76
6.1.2.6.15	pdfsig_title_padding_y – Függőleges margó	76
6.1.2.7	Tárolt kulcsú aláírás (TKASZ)	76
6.1.2.7.1	remote_signer_url – TKASZ URL	76
6.1.2.7.2	remote_signer_user – TKASZ felhasználónév	76
6.1.2.7.3	remote_signer_pass – TKASZ jelszó	76
6.1.2.7.4	remote_signer_auth_cert – TKASZ autentkációs tanúsítvány	76
6.1.2.7.5	remote_signer_auth_cert_pass – TKASZ autentkációs tanúsítvány jelszava	77
6.1.2.7.6	remote_signer_pin – TKASZ felhasználó pin kódja	77

6.2	Monitorozó rendszer konfiguráció	81
6.2.1	A monitorozó rendszer tulajdonságai (MonitorProperties)	81
6.2.1.1	Az EHSZ Kliensek URL-jei	81
6.2.1.2	Az EHSZ URL-je	81
6.2.1.3	Az adatbázi elérés	81
6.2.1.4	Értesítési beállítások	81
6.2.1.4.1	Címzettek	81
6.2.1.4.2	A feladó	81
6.2.1.4.3	Értesítés tanúsítvány lejáratáról	81
6.2.1.4.4	Tanúsítvány lejárat ellenőrzése	81
6.2.1.5	A Java Mail API beállításai	82
6.2.1.5.1	SMTP host	82
6.2.1.5.2	SMTP port	82
6.2.1.6	Minta konfigurációs fájl	82
6.3	Adatbázis beállítás Apache Tomcat esetében	84
6.3.1	context.xml	84
6.3.2	microsec-pki-service-server-web.war-ban levő web.xml fájl	84
7	Hibakezelés	85
7.1	Hibakezelés REST-es felület esetén	85
7.1.1	Hibakódok	85
7.1.2	A kliensek számára ajánlott hibakazelés	86
7.1.2.1	Minden rendben	86
7.1.2.2	Dokumentum hiba	86
7.1.2.3	Kliens hiba	86
7.1.2.4	Szerver hiba	86
7.2	Hibakezelés MQ felület esetén	86
8	Naplózás	86
8.1	Műszaki naplózás	86
8.1.1	Naplózási szintek	86
8.1.1.1	DEBUG szint	86
8.1.1.2	INFO szint	86
8.1.1.3	WARNING szint	86
8.1.1.4	ERROR szint	87
8.1.2	log4j.properties	87
8.1.3	log4j-monitor.properties	87
8.2	Auditnaplózás	87
9	A PKI rendszer működéséhez szükséges URL-ek a tűzfal konfigurációs beállításokhoz	87
9.1.1	Időbélyegzés	87

9.1.2	Tanúsítványok	87
9.1.3	OCSP kérés	88
9.1.4	CRL letöltés	88
9.1.5	Teszt időbélyegzés	88
9.1.6	Teszt tanúsítványok.....	88
9.1.7	Teszt OCSP kérés	88
9.1.8	Teszt CRL letöltés:	88
9.1.9	IP címek	88

1 Bevezetés

Az e-Szignó Hitelesítő Szerver (EHSZ) szolgáltatásként nyújt PKI funkciókat. Segítségével házon belül könnyen kialakítható elektronikus aláíró központ. REST API segítségével az integráció gyorsan elvégezhető.

Jelen dokumentáció leírja az EHSZ működését, kapcsolódási felületeit és architektúráját.

2 Fizikai rendszerterv

2.1 Architektúra

A teljes rendszer négyféle felületet biztosít különböző felhasználók, programok számára, hogy PKI műveleteket végezhesenek:

- automatizálható rendszerek számára az EHSZ-hez kifejlesztett kliensek nyújtanak MQ2File interfészen keresztül PKI szolgáltatásokat,
- Ugyancsak programok számára MQ-s felülettel rendelkező interfésszel is rendelkezik a rendszer.
- Az EHSZ közvetlenül is megszólítható egy REST alapú interfész segítségével.
- A rendszerhez opcionálisan tartozik egy monitorozó modul is, mely a szerver működését monitorozza és admin funkciókkal látja el.

A rendszer része az adminisztrációs és monitorozó funkciókat ellátó modul. Ezen modul webes felületén keresztül adminisztrálható a többi rendszerkomponens. Itt lehet lekérdezéseket és statisztikákat készíteni.

A teljes rendszer (szerver, kliens, adatbázis, monitorozó modul) egy virtuális gépen futtatható.

2.2 EHSZ minta konfigurációja

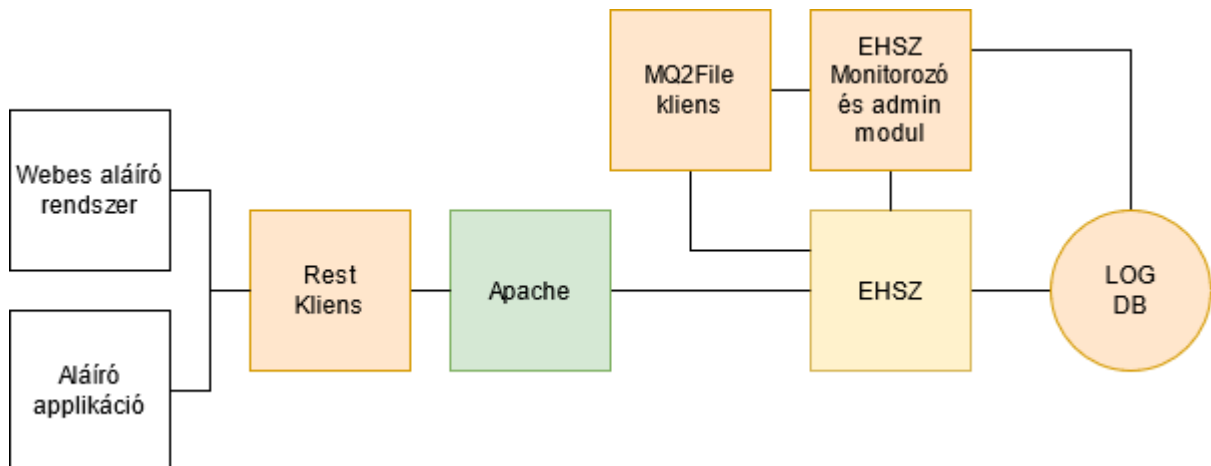
Operációs rendszer:	Red Hat Enterprise Linux 6.4 x64, alap telepítés (vagy újabb) Windows Server 2008 R2 (vagy újabb)
Java virtuális gép:	Java 8
Java EE6 vagy 7 minősítésű alkalmazás szerver:	Payara Server 4.1.2.x (Full) (vagy újabb) GlassFish 4.1.2.2 (vagy újabb) JBoss 7.1.1 (vagy újabb) WildFly 12.x (vagy újabb) Oracle WebLogic 12C (vagy újabb) Apache Tomcat 9.0.43 (vagy újabb)
Adatbázis kezelő:	PostgreSQL v9.2 (vagy újabb)

2.3 Architektúra terv

Az EHSZ gépen fut egy Java Alkalmazás Szerver melyben futnak az aláírási szolgáltatásokat ellátó EHSZ, EHSZ Kliens és Monitorozó Rendszer komponensek. A monitorozó rendszer része a PostgreSQL alapú napló adatbázis is.

Ezen a gépen kaphat helyet egy opcionális webes aláíró rendszer is, melyet Pl.: egy Apache webszerver futtat, lehetőséget teremtve céges aláírás és ügyfél oldali webes felületű aláírás elhelyezésére egyazon dokumentumon. Az Apache alkalmazásával lehetőség nyílik TLS használatára, illetve tanúsítvány vagy jelszó alapú ügyfél azonosításra. Ez utóbbi megoldások erősen ajánlottak. A rendszer képes aláírni megfelelően felkészített aláíró vastag klienssel, applikációval, webes felületű aláíró rendszerekkel is. Ezekhez tartalmaz a rendszer egy Java-ban

kifejlesztett EHSZ klienst is.



1. ábra

Teljes EHSZ rendszer felépítése

2.4 Belépés a rendszerbe

Az EHSZ elérését a Java Alkalmazás Szerver elé telepített Apache webserveren vagy magán a Java Alkalmazás Szerveren kell beállítani. Lehetséges HTTP Basic vagy TLS Cert alapú autentikáció. Az EHSZ gép adminisztrálása SSH-n keresztül történik.

3 Az EHSZ architektúra leírás

A rendszer hitelesítést végző komponense. Az EHSZ egyszerre több szálon képes különböző dokumentumok hitelesítésére, vagy más PKI műveletek végrehajtására. Az EHSZ MQ alapú interfészen keresztül vagy REST alapú web szolgáltatás interfészen keresztül tartja a kapcsolatot a többi rendszerrel. Az EHSZ-t az EHSZ Kliensek, a web-Szignó és egyéb külső rendszerek látják el feladatokkal.

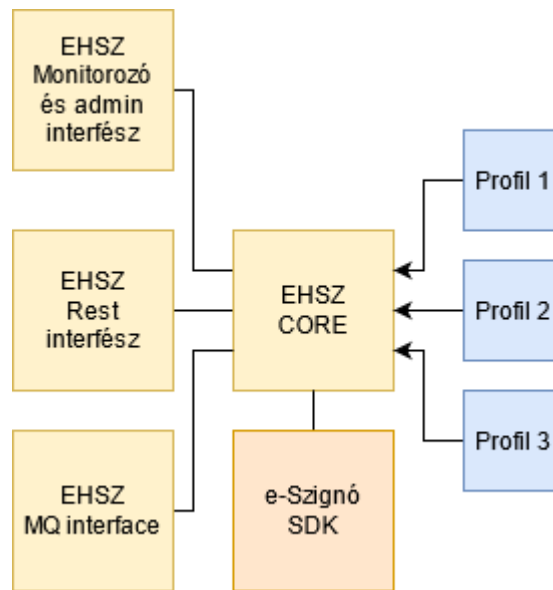
Az EHSZ a következő szolgáltatásokat nyújtja:

- ASiC, PAdES, XAdES aláírási,
- XAdES titkosítási és titkosítás visszafejtési,
- validálási szolgáltatások,
- ezen kívül támogatja az ügyfél általi kétmenetes webes aláírást is.

Az EHSZ azon szabály alapján működik, hogy a kapott dokumentumon a megszólított szolgáltatás felhasználói profiljához tartozó helyi konfigurációja alapján elvégzi a feladatát és az eredményként mindig visszaadja annak a rendszernek, vagy felhasználónak, aki küldte. Hiba esetén hibakódot ad vissza válaszként a küldő kliens számára.

Az EHSZ a Java Alkalmazás Szerverben futó webes alkalmazás.

3.1 Az EHSZ felépítése



2. ábra

Az EHSZ felépítése

A monitorozó és adminisztrációs modul használata opcionális. Az aláíró server ezen modulok nélkül is képes ellátni a szükséges PKI funkciókat.

3.1.1 Rest interfész

Ezen a REST alapú webszolgáltatás felületen keresztül kapja az EHSZ a feladatokat és ezen keresztül küldi vissza az eredményt a hívó rendszernek szinkron módon.

Az interfészt jellemzően az EHSZ Kliens hívja és látja el feladatokkal. Mivel a webservice felülete általános PKI funkciókat valósít meg, így a későbbiekben bármilyen másik rendszer is illeszthető hozzá.

Az interfész funkciók logikailag két csoportra oszthatók:

- **PKI funkciók:** Ezek az aláírással, aláírás ellenőrzéssel, titkosítással kapcsolatos funkciók.
- **Üzemeltetési funkciók:** Az EHSZ adminisztrálásával és monitorozásával kapcsolatos funkciók. Ilyen funkciók pl.: a server újraindítása, a tanúsítványok állapotának lekérdezése. Ezen funkciók opcionálisan részei a servernek.

3.1.2 MQ interfész

A webszolgáltatás felülethez hasonló – funkcionalitásában megegyező interfészről van szó.

Az interfészt jellemzően az EHSZ Kliens hívja és látja el feladatokkal. Mivel a webservice felülete általános PKI funkciókat valósít meg, így a későbbiekben bármilyen másik rendszer is illeszthető hozzá.

Az interface részletes leírása a következő fejezetekben található.

4 Adatmodell és entitás specifikáció

4.1 Adatbázis

A naplóbejegyzések mentése opcionálisan egy PostgreSQL v9.2 alapú adatbázisba történik. Beállítás hiányában fájlba történik a naplózás.

4.1.1 Adatbázis méretezés

Az adatbázisba az EHSZ által végzett műveletek sikerességéről szóló státusz üzenetek kerülnek. Így tranzakciónként –aláírás, ellenőrzés, titkosítás, ... - 2-3 bejegyzés kerül az adatbázisba.

4.1.2 Adatszerkezet

EHSZ naplóját tartalmazó tábla:

```
CREATE TABLE hsz.server_operation_log
(
    profile_name character varying(50),
    function_name character varying(50),
    file_name character varying(256),
    parameters character varying(1000),
    status_code integer,
    creation_date timestamp without time zone
)
```

A `server_operation_log` tábla minden rekordja egy-egy fájlban végzett pki műveletet jelent. A tábla oszlopainak magyarázata:

- `profile_name` – a művelethez tartozó profil neve és beállításai
- `function_name` – a művelet megnevezése
- `file_name` – a fájl(ok) neve, amin a műveletet elvégezték
- `parameters` – a műveletet végrehajtó e-Szignó hívás paraméterei
- `status_code` – a művelet sikerességét vagy hiba esetén a hiba okát jelzi. e-Szignó exit kód.
- `creation_date` – a rekord keletkezésének, a művelet kezdetének időpontja

4.2 Adatbázis létrehozás Pl.: PostgreSQL-en

Adatabázis létrehozása Pl.: PostgreSQL esetében Windowson

```
psql -U postgres
[postgres]$ CREATE USER signer WITH ENCRYPTED PASSWORD 'signer';
[postgres]$ CREATE DATABASE signer WITH OWNER = signer ENCODING = 'UTF8' TABLESPACE=pg_default
CONNECTION LIMIT = -1;
[postgres]$ GRANT ALL PRIVILEGES ON DATABASE signer TO signer;
[postgres]$ ALTER USER signer WITH PASSWORD 'signer';
[postgres]$ \q

psql -d signer -U signer -l -f create_hsz_schema.sql
```

Master SQL (create_hsz_schema.sql)

```
DROP TABLE IF EXISTS hsz.server_operation_log;
DROP TABLE IF EXISTS hsz.client_operation_log;
DROP TABLE IF EXISTS hsz.message_log;

DROP SCHEMA IF EXISTS hsz;

CREATE SCHEMA hsz
    AUTHORIZATION signer;

CREATE TABLE hsz.server_operation_log
(
    profile_name character varying(50),
    function_name character varying(50),
    file_name character varying(256),
    request_message_id VARCHAR(24),
    parameters character varying(1000),
    status_code integer,
    creation_date timestamp with time zone
)
```

```
)
WITH (
  OIDS=FALSE
);
ALTER TABLE hsz.server_operation_log
  OWNER TO signer;
```

4.3 Adatbázis létrehozása Liquibase segítségével

Az EHSZ csomag tartalmaz egy Liquibase 3.8.0 (vagy újabb) segítségével futtatható script-et is. Ennek használata megkönnyíti majd az adatbázis frissítést, ha a későbbi EHSZ release-ek során változna az adatbázis szerkezete. PostgreSQL esetében a postgresql-42.2.18.jar-t elérhetővé kell tenni (lásd a „Changelog futtatása Liquibase 3.8.0.-val” példát).

db_change_log_main.xml tartalma

```
<?xml version="1.1" encoding="UTF-8" standalone="no"?>
<databaseChangeLog
  xmlns="http://www.liquibase.org/xml/ns/dbchangelog"
  xmlns:appdba="http://www.datical.net/xml/ns/appdba"
  xmlns:datical="http://www.datical.net/xml/ns/datical"
  xmlns:ext="http://www.liquibase.org/xml/ns/dbchangelog-ext"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.liquibase.org/xml/ns/dbchangelog-ext
http://www.liquibase.org/xml/ns/dbchangelog/dbchangelog-ext.xsd
http://www.liquibase.org/xml/ns/dbchangelog http://www.liquibase.org/xml/ns/dbchangelog/dbchangelog-
3.8.xsd">
  <changeSet author="microsec" id="1">
    <sql dbms="postgresql" endDelimiter=";">
      CREATE SCHEMA hsz
    </sql>
  </changeSet>
  <changeSet author="microsec" id="2">
    <createTable tableName="server_operation_log" schemaName="hsz">
      <column name="profile_name" type="VARCHAR(50)" />
      <column name="function_name" type="VARCHAR(50)" />
      <column name="file_name" type="VARCHAR(255)" />
      <column name="request_message_id" type="VARCHAR(24)" />
      <column name="parameters" type="VARCHAR(1000)" />
      <column name="status_code" type="INTEGER" />
      <column name="creation_date" type="TIMESTAMP WITH TIME ZONE" />
    </createTable>
  </changeSet>
</databaseChangeLog>
```

Changelog futtatása Liquibase 3.8.0-val (Linux)

```
./liquibase-3.8.0/liquibase --logLevel=DEBUG --classpath=./postgresql-42.2.8.jar --
driver=org.postgresql.Driver --url=jdbc:postgresql://localhost:5432/ --username=signer --
password=signer --changeLogFile=./db_change_log_main.xml update
```

Changelog futtatása Liquibase 3.8.0-val (Windows)

```
liquibase-3.8.0\liquibase.bat --logLevel=DEBUG --classpath=postgresql-42.2.8.jar --
driver=org.postgresql.Driver --url=jdbc:postgresql://localhost:5432/ --username=signer --
password=signer --changeLogFile=db_change_log_main.xml update
```

5 Részletes interfész leírás

5.1 EHSZ webservice interfész funkciók

Három bemeneti információ szükséges egy funkció meghívásához:

- **Funkció neve** – Ez határozza meg a bemeneti adaton elvégzendő műveletet.
- **Profil** – A PKI környezet beállításai. Részletesebb leírás a „Profil leírása” című fejezetben található
- **Bemeneti adatok** – Ezen az adat(ok)on végzi el a szerver a műveletet.

A szerver http csatornán keresztül érhető el. Mivel az EHSZ rendszert csak más belső rendszerek használhatják, így felhasználó azonosítást nem követel meg a szerver. Erről igény esetében a

rendszer üzemeltetőnek kell gondoskodnia úgy, mint a TLS csatorna használatáról is.

Az EHSZ rendszer interfészt leíró WADL fájlok az alábbiakban találhatók.

5.1.1 Szerver XML válasz formátumának leírása

Az egyes funkciók jellemzően vagy az aláírt fájlal térnek vissza, vagy az adott aláírt állományról készített xml fomátumú riporttal.

Amennyiben a XAdES aláírásról van szó, úgy az xml formátuma megfelel az érvényben lévő szabványnak:

https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.00.00_20/en_31913201v010000a.pdf

Ha e-akta fomrátumú a visszatérési érték, akkor a következő linken található a formátum leírás: <https://e-szigno.hu/tudasbazis/e-akta-formatum-specifikacioja.html>

Az xml formátumú riportok leírását az e-Szignó fejlesztő csomagban található parancssori e-Szignó intefész dokuemtációban találja: doc/eszigno3_ref.html

5.1.2 ASiC_sign

Asic_signinterfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application
    xsi:schemaLocation="http://wadl.dev.java.net/2009/02
                        http://wadl.dev.java.net/2009/02 wadl.xsd"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="/pki">
      <resource path="/asicsign">
        <method name="POST" id="asicsign">
          <request>
            <doc title="ASiC aláírás" xml:lang="hu">Egy vagy több dokumentum ASiC
konténerbe helyezése és XAdES aláírása.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="containerTitle" required="true" type="String">
                <doc title="containerTitle" xml:lang="hu">Az ASiC konténer zip fejléc
szöveg</doc>
              </param>
              <param name="inFileX" required="true" repeating="true" type="File">
                <doc title="inFileX" xml:lang="hu">
                  Az aláírandó fájlok, melyek name paramétere inFile-lal kezdődik
és egymástól eltérő értékű.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/vnd.etsi.asic-e+zip">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab ASiC formátumú konténer. A fájl nevét a headerből
lehet kiolvasni.
                A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve	Asic_sign
Bemeneti adatok	- profileId - Szerver profil megnevezés

	- containerTitle – Az elkészülő konténer zip fejléc szöveg - inFileX - Aláírandó fájlok listája
Funkció leírása	A bemeneti fájl lista tartalmát elhelyezi egy ASiC konténerben és a megadott profil alapján aláírja őket (az összeset). A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren a program hibára fut. A feltöltött aláírandó fájloknak tetszőleges a neve. A program a feltöltött névvel fogja beilleszteni a konténerbe. A konténernek a containerTitle paraméterben megadott zip fejléc szöveget fogja adni. A válasz az elkészült ASiC konténer.
Visszatérő adatok	Az ASiC konténer, hiba esetén az „Hibakódok” fejezetben meghatározott hibakódok egyike.
URL	localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/asicsign

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/asicsign" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="text" id="containerTitle" name="containerTitle" value="Megjegyzés"/>
  <input type="file" id="inFile0" name="inFile0" />
  <input type="file" id="inFile1" name="inFile1" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.3 ASiC_validate

Asic_validate interfész leíró wadl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="asicvalidate">
        <method name="POST" id="asicvalidate">
          <request>
            <doc title="ASiC aláírás ellenőrzése" xml:lang="hu">Pontosan egy darab ASiC
konténer illetve az ebben lévő összes aláírás ellenőrzése.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">Az ellenőrizendő ASiC
konténer.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="text/xml">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab eredmény xml dokumentumot tartalmaz. A fájl nevét
a headerből lehet kiolvasni.
                A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
```

```
</application>
```

Funkció neve	ASiC_validate
Bemeneti adatok	- inFile – Az aláírást tartalmazó ASiC konténer - profileId - Szerver profil megnevezés
Funkció leírása	A bemeneti ASiC konténert megnyitja és ellenőrzi a benne található összes aláírást és időbélyeget. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren a program hibára fut. Az ellenőrzés végén a program egy XML formátumú választ ad.
Visszatérő adatok	Az aláírás ellenőrzés eredményét jelző validációs XMLt ad. Az XML formátuma a „Szerver XML válasz formátumának leírása” fejezetben található
URL	localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/asicvalidate

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/asicvalidate" enctype="multipart/form-data" id="formid" name="formname">
<input type="text" id="profileid" name="profileId" value="client1"/>
<input type="file" id="inFile" name="inFile" />
<input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.4 ASiC_extension

Asicextension requestet leíró xml séma

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="asicextension">
        <method name="POST" id="asicextension">
          <request>
            <doc title="ASiC aláírások kiterjesztése" xml:lang="hu">Az ASiC konténerben
lévő összes aláírás ellenőrzése és kiterjesztése. A kiterjesztés típusa a profileId paraméter által
meghivatkozott profil alapján kerül meghatározásra.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">A kiterjesztendő ASiC
konténer.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/vnd.etsi.asic-e+zip">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab eredmény ASiC konténert tartalmaz. A fájl nevét a
headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
```



```
</resource>
</resources>
</application>
n>
```

Funkció neve	ASiC_extension
Bemeneti adat	- inFile– A kiterjesztendő ASiC konténer - profileId – Szerver profil megnevezés
Funkció leírása	Az ASiC konténerben lévő összes aláírás ellenőrzése és kiterjesztése. A kiterjesztés típusa a profileId paraméter által meghivatkozott profil alapján kerül meghatározásra. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A válasz egy darab eredmény ASiC konténert tartalmaz. A fájl nevét a headerből lehet kiolvasni. A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/asicextension

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-
web/PKIServlet/pki/asicextension" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inFile" name="inFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.5 ASiC_addarchivetimestamp

Asicaddarchivetimestamp requestet leíró xml séma

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="asicaddarchivetimestamp">
        <method name="POST" id="asicaddarchivetimestamp">
          <request>
            <doc title="Archív időbélyeg hozzáadása" xml:lang="hu">ASiC konténer archiv
            időbélyegzése</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
                azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">Az archiv időbélyegezendő ASiC
                konténer.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/vnd.etsi.asic-e+zip">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab eredmény ASiC konténert tartalmaz. A fájl nevét a
                headerből lehet kiolvasni.
            </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.

```

        </doc>
      </representation>
    </response>
  </method>
</resource>

</resource>
</resources>
</application>

```

Funkció neve	ASiC_addarchivetimestamp
Bemeneti adat	- inFile– Az archív időbélyegezendő ASiC konténer - profileId – Szerver profil megnevezés
Funkció leírása	ASiC konténer archív időbélyegzése. Megjegyzés: Ha a konténerben található bármely aláírás nem A típusú, akkor időbélyegzés helyett kiterjesztést csinál. Ez BES típusú aláírás esetén 2 időbélyeg lekérést jelent (signaturetimestamp, archivetimestamp). A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A válasz egy darab eredmény ASiC konténert tartalmaz. A fájl nevét a headerből lehet kiolvasni. A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/asicaddarchivetimestamp

Példa form:

```

<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/asicaddarchivetimestamp" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inFile" name=" inFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>

```

5.1.6 XAdES_sign

Xades_sign interfész leíró wadl fájl

```

<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">

      <resource path="xadesign">
        <method name="POST" id="xadesign">
          <request>
            <doc title="XAdES aláírás" xml:lang="hu">Egy vagy több dokumentum e-Aktába helyezése és az e-Akta XAdES aláírása.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil azonosítója</doc>
              </param>
              <param name="dossierTitle" required="true" type="String">
                <doc title="dossierTitle" xml:lang="hu">Az e-Akta címe</doc>

```

```

        </param>
        <param name="inFileX" required="true" repeating="true" type="File">
          <doc title="inFileX" xml:lang="hu">
            Az aláírandó fájlok, melyek name paramétere inFile-lal kezdődik
            és egymástól eltérő értékű.
            Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
          </doc>
        </param>
        <param name="isDetached" required="false" type="Boolean">
          <doc title="isDetached" xml:lang="hu">Különálló aláírást készítsen-e?
            Alapértelmezett értéke false.</doc>
        </param>
      </representation>
    </request>
  </response>
  <representation mediaType="application/es3">
    <doc title="válasz" xml:lang="hu">
      A válasz egy darab es3 formátumú akta. A fájl nevét a headerből lehet
      kiolvasni.
      A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
      hibát vagy rendszerhibát.
    </doc>
  </representation>
</response>
</method>
</resource>

</resource>
</resources>
</application>

```

Funkció neve	XAdES_sign
Bemeneti adat(ok)	- profileId - Szerver profil megnevezés - dossierTitle - Az elkészülő e-akta címe - inFileX - Aláírandó fájlok listája - isDetached - Különálló aláírás készüljön-e. Opcionális, alapértelmezett értéke false.
Funkció leírása	A bemeneti fájl lista tartalmát elhelyezi egy e-aktában és a megadott profil alapján aláírja őket. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren a program hibára fut. A feltöltött aláírandó fájloknak tetszőleges a neve. A program a feltöltött névvel fogja beilleszteni a fájlt az elektronikus aktába. Az aktának a dossierTitle paraméterben megadott nevet fogja adni. A válasz az elkészült e-akta. Amennyiben isDetached értéke true, akkor nem elektronikus akta készül, hanem különálló aláírás.
Visszatérő adatok	Az aláírt elektronikus akta, vagy a különálló aláírást tartalmazó XML, hiba esetén a „Hibakódok” fejezetben meghatározott hibakódok egyike.
URL	server/microsec-pki-service-server-web/PKIServlet/pki/xadessign

Példa form:

```

<form method="post" action="http://localhost:8080/microsec-pki-service-server-
web/PKIServlet/pki/xadessign" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="text" id="dossierTitle" name="dossierTitle" value="Cím"/>
  <input type="file" id="inFile0" name="inFile0" />
  <input type="file" id="inFile1" name="inFile1" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>

```

5.1.7 Add_archive_timestamp

Add_archive_timestamp interfészt leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application
    xmlns="http://wadl.dev.java.net/2009/02"
    xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
        <resource path="pki">

            <resource path="addarchivetimestamp">
                <method name="POST" id="addarchivetimestamp">
                    <request>
                        <doc title="Archív időbélyeg hozzáadása" xml:lang="hu">
                            XAdES formátumú e-Akta vagy különálló aláírás kiterjesztése XAdES-A archív
                            időbélyeggel védetté.
                            Ha eleve XAdES-A az aláírás típusa, akkor újra archív időbélyegzi.
                        </doc>
                        <representation mediaType="multipart/form-data">
                            <param name="profileId" required="true" type="String">
                                <doc title="profileId" xml:lang="hu">A felhasználói profil azonosítója</doc>
                            </param>
                            <param name="inFile" required="true" repeating="false" type="File">
                                <doc title="inFile" xml:lang="hu">A kiterjesztendő e-Akta, vagy különálló
                                aláírás.</doc>
                            </param>
                            <param name="inFileX" required="false" repeating="true" type="File">
                                <doc title="inFileX" xml:lang="hu">
                                    Különálló aláírásnál azon fájlok, melyekre hivatkozik az aláírás
                                    fájl.
                                    A name paramétere inFile-lal kezdődik és egymástól eltérő értékű.
                                    Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                                </doc>
                            </param>
                        </representation>
                    </request>
                    <response>
                        <representation mediaType="application/es3">
                            <doc title="válasz" xml:lang="hu">
                                A válasz egy darab es3 formátumú akta. A fájl nevét a headerből lehet
                                kiolvasni.
                                A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum
                                hibát vagy rendszerhibát.
                            </doc>
                        </representation>
                    </response>
                </method>
            </resource>
        </resources>
    </application>
```

Funkció neve	Add_archive_timestamp
Bemeneti adat(ok)	- profileId - Szerver profil megnevezés - inFile – Az aláírást tartalmazó e-akta, vagy a különálló aláírást tartalmazó XML. - inFileX – Különálló aláírás esetén az aláírt fájlok. - isDetached – Különálló aláírás készüljön-e. Opcionális, alapértelmezett értéke false.
Funkció leírása	A feltöltött aláírást ellenőrzi az alkalmazás és kiegészíti még egy időbélyeggel. Megjegyzés: Ha az időbélyegezendő aláírás nem A típusú, akkor időbélyegzés helyett kiterjesztést csinál. Ez BES típusú aláírás esetén 2 időbélyeg lekérést jelent (signaturetimestamp, archivetimestamp).

Visszatérő adatok	Az aláírt elektronikus akta, vagy a különálló aláírást tartalmazó XML, hiba esetén a „Hibakódok” fejezetben meghatározott hibakódok egyike.
URL	localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/addarchivetimestamp

5.1.8 XAdES_validate

Xades_validate interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="xadesvalidate">
        <method name="POST" id="xadesvalidate">
          <request>
            <doc title="XAdES aláírás ellenőrzése" xml:lang="hu">Pontosan egy darab e-Akta
            illetve az e-Aktában lévő összes XAdES aláírás ellenőrzése.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil azonosítója</doc>
              </param>
              <param name="minXadesType" required="true" type="String">
                <doc title="minXadesType" xml:lang="hu">Elfogadott minimális XAdES aláírás
                típus (bes/t/c/x/x-l/a)</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">Az ellenőrizendő e-Akta, vagy különálló
                aláírás.</doc>
              </param>
              <param name="inFileX" required="false" repeating="true" type="File">
                <doc title="inFileX" xml:lang="hu">
                  Különálló aláírásnál azon fájlok, melyekre hivatkozik az aláírás
                  fájl.
                  A name paramétere inFile-lal kezdődik és egymástól eltérő értékű.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="text/xml">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab eredmény xml dokumentumot tartalmaz. A fájl nevét
                a headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
                hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve	XAdES_validate
Bemeneti adat(ok)	- inFile – Az aláírást tartalmazó e-akta - profileId - Szerver profil megnevezés - minXadesType <bes/t/c/x/x-l/a> - Elfogadott minimális XAdES típus. - inFileX -Különálló aláírásnál azon fájlok, melyekre hivatkozik az aláírás fájl. Az X 0-tól kezdődő folyamatosan növekvő

	számot jelöl. A name attribútumba az aláírásban meghivatkozott eredeti fájl nevet kell megadni.
Funkció leírása	A bemeneti e-aktát megnyitja és ellenőrzi a benne található összes aláírást és időbélyeget. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut. Az ellenőrzés végén a program egy XML formátumú választ ad.
Visszatérő adatok	Az aláírás ellenőrzés eredményét jelző validációs XMLt ad. Az XML formátuma a „Szerver XML válasz formátumának leírása” fejezetben található
URL	localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/xadesvalidate

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/xadesvalidate" enctype="multipart/form-data" id="formid" name="formname">
<input type="text" id="profileid" name="profileId" value="client1"/>
<input type="text" id="minXadesType" name="minXadesType" value="t"/>
<input type="file" id="inFile" name="inFile" />
<input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.9 Info

Info interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="info">
        <method name="POST" id="info">
          <request>
            <doc title="e-Akta, ASiC konténer vagy PDF dokumentumról információk kinyerése" xml:lang="hu">Pontosan egy darab e-Akta vagy PDF dokumentumról információk kinyerése.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">
                  A fájl, amiről PKI információkat kell szolgáltatni.
                </doc>
              </param>
              <param name="pdfPassword" required="false" type="String">
                <doc title="pdfPassword" xml:lang="hu">A PDF fájl jelszava, ha az jelszóval védett.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="text/xml">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab eredmény xml dokumentumot tartalmaz. A fájlnevét a headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
```

```
</resource>
</resources>
</application>
```

Funkció neve	Info
Bemeneti adat(ok)	- inFile – e-akta, ASiC konténer vagy PDF dokumentum - pdfPassword – A PDF fájl jelszava, ha az jelszóval védett. Opcionális
Funkció leírása	A bemeneti ASiC konténert/e-aktát/PDF-et megnyitja és a tartalmát listázza. A listát XML formában állítja elő. A lista tartalmazza a dokumentumok, az aláírások részleteit is. A HTTP POST formátumban érkezik a kérés. A listázandó fájlt az inFile paraméterben kell feltölteni.
Visszatérő adatok	A dosszié tartalom XML. Az XML formátuma a „Szerver XML válasz formátumának leírása” fejezetben található
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/info

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-
web/PKIServlet/pki/info" enctype="multipart/form-data" id="formid"
name="formname">
  <input type="file" id="inFile" name="inFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.10 Encrypt

Encrypt interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="encrypt">
        <method name="POST" id="encrypt">
          <request>
            <doc title="Dokumentum titkosítása" xml:lang="hu">Pontosan egy darab
dokumentum titkosítása.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">
                  A titkosítandó fájl.
                </doc>
              </param>
              <param name="inCertX" required="true" repeating="true" type="File">
                <doc title="inCertX" xml:lang="hu">
                  A titkosító tanúsítványok, melyek name paramétere inCert-tel
kezdődik és egymástól eltérő értékű.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
            </representation>
          </request>
          <response>
```

```

        <representation mediaType="application/es3">
          <doc title="válasz" xml:lang="hu">
            A válasz egy darab titkosított e-Akta. A fájl nevét a headerből lehet
kiolvasni.
            A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
          </doc>
        </representation>
      </response>
    </method>
  </resource>

</resource>
</resources>
</application>

```

Funkció neve	Encrypt
Bemeneti adat(ok)	- inFile – A titkosítani kívánt e-akta - profileId – Szerver profil megnevezése - inCertX – Címzett tanúsítványok listája
Funkció leírása	A bemenetben szereplő elektronikus aktát betitkosítja a megadott címzettek számára. A címzett tanúsítvány fájlokat bármilyen néven föl lehet tölteni, kivéve az inFile paramétert. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A titkosított e-akta
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/encrypt

Példa form:

```

<form method="post" action="http://localhost:8080/microsec-pki-service-server-
web/PKIServlet/pki/encrypt" enctype="multipart/form-data" id="formid"
name="formname">
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="file" id="inFile" name="inFile" />
  <input type="file" id="enc1" name="enc1" />
  <input type="file" id="enc2" name="enc2" />
  <input type="file" id="enc3" name="enc3" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>

```

5.1.11 Decrypt

Decrypt interfész leíró wadl fájl

```

<?xml version="1.0" encoding="UTF-8"?>
<application
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02" xmlns="http://wadl.dev.java.net/2009/02"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="decrypt">
        <method name="POST" id="decrypt">

```



```

<request>
  <doc title="Titkosított dokumentum visszafejtése" xml:lang="hu">Pontosan egy
darab titkosított e-Akta visszafejtése.</doc>
  <representation mediaType="multipart/form-data">
    <param name="profileId" required="true" type="String">
      <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
    </param>
    <param name="inFile" required="true" repeating="false" type="File">
      <doc title="inFile" xml:lang="hu">
        A titkosított e-Akta.
      </doc>
    </param>
  </representation>
</request>
<response>
  <representation mediaType="application/zip">
    <doc title="válasz" xml:lang="hu">
      A válasz egy darab zip formátumú tömörített állomány, amely
tartalmazza a dokumentum(ka)t. A fájl nevét a headerből lehet kiolvasni.
      A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
    </doc>
  </representation>
</response>
</method>
</resource>

</resource>
</resources>
</application>

```

Funkció neve	Decrypt
Bemeneti adat(ok)	- inFile -Titkosított e-akta - profileId - Szerver profil megnevezés
Funkció leírása	A bemeneti e-aktán lévő titkosítást feloldja a profilban szereplő kulccsal.
Visszatérő adatok	A ktitkosított e-akta tartalma.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/decrypt

5.1.12 Pades_sign

Pades_sign interfész leíró wadl fájl

```

<?xml version="1.0" encoding="UTF-8"?>
<application
  xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="padesign">
        <method name="POST" id="padesign">
          <request>
            <doc title="PAdES aláírás" xml:lang="hu">Egy PDF v1.5+ dokumentum PAdES
aláírása.</doc>
          <representation mediaType="multipart/form-data">
            <param name="profileId" required="true" type="String">
              <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
            </param>
            <param name="inFile" required="true" type="File">
              <doc title="inFile" xml:lang="hu">Az aláírandó PDF fájl.</doc>
            </param>
            <param name="pdfPassword" required="false" type="String">

```

```

<doc title="pdfPassword" xml:lang="hu">A PDF fájl jelszava, ha az
jelszóval védett.</doc>
</param>
<param name="hsmKeyId" required="false" type="String">
<doc title="hsmKeyId" xml:lang="hu">A HSM-ben tárolt kulcs
azonosítója</doc>
</param>
<param name="metadataList" required="false" type="String">
<doc title="metadataList" xml:lang="hu">A PDF-ben elhelyezendő meta
adatok listája pontos vesszővel elválasztva kulcs=érték formátumban.</doc>
</param>
<param name="pdfSigningReason" required="false" type="String">
<doc title="pdfSigningReason" xml:lang="hu">Aláírás oka.</doc>
</param>
</representation>
</request>
<response>
<representation mediaType="application/pdf">
<doc title="válasz" xml:lang="hu">
A válasz egy darab aláírt PDF. A fájl nevét a headerből lehet
kiolvasni.
A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
</doc>
</representation>
</response>
</method>
</resource>
</resources>
</application>

```

Funkció neve	Pades_sign
Bemeneti adatok	- inFile -Az aláírandó PDF dokumentum - pdfPassword – A PDF fájl jelszava, ha az jelszóval védett - profileId - Szerver profil megnevezés - hsmKeyId – A kulcs azonosítója HSM-el történő aláírásnál - metadataList - A PDF-ben elhelyezendő meta adatok listája pontos vesszővel elválasztva kulcs=érték formátumban. - pdfSigningReason – Aláírás oka.
Funkció leírása	A bejövő pdf dokumentumot aláírja a meghivatkozott profil alapján. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	Aláírt pdf fájl
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/padessign

Példa form:

```

<form method="post" action="http://localhost:8080/microsec-pki-service-server-
web/PKIServlet/pki/padessign" enctype="multipart/form-data" id="formid" name="formname">
<input type="text" id="profileid" name="profileId" value="client2"/>
<input type="file" id="inFile" name="inFile" />
<input type="file" id="metadataList" name="metadataList" />
<input type="submit" id="sbmt_btn" name="sbmt_btn"/>

```

</form>

5.1.13 Pades_validate

Pades_validate interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application
    xmlns="http://wadl.dev.java.net/2009/02"
    xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
        <resource path="/pki">

            <resource path="/padesvalidate">
                <method name="POST" id="padesvalidate">
                    <request>
                        <doc title="PAdES aláírás ellenőrzése" xml:lang="hu">Egy PDF v1.5+ dokumentum
                        illetve a PDF v1.5+ dokumentumban lévő összes PAdES aláírás ellenőrzése.</doc>
                        <representation mediaType="multipart/form-data">
                            <param name="profileId" required="true" type="String">
                                <doc title="profileId" xml:lang="hu">A felhasználói profil
                                azonosítója</doc>
                            </param>
                            <param name="inFile" required="true" type="File">
                                <doc title="inFile" xml:lang="hu">Az ellenőrizendő PDF.</doc>
                            </param>
                            <param name="pdfPassword" required="false" type="String">
                                <doc title="pdfPassword" xml:lang="hu">A PDF fájl jelszava, ha az
                                jelszóval védett.</doc>
                            </param>
                            <param name="minPadesType" required="false" type="String">
                                <doc title="minPadesType" xml:lang="hu">Ellenőrizhetjük, hogy a PDF-
                                en lévő összes aláírás megfelel-e az itt megadott legalacsonyabb PAdES-típus követelményeinek </doc>
                            </param>
                        </representation>
                    </request>
                    <response>
                        <representation mediaType="text/xml">
                            <doc title="válasz" xml:lang="hu">
                                A válasz egy darab eredmény xml dokumentumot tartalmaz. A fájl nevét
                                a headerből lehet kiolvasni.
                                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
                                hibát vagy rendszerhibát.
                            </doc>
                        </representation>
                    </response>
                </method>
            </resource>
        </resources>
    </application>
```

Funkció neve	Pades_validate
Bemeneti adat(ok)	- inFile - Az aláírást tartalmazó pdf fájl - pdfPassword – A PDF fájl jelszava, ha az jelszóval védett - profileId - Szerver profil megnevezés - minPadesType - Ellenőrizhetjük, hogy a PDF-en lévő összes aláírás megfelel-e az itt megadott legalacsonyabb PAdES-típus követelményeinek
Funkció leírása	A bemeneti pdf dokumentumot megnyitja és ellenőrzi a benne található összes aláírást és időbélyeget. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren a program hibára fut.

Visszatérő adatok	Az aláírás ellenőrzés eredményét jelző hibakód (validációs XML)
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/padesvalidate

5.1.14 Pades_extension

Padesextension requestet leíró xml séma

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="padesextension">
        <method name="POST" id="padesextension">
          <request>
            <doc title="PAdES aláírások kiterjesztése" xml:lang="hu">A PDF dokumentumban
lévő összes PAdES aláírás ellenőrzése és kiterjesztése. A kiterjesztés típusa a profileId paraméter
által meghivatkozott profil alapján kerül meghatározásra.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">A kiterjesztendő PDF fájl.</doc>
              </param>
              <param name="pdfPassword" required="false" type="String">
                <doc title="pdfPassword" xml:lang="hu">A PDF fájl jelszava, ha az
jelszóval védett.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/pdf">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab PDF fájl. A fájl nevét a headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve	PAdES_extension
Bemeneti adat	- inFile– A kiterjesztendő PDF fájl - profileId – Szerver profil megnevezés - pdfPassword – A PDF fájl jelszava, ha az jelszóval védett
Funkció leírása	A PDF dokumentumban lévő összes PAdES aláírás ellenőrzése és kiterjesztése. A kiterjesztés típusa a profileId paraméter által meghivatkozott profil alapján kerül meghatározásra. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A válasz egy darab PDF fájl. A fájl nevét a headerből lehet kiolvasni. A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet

	dokumentum hibát vagy rendszerhibát.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/padesextension

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/padesextension" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inFile" name="inFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.15 Pades_addarchivetimestamp

Padesaddarchivetimestamp requestet leíró xml séma

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="padesaddarchivetimestamp">
        <method name="POST" id="padesaddarchivetimestamp">
          <request>
            <doc title="Archív időbélyeg hozzáadása" xml:lang="hu">PDF dokumentum archív
            időbélyegzése.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
                azonosítója.</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">Az archív időbélyegezendő PDF
                fájl.</doc>
              </param>
              <param name="pdfPassword" required="false" type="String">
                <doc title="pdfPassword" xml:lang="hu">A PDF fájl jelszava, ha az
                jelszóval védett.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/pdf">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab PDF fájl. A fájl nevét a headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
                hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve	PAdES_addarchivetimestamp
Bemeneti adat	- inFile– Az archív időbélyegezendő PDF fájl - profileId – Szerver profil megnevezés - pdfPassword – A PDF fájl jelszava, ha az jelszóval védett
Funkció leírása	PDF dokumentum archív időbélyegzése.

	A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A válasz egy darab PDF fájl. A fájl nevét a headerből lehet kiolvasni. A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/padesaddarchivetimestamp

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/padesaddarchivetimestamp" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inFile" name="inFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.16 Create_acknowledgement

Create_acknowledgement interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="createack">
        <method name="POST" id="createack">
          <request>
            <doc title="Átvételi elismervény készítése" xml:lang="hu">Pontosan egy darab
tetszőleges fájlról átvételi elismervény készítése.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">
                  A fájl, amiről átvételi elismervényt kell készíteni.
                </doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/et3">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab et3 formátumú átvételi elismervény. A fájl nevét
a headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve

Create_acknowledgement

Bemeneti adat(ok)	- InFile - A tértivevényezni kívánt dokumentum - profileId - Szerver profil megnevezés
Funkció leírása	Az inFile paraméterben feltöltött bemeneti fájlra készít tértivevényt a kiválasztott szerver profil alapján. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren a program hibára fut.
Visszatérő adatok	Az elkészült tértivevény
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/createack

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/createack" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="file" id="inFile" name="inFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.17 Check_acknowledgement

Check_acknowledgement interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="checkack">
        <method name="POST" id="checkack">
          <request>
            <doc title="Átvételi elismervény ellenőrzése egy fájlra vonatkozóan"
              xml:lang="hu">Pontosan egy darab átvételi elismervény ellenőrzése egy fájlra vonatkozóan</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">
                  A fájl, amiről az átvételi elismervény készült.
                </doc>
              </param>
              <param name="inEt3" required="true" repeating="false" type="File">
                <doc title="inEt3" xml:lang="hu">
                  Az ellenőrizendő átvételi elismervény.
                </doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="text/xml">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab eredmény xml dokumentumot tartalmaz. A fájl nevét a headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
```

```
</resource>

</resource>
</resources>
</application>
```

Funkció neve	Check_acknowledgement
Bemeneti adat(ok)	- inEt3 – Az ellenőrizni kívánt tértivevény - inFile – Az eredeti fájl amiről a tértivevény készült - profileId – Szerver profil megnevezés
Funkció leírása	Az inEt3 paraméterben feltöltött tértivevényt ellenőrzi az inFile paraméterben feltöltött fájl alapján. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren a program hibára fut.
Visszatérő adatok	Az ellenőrzésről készült validációs XML. Az XML formátuma a „Szerver XML válasz formátumának leírása” fejezetben található
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/checkack

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/checkack" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="file" id="inEt3" name="inEt3" />
  <input type="file" id="originalFile" name="originalFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.18 XAdES_extension

Xadesextension requestet leíró xml séma

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="xadesextension">
        <method name="POST" id="xadesextension">
          <request>
            <doc title="XAdES aláírás kiterjesztése" xml:lang="hu">Pontosan egy darab e-Akta illetve az e-Aktában lévő összes XAdES aláírás ellenőrzése és kiterjesztése.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil azonosítója</doc>
              </param>
              <param name="inFile" required="true" repeating="false" type="File">
                <doc title="inFile" xml:lang="hu">A kiterjesztendő e-Akta, vagy különálló aláírás.</doc>
              </param>
              <param name="inFileX" required="false" repeating="true" type="File">
                <doc title="inFileX" xml:lang="hu">
```


Különálló aláírásnál azon fájlok, melyekre hivatkozik az aláírás fájl.

A name paramétere inFile-lal kezdődik és egymástól eltérő értékű. Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.

```

</doc>
</param>
</representation>
</request>
<response>
  <representation mediaType="text/xml">
    <doc title="válasz" xml:lang="hu">
      A válasz egy darab eredmény e-akta dokumentumot vagy különálló aláírást tartalmaz. A fájl nevét a headerből lehet kiolvasni.
      A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
    </doc>
  </representation>
</response>
</method>
</resource>
</resources>
</application>

```

Funkció neve	XAdES_extension
Bemeneti adat	- inFile– A kiterjesztendő e-Akta, vagy különálló aláírás - inFileX– Különálló aláírásnál azon fájlok, melyekre hivatkozik az aláírás fájl. A paraméter inFile-lal kezdődik és egymástól eltérő értékű. Az X 0-tól kezdődő folyamatosan növekvő számot jelöl. - profileId – Szerver profil megnevezés
Funkció leírása	Pontosan egy darab e-Akta illetve az e-Aktában lévő összes XAdES aláírás ellenőrzése és kiterjesztése. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A válasz egy darab eredmény e-akta dokumentumot vagy különálló aláírást tartalmaz. A fájl nevét a headerből lehet kiolvasni. A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/xadesextension

Példa form:

```

<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/xadesextension" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="file" id="inFile" name="inFile" />
  <input type="file" id="inFile0" name="inFile0" />
  <input type="file" id="inFile1" name="inFile1" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>

```

5.1.19 Esign

Esign requestet leíró xml séma

```
<?xml version="1.0" encoding="UTF-8"?>
<application
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02"
  xmlns="http://wadl.dev.java.net/2009/02"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="esignpdfsign">
        <method name="POST" id="pdfsign">
          <request>
            <doc title="PDF aláírás" xml:lang="hu">Kétmenetes aláírás készítése
            ESignProxy szerver támogatásával MicroSigner vagy mobil aláírás felhasználásával. Ekkor az aláíró nem
            a technikai felhasználó, hanem az a természetes személy, akinek a készülékére el kell juttatni az
            ESignProxy által kiadott sessiont. Ez megoldható QR kód segítségével is.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
                azonosítója</doc>
              </param>
              <param name="inFileX" required="true" type="File">
                <doc title="inFileX" xml:lang="hu">
                  Az aláírandó PDF fájl.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
              <param name="pdfPasswordX" required="false" type="String">
                <doc title="pdfPasswordX" xml:lang="hu">
                  Az X azonosítójú PDF fájl jelszava, ha az jelszóval védett.
                  Az X a jelszavas PDF fájl azonosítója. A jelszóval nem védett
                  fájlokhoz nem kell pdfPasswordX paramétert küldeni.
                </doc>
              </param>
              <param name="fileNameX" required="true" type="String">
                <doc title="fileNameX" xml:lang="hu">
                  Az aláírandó PDF fájl neve az esign protokoll használata során.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
              <param name="downloadUrlX" required="false" type="String">
                <doc title="downloadUrlX" xml:lang="hu">
                  Az aláírandó/aláírt PDF fájl letöltési URL-je az esign protokoll
                  használata során.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
              <param name="downloadExpiryISO8601DateX" required="false" type="String">
                <doc title="downloadExpiryISO8601DateX" xml:lang="hu">
                  Az aláírt fájl letöltési határideje.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
              <param name="callbackUrl" required="false" type="String">
                <doc title="callbackUrl" xml:lang="hu">Visszahívási URL, amely akkor
                hívódik, ha az aláírások elkészültek.</doc>
              </param>
              <param name="loadQRCode" required="false" type="String">
                <doc title="loadQRCode" xml:lang="hu">Visszaadja-e a QR kódot is?
                Alapértelmezett értéke: no.</doc>
              </param>
              <param name="pdfSigningReason" required="false" type="String">
                <doc title="pdfSigningReason" xml:lang="hu">Aláírás oka, minden PDF
                fájlra egységesen megadva.</doc>
              </param>
              <param name="esignMessage" required="false" type="String">
                <doc title="esignMessage" xml:lang="hu">Aláírói üzenet, amit a másik
                fél aláíró alkalmazása megjelenít aláírásra való felszólításnál.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/json">
              <doc title="válasz" xml:lang="hu">
                {
```

```

        "sessionUrl":"string",
        "sessionId":"string",
        "mode":"string",
        "qrCode":"array",
        "qrImageMimeType":"string",
        "documents": array
    }
</doc>
</representation>
</response>
</method>
</resource>

<resource path="/esignxadesign">
    <method name="POST" id="xadesign">
        <request>
            <doc title="XAdES aláírás" xml:lang="hu">Kétmenetes aláírás készítése
ESignProxy szerver támogatásával MicroSigner vagy mobil aláírás felhasználásával. Ekkor az aláíró nem
a technikai felhasználó, hanem az a természetes személy, akinek a készülékére el kell juttatni az
ESignProxy által kiadott sessiont. Ez megoldható QR kód segítségével is.</doc>
            <representation mediaType="multipart/form-data">
                <param name="profileId" required="true" type="String">
                    <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
                </param>
                <param name="inFileX" required="true" type="File">
                    <doc title="inFileX" xml:lang="hu">
                        Az aláírandó X. fájl.
                        Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                    </doc>
                </param>
                <param name="fileNameX" required="true" type="String">
                    <doc title="fileNameX" xml:lang="hu">
                        Az aláírandó X. fájl neve az esign protokoll használata során.
                        Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                    </doc>
                </param>
                <param name="dossierTitle" required="true" type="String">
                    <doc title="dossierTitle" xml:lang="hu">
                        Az aláírt e-Akta fájl címe.
                    </doc>
                </param>
                <param name="dossierFileName" required="true" type="String">
                    <doc title="dossierFileName" xml:lang="hu">
                        Az aláírt e-Akta fájl letöltési neve az esign protokoll használata
során.
                    </doc>
                </param>
                <param name="dossierDownloadUrl" required="false" type="String">
                    <doc title="dossierDownloadUrl" xml:lang="hu">
                        Az aláírt e-Akta fájl letöltési URL-je az esign protokoll
használata során.
                    </doc>
                </param>
                <param name="downloadExpiryISO8601Date" required="false" type="String">
                    <doc title="downloadExpiryISO8601Date" xml:lang="hu">
                        Az aláírt e-Akta fájl letöltési határideje.
                    </doc>
                </param>
                <param name="isDetached" required="false" type="String">
                    <doc title="isDetached" xml:lang="hu">
                        Különálló aláírás készüljön-e?
                    </doc>
                </param>
                <param name="callbackUrl" required="false" type="String">
                    <doc title="callbackUrl" xml:lang="hu">Visszahívási URL, amely akkor
hívódik, ha az aláírás elkészült.</doc>
                </param>
                <param name="loadQRCode" required="false" type="String">
                    <doc title="loadQRCode" xml:lang="hu">Visszaadja-e a QR kódot is?
Alapértelmezett értéke: no.</doc>
                </param>
                <param name="esignMessage" required="false" type="String">
                    <doc title="esignMessage" xml:lang="hu">Aláírói üzenet, amit a másik
fél aláíró alkalmazása megjelenít aláírásra való felszólításnál.</doc>
                </param>
            </representation>
        </request>
    </method>
</resource>

```

```

        </representation>
    </request>
    <response>
        <representation mediaType="application/json">
            <doc title="válasz" xml:lang="hu">
                {
                    "sessionUrl":"string",
                    "sessionId":"string",
                    "mode":"string",
                    "qrcode":"array",
                    "qrImageMimeType":"string",
                    "documents": array
                }
            </doc>
        </representation>
    </response>
</method>
</resource>

<resource path="esignasicsign">
    <method name="POST" id="asicsign">
        <request>
            <doc title="ASiC aláírás" xml:lang="hu">Kétmenetes aláírás készítése
ESignProxy szerver támogatásával MicroSigner vagy mobil aláírás felhasználásával. Ekkor az aláíró nem
a technikai felhasználó, hanem az a természetes személy, akinek a készülékére el kell juttatni az
ESignProxy által kiadott sessiont. Ez megoldható QR kód segítségével is.</doc>
            <representation mediaType="multipart/form-data">
                <param name="profileId" required="true" type="String">
                    <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
                </param>
                <param name="inFileX" required="true" type="File">
                    <doc title="inFileX" xml:lang="hu">
                        Az aláírandó X. fájl.
                        Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                    </doc>
                </param>
                <param name="fileNameX" required="true" type="String">
                    <doc title="fileNameX" xml:lang="hu">
                        Az aláírandó X. fájl neve az esign protokoll használata során.
                        Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                    </doc>
                </param>
                <param name="containerTitle" required="true" type="String">
                    <doc title="containerTitle" xml:lang="hu">
                        Az aláírt ASiC konténer fájl zip fejléc megjegyzése.
                    </doc>
                </param>
                <param name="containerFileName" required="true" type="String">
                    <doc title="containerFileName" xml:lang="hu">
                        Az aláírt ASiC konténer fájl letöltési neve az esign protokoll
használata során.
                    </doc>
                </param>
                <param name="containerDownloadUrl" required="false" type="String">
                    <doc title="containerDownloadUrl" xml:lang="hu">
                        Az aláírt ASiC konténer fájl letöltési URL-je az esign protokoll
használata során.
                    </doc>
                </param>
                <param name="downloadExpiryISO8601Date" required="false" type="String">
                    <doc title="downloadExpiryISO8601Date" xml:lang="hu">
                        Az aláírt ASiC konténer fájl letöltési határideje.
                    </doc>
                </param>
                <param name="callbackUrl" required="false" type="String">
                    <doc title="callbackUrl" xml:lang="hu">Visszahívási URL, amely akkor
hívódik, ha az aláírás elkészült.</doc>
                </param>
                <param name="loadQRCode" required="false" type="String">
                    <doc title="loadQRCode" xml:lang="hu">Visszaadja-e a QR kódot is?
Alapértelmezett értéke: no.</doc>
                </param>
                <param name="esignMessage" required="false" type="String">
                    <doc title="esignMessage" xml:lang="hu">Aláírói üzenet, amit a másik
fél aláíró alkalmazása megjelenít aláírásra való felszólításnál.</doc>
            </representation>
        </request>
    </method>
</resource>

```

```

        </param>
    </representation>
</request>
</response>
    <representation mediaType="application/json">
        <doc title="válasz" xml:lang="hu">
            {
                "sessionUrl":"string",
                "sessionId":"string",
                "mode":"string",
                "qrcode":"array",
                "qrImageMimeType":"string",
                "documents": array
            }
        </doc>
    </representation>
</response>
</method>
</resource>

<resource path="esignsignhash">
    <method name="POST" id="signhash">
        <request>
            <doc title="Aláíratlan lenyomat aláírása szerver oldalon."
xml:lang="hu">Kétmenetes aláírásnál, ha technikai userrel kell aláírni (Pl.: tesztelési célból).</doc>
            <representation mediaType="multipart/form-data">
                <param name="profileId" required="true" type="String">
                    <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója, amely technikai user nevében alá kell írni.</doc>
                </param>
                <param name="unsignedHash" required="true" type="String">
                    <doc title="unsignedHash" xml:lang="hu">Az aláírandó lenyomat Base64
kódolással.</doc>
            </param>
        </representation>
    </request>
    <response>
        <representation mediaType="text/plain">
            <doc title="válasz" xml:lang="hu">
                Az aláírt lenyomat Base64 kódolással.
            </doc>
        </representation>
    </response>
</method>
</resource>

<resource path="esigndownloadssignedfile">
    <method name="POST" id="downloadssignedfile">
        <request>
            <doc title="Az aláírt fájl letöltése." xml:lang="hu">A sessionId-vel
beazonosítható aláírt fájl letöltése.</doc>
            <representation mediaType="multipart/form-data">
                <param name="profileId" required="true" type="String">
                    <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
                </param>
                <param name="sessionId" required="true" type="String">
                    <doc title="sessionId" xml:lang="hu">Az aláírt fájl sessionId-
je.</doc>
            </param>
        </representation>
    </request>
    <response>
        <representation mediaType="application/pdf, application/eszigno3,
application/vnd.etsi.asic-e+zip">
            <doc title="válasz" xml:lang="hu">
                A válasz egy vagy több darab aláírt fájl. A fájl nevét a headerből
lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
            </doc>
        </representation>
    </response>
</method>
</resource>
</resource>

```

```
</resources>
</application>
```

5.1.19.1 Esign_pdfsign

Funkció neve	Esign_pdfsign
Bemeneti adat	- inFileX – Az aláírandó PDF fájlok - pdfPasswordX – Az X PDF fájl jelszava, ha az jelszóval védett (csak a szükséges PDF dokumentumokhoz kell megadni) - fileNameX – A fájlok megjelenítendő nevei. - downloadUrIX – A fájlok letöltési URL-jei. - downloadExpiryISO8601DateX – A letöltési határidő. - callbackUrl – A visszahívási URL (további információkért lásd a „ESignProxy_callback” funkció leírását). - profileId – Szerver profil megnevezés - loadQRCode – A válasz JSON-ban tartalmazzon-e QR kódot. - pdfSigningReason – Aláírás oka, minden PDF fájlra egységesen megadva. - esignMessage – Aláírói üzenet, amit a másik fél aláíró alkalmazása megjelenít aláírásra való felszólításnál.
Funkció leírása	Kétmenetes aláírás készítése ESignProxy szerver támogatásával MicroSigner vagy mobil aláírás felhasználásával. Ekkor az aláíró nem a technikai felhasználó, hanem az a természetes személy, akinek a készülékére el kell juttatni az ESignProxy által kiadott sessiont. Ez megoldható QR kód segítségével is. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	JSON objektummal tér vissza a szolgáltatás, melynek felépítése a következő: <pre>{ "sessionUrl":"string", "sessionId":"string", "mode":"string", "qrcode":"array", "qrImageMimeType":"string" }</pre> Példa: <pre>{ "sessionUrl":"https://proxy- test.microsigner.com/esign/getConfig", "sessionId":"3pdyv1140ip5m", "mode":"SELECT_CERTIFICATE_AND_SIGN", "qrcode":[-119,80,78,71,13,10,26,10,0,...], "qrImageMimeType":"image/png" }</pre>

	<pre>} Az objektumban benne van minden szükséges adat a felhasználó kétmenetes aláírásához, de önmagában a QR kód is elegendő. A természetes aláíró személy kliensétől függ, hogy mit kell hozzá eljuttatni. A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.</pre>
URL	<pre><server>/microsec-pki-service-server- web/PKIServlet/pki/esignpdfsign</pre>

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-
web/PKIServlet/pki/esignpdfsign" enctype="multipart/form-data" id="formid"
name="formname">
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="file" id="inFile0" name="inFile0" />
  <input type="file" id="fileName0" name="fileName0" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.19.2 Esign_xadessign

Funkció neve	Esign_xadessign
Bemeneti adat	- inFileX – Az aláírandó X. fájl. - fileNameX – A fájlok megjelenítendő nevei. - dossierTitle – Az aláírt e-Akta fájl címe. - dossierFileName – Az aláírt e-Akta fájl letöltési neve. - dossierDownloadUrl – A fájl letöltési URL-je. - callbackUrl – A visszahívási URL (további információkért lásd a „ESignProxy_callback” funkció leírását). - downloadExpiryISO8601Date – Az aláírt e-Akta fájl letöltési határideje UTC-ben. - isDetached – Különálló aláírás készüljön-e? - profileId – Szerver profil megnevezés - loadQRCode – A válasz JSON-ban legyen QR kód vagy ne. - esignMessage – Aláírói üzenet, amit a másik fél aláíró alkalmazása megjelenít aláírásra való felszólításnál.
Funkció leírása	Kétmenetes keret aláírás készítése ESignProxy szerver támogatásával MicroSigner vagy mobil aláírás felhasználásával. Ekkor az aláíró nem a technikai felhasználó, hanem az a természetes személy, akinek a készülékére el kell juttatni az ESignProxy által kiadott sessiont. Ez megoldható QR kód segítségével is. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	JSON objektummal tér vissza a szolgáltatás, melynek felépítése a következő: <pre>{ "sessionUrl": "string",</pre>

	<pre>"sessionId":"string", "mode":"string", "qrcode":"array", "qrImageMimeType":"string" }.</pre> Példa: <pre>{ "sessionId":"https://proxy- test.microsigner.com/esign/getConfig", "sessionId":"3pdyv1140ip5m", "mode":"SELECT_CERTIFICATE_AND_SIGN", "qrcode":[-119,80,78,71,13,10,26,10,0,...], "qrImageMimeType":"image/png" }</pre> Az objektumban benne van minden szükséges adat a felhasználó kétmenetes aláírásához, de önmagában a QR kód is elegendő. A természetes aláíró személy kliensétől függ, hogy mit kell hozzá eljuttatni. A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
URL	<pre><server>/microsec-pki-service-server- web/PKIServlet/pki/esignxadesign</pre>

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-
web/PKIServlet/pki/esignxadesign" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="file" id="inFile0" name="inFile0" />
  <input type="file" id="fileName0" name="fileName0" />
  <input type="file" id="dossierTitle" name="TITLE" />
  <input type="file" id="dossierFileName" name="signed.es3" />
  <input type="file" id="dosserDownloadUrl" name="https://msc.hu/signed-232323" />
  <input type="file" id="downloadExpiryISO8601Date" name="2017-10-25T13:54:59.973Z" />
  <input type="file" id="callbackUrl" name="http://localhost:8080/contract-callback?id=232323" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.19.3 ESign_asicsign

Funkció neve	Esign_asicsign
Bemeneti adat	- inFileX – Az aláírandó X. fájl. - fileNameX – A fájlok megjelenítendő nevei. - containerTitle – Az aláírt e-Akta fájl címe. - containerFileName – Az aláírt e-Akta fájl letöltési neve. - containerDownloadUrl – A fájl letöltési URL-je. - callbackUrl – A visszahívási URL (további információkért lásd a „ESignProxy_callback” funkció leírását). - downloadExpiryISO8601Date – Az aláírt e-Akta fájl letöltési határideje UTC-ben. - profileId – Szerver profil megnevezés.

	- loadQRCode – A válasz JSON-ban legyen QR kód vagy ne. - esignMessage – Aláírói üzenet, amit a másik fél aláíró alkalmazása megjelenít aláírásra való felszólításnál.
Funkció leírása	Kétmenetes aláírás készítése minden feltöltött dokumentumra ESignProxy szerver támogatásával MicroSigner vagy mobil aláírás felhasználásával. Ekkor az aláíró nem a technikai felhasználó, hanem az a természetes személy, akinek a készülékére el kell juttatni az ESignProxy által kiadott sessiont. Ez megoldható QR kód segítségével is. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	JSON objektummal tér vissza a szolgáltatás, melynek felépítése a következő: <pre>{ "sessionUrl":"string", "sessionId":"string", "mode":"string", "qrcode":"array", "qrImageMimeType":"string" }</pre> Példa: <pre>{ "sessionUrl":"https://proxy- test.microsigner.com/esign/getConfig", "sessionId":"3pdyv1140ip5m", "mode":"SELECT_CERTIFICATE_AND_SIGN", "qrcode":[-119,80,78,71,13,10,26,10,0,...], "qrImageMimeType":"image/png" }</pre> Az objektumban benne van minden szükséges adat a felhasználó kétmenetes aláírásához, de önmagában a QR kód is elegendő. A természetes aláíró személy kliensétől függ, hogy mit kell hozzá eljuttatni. A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/esignasicsign

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-
web/PKIServlet/pki/esignasicsign" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="file" id="inFile0" name="inFile0" />
  <input type="file" id="fileName0" name="fileName0" />
  <input type="file" id="containerTitle" name="User Contract" />
  <input type="file" id="containerFileName" name="signed.es3" />
  <input type="file" id="containerDownloadUrl" name="https://msc.hu/signed-222323" />
```

```
<input type="file" id="downloadExpiryISO8601Date" name="2017-10-25T13:54:59.973Z" />
<input type="file" id="callbackUrl" name="http://localhost:8080/contract-callback?id=222323" />
<input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.19.4 Esign_signhash

Funkció neve	Esign_signhash
Bemeneti adat	- unsignedHash– Az aláíratlan lenyomat Base64 kódolással - profileId – Szerver profil megnevezés
Funkció leírása	Kétmenetes aláírásnál, ha technikai userrel kell aláírni (Pl.: tesztelési célból). Magában a természetes személy által végzett kétmenetes aláírásban nem vesz részt. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	Az aláírt lenyomat Base64 kódolással. A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet lenyomat hibát vagy rendszerhibát.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/esignsignhash

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/esignsignhash" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="text" id="unsignedHash" name="unsignedHash" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.19.5 Esign_downloadsIGNEDfile

Funkció neve	Esign_downloadsIGNEDfile
Bemeneti adat	- sessionId– Az aláírt fájl ESignProxy sessionId-je. - profileId – Szerver profil megnevezés
Funkció leírása	Az ESignProxy sessionId-vel beazonosítható aláírt fájl letöltése. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A válasz multipart formátumú és több darab aláírt fájl tartalmazhat. A fájlok eredeti nevét a válasz tartalmazza. A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát. Jelölhet kliens hibát is, tipikusan, hogy a rendszer még nem készítette el a letöltendő fájlt, - próbálkozzon később.

URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/esigndownloadsIGNEDfile
-----	---

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/esigndownloadsIGNEDfile" enctype="multipart/form-data" id="formid"
  <input type="text" id="profileid" name="profileId" value="client1"/>
  <input type="text" id="sessionId" name="sessionId" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.20 RemoteSign_PAdES

Pades_sign interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02" xmlns="http://wadl.dev.java.net/2009/02"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="remotesignpades">
        <method name="POST" id="remotesignpades">
          <request>
            <doc title="Tárolt kulcsú PAdES aláírás indítása" xml:lang="hu">Egy PDF v1.5+
dokumentum PAdES aláírása tárolt kulcs szolgáltatás segítségével.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="inFile" required="true" type="File">
                <doc title="inFile" xml:lang="hu">Az aláírandó PDF fájl.</doc>
              </param>
              <param name="pdfPassword" required="false" type="String">
                <doc title="pdfPassword" xml:lang="hu">A PDF fájl jelszava, ha az
jelszóval védett.</doc>
              </param>
              <param name="metadataList" required="false" type="String">
                <doc title="metadataList" xml:lang="hu">A PDF-ben elhelyezendő meta
adatok listája pontos vesszővel elválasztva kulcs=érték formátumban.</doc>
              </param>
              <param name="pdfSigningReason" required="false" type="String">
                <doc title="pdfSigningReason" xml:lang="hu">Aláírás oka.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/json">
              <doc title="válasz" xml:lang="hu">
                A válasz egy json fájl, ami tartalmazza az indított session
azonosítót. A fájl nevét a headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve	PadesSign_remote
Bemeneti adatok	- inFile -Az aláírandó PDF dokumentum - pdfPassword – A PDF fájl jelszava, ha az jelszóval védett

	- profileId - Szerver profil megnevezés - metadataList - A PDF-ben elhelyezendő meta adatok listája pontos vesszővel elválasztva kulcs=érték formátumban. - pdfSigningReason - Aláírás oka.
Funkció leírása	A bejövő (inFile) pdf dokumentumot aláírja a meghivatkozott profilban található tárolt kucslú szolgáltatással. Ez a funkció megkezdje az aláírást és visszaad egy session azonosítót, amivel le lehet kérdezni az aláírás állapotát. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A session azonosítót tartalmazó json file.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/remotesignpades

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/remotesignpades" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inFile" name="inFile" />
  <input type="file" id="metadataList" name="metadataList" value="signerApp=eszigno3"/>
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.21 RemoteSign_PAdES_Status

Pades_sign interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="remotesignpadesstatus">
        <method name="POST" id="remotesignpadesstatus">
          <request>
            <doc title="Tárolt kulcsú PAdES aláírás állapotának lekérdezése"
xml:lang="hu">Session azonosító alapján visszaadja az aláírt PAdES dokumentumot, ha az aláírás
elkészült.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="inJsonFile" required="true" repeating="false" type="File">
                <doc title="inJsonFile" xml:lang="hu">A session azonosítót tartalmazó
json file.</doc>
              </param>
              <param name="pdfPassword" required="false" type="String">
                <doc title="pdfPassword" xml:lang="hu">Az aláíráshoz beküldött PDF
fájl jelszava újra megadva, ha az jelszóval védett volt (a szerver nem tárol jelszavakat, ezért itt
is meg kell adni).</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/pdf">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab PDF formátumú dokumentum, amennyiben az aláírás
elkészült. A fájl nevét a headerből lehet kiolvasni.
            </doc>
          </representation>
        </method>
      </resource>
    </resources>
  </application>
```

A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát vagy azt is hogy az aláírás még nem készült el.

```

</doc>
</representation>
</response>
</method>
</resource>
</resources>
</application>

```

Funkció neve	PadesSign_remote_status
Bemeneti adatok	- inJsonFile –A session azonosítót tartalmazó json fájl. - profileId - Szerver profil megnevezés - pdfPassword – Az aláírásra küldött PDF fájl jelszava, ha az jelszóval védett volt (a szerver nem tárol jelszavakat, ezért szükséges újra megadni)
Funkció leírása	A bejövő (inJsonFile) json fájlban található session azonosító alapján lekérdezi az aláírás állapotát. Ha az aláírás készen van, akkor visszaadja az aláírt pdf fájlt, ha nem, akkor hibakódot ad. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	Az aláírt pdf fájl.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/remotesignpadesstatus

Példa form:

```

<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/remotesignpadesstatus" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inJsonFile" name="inJsonFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>

```

5.1.22 RemoteSign_PAdES_Multiple

Pades_sign interfész leíró wadl fájl

```

<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="remotesignpadesmultiple">
        <method name="POST" id="remotesignpadesmultiple">
          <request>
            <doc title="Tárolt kulcsú PAdES aláírás indítása több dokumentumra"
              xml:lang="hu">Több PDF v1.5+ dokumentum PAdES aláírása tárolt kulcs szolgáltatás segítségével.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil azonosítója</doc>
              </param>
              <param name="inFileX" required="true" type="File">
                <doc title="inFileX" xml:lang="hu">
                  Az aláírandó PDF fájl.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
            </representation>
          </request>
        </method>
      </resource>
    </resource>
  </resources>
</application>

```

```

        </doc>
    </param>
    <param name="pdfPasswordX" required="false" type="String">
        <doc title="pdfPasswordX" xml:lang="hu">
            Az X azonosítójú PDF fájl jelszava, ha az jelszóval védett.
            Az X a jelszavas PDF fájl azonosítója. A jelszóval nem védett
            fájlokhoz nem kell pdfPasswordX paramétert küldeni.
        </doc>
    </param>
    <param name="metadataList" required="false" type="String">
        <doc title="metadataList" xml:lang="hu">A PDF fájlokban elhelyezendő
        meta adatok listája pontos vesszővel elválasztva kulcs=érték formátumban.</doc>
    </param>
    <param name="pdfSigningReason" required="false" type="String">
        <doc title="pdfSigningReason" xml:lang="hu">Aláírás oka, minden PDF
        fájlra egységesen megadva.</doc>
    </param>
</representation>
</request>
<response>
    <representation mediaType="application/json">
        <doc title="válasz" xml:lang="hu">
            A válasz egy json fájl, ami tartalmazza az indított session
            azonosítót. A fájl nevét a headerből lehet kiolvasni.
            A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum
            hibát vagy rendszerhibát.
        </doc>
    </representation>
</response>
</method>
</resource>
</resources>
</application>

```

Funkció neve	PadesSign_remote
Bemeneti adatok	- inFileX -Az aláírandó PDF dokumentumok listája - pdfPasswordX - Az X PDF fájl jelszava, ha az jelszóval védett (csak a szükséges PDF dokumentumokhoz kell megadni) - profileId - Szerver profil megnevezés - metadataList - A PDF dokumentumokban elhelyezendő meta adatok listája pontos vesszővel elválasztva kulcs=érték formátumban. - pdfSigningReason - Aláírás oka, minden PDF fájlra egységesen megadva.
Funkció leírása	A bejövő dokumentumokat aláírja a meghivatkozott profilban található tárolt kucslú szolgáltatással. Ez a funkció megkezdi az aláírást és visszaad egy session azonosítót, amivel le lehet kérdezni az aláírás állapotát. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	A session azonosítót tartalmazó json file.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/remotesignpadesmultiple

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/remotesignpadesmultiple" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inFile0" name=" inFile0" />
  <input type="file" id="inFile1" name=" inFile1" />
  <input type="string" id="pdfPassword1" name=" pdfPassword1" value="test" />
  <input type="file" id="metadataList" name="metadataList" value="signerApp=eszigno3"/>
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.23 RemoteSign_PAdES_Status_Multiple

Pades_sign interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="remotesignpadesstatusmultiple">
        <method name="POST" id="remotesignpadesstatusmultiple">
          <request>
            <doc title="Több dokumentumos tárolt kulcsú PAdES aláírás állapotának lekérdezése" xml:lang="hu">Session azonosító alapján visszaadja az aláírt PAdES dokumentumokat, ha minden aláírás elkészült.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil azonosítója</doc>
              </param>
              <param name="inJsonFile" required="true" repeating="false" type="File">
                <doc title="inJsonFile" xml:lang="hu">A session azonosítót tartalmazó json file.</doc>
              </param>
              <param name="pdfPasswordX" required="false" type="String">
                <doc title="pdfPasswordX" xml:lang="hu">
                  Az X azonosítójú aláírásra beküldött PDF fájl jelszava, ha az jelszóval védett volt.
                  Az X a jelszavas PDF fájl azonosítója. A jelszóval nem védett fájlokhoz nem kell pdfPasswordX paramétert küldeni.
                  A szerver nem tárol jelszavakat, ezért újra meg kell adni ezeket a paramétereket.
                </doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/pdf">
              <doc title="válasz" xml:lang="hu">
                A válasz több PDF formátumú dokumentum, amennyiben az összes aláírás elkészült. A fájlok neveit a headerből lehet kiolvasni.
                A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát vagy azt is hogy az aláírások még nem készültek el.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve	PadesSign_remote_status
Bemeneti adatok	inJsonFile – A session azonosítót tartalmazó json fájl. profileId - Szerver profil megnevezés pdfPasswordX – Az eredetileg beküldött X PDF fájl jelszava,

	ha az jelszóval védett volt (a szerver nem tárol jelszavakat, ezért szükséges újra megadni)
Funkció leírása	A bejövő (inJsonFile) json fájlban található session azonosító alapján lekérdezi az aláírás állapotát. Ha minden aláírás készen van, akkor visszaadja az aláírt pdf fájlokat, ha nem, akkor hibakódot ad. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	Az aláírt pdf fájlok.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/remotesignpadesstatusmultiple

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/remotesignpadesstatusmultiple" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inJsonFile" name=" inJsonFile" />
  <input type="string" id="pdfPassword1" name=" pdfPassword1" value="test" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.24 RemoteSign_XAdES

Pades_sign interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="remotesignxades">
        <method name="POST" id="remotesignxades">
          <request>
            <doc title="Tárolt kulcsú XAdES aláírás indítása" xml:lang="hu">Egy vagy több
dokumentum e-Aktába helyezése és az e-Akta XAdES aláírása tárolt kulcs szolgáltatás
segítségével.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="dossierTitle" required="true" type="String">
                <doc title="dossierTitle" xml:lang="hu">Az e-Akta címe</doc>
              </param>
              <param name="inFileX" required="true" repeating="true" type="File">
                <doc title="inFileX" xml:lang="hu">
                  Az aláírandó fájlok, melyek name paramétere inFile-lal kezdődik
és egymástól eltérő értékű.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
              <param name="isDetached" required="false" type="Boolean">
                <doc title="isDetached" xml:lang="hu">Különálló aláírást készítsen-
e? Alapértelmezett értéke false.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/json">
              <doc title="válasz" xml:lang="hu">
                A válasz egy json fájl, ami tartalmazza az indított session
azonosítót. A fájl nevét a headerből lehet kiolvasni.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resource>
  </resources>
</application>
```


A HTTP státuskód jelölheti, hogy minden rendben, jelölhet dokumentum hibát vagy rendszerhibát.

```

        </doc>
      </representation>
    </response>
  </method>
</resource>

</resource>
</resources>
</application>

```

Funkció neve	XadesSign_remote
Bemeneti adatok	- profileId - Szerver profil megnevezés - dossierTitle - Az elkészülő e-akta címe - inFileX - Aláírandó fájlok listája - isDetached - Különálló aláírás készüljön-e. Opcionális, alapértelmezett értéke false.
Funkció leírása	A bemeneti fájl lista tartalmát elhelyezi egy e-aktában és a megadott profilban található tárolt kucslú szolgáltatással aláírja. Ez a funkció megkezdje az aláírást és visszaad egy session azonosítót, amivel le lehet kérdezni az aláírás állapotát. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren a program hibára fut. A feltöltött aláírandó fájloknak tetszőleges a neve. A program a feltöltött névvel fogja beilleszteni a fájlt az elektronikus aktába. Az aktának a dossierTitle paraméterben megadott nevet fogja adni. A válasz az elkészült e-akta. Amennyiben isDetached értéke true, akkor nem elektronikus akta készül, hanem különálló aláírás.
Visszatérő adatok	A session azonosítót tartalmazó json file.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/remotesignxades

Példa form:

```

<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/xadessign" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="text" id="dossierTitle" name="dossierTitle" value="Cím"/>
  <input type="file" id="inFile0" name="inFile0" />
  <input type="file" id="inFile1" name="inFile1" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>

```

5.1.25 RemoteSign_XAdES_Staus

Pades_sign interfész leíró wadl fájl

```

<?xml version="1.0" encoding="UTF-8"?>
<application
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 http://wadl.dev.java.net/2009/02/wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="remotesignxadesstatus">

```

```

<method name="POST" id="remotesignxadesstatus">
  <request>
    <doc title="Tárolt kulcsú XAdES aláírás állapotának lekérdezése"
xml:lang="hu">Session azonosító alapján visszaadja az aláírt XAdES dokumentumot, ha az aláírás
elkészült.</doc>
    <representation mediaType="multipart/form-data">
      <param name="profileId" required="true" type="String">
        <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
      </param>
      <param name="inJsonFile" required="true" repeating="false" type="File">
        <doc title="inJsonFile" xml:lang="hu">A session azonosítót tartalmazó
json file.</doc>
      </param>
    </representation>
  </request>
  <response>
    <representation mediaType="application/pdf">
      <doc title="válasz" xml:lang="hu">
        A válasz egy darab XAdES formátumú dokumentum, amennyiben az aláírás
elkészült. A fájl nevét a headerből lehet kiolvasni.
        A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát vagy azt is hogy az aláírás még nem készült el.
      </doc>
    </representation>
  </response>
</method>
</resource>
</resources>
</application>

```

Funkció neve	XadesSign_remote_status
Bemeneti adatok	- inJsonFile –A session azonosítót tartalmazó json fájl. - profileId - Szerver profil megnevezés
Funkció leírása	A bejövő (inJsonFile) json fájlban található session azonosító alapján lekérdezi az aláírás állapotát. Ha az aláírás készen van, akkor visszaadja az aláírt pdf fájlt, ha nem, akkor hibakódot ad. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.
Visszatérő adatok	Az aláírt XAdES fájl.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/remotesignxadesstatus

Példa form:

```

<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/remotesignxadesstatus" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inJsonFile" name=" inJsonFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>

```

5.1.26 RemoteSign_ASiC

Asic_signinterfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<application xmlns="http://wadl.dev.java.net/2009/02"
xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="remotesignasic">
        <method name="POST" id="remotesignasic">
          <request>
            <doc title="ASiC aláírás tárolt kulcs segítségével" xml:lang="hu">Egy vagy
több dokumentum ASiC konténerbe helyezése és XAdES aláírása tárolt kulcs szolgáltatás
segítségével.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
azonosítója</doc>
              </param>
              <param name="containerTitle" required="true" type="String">
                <doc title="containerTitle" xml:lang="hu">Az ASiC konténer zip fejléc
szöveg</doc>
              </param>
              <param name="inFileX" required="true" repeating="true" type="File">
                <doc title="inFileX" xml:lang="hu">
                  Az aláírandó fájlok, melyek name paramétere inFile-lal kezdődik
és egymástól eltérő értékű.
                  Az X 0-tól kezdődő folyamatosan növekvő számot jelöl.
                </doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/json">
              <doc title="válasz" xml:lang="hu">
                A válasz egy json fájl, ami tartalmazza az indított session
azonosítót. A fájl nevét a headerből lehet kiolvasni.
                A HTTP státuszkód jelölheti, hogy minden rendben, jelölhet dokumentum
hibát vagy rendszerhibát.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve	AsicSign_remote
Bemeneti adatok	- profileId - Szerver profil megnevezés - containerTitle – Az elkészülő konténer zip fejléc szöveg - inFileX - Aláírandó fájlok listája
Funkció leírása	A bemeneti fájl lista tartalmát elhelyezi egy ASiC konténerben és a megadott profilban található tárolt kulcsú szolgáltatás segítségével aláírja őket (az összeset). Ez a funkció megkezdi az aláírást és visszaad egy session azonosítót, amivel le lehet kérdezni az aláírás állapotát. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren a program hibára fut. A feltöltött aláírandó fájloknak tetszőleges a neve. A program a feltöltött névvel fogja beilleszteni a konténerbe. A konténernek a containerTitle paraméterben megadott zip fejléc szöveget fogja adni. A válasz az elkészült ASiC konténer.
Visszatérő adatok	SessionId-t tartalmazó json
URL	<server>/microsec-pki-service-server-

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/remotesignasic" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileid" value="client2"/>
  <input type="text" id="containerTitle" name="containerTitle" value="Megjegyzés"/>
  <input type="file" id="inFile0" name="inFile0" />
  <input type="file" id="inFile1" name="inFile1" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.1.27 RemoteSign_ASIC_Staus

Pades_sign interfész leíró wadl fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<application xmlns="http://wadl.dev.java.net/2009/02"
  xsi:schemaLocation="http://wadl.dev.java.net/2009/02 wadl.xsd"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <resources base="http://localhost:8080/microsec-pki-service-server-web/PKIServlet">
    <resource path="pki">
      <resource path="remotesignasicstatus">
        <method name="POST" id="remotesignasicstatus">
          <request>
            <doc title="Tárolt kulcsú ASIC aláírás állapotának lekérdezése"
              xml:lang="hu">Session azonosító alapján visszaadja az aláírt ASIC dokumentumot, ha az aláírás
              elkészült.</doc>
            <representation mediaType="multipart/form-data">
              <param name="profileId" required="true" type="String">
                <doc title="profileId" xml:lang="hu">A felhasználói profil
                azonosítója</doc>
              </param>
              <param name="inJsonFile" required="true" repeating="false" type="File">
                <doc title="inJsonFile" xml:lang="hu">A session azonosítót tartalmazó
                json file.</doc>
              </param>
            </representation>
          </request>
          <response>
            <representation mediaType="application/pdf">
              <doc title="válasz" xml:lang="hu">
                A válasz egy darab ASIC formátumú dokumentum, amennyiben az aláírás
                elkészült. A fájl nevét a headerből lehet kiolvasni.
                A HTTP státusz kód jelölheti, hogy minden rendben, jelölhet dokumentum
                hibát vagy rendszerhibát vagy azt is hogy az aláírás még nem készült el.
              </doc>
            </representation>
          </response>
        </method>
      </resource>
    </resources>
  </application>
```

Funkció neve	AsicSign_remote_status
Bemeneti adatok	- inJsonFile –A session azonosítót tartalmazó json fájl. - profileId - Szerver profil megnevezés
Funkció leírása	A bejövő (inJsonFile) json fájlban található session azonosító alapján lekérdezi az aláírás állapotát. Ha az aláírás készen van, akkor visszaadja az aláírt ASIC fájlt, ha nem, akkor hibakódot ad. A HTTP POST formátumban érkezik a kérés, a profil azonosítót a profileId mezőben kell szerepeltetni. Amennyiben a megadott profil azonosító nem szerepel a szerveren, a program hibára fut.

Visszatérő adatok	Az aláírt ASiC fájl.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/remotesignasicstatus

Példa form:

```
<form method="post" action="http://localhost:8080/microsec-pki-service-server-web/PKIServlet/pki/remotesignasicstatus" enctype="multipart/form-data" id="formid" name="formname">
  <input type="text" id="profileid" name="profileId" value="client2"/>
  <input type="file" id="inJsonFile" name=" inJsonFile" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.2 ESignProxy Callback funkció

Funkció neve	ESignProxy_callback
Bemeneti adat	- sessionId– Az aláírt fájl ESignProxy sessionId-je. - type – A visszahívás típusa.
Funkció leírása	Az ESign protokoll lehetőséget ad arra, hogy a státusz változásokat (Pl.: feltöltötte a felhasználó a tanúsítványát vagy aláírta és feltöltötte a lenyomatot) egy callback URL-en keresztül jelezze az ESignProxyServer. Ehhez az ESignProxy szerveren előzetesen regisztrálni kell a szerverünk ezen callback URL-jét, illetve az EHSZ konfigurációja során beállítani a CALLBACK opciót az „ESign szerver beállítások” bekezdésben megadott módon. Ez a funkció várja, hogy az ESignProxy visszajelezzon, ha státusz változás következett be. A változás típusáról a type http POST paraméterben értesíti a szervert, míg a sessionId-vel pedig beazonosítható a munkamenet.
Visszatérő adatok	Amennyiben a megadott type nem szerepel a szerveren, a program ezt válaszként közli az ESignProxy-val és kilép. A HTTP státuszkód jelölheti, hogy minden rendben vagy jelölhet rendszerhibát.
URL	<server>/microsec-pki-service-server-web/PKIServlet/pki/esignproxycallback

Példa form:

```
<form method="post" action="https://esignservice.eszigno.hu/esignservice/PKIServlet/pki/esignproxycallback" id="formid" name="formname">
  <input type="text" id="type" name="type" value="signed_hash"/>
  <input type="text" id="sessionId" name="sessionId" />
  <input type="submit" id="sbmt_btn" name="sbmt_btn"/>
</form>
```

5.3 Szerver PKI MQ interfész funkciók

Az MQ üzenetek adat részében az alábbi xml sémadefinícióknak megfelelő xml-t kell elhelyezni. Egy ilyen kérésre az ugyancsak sémával leírt xml válasz érkezik.

5.3.1 XAdES_sign

Xades_sign requestet leíró xml séma

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="XAdESSignRequest" type="XAdESSignRequestType"/>
  <xs:complexType name="XAdESSignRequestType">
    <xs:sequence>
      <xs:element type="xs:string" name="profileId"/>
      <xs:element type="xs:string" name="dossierTitle"/>
      <xs:element type="xs:base64Binary" name="inFile" minOccurs="1" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Xades_sign response-t leíró xml séma

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="XAdESSignResponse" type="XAdESSignResponseType"/>
  <xs:complexType name="XAdESSignResponseType">
    <xs:sequence>
      <xs:element type="xs:base64Binary" name="signedFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

5.3.2 XAdES_validate

Xades_validate requestet leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="XAdESValidateRequest" type="XAdESValidateRequestType"/>
  <xs:complexType name="XAdESValidateRequestType">
    <xs:sequence>
      <xs:element type="xs:string" name="profileId"/>
      <xs:element name="minXadesType">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="bes"/>
            <xs:enumeration value="t"/>
            <xs:enumeration value="c"/>
            <xs:enumeration value="x"/>
            <xs:enumeration value="x-1"/>
            <xs:enumeration value="a"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element type="xs:base64Binary" name="inFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Xades_validate response-t leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="XAdESValidateResponse" type="XAdESValidateResponseType"/>
  <xs:complexType name="XAdESValidateResponseType">
    <xs:sequence>
      <xs:element type="xs:base64Binary" name="vaildationFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

5.3.3 Encrypt

Encrypt requestet leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="EncryptRequest" type="EncryptRequestType"/>
  <xs:complexType name="EncryptRequestType">
    <xs:sequence>
      <xs:element type="xs:string" name="profileId"/>
      <xs:element type="xs:base64Binary" name="inFile"/>
      <xs:element type="xs:base64Binary" name="inCert" minOccurs="1" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Encrypt response-t leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="EncryptResponse" type="EncryptResponseType"/>
  <xs:complexType name="EncryptResponseType">
    <xs:sequence>
      <xs:element type="xs:base64Binary" name="encryptedFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

5.3.4 Decrypt

Decrypt requestet leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="DecryptRequest" type="DecryptRequestType"/>
  <xs:complexType name="DecryptRequestType">
    <xs:sequence>
      <xs:element type="xs:string" name="profileId"/>
      <xs:element type="xs:base64Binary" name="inFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Decrypt response-t leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="DecryptResponse" type="DecryptResponseType"/>
  <xs:complexType name="DecryptResponseType">
    <xs:sequence>
      <xs:element type="xs:base64Binary" name="decryptedFiles"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

5.3.5 Pades_sign

Pades_sign requestet leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="PAdESSignRequest" type="PAdESSignRequestType"/>
  <xs:complexType name="PAdESSignRequestType">
    <xs:sequence>
      <xs:element type="xs:string" name="profileId"/>
      <xs:element type="xs:base64Binary" name="inFile"/>
    </xs:sequence>
  </xs:complexType>
```

```
</xs:schema>
```

Pades_sign response-t leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="PAdESSignResponse" type="PAdESSignResponseType"/>
  <xs:complexType name="PAdESSignResponseType">
    <xs:sequence>
      <xs:element type="xs:base64Binary" name="signedPdfFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

5.3.6 Pades_validate

Pades_validate requestet leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="PAdESValidateRequest" type="PAdESValidateRequestType"/>
  <xs:complexType name="PAdESValidateRequestType">
    <xs:sequence>
      <xs:element type="xs:string" name="profileId"/>
      <xs:element type="xs:base64Binary" name="inFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Pades_validate response-t leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="PAdESValidateResponse" type="PAdESValidateResponseType"/>
  <xs:complexType name="PAdESValidateResponseType">
    <xs:sequence>
      <xs:element type="xs:base64Binary" name="validationFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

5.3.7 Create_acknowledgement

Create_acknowledgement requestet leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="CreateAckRequest" type="CreateAckRequestType"/>
  <xs:complexType name="CreateAckRequestType">
    <xs:sequence>
      <xs:element type="xs:string" name="profileId"/>
      <xs:element type="xs:base64Binary" name="inFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Create_acknowledgement response-t leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="CreateAckResponse" type="CreateAckResponseType"/>
  <xs:complexType name="CreateAckResponseType">
    <xs:sequence>
      <xs:element type="xs:base64Binary" name="ackFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```



```
</xs:schema>
```

5.3.8 Check_acknowledgement

Check_acknowledgement requestet leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="CheckAckRequest" type="CheckAckRequestType"/>
  <xs:complexType name="CheckAckRequestType">
    <xs:sequence>
      <xs:element type="xs:string" name="profileId"/>
      <xs:element type="xs:base64Binary" name="inFile"/>
      <xs:element type="xs:base64Binary" name="inEt3"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Check_acknowledgement requestet leíró xsd fájl

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="CheckAckResponse" type="CheckAckResponseType"/>
  <xs:complexType name="CheckAckResponseType">
    <xs:sequence>
      <xs:element type="xs:base64Binary" name="validationFile"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

5.4 EHSZ teszt oldalak

Monitorozó modul nélküls is ad vissza magáról információt az EHSZ. Ezeknek az oldalaknak a leírása található itt.

5.4.1 Regisztrációs információk

Az EHSZben futó eszignó aláíró motor regisztrációjáról ad vissza információkat az alábbi címen: http://<server>/microsec-pki-service-server-web/info/reg_info.jsp

Itt ellenőrizhetjük, hogy az aláíró motor regisztrációja rendben van-e.

5.5 Monitor funkciók leírása

- A profilok, mint szövegfájlok megtekintése és szerkesztése
- Szerver napló megtekintése egy megadott időintervallumban

6 Konfiguráció

A konfigurációs fájlok helyét a Java futtató környezet tulajdonságaiban kell beállítani. A JVM indításakor a `-D<propName>=<value>` paraméterekkel állíthatjuk be az elérési utakat.

6.1 Szerver konfigurációs fájlok

A szerver két property fájl alapján végzi a működését. Az egyik a szerver tulajdonságok, másik a szerverhez tartozó profilok.

Konfigurációs paraméterek:

- `-Dmicrosec.pki.server.userProfilesDir` – felhasználói profilokat tartalmazó könyvtár
- `-Dmicrosec.pki.server.propertyFile` – szerver tulajdonságok

Proxy esetében JVM opcióként ennek a beállításait is meg kell adni.

6.1.1 A szerver tulajdonságai (ServerContext)

A szerver tulajdonságok határozzák meg a különböző PKI folyamatok alap beállításait. Ezek a

beállítások ritkán változó paraméterek, jellemzően a rendszer egész életciklusára szólnak. A szerver tulajdonságok elérési helyét a `microsec.pki.server.propertyFile` JVM opcióban kell megadni.

6.1.1.1 A szerver dedikált könyvtárai és fájljai

A szerver előre definiált könyvtárakban keresi az azonos típusú és nem meghatározott darabszámú fájlokat, például a megbízható gyökértanúsítványokat.

6.1.1.1.1 `eszigno_cert_auth_dir` - azonosítási tanúsítványokat tartalmazó könyvtár útvonala

Ebbe a könyvtárba kell bemásolni az SSL/TLS azonosításhoz szükséges tanúsítványokat (pl.: `auth.pfx`) az e-Szignó számára, ha az időbélyeg- vagy más szolgáltató tanúsítvány alapú azonosítást kér.

```
Példa: eszigno_cert_auth_dir=/msc/opt/eszigno3/product/current/auth
```

6.1.1.1.2 `eszigno_dir` - e-Szignó telepítési könyvtár útvonala

Azt a könyvtárat kell beállítani, amiben az e-Szignó található. Ebből a könyvtárból származtatható a futtatható állomány helye.

```
Példa: eszigno_dir=/msc/opt/eszigno3/product/current
```

6.1.1.1.3 `eszigno_work_dir` - e-Szignó munkakönyvtár útvonala

Egy munkakönyvtárat kell megadni, melybe az e-Szignó átmeneti fájlokat helyez el a futás során.

```
Példa: eszigno_work_dir=/msc/srv/eszignoservice/var/eszigno
```

6.1.1.1.4 `eszigno_intermediate_cert_dir` - Köztes tanúsítványok könyvtárának útvonala

A tanúsítványok ellenőrzéséhez használható köztes HSZ tanúsítványokat tartalmazó könyvtár(ak). Több könyvtár is megadható szóköz karakterrel elválasztva.

```
Példa: eszigno_intermediate_cert_dir=/msc/opt/eszigno3/product/current/intermediate_certs
```

6.1.1.1.5 `eszigno_trusted_cert_dir` - Megbízható tanúsítványok könyvtárának útvonala

Az e-Szignó által megbízhatónak elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM vagy DER formátumban, `.cer` vagy `.crt` kiterjesztéssel a megadott könyvtárban található). Több könyvtár is megadható szóköz karakterrel elválasztva.

```
Példa: eszigno_trusted_cert_dir=/msc/opt/eszigno3/product/current/trusted_certs
```

6.1.1.1.6 `eszigno_ocsp_trusted_cert_dir` - OCSP tanúsítványok könyvtárának útvonala

Az e-Szignó által az OCSP válaszadó tanúsítványok ellenőrzésekor megbízhatónak elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM vagy DER formátumban, `.cer` vagy `.crt` kiterjesztéssel a megadott könyvtárban található). Több könyvtár is megadható szóköz karakterrel elválasztva.

```
Példa: eszigno_ocsp_trusted_cert_dir=/msc/opt/eszigno3/product/current/ocsp_trusted_certs
```

6.1.1.1.7 `eszigno_signer_trusted_cert_dir` - Aláírás ellenőrzésekor megbízhatónak elfogadott gyökértanúsítványok könyvtárának útvonala

Az e-Szignó által az aláírói tanúsítványok ellenőrzésekor megbízhatónak elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM vagy DER formátumban, `.cer` vagy `.crt` kiterjesztéssel a megadott könyvtárban található). Több könyvtár is megadható szóköz karakterrel elválasztva. Alapértelmezett értéke a `eszigno_trusted_cert_dir` értéke.

```
Példa: eszigno_signer_trusted_cert_dir=/msc/opt/eszigno3/product/current/signer_trusted_certs
```

6.1.1.1.8 eszigno_tsa_trusted_cert_dir - Időbélyeg tanúsítványok könyvtárának útvonala

Az e-Szignó által az időbélyeg szolgáltató tanúsítványok ellenőrzésekor megbízhatónak elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM vagy DER formátumban, .cer vagy .crt kiterjesztéssel a megadott könyvtárban található). Több könyvtár is megadható szóköz karakterrel elválasztva.

```
Példa: eszigno_tsa_trusted_cert_dir=/msc/opt/eszigno3/product/current/tsa_trusted_certs
```

6.1.1.1.9 eszigno_ssl_trusted_cert_dir - SSL tanúsítványok könyvtárának útvonala

Az e-Szignó által a web server tanúsítványok ellenőrzésekor megbízhatónak elfogadható tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM vagy DER formátumban, .cer vagy .crt kiterjesztéssel a megadott könyvtárban található). Több könyvtár is megadható szóköz karakterrel elválasztva.

```
Példa: eszigno_ssl_trusted_cert_dir=/msc/opt/eszigno3/product/current/ssl_trusted_certs
```

6.1.1.1.10 server_upload_dir - A szerver feltöltési könyvtárának útvonala

A szerverre feltöltött fájlok ebbe a könyvtárba kerülnek ideiglenesen. A rendszer automatikusan törli ezeket a fájlokat.

```
Példa: server_upload_dir=/msc/srv/eszignoservice/var/server/uploaded
```

6.1.1.1.11 eszigno_reg_file_path – e-Szignó regisztrációs fájl elérési útja

A rendszer kipróbálható teszt regisztrációval, de ekkor csak teszt tanúsítványokat fogad el. Az éles regisztrációban benne kell lennie ESignServer engedélynek is.

```
Példa: eszigno_reg_file_path=/msc/opt/eszigno3/server_reg.xml
```

6.1.1.2 e-Szignó naplózás

Szükségessé válhat az összes PKI művelet részletes kinaplózása hibafeltárás miatt. Pl.: Nem jött OSCP válasz egy tanúsítvány esetében, stb... A naplózással kapcsolatban akövetkező beállítások lehetségesek:

6.1.1.2.1 eszigno_log_dir - Az e-Szignó napló könyvtárának útvonala

Az e-Szignó ebbe a könyvtárba helyezi el a log fájlokat. Ha nincs megdva nem naplóz.

```
Példa: eszigno_log_dir=/msc/logs/ESZIGNOSERVICE-LOGS/eszigno
```

6.1.1.2.2 eszigno_log_level – Az e-Szignó naplózási szintje

A lehetséges értékek: TRACE, DEBUG, INFO, WARN, ERROR, NO. A naplózási szintek a naplózott adatok tartamát és részletességét befolyásolják. Tesztleletlen rendszernél a legrészletesebb naplózás szükséges, míg üzemszerű működésnél elegendő a hibák okainak kiírása.

```
Példa: eszigno_log_level=TRACE
```

6.1.1.2.3 eszigno_log_max_size – e-Szignó naplómérete

A debug log fájl maximális méretét kell megadni kByte-ban. Ha a log eléri ezt a méretet, akkor az alkalmazás átmozgatja egy '.1' postfixszel ellátott fájlba és egy új üres log fájl nyit.

```
Példa: eszigno_log_max_size=10000
```

6.1.1.3 Proxy beállítások

Az e-Szignó számára külön kell beállítani a proxy-t, amennyiben van.

6.1.1.3.1 eszigno_proxy_host – e-Szignó proxy host beállítása

A HTTP kapcsolódáskor igénybe veendő HTTP/1.1 proxy szerver elérési címe.

Példa: eszigno_proxy_host=proxy.domain.com

6.1.1.3.2 eszigno_proxy_port – e-Szignó proxy port beállítása

A HTTP kapcsolódáskor igénybe veendő HTTP/1.1 proxy szerver elérési címének portja.

Példa: eszigno_proxy_port=3344

6.1.1.3.3 eszigno_proxy_user – e-Szignó proxy felhasználó

A proxy szerver eléréshez tartozó felhasználónév, ha szükséges.

Példa: eszigno_proxy_user=pki-user

6.1.1.3.4 eszigno_proxy_password – e-Szignó proxy felhasználó jelszava

A proxy szerver eléréshez tartozó jelszó, ha szükséges.

Példa: eszigno_proxy_password=Pwd-12345

6.1.1.3.5 eszigno_proxy_exception_list – e-Szignó proxy kivétel lista

Azon URL-ek listája, ahová proxy használata nélkül kell csatlakozni. A lista elemeket szóközzel kell elválasztani.

Példa: eszigno_proxy_exception_list=timestamp.e-szigno.hu upload.e-szigno.hu

6.1.1.4 e-Szignó futási módok

Az e-Szignót többféleképpen lehet futtatni operációs rendszertől függően.

6.1.1.4.1 eszigno_run_mode – e-Szignó futási mód

Lehetséges értékek: cmd, daemon, daemon+soap

A cmd érték a parancssori e-Szignó futtatását jelenti. A daemon és a daemon+soap daemon módban futtatja az e-Szignót, ezek windows operációs rendszeren nem értelmezettek. Használatukkal nagyobb performancia érhető el.

Példa: eszigno_run_mode=cmd

6.1.1.4.2 daemon_port – e-Szignó daemon port

A port, amelyen az e-Szignó démon folyamat fogadja a beérkező kéréseket. Csak akkor van értelme megadni, ha démon módban fut az e-Szignó.

Példa: daemon_port=5416

6.1.1.4.3 daemon_children_number – e-Szignó daemon gyereke száma

Az e-Szignó fő démon folyamat által létrehozandó gyermekfolyamatok száma. Csak akkor van értelme megadni, ha démon módban fut az e-Szignó.

Példa: daemon_children_number=30

6.1.1.5 e-Szignó egyéb beállítások

Az e-Szignót működéséhez szükséges egyéb beállítások a következők:

6.1.1.5.1 eszigno_digest_algorithm – e-Szignó lenyomatképző algoritmus

A használandó lenyomatképző algoritmus az aláírás létrehozása esetén.

```
Példa: eszigno_digest_algorithm=sha256
```

6.1.1.5.2 eszigno_sdk_password – e-Szignó SDK jelszó

Az SDK használatához szükséges jelszó (kód), amennyiben a regisztráció típusa ezt is megköveteli.

```
Példa: eszigno_sdk_password=sha256
```

6.1.1.5.3 eszigno_time_out_millsec – e-Szignó kapcsolódási timeout

A kapcsolódási timeout érték milliszekundum egységben.

```
Példa: eszigno_time_out_millsec=60000
```

6.1.1.5.4 eszigno_xades_version – aláírásoknál használt XAdES verzió

Az újonnan létrehozandó aláírások XAdES verzióját állítja be. Lehetséges értékei: 1.2.2, 1.3.2, 1.4.1, 1.4.2

```
Példa: eszigno_xades_version=1.4.2
```

6.1.1.5.5 verbose – e-Szignó verbose mód

Státuszüzenetek küldése a stderr adatfolyamra. Az alapértelmezett értéke „no”.

```
Példa: verbose=yes
```

6.1.1.6 ESign szerver beállítások

Kétmenetes aláírásnál az ESignProxy szerverrel kell kommunikálni. Ehez a következő beállítások kellenek:

6.1.1.6.1 esign_proxy_mode – ESignProxy-n történő állapotváltozás nyomonkövetése

Lehetséges értékei: POLL, CALLBACK. Kétféleképpen lehet nyomonkövetni az aszinkron állapotváltozásokat:

- **Pollozás:** ez esetben a státusz változásokat (feltöltötte a felhasználó a tanúsítványát vagy aláírta és feltöltötte a lenyomatot) az EHSZ folyamatosan lekérdezi az ESignProxy szerverről.
- **Callback URL:** Az ESign protokoll lehetőséget ad arra is, hogy a státusz változásokat (feltöltötte a felhasználó a tanúsítványát vagy aláírta és feltöltötte a lenyomatot) egy callback URL-en keresztül jelezze az ESignProxyServer. Ehhez az ESignProxy szerveren előzetesen regisztrálni kell a szerverünk callback URL-jét (további információért lásd: „ESignProxy_callback” funkció leírása), illetve itt beállítani a CALLBACK opciót.

```
Példa: esign_proxy_mode=POLL
```

6.1.1.6.2 esign_max_thread_num – várakozó szálak maximális száma

Kétmenetes aláírás esetében mennyi lehet a várakozó szálak száma. Ez az érték csak nagyobb lehet nullánál.

```
Példa: esign_max_thread_num=10
```

6.1.1.7 Dokumentum törlési beállítások

A szerveren a tranzakció lejáratáig dokumentumok maradnak, utána törlődnek, kivétel a kétmenetes aláírás. Ekkor meg kell várni, hogy a kliens is értesüljön az aláírás elkészültéről és csak ez után tudja letölteni. Itt lehet beállítani, hogy mennyi legyen a várakozási idő.

6.1.1.7.1 delete_poll_second – A fájlok életkorának ellenőrzési periódusa

Másodpercben meg kell adni, hogy mennyi időnként ellenőrizze a fájlok vagy könyvtárak

életkorát.

Példa: `delete_poll_second=3600`

6.1.1.7.2 `delete_period_second` – A fájlok maximális életkora

Ennél öregebb fájl vagy könyvtár kitörlésre kerül.

Példa: `delete_period_second=86400`

6.1.1.8 Adatbázis elérés

6.1.1.8.1 `db_resource_jndi_name` – Adatbázis elérés

Az Alkalmazás Szerverben beállított JNDI név. Opcionális paraméter. Ha meg van adva, akkor az EHSZ kapcsolódik a JNDI névvel megjelölt adatforráshoz, és minden műveletről készít egy naplóbejegyzést a `hsz.server_operation_log` táblába. Ha nincs megadva, akkor a bejegyzések az alkalmazás naplófájlba kerülnek.

Példa: `db_resource_jndi_name=java:/comp/env/jdbc/signer`

6.1.1.9 MQ beállítások (MQWorkerContext)

A következő paraméterek az online mq feldogozó szálak egy-egy csoportjára vonatkoznak, a csoportokat az mq prefix utáni egész számmal azonosítjuk.

6.1.1.9.1 Queue manager csoport

A csoportokat egymástól a mq prefix végén levő szám különbözteti meg.

6.1.1.9.1.1 Queue manager neve

Azon queue manager neve amihez a feldolgozó szálak ezen csoportja kapcsolódik.

Példa: `mq0_qmgr=ESIG_DV`

6.1.1.9.1.2 Gépnév vagy IP cím

Host gép, amin a queue manager található.

Példa: `mq0_host=127.0.0.1`

6.1.1.9.1.3 Port szám

MQ kommunikációs port.

Példa: `mq0_port=1414`

6.1.1.9.1.4 Kommunikációs csatorna neve

Azon csatorna neve amin a feldolgozó szálak ezen csoportja kapcsolódik.

Példa: `mq0_channel=ESIG_DV_CH_01`

6.1.1.9.1.5 Input queue neve

A feldolgozó szálak ezen csoportja erről a queue-ról fogja fogadni az üzeneteket.

Példa: `mq0_input_queue=ESIGMAIN_IN_P`

6.1.1.9.1.6 Input időtúllépés

A feldolgozó szálak ezen csoportja üzenet olvasásakor maximum ennyi másodpercig várakozik arra, hogy beérkezzen egy üzenet. Ha ez az idő letelik, a program újrapróbálkozik az üzenetolvasással.

Példa: mq0_input_timeout_sec=5

6.1.1.9.1.7 *Output queue neve*

A feldolgozó szálak ezen csoportja erre a queue-ra írja a válaszüzeneteket.

Példa: mq0_output_queue=ESIGMAIN_OUT_A

6.1.1.9.1.8 *Várakozás hiba esetén*

A feldolgozó szálak ezen csoportja kapcsolati hiba esetén ennyi másodpercig várakozik, majd újra kiépíti a kapcsolatot a queue managerrel és megnyitja az input és output queue-kat.

Példa: mq0_reconnect_wait_sec=30

6.1.1.9.1.9 *Próbálkozások száma hiba esetén*

A feldolgozó szálak ezen csoportja kapcsolati hiba esetén ennyiszor próbálja meg újraépíteni a kapcsolatot a queue managerrel.

Példa: mq0_reconn_count=30

6.1.1.9.1.10 *A feldolgozó szálak száma*

A feldolgozó szálak száma ezen a csoporton belül.

Példa: mq0_workers_count=2

6.1.1.9.2 *Globális MQ beállítások*

Az összes csatornára érvényes beállítások.

6.1.1.9.2.1 *Az üzenetek maximális hossza*

Az üzenetek maximális hossza bájtokban megadva.

Példa: mq_max_message_length=3145728

6.1.1.9.2.2 *Az üzenetek karakterkódolása*

Az üzenetek karakter kódolásának kódja. Latin 1 esetében: 819

Példa: mq_message_charset=819

6.1.1.9.2.3 *Az üzenetek ID-jének prefixe*

Az üzenetek küldésénél a prefix.

Példa: mq_messageid_prefix=ESIG

6.1.1.9.2.4 *A leállítási időtúllépés*

Ennyit várakozik a leállításra.

Példa: mq_stop_timeout_sec=5

6.1.1.10 *Tárolt kulcsú aláírás szolgáltatás (TKSZ)*

Amennyiben az aláírás tárolt kulcsú aláírás szolgáltató segítségével történik, a következő paramétereket kell beállítani.

6.1.1.10.1 *remote_sign_session_dir – Session könyvtár*

Az aláírás során keletkező ideiglenes fájlokat tartalmazó könyvtárat kell megadni. Az alkalmazásnak kell tudni írni ebbe a könyvtárba.

Példa: remote_sign_session_dir=/msc/config/sessions

6.1.1.10.2 clean_poll_remote_sign_session_dir_second – Ideiglenes fájlok vizsgálatának ideje

A paraméter azt adja meg, hogy az alkalmazás milyen időközönként vizsgálja meg az ideiglenes fájlok könyvtárát. Értéke másodpercben értendő. Alapértelmezett értéke: 3600.

Példa: `clean_poll_remote_sign_session_dir_second=3600`

6.1.1.10.3 clean_period_remote_sign_session_dir_second – Ideiglenes fájlok élettartama

A paraméter azt adja meg, hogy az alkalmazás milyen idős ideiglenes fájlokat töröljön. Alapértelmezett értéke: 17280.

Példa: `clean_period_remote_sign_session_dir_second=17280`

6.1.1.11 Bizalmi listák kezelése (EU TSL)

Az EU-s bizalmi listák kezelését szabályozó paramétereket a következő módon kell beállítani.

6.1.1.11.1 tsl_usage_mode – TSL használat módja

Paraméter megadja, hogy az alkalmazás használja-e a bizalmi listákat a tanúsítvány megbízhatóságának eldöntésekor.

Lehetséges értékei:

- `yes` - Az alkalmazás a tanúsítvány ellenőrzésekor egyaránt figyelembe veszi a TSL-en található információkat és a megbízható tanúsítványokat tartalmazó könyvtárakat is.
- `only_tsl` - Az alkalmazás kizárólag a TSL alapján fogja ellenőrizni a tanúsítványok megbízhatóságát.
- `no` - Tanúsítvány megbízhatóságának ellenőrzéséhez nem használja a TSL-t a program.

Alapértelmezett értéke: `yes`.

Példa: `tsl_usage_mode=yes`

6.1.1.11.2 tsl_cache_dir – TSL munkakönyvtár

Az alkalmazás a megadott könyvtárat használja cache könyvtárként. Ezért írási jog szükséges a könyvtárra. Alapértelmezett értéke: `„.”` (aktuális munkakönyvtár).

Példa: `tsl_cache_dir=./tsl/cache`

6.1.1.11.3 tsl_service_info_usage – TSL használatot segítő Microsec szolgáltatás használata

A biztonságos TSL validáláshoz szükséges információk beszerzése Microsec szolgáltatáson keresztül. Bekapcsolása esetén nem szükséges a `tsl_trusted_cert_dir` és a `root_tsl_url` opciók használata és azokat az alkalmazás figyelmen kívül is hagyja. Kikapcsolása akkor ajánlott, ha nem elérhető a `download.e-szigno.hu` Microsec-es domain.

Alapértelmezett értéke: `yes`.

Példa: `tsl_service_info_usage=no`

6.1.1.11.4 tsl_root_url – Gyöker TSL elérési URL-je

A megadott URL-en keresi a gyöker TSL-t. Ez a TSL tartalmazza a többi TSL elérhetőségét. A `tsl_service_info_usage` opció bekapcsolása esetén az alkalmazás figyelmen kívül hagyja ezt a paramétert.

Alapértelmezett értéke: <https://ec.europa.eu/tools/lotl/eu-lotl.xml>

Példa: `tsl_root_url=https://ec.europa.eu/tools/lotl/eu-lotl.xml`

6.1.1.11.5 tsl_trusted_cert_dir – TSL megbízható tanúsítványok könyvtára

A gyöker TSL aláíró tanúsítványának ellenőrzéséhez szükséges megbízható tanúsítványokat

tartalmazó könyvtárnak az elérési útját kell megadni. A `tsl_service_info_usage` opció bekapcsolása esetén az alkalmazás figyelmen kívül hagyja ezt a paramétert.

Példa: `tsl_trusted_cert_dir=./tsl_trusted_certs`

6.1.1.12 Szerver konfiguráció MQ használatával

Példa server.properties:

```
#####
#####          A szerver tulajdonságai          #####
#####          (ServerContext)          #####
#####
# A szerver tulajdonságok határozzák meg a különböző PKI folyamatok alap
# beállításait. Ezek a beállítások ritkán változó paraméterek, jellemzően a
# rendszer egész életciklusára szólnak. A szerver tulajdonságok elérési helyét
# a microsec.pki.server.propertyFile JVM opcióban kell megadni.

#####          A szerver dedikált könyvtárai és fájlljai          #####
#####
# A szerver előre definiált könyvtárakban keresi az azonos típusú és nem
# meghatározott darabszámú fájlokat, például a megbízható
# gyökértanúsítványokat.

#####          Az e-Szignó telepítési könyvtár          #####
#####          útvonala          #####
# Azt a könyvtárat kell beállítani, amiben az e-Szignó található. Ebből a
# könyvtárból származtatható az futtatható állomány helye.
eszigno_dir=/msc/opt/eszigno3/product/current

#####          Az e-Szignó munkakönyvtár útvonala          #####
# Egy munkakönyvtárat kell megadni, melybe az e-Szignó átmeneti fájlokat
# helyez el a futás során.
eszigno_work_dir=/msc/srv/signer/var/eszigno

#####          Köztes tanúsítványok könyvtárának          #####
#####          útvonala          #####
# A tanúsítványok ellenőrzéséhez használható köztes HSZ tanúsítványokat
# tartalmazó könyvtár(ak). Több könyvtár is megadható szóköz karakterrel
# elválasztva.
eszigno_intermediate_cert_dir=/msc/srv/signer/truststore/intermediate_certs

#####          Megbízható tanúsítványok könyvtárának          #####
#####          útvonala          #####
# Az e-Szignó által megbízhatónak elfogadandó tanúsítványokat tartalmazó
# könyvtár(ak) (a tanúsítványok PEM vagy DER formátumban, .cer vagy .crt
# kiterjesztéssel a megadott könyvtárban található). Több könyvtár is
# megadható szóköz karakterrel elválasztva.
eszigno_trusted_cert_dir=/msc/srv/signer/truststore/crypter_trusted_certs_teszt

#####          OCSP tanúsítványok könyvtárának          #####
#####          útvonala          #####
# Az e-Szignó által az OCSP válaszadó tanúsítványok ellenőrzésekor
# megbízhatónak elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a
# tanúsítványok PEM vagy DER formátumban, .cer vagy .crt kiterjesztéssel a
# megadott könyvtárban található). Több könyvtár is megadható szóköz
# karakterrel elválasztva.
eszigno_ocsp_trusted_cert_dir=/msc/srv/signer/truststore/ocsp_trusted_certs_teszt

#####          Aláírás ellenőrzésekor megbízhatónak          #####
#####          elfogadott gyökértanúsítványok          #####
#####          könyvtárának útvonala          #####
# Az e-Szignó által az aláírói tanúsítványok ellenőrzésekor megbízhatónak
# elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM
# vagy DER formátumban, .cer vagy .crt kiterjesztéssel a megadott könyvtárban
# található). Több könyvtár is megadható szóköz karakterrel elválasztva.
# Alapértelmezett értéke a eszigno_trusted_cert_dir értéke.
eszigno_signer_trusted_cert_dir=/msc/srv/signer/truststore/signer_trusted_certs_teszt

#####          Időbélyeg tanúsítványok könyvtárának          #####
#####          útvonala          #####
# Az e-Szignó által az időbélyeg szolgáltató tanúsítványok ellenőrzésekor
# megbízhatónak elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a
# tanúsítványok PEM vagy DER formátumban, .cer vagy .crt kiterjesztéssel a
```

```
# megadott könyvtárban található). Több könyvtár is megadható szóköz
# karakterrel elválasztva.
eszigno_tsa_trusted_cert_dir=/msc/srv/signer/truststore/tsa_trusted_certs_teszt

#####      SSL tanúsítványok könyvtárának      #####
#####      útvonala      #####
# Az e-Szignó által a web server tanúsítványok ellenőrzésekor megbízhatónak
# elfogadható tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM
# vagy DER formátumban, .cer vagy .crt kiterjesztéssel a megadott könyvtárban
# található). Több könyvtár is megadható szóköz karakterrel elválasztva.
eszigno_ssl_trusted_cert_dir=/msc/srv/signer/truststore/ssl_trusted_certs

#####      Az e-Szignó napló könyvtárának      #####
#####      útvonala      #####
# Az e-Szignó ebbe a könyvtárba helyezi el a log fájlokat. Ha nincs megdva nem
# naplóz.
eszigno_log_dir=/msc/logs/SIGNER-LOGS/eszigno

#####      A szerver feltöltési könyvtárának      #####
#####      útvonala      #####
# A szerverre feltöltött fájlok ebbe a könyvtárba kerülnek ideiglenesen. A
# rendszer automatikusan törli ezeket a fájlokat.
server_upload_dir=/msc/srv/signer/var/server/uploaded

#####      Az e-Szignó regisztrációs fájl elérési #####
#####      útja      #####
# A rendszer kipróbálható teszt regisztrációval, de ekkor csak teszt
# tanúsítványokat fogad el. Az éles regisztrációban benne kell lennie
# ESigntServer engedélynek is.
eszigno_reg_file_path=/msc/opt/eszigno3/server_reg.xml

#####      e-Szignó futási módok      #####
#####
# Az e-Szignót többféleképpen lehet futtatni operációs rendszertől függően.

#####      Az e-Szignó futási mód      #####
# Lehetséges értékek: cmd, daemon, daemon+soap, winservice
# A cmd érték a parancssori e-Szignó futtatását jelenti.
# A daemon és a daemon+soap daemon módban futtatja az e-Szignót, ezek windows
# operációs rendszeren nem értelmezettek. Használatukkal nagyobb performancia
# érhető el.
# A winservice csak windows operációs rendszeren használható.
eszigno_run_mode=cmd

#####      e-Szignó egyéb beállítások      #####
#####
# Az e-Szignót működéséhez szükséges egyéb beállítások a következők:

#####      Az e-Szignó lenyomatképző algoritmus      #####
# A használandó lenyomatképző algoritmus az aláírás létrehozása esetén.
eszigno_digest_algorithm=sha256

#####      Az e-Szignó SDK jelszó      #####
# Az SDK használatához szükséges jelszó (kód), amennyiben a regisztráció
# típusa ezt is megköveteli.
#eszigno_sdk_password=sha256

#####      Az e-Szignó kapcsolódási timeout      #####
# A kapcsolódási timeout érték milliszekundum egységben.
eszigno_time_out_millisec=10000

#####      Az aláírásoknál használt XAdES verzió      #####
# Az újonnan létrehozandó aláírások XAdES verzióját állítja be. Lehetséges
# értékei: 1.2.2, 1.3.2, 1.4.1, 1.4.2
eszigno_xades_version=1.3.2

#####
#####      MQ beállítások      #####
#####      (MQWorkerContext)      #####
#####
# A következő paraméterek az online mq feldogozó szálak egy-egy csoportjára
# vonatkoznak, a csoportokat az mq prefix utáni egész számmal azonosítjuk.
```

```
##### Queue manager csoport #####
#####
# A csoportokat egymástól a mq prefix végén levő szám különbözteti meg.

##### Queue manager neve #####
# Azon queue manager neve amihez a feldolgozó szálak ezen csoportja
# kapcsolódik.
mq0_qmgr=ESIG_DV

##### Gépnév vagy IP cím #####
# Host gép, amin a queue manager található.
mq0_host=127.0.0.1

##### Port szám #####
# MQ kommunikációs port.
mq0_port=1414

##### Kommunikációs csatorna neve #####
# Azon csatorna neve amin a feldolgozó szálak ezen csoportja kapcsolódik.
mq0_channel=ESIG_DV_CH_01

##### Input queue neve #####
# A feldolgozó szálak ezen csoportja erről a queue-ról fogja fogadni az
# üzeneteket.
mq0_input_queue=ESIGMAIN_IN_P

##### Input időtúllépés #####
# A feldolgozó szálak ezen csoportja üzenet olvasásakor maximum ennyi
# másodpercig várakozik arra, hogy beérkezzen egy üzenet. Ha ez az idő
# letelik, a program újrapróbálkozik az üzenetolvasással.
mq0_input_timeout_sec=5

##### Output queue neve #####
# A feldolgozó szálak ezen csoportja erre a queue-ra írja a válaszüzeneteket.
mq0_output_queue=ESIGMAIN_OUT_A

##### Várakozás hiba esetén #####
# A feldolgozó szálak ezen csoportja kapcsolati hiba esetén ennyi másodpercig
# várakozik, majd újra kiépíti a kapcsolatot a queue managerrel és megnyitja
# az input és output queue-kat.
mq0_reconnect_wait_sec=30

##### Próbálkozások száma hiba esetén #####
# A feldolgozó szálak ezen csoportja kapcsolati hiba esetén ennyiszer próbálja
# meg újraépíteni a kapcsolatot a queue managerrel.
mq0_reconn_count=2

##### A feldolgozó szálak száma #####
# A feldolgozó szálak száma ezen a csoporton belül.
mq0_workers_count=2

##### Globális MQ beállítások #####
#####
# Az összes csatornára érvényes beállítások.

##### Az üzenetek maximális hossza #####
# Az üzenetek maximális hossza bájtokban megadva.
mq_max_message_length=3145728

##### Az üzenetek karakterkódolása #####
# Az üzenetek karakter kódolásának kódja. Latin 1 esetében: 819
mq_message_charset=819

##### Az üzenetek ID-jének prefixe #####
# Az üzenetek küldésénél a prefix.
mq_messageid_prefix=ESIG

##### A leállítási időtúllépés #####
# Ennyit várakozik a leállításra.
mq_stop_timeout_sec=5
```

6.1.1.13 Szerver konfiguráció MQ nélkül

server.properties

```
#####
#####          A szerver tulajdonságai          #####
#####          (ServerContext)                   #####
#####
#####
# A szerver tulajdonságok határozzák meg a különböző PKI folyamatok alap
# beállításait. Ezek a beállítások ritkán változó paraméterek, jellemzően a
# rendszer egész életciklusára szólnak. A szerver tulajdonságok elérési helyét
# a microsec.pki.server.propertyFile JVM opcióban kell megadni.

#####      Az e-Szignó telepítési könyvtár      #####
#####      útvonala                             #####
# Azt a könyvtárat kell beállítani, amiben az e-Szignó található. Ebből a
# könyvtárból származtatható az futtatható állomány helye.
eszigno_dir=/msc/opt/eszigno3/product/current

#####      Az e-Szignó munkakönyvtár útvonala    #####
# Egy munkakönyvtárat kell megadni, melybe az e-Szignó átmeneti fájlokat
# helyez el a futás során.
eszigno_work_dir=/msc/srv/eszignoservice/var/eszigno

#####      Köztes tanúsítványok könyvtárának      #####
#####      útvonala                             #####
# A tanúsítványok ellenőrzéséhez használható köztes HSZ tanúsítványokat
# tartalmazó könyvtár(ak). Több könyvtár is megadható szóköz karakterrel
# elválasztva.
eszigno_intermediate_cert_dir=/msc/srv/eszignoservice/truststore/intermediate_certs

#####      Megbízható tanúsítványok könyvtárának #####
#####      útvonala                             #####
# Az e-Szignó által megbízhatónak elfogadandó tanúsítványokat tartalmazó
# könyvtár(ak) (a tanúsítványok PEM vagy DER formátumban, .cer vagy .crt
# kiterjesztéssel a megadott könyvtárban található). Több könyvtár is
# megadható szóköz karakterrel elválasztva.
eszigno_trusted_cert_dir=/msc/srv/eszignoservice/truststore/crypter_trusted_certs_teszt

#####      OCSP tanúsítványok könyvtárának        #####
#####      útvonala                             #####
# Az e-Szignó által az OCSP válaszadó tanúsítványok ellenőrzésekor
# megbízhatónak elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a
# tanúsítványok PEM vagy DER formátumban, .cer vagy .crt kiterjesztéssel a
# megadott könyvtárban található). Több könyvtár is megadható szóköz
# karakterrel elválasztva.
eszigno_ocsp_trusted_cert_dir=/msc/srv/eszignoservice/truststore/ocsp_trusted_certs_teszt

#####      Aláírás ellenőrzésekor megbízhatónak    #####
#####      elfogadott gyökértanúsítványok        #####
#####      könyvtárának útvonala                  #####
# Az e-Szignó által az aláírói tanúsítványok ellenőrzésekor megbízhatónak
# elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM
# vagy DER formátumban, .cer vagy .crt kiterjesztéssel a megadott könyvtárban
# található). Több könyvtár is megadható szóköz karakterrel elválasztva.
# Alapértelmezett értéke a eszigno_trusted_cert_dir értéke.
eszigno_signer_trusted_cert_dir=/msc/srv/eszignoservice/truststore/signer_trusted_certs_teszt

#####      Időbélyeg tanúsítványok könyvtárának    #####
#####      útvonala                             #####
# Az e-Szignó által az időbélyeg szolgáltató tanúsítványok ellenőrzésekor
# megbízhatónak elfogadandó tanúsítványokat tartalmazó könyvtár(ak) (a
# tanúsítványok PEM vagy DER formátumban, .cer vagy .crt kiterjesztéssel a
# megadott könyvtárban található). Több könyvtár is megadható szóköz
# karakterrel elválasztva.
eszigno_tsa_trusted_cert_dir=/msc/srv/eszignoservice/truststore/tsa_trusted_certs_teszt

#####      SSL tanúsítványok könyvtárának          #####
#####      útvonala                             #####
# Az e-Szignó által a web server tanúsítványok ellenőrzésekor megbízhatónak
# elfogadható tanúsítványokat tartalmazó könyvtár(ak) (a tanúsítványok PEM
# vagy DER formátumban, .cer vagy .crt kiterjesztéssel a megadott könyvtárban
# található). Több könyvtár is megadható szóköz karakterrel elválasztva.
eszigno_ssl_trusted_cert_dir=/msc/srv/eszignoservice/truststore/ssl_trusted_certs
```

```
##### Az e-Szignó napló könyvtárának #####
##### útvonala #####
# Az e-Szignó ebbe a könyvtárba helyezi el a log fájlokat. Ha nincs megdva nem
# naplóz.
eszigno_log_dir=/msc/logs/ESZIGNOSERVICE-LOGS/eszigno

##### A szerver feltöltési könyvtárának #####
##### útvonala #####
# A szerverre feltöltött fájlok ebbe a könyvtárba kerülnek ideiglenesen. A
# rendszer automatikusan törli ezeket a fájlokat.
server_upload_dir=/msc/srv/eszignoservice/var/server/uploaded

##### Az e-Szignó regisztrációs fájl elérési #####
##### útja #####
# A rendszer kipróbálható teszt regisztrációval, de ekkor csak teszt
# tanúsítványokat fogad el. Az éles regisztrációban benne kell lennie
# ESigServer engedélynek is.
eszigno_reg_file_path=/msc/opt/eszigno3/server_reg.xml

##### e-Szignó naplózás #####
#####
# Szükségessé válhat az összes PKI művelet részletes kinaplózása hibafeltárás
# miatt. Pl.: Nem jött OCSP válasz egy tanúsítvány esetében, stb... A
# naplózással kapcsolatban akövetkező beállítások lehetőségek:

##### Az e-Szignó naplózási szintje #####
# A lehetséges értékek: TRACE, DEBUG, INFO, WARN, ERROR, NO
# A naplózási szintek a naplózott adatok tartamát és részletességét
# befolyásolják. Tesztetletlen rendszernél a legrészletesebb naplózás
# szükséges, míg üzemszerű működésnél elegendő a hibák okainak kiírása.
eszigno_log_level=DEBUG

##### Az e-Szignó naplómérete #####
# A debug log fájl maximális méretét kell megadni kByte-ban. Ha a log eléri
# ezt a méretet, akkor az alkalmazás átmozgatja egy '.1' postfixszel ellátott
# fájlba és egy új üres log fájl nyit.
eszigno_log_max_size=10000

##### e-Szignó futási módok #####
#####
# Az e-Szignót többféleképpen lehet futtatni operációs rendszertől függően.

##### Az e-Szignó futási mód #####
# Lehetséges értékek: cmd, daemon, daemon+soap, winservice
# A cmd érték a parancssori e-Szignó futtatását jelenti.
# A daemon és a daemon+soap daemon módban futtatja az e-Szignót, ezek windows
# operációs rendszeren nem értelmezettek. Használatukkal nagyobb performancia
# érhető el.
# A winservice csak windows operációs rendszeren használható.
eszigno_run_mode=cmd

##### e-Szignó egyéb beállítások #####
#####
# Az e-Szignót működéséhez szükségesegyéb beállítások a következők:

##### Az e-Szignó lenyomatképző algoritmus #####
# A használandó lenyomatképző algoritmus az aláírás létrehozása esetén.
eszigno_digest_algorithm=sha256

##### Az e-Szignó SDK jelszó #####
# Az SDK használatához szükséges jelszó (kód), amennyiben a regisztráció
# típusa ezt is megköveteli.
#eszigno_sdk_password=sha256

##### Az e-Szignó kapcsolódási timeout #####
# A kapcsolódási timeout érték milliszekundum egységben.
eszigno_time_out_millisec=10000

##### Az aláírásoknál használt XAdES verzió #####
# Az újonnan létrehozandó aláírások XAdES verzióját állítja be. Lehetséges
# értékei: 1.2.2, 1.3.2, 1.4.1, 1.4.2
eszigno_xades_version=1.4.1

##### e-Szignó teszt üzemmód #####
# Amennyiben a programhoz tartozó regisztrációs fájl csak a program tesztelési
# célból történő használatát engedélyezi, ezen opciónak true értéket kell
```

```
# adni, különben az e-Szignó 1-es hibakóddal leáll.
eszigno_test=true

#####      ESign szervert beállítások      #####
#####
# Kétmenetes aláírásnál az ESignProxy szervert kell kommunikálni. Ehez a
# következő beállítások kelljenek:

#####      Az ESignProxy-n történő      #####
#####      állapotváltozás nyomonkövetése      #####
# Lehetséges értékei: POLL, POLL. Kétféleképpen lehet nyomonkövetni az
# aszinkron állapotváltozásokat: pollozással és callback-kal. CALLBACK
# esetében az ESignProxy szervert előzetesen regisztrálni kell a szervertől
# callback URL-jét.
esign_proxy_mode=POLL

#####      Az ESignProxy-n történő      #####
#####      állapotváltozás nyomonkövetése      #####
# Kétmenetes aláírás esetében mennyi lehet a várakozó szálak száma. Ez az
# érték csak nagyobb lehet nullánál.
esign_max_thread_num=10

#####      Dokumentum törlési beállítások      #####
#####
# A szervertől a tranzakció lejárataig dokumentumok maradnak, utána törlődnek,
# kivétel a kétmenetes aláírás. Ekkor meg kell várni, hogy a kliens is
# értesüljön az aláírás elkészültéről és csak ez után tudja letölteni. Itt
# lehet beállítani, hogy mennyi legyen a várakozási idő.

#####      A fájlok életkorának ellenőrzési      #####
#####      periódusa      #####
# Másodpercben meg kell adni, hogy mennyi időnként ellenőrizze a fájlok vagy
# könyvtárak életkorát.
delete_poll_second=3600

#####      A fájlok maximális életkora      #####
# Ennél öregebb fájl vagy könyvtár kitörlésre kerül.
delete_period_second=86400
```

6.1.2 Technikai felhasználói profilok (UserProfile)

Profilok segítségével lehet többféle aláírást készíteni. Ezek a beállítások ritkán változó paraméterek. A profilokat egy könyvtárban kell elhelyezni. A könyvtár elérési helyét a `microsec.pki.server.userProfilesDir` JVM opcióban kell megadni.

6.1.2.1 Átvételi elismervény beállításai

6.1.2.1.1 `acknowledgement_version` – átvételi elismervény verziója

Ezzel az opcióval a létrehozandó átvételi elismervények formátumát lehet beállítani. A `v1` az e-akta alapú, régi típusú tértivevényt jelenti, a `v2` a különálló aláírás alapú, egyszerű XAdES tértivevény.

Példa: `acknowledgement_version=v1`

6.1.2.2 Titkosítás visszafejtése

A profil tulajdonosának titkosítva küldött e-Akták visszafejtése a tulajdonos magánkulcsával.

6.1.2.2.1 `decryptor_key` – A profil tulajdonosának magánkulcsa

A PFX formátumú kulcs fájl útvonala

Példa: `decryptor_key=/msc/opt/eszigno3/product/current/pfx/enc_peterke.pfx`

6.1.2.2.2 `decryptor_password` – visszafejtő magánkulcs jelszava

A `decryptor_key` magánkulcs jelszava.

Példa: `decryptor_password=12345`

6.1.2.3 Az ESign protokoll beállításai

Az ESign protokoll a kétmenetes aláíráshoz szükséges, - Pl.: webböngészőn keresztül kliens oldali aláírás esetében. Ekkor nincs a profilhoz tartozó felhasználó magánkulcsa a szerveren.

6.1.2.3.1 `esign_use` – ESign szolgáltatás ki-be kapcsolása

Alapértelmezett értéke: `false`. Abban az esetben, ha be van kapcsolva, akkor a következő paramétereket is meg kell adni.

Példa: `esign_use=false`

6.1.2.3.2 `esign_auth_http_username` – Authentikáció az ESignProxy szerveren

Felhasználói név.

Példa: `esign_auth_http_username=teszt`

6.1.2.3.3 `esign_auth_http_password` – Authentikáció az ESignProxy szerveren

Jelszó.

Példa: `esign_auth_http_password=teszt`

6.1.2.3.4 `esign_use_pkcs7` – Kérelem aláírás

A kérelmet alá kell-e írnia a szervernek az ESignProxy-nak küldéskor. Ha az opció értéke `true`, az ESignProxy szervernek PKCS7 aláírással együtt küldi fel az aláíratlan hash-t az e-Szignó. Ekkor a `userprofile`-nak aláírói kulccsal kell rendelkeznie. Alapértelmezett értéke: `false`.

Példa: `esign_use_pkcs7=false`

6.1.2.3.5 esign_server_url – ESignProxy szerver gyökér URL-je.

A gyökér URL, melynek a végéhez automatikusan illeszti a rendszer a szolgáltatások relatív URL-jét.

```
Példa: esign_server_url=https://proxy-test.microsigner.com/esign/
```

6.1.2.3.6 esign_spname – Kiszolgáló rendszer neve

A kiszolgáló neve, amit a másik fél (Pl.: MicroSigner) aláíró alkalmazása megjelenít.

```
Példa: esign_spname=Microsec Teszt EHSZ
```

6.1.2.3.7 esign_message – üzenet

Aláírói üzenet, amit a másik fél aláíró alkalmazása megjelenít aláírásra való felszólításnál.

```
Példa: esign_message=2018. évi szerződés aláírása
```

6.1.2.3.8 esign_image_format – QR kód képformátuma

A kliens kérheti, hogy ne csak JSON-ban válaszoljon a szerver, hanem QR kódot is adjon vissza. Lehetséges értékek: png, bmp

```
Példa: esign_image_format=png
```

6.1.2.3.9 esign_poll_delay_sec – Két pollozás közti idő

Ezzel az opcióval megadható a lekérési próbálkozások között eltelt idő másodpercben. A pollozások az esign_poll_timeout_sec-ban beállított ideig ismétlődnek.

```
Példa: esign_poll_delay_sec=10
```

6.1.2.3.10 esign_poll_timeout_sec – teljes lekérés időtúllépése

Ezzel az opcióval megadható a teljes lekérés időtúllépése másodpercben. A pollozási próbálkozások ennyi ideig ismétlődhetnek.

```
Példa: esign_poll_timeout_sec=180
```

6.1.2.4 Időbélyeg szerver beállítások

Az e-Szigno időbélyeg szerveren történő autentikációjának beállítása.

6.1.2.4.1 esizigno_timestamp_provider_host – Időbélyeg szolgáltató host

Az időbélyeg előfizetéshez tartozó URL kiszolgálója.

```
Példa: esizigno_timestamp_provider_host=e-szigno.hu
```

6.1.2.4.2 esizigno_timestamp_url_list – Időbélyeg URL-ek

Az időbélyeg előfizetéshez tartozó URL-ek szóközzel elválasztva.

```
Példa: esizigno_timestamp_url_list=https://bteszt.e-szigno.hu/tsa
```

6.1.2.4.3 esizigno_auth_http_username – Időbélyeg hosztra felhasználói név

Az időbélyeg előfizetéshez tartozó felhasználói név. Fontos megjegyezni, hogy bizonyos URL-ekre felhasználói név és jelszó kell, másokra autentikációs tanúsítvány.

```
Példa: esizigno_auth_http_username=teszt
```

6.1.2.4.4 esizigno_auth_http_password – Időbélyeg hosztra jelszó

A felhasználói névhez tartozó jelszó.

Példa: eszigno_auth_http_password=teszt

6.1.2.4.5 eszigno_auth_key – Időbélyeg hoztra autentikációs tanúsítvány

Az autentikációs magánkulcs elérési útvonala. Ez csak akkor kell, ha az időbélyeg URL ezt megköveteli.

Példa: eszigno_auth_key=/msc/opt/eszigno3/product/current/pfx/auth.pfx

6.1.2.4.6 eszigno_auth_key_password – Az autentikáció tanúsítvány jelszava

A jelszó.

Példa: eszigno_auth_key_password=12345

6.1.2.5 Általános aláírási beállítások

Olyan beállítások következnek, melyek általánosan minden aláírásra vonatkoznak.

6.1.2.5.1 eszigno_signer_key_form – aláíró kulcs formátuma

A formátum lehet: pfx, pem, pkcs11, activex, remote

Példa: eszigno_signer_key_form=pfx

6.1.2.5.2 ignore_keyusage – Aláírói kulcshasználat megkövetelése

Hatására (yes) az aláírói tanúsítványban nem követeli meg az aláírói kulcshasználatot a program. Alapértelmezett értéke „no”.

Példa: ignore_keyusage=yes

6.1.2.5.3 ocspl_url_list – e-Szignó dedikált OSCP URL-jei

Először az opcióban megadott URL-eket próbálja használni az OSCP alapú visszavonás-ellenőrzésre, majd csak ez után az AIA kiterjesztésben talált URL-en próbálkozik. A listátát szóközzel kell elválasztani és a leggyakrabban használttal célszerű kezdeni.

Példa: ocspl_url_list=http://rootocsp2009.e-szigno.hu http://a2ca2016-ocsp1.e-szigno.hu
http://www.netlock.hu/ocsp.cgi http://sigkocsp2099.e-szigno.hu http://teszt.e-szigno.hu/tesztroot2008ocsp http://ocsp.kgyhsz.gov.hu/ocsp/

6.1.2.5.4 revocation_checking_mode – Tanúsítvány visszavonási állapot ellenőrzés módja

Amennyiben az ellenőrizendő aláírás már tartalmaz magában csatolt visszavonási információkat, akkor az alkalmazás azok alapján ellenőriz, ha az egyezik a beállított visszavonási móddal. Azaz, ha például az archív aláírás OSCP válaszokat tartalmaz magában, és a visszavonás ellenőrzés is OSCP-re van állítva, akkor a tárolt válasz alapján ellenőriz az alkalmazás. Az archív aláírás ellenőrzése függetlenül ettől a beállítástól kikapcsolható. Az érték lehet: crl, ocsp, ocsp/crl, off.

Példa: revocation_checking_mode=ocsp/crl

6.1.2.5.5 server_cert_validation – Szerver tanúsítvány ellenőrzés

Megadható, hogy SSL kapcsolódás esetén (pl. https címek használatakor) az e-Szignó ellenőrizze a távoli szerver tanúsítványát. Alapértelmezett értéke: true.

Példa: server_cert_validation=true

6.1.2.5.6 validate_ocsp_responder – OSCP válaszadó visszavonási állapot ellenőrzés

Az opció segítségével beállíthatjuk, hogy az e-Szignó ellenőrizze-e az OSCP válaszadó visszavonási állapotát. Alapértelmezett értéke: true.

Példa: validate_ocsp_responder=true

6.1.2.5.7 wait_for_grace_period – Csak megbízható időpont utáni OCSP/CRL-t fogadjon el

Ha ezen opció értéke true, az e-Szignó csak az aláírás (megbízható) időpontja után kibocsátott CRL-eket vagy OCSP válaszokat fogadja el. Alapértelmezett értéke: true. Javasoljuk, hogy OCSP alapú visszavonás-ellenőrzés esetén használja a true beállítást.

Példa: wait_for_grace_period=true

6.1.2.5.8 use_ocsp_cache – e-Szignó OCSP cache

Ezen opció segítségével beállítható, hogy a hálózatról beszerzett OCSP válaszok kerüljenek-e mentésre a munkakönyvtárba. A „yes” beállítás esetén a lementett OCSP válaszokat, ha lehetséges, újrahasznosítja a program. Az alapértelmezett beállítás: no.

VIGYÁZAT: Nem javasoljuk, hogy ezen opciót a -wait_for_grace_period "no" vagy a -validate_ocsp_responder "no" értéke mellett használja, mert az nem releváns visszavonási információk csatolását is eredményezheti. Azt javasoljuk, hogy a use_ocsp_cache opció használata esetén mindkét kapcsolót állítsa "yes" értékre.

Példa: use_ocsp_cache=yes

6.1.2.5.9 xades_type – AdES típus beállítása

Aláíráskor létrehozandó AdES típus, mely érvényes valamennyi aláírás formátumra: XAdES, PAdES és ASiC. Lehetséges értékei: epes, t, a

Példa: xades_type=a

6.1.2.5.10 signer_key – A profilhoz tartozó aláírói magánkulcs

Az aláíró magánkulcsa, az aláírás egy menetben történő létrehozásához szükséges megadni. PFX formátumú kulcsnál az elérési út.

Példa: signer_key=/msc/opt/eszigno3/product/current/pfx/peterke.pfx

6.1.2.5.11 signer_password – Az aláírói magánkulcs jelszava

A jelszó.

Példa: signer_password=12345

6.1.2.6 PDF (PAdES) aláírás

A következőkben a PDF aláírás paramétereit lehet beállítani.

6.1.2.6.1 pdfsig_img_visible – Látható legyen-e az aláírás

Ha true, akkor látható az aláírás. Alapértelmezett értéke false. Ha nem látható az aláírás, akkor az aláírás megjelenésére vonatkozó opcióknak értelemszerűen nincs hatásuk.

Példa: pdfsig_img_visible=true

6.1.2.6.2 pdfsig_adjust – Egymást elfedő aláírások eltolása

A látható aláírások egymást elfedő takarását megakadályozó korrekciónak az engedélyezése, ill. tiltása. Alapértelmezett értéke: true - azaz ha az újonnan létrehozni kívánt aláírás képe eltakarna egy már a dokumentumon szereplő aláírást, akkor az új aláírást automatikusan eltolja úgy, hogy a takarás megszűnjön.

Példa: pdfsig_adjust=true

6.1.2.6.3 pdfsig_align – Látható aláírás igazítása a megadott sarokba

Lehetséges értékei: left-top, right-top, right-bottom, left-bottom.

Példa: pdfsig_align=right-top

6.1.2.6.4 pdfsig_img – Látható aláírás képének útvonala

Látható PDF aláírás létrehozásakor megadható kép fájl elérési útja, amelyet elhelyezhetünk a PDF dokumentum törzsében. A megadott képfájlnak a következő kép formátumok egyikének kell megfelelnie: png, jpg, tif.

```
Példa: pdfsig_img=/msc/srv/eszignoservice/config/server/userimages/sign-logo.png
```

6.1.2.6.5 pdfsig_resize – Új méret[%]

Lehetőségünk van a látható PDF aláírás létrehozásánál a megadott kép átméretezésére. Ha a megadott érték csak számjegyeket tartalmaz, akkor képpontban értelmezett érték, ha viszont az utolsó karaktere: % akkor a dokumentum vonatkozó méretének százalékos értékét jelenti. Például ha a dokumentum szélessége 600 képpont és megadott pdfsig_resize 10%, akkor az új szélesség 60 képpont lesz.

```
Példa: pdfsig_resize=10%
```

6.1.2.6.6 pdfsig_resize_mode – Az átméretezés módja

Átméretezéskor minden esetben arányosan csökkentjük, ill. növeljük a megadott kép függőleges és vízszintes méretét. Tehát az átméretezés után a magasság-szélesség aránya változatlan marad. Így a megadott pdfsig_resize értéket több féle módon értelmezhetjük. Ha a pdfsig_resize_mode értéke: width - A pdfsig_resize-ban megadott érték lesz az új szélessége az átméretezett képnek. height - A pdfsig_resize-ban megadott érték lesz az új magassága az átméretezett képnek. max - Ha a kép magassága nagyobb, mint a szélessége akkor ugyanaz, mint a height, különben a width módot használjuk. Ez az alapértelmezett üzemmód.

```
Példa: pdfsig_resize_mode=height
```

6.1.2.6.7 pdfsig_padding_x – Vízszintes behúzás[%]

Megadhatjuk a látható aláírás vízszintes távolságát a lap szélétől, a pdfsig_resize paraméterezésénél leírt módon, képpontban vagy lapméret százalékban.

```
Példa: pdfsig_padding_x=15%
```

6.1.2.6.8 pdfsig_padding_y – Függőleges behúzás[%]

Megadhatjuk a látható aláírás függőleges távolságát a lap szélétől, a pdfsig_resize paraméterezésénél leírt módon, képpontban vagy lapméret százalékban.

```
Példa: pdfsig_padding_y=17%
```

6.1.2.6.9 pdfsig_page – Az oldal száma

Megadja, hogy a látható PDF aláírást melyik oldalán helyezzük el a dokumentumnak. Alapértelmezett értéke: 1 – amely a dokumentum legelső oldalát jelenti. A dokumentum oldalainak számánál nagyobb érték esetén is az alapértelmezett értéket veszi fel. Ha az értéke - 1, abban az esetben az utolsó oldalt jelenti.

```
Példa: pdfsig_page=1
```

6.1.2.6.10 pdfsig_title_visible – Az aláírás feliratának megjelenítése

Ha az értéke true, akkor megjelenik a felirat a látható aláíráson. Alapértelmezett értéke false. A felirat hosszától függően nem minden esetben helyezhető el esztétikusan és levágás mentesen. A további paraméterek az elhelyezést segítik.

```
Példa: pdfsig_title_visible=true
```

6.1.2.6.11 pdfsig_title_align – Az aláírás felirata

A látható PDF aláíráson opcionálisan elhelyezhető szöveg. Alapértelmezett értéke az aláíró

tanúsítványában szeplő Subject.CN értéke.

Példa: pdfsig_title=Banki Számlakivonat Rendszer

6.1.2.6.12 pdfsig_title_align – A szöveg igazításának módja

A látható PDF aláíráson opcionálisan elhelyezhető szöveg igazításának módja. Ha az értéke top, akkor az aláírás képének bal felső sarkához lesz igazítva, különben a bal alsó az alapértelmezett.

Példa: pdfsig_title_align=bottom

6.1.2.6.13 pdfsig_title_fontsize – A szöveg betűmérete

A megjelenített szöveg betűmérete. Alapértelmezett értéke: 22

Példa: pdfsig_title_fontsize=16

6.1.2.6.14 pdfsig_title_padding_x – Vízszintes margó

A látható aláíráson elhelyezett szöveg, név vízszintes irányú távolsága a látható aláírás képének szélétől. Ha nincs megadva a látható aláírás képe és nincs is tiltva a megjelenítése, akkor ennek a paraméternek nincs hatása.

Példa: pdfsig_title_padding_x=10

6.1.2.6.15 pdfsig_title_padding_y – Függőleges margó

A látható aláíráson elhelyezett szöveg, név függőleges irányú távolsága a látható aláírás képének szélétől. Ha nincs megadva a látható aláírás képe és nincs is tiltva a megjelenítése, akkor ennek a paraméternek nincs hatása.

Példa: pdfsig_title_padding_y=13

6.1.2.7 Tárolt kulcsú aláírás (TKASZ)

6.1.2.7.1 remote_signer_url – TKASZ URL

A tárolt kulcsú aláírás szolgáltató URL elérhetősége

Példa: remote_signer_url=https://tkasz.microsec.com

6.1.2.7.2 remote_signer_user – TKASZ felhasználónév

A tárolt kulcsú aláírás szolgáltónál regisztrált felhasználónév. Ennek a felhasználónak a tanúsítványával fog történni az aláírás. Abban az esetben kell beállítani, ha a szolgáltatóhoz felhasználónév/jelszó alapon történik a kapcsolódás.

Példa: remote_signer_user=test

6.1.2.7.3 remote_signer_pass – TKASZ jelszó

A tárolt kulcsú aláírás szolgáltónál regisztrált felhasználóhoz tartozó jelszó. Abban az esetben kell beállítani, ha a szolgáltatóhoz felhasználónév/jelszó alapon történik a kapcsolódás.

Példa: remote_signer_pass=password1234

6.1.2.7.4 remote_signer_auth_cert – TKASZ autentikációs tanúsítvány

A tárolt kulcsú aláírás szolgáltónál regisztrált felhasználóhoz tartozó autentikációs tanúsítvány elérési útja. Abban az esetben kell beállítani, ha a szolgáltatóhoz tanúsítvány alapon történik a kapcsolódás.

Példa: remote_signer_auth_cert=/msc/certs/auth.pfx

6.1.2.7.5 remote_signer_auth_cert_pass – TKASZ autentikációs tanúsítvány jelszava

A tárolt kulcsú aláírás szolgáltónál regisztrált felhasználóhoz tartozó autentikációs tanúsítványhoz tartozó jelszó. Abban az esetben kell beállítani, ha a szolgáltatóhoz tanúsítvány alapon történik a kapcsolódás.

Példa: remote_signer_auth_cert_pass=certpass1234

6.1.2.7.6 remote_signer_pin – TKASZ felhasználó pin kódja

A tárolt kulcsú aláírás szolgáltatóhoz tartozó pin kód. Ha a szolgáltónál az adott felhasználóhoz a második faktoros autentikáció pin kód, akkor ezt a paramétert ki kell tölteni.

Példa: remote_signer_pin=123456

Példa: esign_profile.properties

```
#####
#####           Technikai felhasználói profilok           #####
#####           (UserProfile)                               #####
#####
# Profilok segítségével lehet többféle aláírást készíteni. Ezek a beállítások
# ritkán változó paraméterek. A profilekat egy könyvtárban kell elhelyezni. A
# könyvtár elérési helyét a microsec.pki.server.userProfilesDir JVM opcióban
# kell megadni.

#####           Átvételi elismervény verziója           #####
#####
# Ezzel az opcióval a létrehozandó átvételi elismervények formátumát lehet
# beállítani. A v1 az e-akta alapú, régi típusú tértivevényt jelenti, a v2 a
# különálló aláírás alapú, egyszerű XAdES tértivevény.
#acknowledgement_version=v1

#####           Titkosítás visszafejtése           #####
#####
# A profil tulajdonosának titkosítva küldött e-Akták visszafejtése a
# tulajdonos magánkulcsával.

#####   A profil tulajdonosának magánkulcsa   #####
# A PFX formátumú kulcs fájl útvonala.
#decryptor_key=/msc/opt/eszigno3/product/current/pfx/enc_peterke.pfx

#####   A visszafejtő magánkulcs jelszava   #####
# A decryptor_key magánkulcs jelszava.
#decryptor_password=12345

#####           Az ESign protokol beállításai           #####
#####
# Az ESign protokol a kétmenetes aláíráshoz szükséges, - Pl.: webböngészőn
# keresztüli kliens oldali aláírás esetében. Ekkor nincs a profilhoz tartozó
# felhasználó magánkulcsa a szerveren.

##### Az ESign szolgáltatás ki-be kapcsolása #####
# Alapértelmezett értéke: false. Abban az esetben, ha be van kapcsolva, akkor
# a következő paramétereket is meg kell adni.
esign_use=true

##### Autentikáció az ESignProxy szerveren #####
# Felhasználói név.
esign_auth_http_username=esignuser

##### Autentikáció az ESignProxy szerveren #####
# Jelszó.
esign_auth_http_password=user

#####           Kérelem aláírás           #####
# A kérelmet alá kell-e írnia a szervernek az ESignProxy-nak küldéskor. Ha az
# opció értéke true, az ESignProxy szervernek PKCS7 aláírással együtt küldi
# fel az aláíratlan hash-t az e-Szignó. Ekkor a userprofile-nak aláírói
# kulccsal kell rendelkeznie. Alapértelmezett értéke: false.
esign_use_pkcs7=false
```

```
##### Az ESignProxy szerver gyökér URL-je. #####
# A gyökér URL, melynek a végéhez automatikusan illeszti a rendszer a
# szolgáltatások relatív URL-jét.
esign_server_url=https://proxy-test.microsigner.com/esign/

##### Kiszolgáló rendszer neve #####
# A kiszolgáló neve, amit a másik fél (Pl.: MicroSigner) aláíró alkalmazása
# megjelenít.
esign_spname=e-Szignó Hitelesítő Szerver

##### Az üzenet #####
# Aláírói üzenet, amit a másik fél aláíró alkalmazása megjelenít aláírásra
# való felszólításnál.
esign_message= e-Szignó Hitelesítő Szerver Client Test

##### A QR kód képformátuma #####
# A kliens kérheti, hogy ne csak JSON-ban válaszoljon a szerver, hanem QR
# kódot is adjon vissza. Lehetséges értékek: png, bmp
#esign_image_format=png

##### Két pollozás közti idő #####
# Ezzel az opcióval megadható a lekérési próbálkozások között eltelt idő
# másodpercben. A pollozások a esign_poll_timeout_sec-ban beállított ideig
# ismétlődnek.
esign_poll_delay_sec=10

##### A teljes lekérés időtúllépése #####
# Ezzel az opcióval megadható a teljes lekérés időtúllépése másodpercben. A
# pollozási próbálkozások ennyi ideig ismétlődhetnek.
esign_poll_timeout_sec=300

##### Időbélyeg szerver beállítások #####
#####
# Az e-Szignó időbélyeg szerveren történő autentikációjának beállítása.

##### Időbélyeg szolgáltató host #####
# Az időbélyeg előfizetéshez tartozó URL kiszolgálója.
esizigno timestamp provider host=e-szigno.hu

##### Időbélyeg URL-ek #####
# Az időbélyeg előfizetéshez tartozó URL-ek szóközzel elválasztva.
esizigno_timestamp_url_list=https://bteszt.e-szigno.hu/tsa

##### Időbélyeg hosztra felhasználói név #####
# Az időbélyeg előfizetéshez tartozó felhasználói név. Fontos megjegyezni,
# hogy bizonyos URL-ekre felhasználói név és jelszó kell, másokra
# autentikációs tanúsítvány.
esizigno_auth_http_username=teszt

##### Időbélyeg hosztra jelszó #####
# A felhasználói névhez tartozó jelszó.
esizigno_auth_http_password=teszt

##### Időbélyeg hosztra autentikációs #####
#####
# Az autentikációs magánkulcs elérési útvonala. Ez csak akkor kell, ha az
# időbélyeg URL ezt megköveteli.
#esizigno_auth_key=/msc/opt/esizigno3/product/current/pfx/auth.pfx

##### Az autentikáció tanúsítvány jelszava #####
# A jelszó.
#esizigno_auth_key_password=12345

##### Általános aláírási beállítások #####
#####
# Olyan beállítások következnek, melyek általánosan minden aláírásra
# vonatkoznak.

##### Az aláíró kulcs formátuma #####
# A formátum lehet: pfx, pem, pkcs11, activex
esizigno_signer_key_form=pfx

##### Az e-Szignó dedikált OCSP URL-jei #####
```

```
# Először az opcióban megadott URL-eket próbálja használni az OCSP alapú
# visszavonás-ellenőrzésre, majd csak ez után az AIA kiterjesztésben talált
# URL-en próbálkozik. A listátát szóközzel kell elválasztani és a
# leggyakrabban használttal célszerű kezdeni.
ocsp_url_list=http://rootocsp2009.e-szigno.hu http://teszt.e-szigno.hu/testroot2008ocsp

##### Tanúsítvány visszavonási állapot #####
##### ellenőrzés módja #####
# Amennyiben az ellenőrizendő aláírás már tartalmaz magában csatolt
# visszavonási információkat, akkor az alkalmazás azok alapján ellenőriz, ha
# az egyezik a beállított visszavonási móddal. Azaz, ha például az archív
# aláírás OCSP válaszokat tartalmaz magában, és a visszavonás ellenőrzés is
# OCSP-re van állítva, akkor a tárolt válasz alapján ellenőriz az alkalmazás.
# Az archív aláírás ellenőrzése függetlenül ettől a beállítástól
# kikapcsolható.
# Az érték lehet: crl, ocsp, ocsp/crl, off.
revocation_checking_mode=ocsp

##### Szerver tanúsítvány ellenőrzés #####
# Megadható, hogy SSL kapcsolódás esetén (pl. https címek használatakor) az
# e-Szignó ellenőrizze a távoli szerver tanúsítványát. Alapértelmezett értéke:
# true.
#server cert validation=true

##### OCSP válaszadó visszavonási állapot #####
##### ellenőrzés #####
# Az opció segítségével beállíthatjuk, hogy az e-Szignó ellenőrizze-e az OCSP
# válaszadó visszavonási állapotát. Alapértelmezett értéke: true.
#validate ocsp responder=true

##### Csak megbízható időpont utáni #####
##### OCSP/CRL-t fogadjon el #####
# Ha ezen opció értéke true, az e-Szignó csak az aláírás (megbízható)
# időpontja után kibocsátott CRL-eket vagy OCSP válaszokat fogadja el.
# Alapértelmezett értéke: true. Javasoljuk, hogy OCSP alapú
# visszavonás-ellenőrzés esetén használja a true beállítást.
wait_for_grace_period=yes

##### AdES típus beállítása #####
# Aláíráskor létrehozandó AdES típus, mely érvényes valamennyi aláírás
# formátumra: XAdES, PAdES és ASiC. Lehetséges értékei: epes, t, a
xades_type=a

##### A profilhoz tartozó aláírói magánkulcs #####
# Az aláíró magánkulcsa, az aláírás egy menetben történő létrehozásához
# szükséges megadni. PFX formátumú kulcsnál az elérési út.
signer_key=msc/opt/eszigno3/product/current/pfx/peterke.pfx

##### Az aláírói magánkulcs jelszava #####
# A jelszó.
signer_password=12345

##### PDF (PAdES) aláírás #####
#####
# A következőkben a PDF aláírás paramétereit lehet beállítani.

##### Látható legyen-e az aláírás #####
# Ha true, akkor látható az aláírás. Alapértelmezett értéke false. Ha nem
# látható az aláírás, akkor az aláírás megjelenésére vonatkozó opcióknak
# értelemszerűen nincs hatásuk.
#pdfsig_img_visible=true

##### Egymást elfedő aláírások eltolása #####
# A látható aláírások egymást elfedő takarását megakadályozó korrekciónak az
# engedélyezése, ill. tiltása. Alapértelmezett értéke: true - azaz ha az
# újonnan létrehozni kívánt aláírás képe eltakarna egy már a dokumentumon
# szereplő aláírást, akkor az új aláírást automatikusan eltolja úgy, hogy a
# takarás megszűnjön.
#pdfsig_adjust=true

##### Látható aláírás igazítása a megadott #####
##### sarokba #####
# Lehetséges értékei: left-top, right-top, right-bottom, left-bottom.
#pdfsig_align=right-top
```

```
##### Látható aláírás képének útvonala #####
# Látható PDF aláírás létrehozásakor megadható kép fájl elérési útja, amelyet
# elhelyezhetünk a PDF dokumentum törzsében. A megadott képfájlnak a következő
# kép formátumok egyikének kell megfelelnie: png, jpg, tif.
#pdfsig_img=/msc/srv/eszignoservice/config/server/userimages/sign-logo.png

##### Új méret[%] #####
# Lehetőségünk van a látható PDF aláírás létrehozásánál a megadott kép
# átméretezésére. Ha a megadott érték csak számjegyeket tartalmaz, akkor
# képpontban értelmezett érték, ha viszont az utolsó karaktere: % akkor a
# dokumentum vonatkozó méretének százalékos értékét jelenti. Például ha a
# dokumentum szélessége 600 képpont és megadott pdfsig_resize 10%, akkor az új
# szélesség 60 képpont lesz.
#pdfsig_resize=10%

##### Az átméretezés módja #####
# Átméretezéskor minden esetben arányosan csökkentjük, ill. növeljük a
# megadott kép függőleges és vízszintes méretét. Tehát az átméretezés után a
# magasság-szélesség aránya változatlan marad. Így a megadott pdfsig_resize
# értéket többféle módon értelmezhetjük. Ha a pdfsig_resize_mode értéke:
# width - A pdfsig_resize-ban megadott érték lesz az új szélessége az
# átméretezett képnek.
# height - A pdfsig_resize-ban megadott érték lesz az új magassága az
# átméretezett képnek.
# max - Ha a kép magassága nagyobb, mint a szélessége akkor ugyanaz, mint a
# height, különben a width módot használjuk. Ez az alapértelmezett üzemmód.
#pdfsig_resize_mode=height

##### Vízszintes behúzás[%] #####
# Megadhatjuk a látható aláírás vízszintes távolságát a lap szélétől, a
# pdfsig_resize paraméterezésénél leírt módon, képpontban vagy lapméret
# százalékban.
#pdfsig_padding_x=15%

##### Függőleges behúzás[%] #####
# Megadhatjuk a látható aláírás függőleges távolságát a lap szélétől, a
# pdfsig_resize paraméterezésénél leírt módon, képpontban vagy lapméret
# százalékban.
#pdfsig_padding_y=17%

##### Az oldal száma #####
# Megadja, hogy a látható PDF aláírást melyik oldalán helyezzük el a
# dokumentumnak. Alapértelmezett értéke: 1 - amely a dokumentum legelső
# oldalát jelenti. A dokumentum oldalainak számánál nagyobb érték esetén is az
# alapértelmezett értéket veszi fel. Ha az értéke -1, abban az esetben az
# utolsó oldalt jelenti.
#pdfsig_page=1

##### Az aláírás feliratának megjelenítése #####
# Ha az értéke true, akkor megjelenik a felirat a látható aláíráson.
# Alapértelmezett értéke false. A felirat hosszától függően nem minden esetben
# helyezhető el esztétikusan és levágás mentesen. A további paraméterek az
# elhelyezést segítik.
#pdfsig_title_visible=true

##### Az aláírás felirata #####
# A látható PDF aláíráson opcionálisan elhelyezhető szöveg. Alapértelmezett
# értéke az aláíró tanúsítványában szereplő Subject.CN értéke.
#pdfsig_title=Banki Számlakivonat Rendszer

##### A szöveg igazításának módja #####
# A látható PDF aláíráson opcionálisan elhelyezhető szöveg igazításának módja.
# Ha az értéke top, akkor az aláírás képének bal felső sarkához lesz igazítva,
# különben a bal alsó az alapértelmezett.
#pdfsig_title_align=bottom

##### A szöveg betűmérete #####
# A megjelenített szöveg betűmérete. Alapértelmezett értéke: 22
#pdfsig_title_fontsize=16

##### Vízszintes margó #####
# A látható aláíráson elhelyezett szöveg, név vízszintes irányú távolsága a
# látható aláírás képének szélétől. Ha nincs megadva a látható aláírás képe és
# nincs is tiltva a megjelenítése, akkor ennek a paraméternek nincs hatása.
#pdfsig_title_padding_x=10
```



```
#####          Függőleges margó          #####
# A látható aláíráson elhelyezett szöveg, név függőleges irányú távolsága a
# látható aláírás képének szélétől. Ha nincs megadva a látható aláírás képe és
# nincs is tiltva a megjelenítése, akkor ennek a paraméternek nincs hatása.
#pdfsig_title_padding_y=13
```

6.2 Monitorozó rendszer konfiguráció

A monitorozó rendszer kétfajta szerverrel tudja tartani a kapcsolatot, ezek az EHSZ és az EHSZ Specifikált Kliensei. Ezeket a megfelelő webes interfészen keresztül tudja elérni a monitorozó rendszer.

6.2.1 A monitorozó rendszer tulajdonságai (MonitorProperties)

A monitorozó rendszer konfigurációs állományának helyét a `microsec.pki.monitor.propertyFile` JVM opcióban kell megadni.

6.2.1.1 Az EHSZ Kliensek URL-jei

A szerverhez tartozó monitorozandó specifikált kliensek URL-jeinek megadása. A paramétereket sorszámozni kell. A paraméter megadása nem kötelező.

```
Példa:          pki_client0_url=http://127.0.0.1:8080/microsec-pki-service-client-bank-
web/pkiclientfolderworker
```

6.2.1.2 Az EHSZ URL-je

A monitorozandó Hitelestő Szerever URL-je.

```
Példa: pki_server_url=http://127.0.0.1:8080/microsec-pki-service-server-web/PKIServlet
```

6.2.1.3 Az adatbázi elérés

Az Alkalmazás Szerverben beállított JDBC resource neve. Az EHSZ Kliens és Szerver logokat tartalmazó adatbázis elérhetősége.

```
Példa: db_resource_jndi_name=java:/comp/env/jdbc/signer
```

6.2.1.4 Értesítési beállítások

Az email értesítések beállításai.

6.2.1.4.1 Címzettek

A rendszer által küldött e-mail üzenetek címzettjei. A rendszer akkor is elindul, ha nincs megadva, de az e-mail értesítések funkció ki lesz kapcsolva. Az email címeket ; -vel kell elválasztani.

```
Példa: notification_email_recipients=admin@bank.hu;security@bank.hu
```

6.2.1.4.2 A feladó

A rendszer által küldött e-mail üzenetek feladója. Ha nincs megadva, akkor `pki_service_monitor@microsec.hu`.

```
Példa: notification_email_sender=pki_service_monitor@bank.hu
```

6.2.1.4.3 Értesítés tanúsítvány lejáratáról

A tanúsítványok lejáratáról ennyi nappal a lejárat előtt értesít. Ha nincs megadva, akkor 0, tehát csak a lejárat napján értesít.

```
Példa: notification_cert_days_till_expiration=30
```

6.2.1.4.4 Tanúsítvány lejárat ellenőrzése

A tanúsítványok lejáratát minden nap ebben az időpontban ellenőrzi. Ha nincs megadva, akkor 10:00:00

Példa: notification_cert_start_time=10:00:00

6.2.1.5 A Java Mail API beállításai

A konfigurációs fájl tartalmazhat a Java mail api-nak szóló beállításokat. Ilyenek például:

6.2.1.5.1 SMTP host

Az smtp szerver címe. Ha nincs megadva, akkor az e-mail értesítések funkció ki lesz kapcsolva.

Példa: mail.smtp.host=teszt.smtp.hu

6.2.1.5.2 SMTP port

Az smtp szerver portja. Ha nincs megadva, akkor 25

Példa: mail.smtp.port=25

6.2.1.6 Minta konfigurációs fájl

Példa: monitor.properties

```
#####
#####          A monitorozó rendszer tulajdonságai          #####
#####          (MonitorProperties)          #####
#####
# A monitorozó rendszer konfigurációs állományának helyét a
# microsec.pki.monitor.propertyFile JVM opcióban kell megadni.

#####          Az EHSZ Kliensek URL-jei          #####
#####
# A szerverhez tartozó monitorozandó specifikált kliensek URL-jeinek megadása.
# A paramétereket sorszámozni kell. A paraméter megadása nem kötelező.
#pki_client0_url=http://127.0.0.1:8080/microsec-pki-service-client-bank-web/pkiclientfolderworker

#####          Az EHSZ URL-je          #####
#####
# A monitorozandó Hitelestő Szerever URL-je.
pki_server_url=http://pkiserver/microsec-pki-service-server-web/PKIServlet

#####          Az adatbázi elérés          #####
#####
# Az Alkalmazás Szerverben beállított JDBC resource neve. Az EHSZ
# Kliens és Szerver logokat tartalmazó adatbázis elérhetősége.
db_resource_jndi_name=java:/comp/env/jdbc/signer

#####          Értesítési beállítások          #####
#####
# Az email értesítések beállításai.

#####          Címzettek          #####
# A rendszer által küldött e-mail üzenetek címzettjei. A rendszer akkor is
# elindul, ha nincs megadva, de az e-mail értesítések funkció ki lesz
# kapcsolva. Az email címeket ;-vel kell elválasztani.
notification_email_recipients=tesztelo.peterke@microsec.hu

#####          A feladó          #####
# A rendszer által küldött e-mail üzenetek feladója. Ha nincs megadva, akkor
# pki_service_monitor@microsec.hu.
notification_email_sender=pki_monitor.teszt@microsec.hu

#####          Értesítés tanúsítvány lejáratáról          #####
# A tanúsítványok lejáratáról ennyi nappal a lejárat előtt értesít. Ha nincs
# megadva, akkor 0, tehát csak a lejárat napján értesít.
notification_cert_days_till_expiration=30

#####          Tanúsítvány lejárat ellenőrzése          #####
```

```
# A tanúsítványok lejáratát minden nap ebben az időpontban ellenőrzi. Ha nincs  
# megadva, akkor 10:00:00  
notification_cert_start_time=10:30:00
```

```
##### A Java Mail API beállításai #####  
#####  
# A konfigurációs fájl tartalmazhat a Java mail api-nak szóló beállításokat.  
# Ilyenek például:
```

```
##### SMTP host #####  
# Az smtp szerver címe. Ha nincs megadva, akkor az e-mail értesítések funkció  
# ki lesz kapcsolva.  
mail.smtp.host=teszt.smtp.hu
```

```
##### SMTP port #####  
# Az smtp szerver portja. Ha nincs megadva, akkor 25  
mail.smtp.port=25
```

6.3 Adatbázis beállítás Apache Tomcat esetében

Az Apache Tomcat lib könyvtárába be kell másolni a megfelelő JDBC fájlt. PostgreSQL esetében a Pl.: postgresql-42.2.18.jar-t.

6.3.1 context.xml

context.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Context>
  <WatchedResource>WEB-INF/web.xml</WatchedResource>
  <WatchedResource>WEB-INF/tomcat-web.xml</WatchedResource>
  <WatchedResource>${catalina.base}/conf/web.xml</WatchedResource>
  <Resource
    name="jdbc/signer"
    auth="Container"
    type="javax.sql.DataSource"
    driverClassName="org.postgresql.Driver"
    url="jdbc:postgresql://127.0.0.1:5432/signer"
    username="signer" password="signer" maxTotal="20" maxIdle="10" maxWaitMillis="-1"/>
</Context>
```

6.3.2 microsec-pki-service-server-web.war-ban levő web.xml fájl

web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app version="3.0" xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd">
  <resource-ref>
    <description>Signer Datasource</description>
    <res-ref-name>jdbc/signer</res-ref-name>
    <res-type>javax.sql.DataSource</res-type>
    <res-auth>Container</res-auth>
  </resource-ref>
  <filter>
    <filter-name>ClickjackFilterSameOrigin</filter-name>
    <filter-class>hu.microsec.pki.service.api.common.ClickjackFilter</filter-class>
    <init-param>
      <param-name>mode</param-name>
      <param-value>SAMEORIGIN</param-value>
    </init-param>
  </filter>
  <filter>
    <filter-name>ClickjackFilterDeny</filter-name>
    <filter-class>hu.microsec.pki.service.api.common.ClickjackFilter</filter-class>
    <init-param>
      <param-name>mode</param-name>
      <param-value>DENY</param-value>
    </init-param>
  </filter>
  <!-- use the SameOrigin version to allow your application to frame, but nobody else -->
  <filter-mapping>
    <filter-name>ClickjackFilterSameOrigin</filter-name>
    <url-pattern>*/</url-pattern>
  </filter-mapping>
  <!-- use the Deny version to prevent anyone, including yourself, from framing the page -->
  <!--filter-mapping>
    <filter-name>ClickjackFilterDeny</filter-name>
    <url-pattern>*/</url-pattern>
  </filter-mapping-->
  <servlet>
    <servlet-name>PKIServlet</servlet-name>
    <servlet-class>hu.microsec.pki.service.server.http.PKIServlet</servlet-class>
    <load-on-startup>1</load-on-startup>
    <multipart-config>
      <!--max-file-size>20848820</max-file-size>
      <max-request-size>418018841</max-request-size-->
      <file-size-threshold>1048576</file-size-threshold>
```

```

    </multipart-config>
</servlet>
<servlet-mapping>
  <servlet-name>PKIServlet</servlet-name>
  <url-pattern>/PKIServlet/*</url-pattern>
</servlet-mapping>
<error-page>
  <location>
    /error.jsp
  </location>
</error-page>
<session-config>
  <session-timeout>
    30
  </session-timeout>
</session-config>

<!--login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>esznoservice-realm</realm-name>
</login-config>
<security-constraint>
  <display-name>ESZIGNO-SERVICE</display-name>
  <web-resource-collection>
    <web-resource-name>esznoservice</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>esznoservice-role</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
<security-role>
  <description>Csak a szerepkörben levők küldhetnek adatot.</description>
  <role-name>esznoservice-role</role-name>
</security-role-->
</web-app>

```

7 Hibakezelés

A Hitelestő Szerver HTTP státusz kódokkal tudatja a klienssel a hiba tényét. MQ esetében pedig maga a szerver kommunikál az MQ-val.

7.1 Hibakezelés REST-es felület esetén

7.1.1 Hibakódok

Kód	Leírás
200	Minden rendben.
202	Szerver hiba. A folyamat még nem fejeződött be, próbálkozzon a kliens később.
470	Szerver hiba. Az e-Szignó külső vagy belső rendszerhibát jelzett.
471	Dokumentum hiba.
400-499, kivétel 470, 471	Kliens hiba.
500-599	Szerver hiba.

7.1.2 A kliensek számára ajánlott hibakazelés

7.1.2.1 Minden rendben

A kliensnek a szokásos normál folyamaton kell végigmennie és az elkészült és visszakapott dokumentumot a specifikált módon átadnia a Megrendelő belső core rendszerei számára.

7.1.2.2 Dokumentum hiba

Ebben az esetben a kliensnek el kell mentenie a dokumentumot egy kivételeket tartalmazó könyvtárba további szakértői vizsgálat céljából. Ezt a dokumentumot nem szabad újraküldenie.

7.1.2.3 Kliens hiba

A kliens hibájából hiúsul meg a művelet a szerver oldalon. Tipikusan hibásak a szervernek átadott adatok, Pl.: nem létező profilra hivatkozik a kliens. Ekkor a klienst le kell állítani és elhárítani a hibát.

7.1.2.4 Szerver hiba

Szerver hibát akkor dob a rendszer, ha maga a szerver hibásan működik, vagy külső szolgáltatók nem érhetőek el. A kliensnek ekkor át kell kapcsolni várakozásra, majd a specifikált idő elteltével újra kell próbálkoznia.

7.2 Hibakezelés MQ felület esetén

Az MQ felület RuntimeExceptionot dob hiba esetében és naplóban rögzíti a hiba tényét és a tranzakciót visszavonja (rollback).

8 Naplózás

A rendszerek kétféle naplózást használnak: műszaki és dokumentum-auditnaplózás. A műszaki csak fájl alapú, míg az audit napló lehet fájl, vagy adatbázis alapú naplózás.

8.1 Műszaki naplózás

A rendszer működési folyamatainak idő- és térbeli követésére és a hibák pontos feltérképezésére való. A naplók alapján az üzemeltetőknek esélyük van a hibák okainak kiderítésére, a szoftverfejlesztőknek pedig a forráskódokban a hibás működést előidéző-, vagy nem megfelelően kezelő részek beazonosítására és kijavítására.

8.1.1 Naplózási szintek

A naplózási szintek a naplózott adatok tartamát és részletességét befolyásolják. Teszteletlen rendszernél a legrészletesebb naplózás szükséges, míg üzemszerű működésnél elegendő a hibák okainak kiírása.

8.1.1.1 DEBUG szint

Lépésről lépésre nyomon követi a folyamatokat. Minden egyes lépésről érdemi információkat ír ki. Azaz mely dokumentumnak, mikor és hol kezdte meg a feldolgozását, ez milyen lépéseken keresztül zajlott le, és mi lett a végeredmény.

8.1.1.2 INFO szint

A rendszeren áthaladó dokumentumok feldolgozásainak mérföldköveit írja ki. Ezek általában tartalmazzák a könyvtár és a dokumentum nevét és a feldolgozás sikerességét.

8.1.1.3 WARNING szint

Rendellenes működésre vagy dokumentumra utaló jelek esetén használjuk, amikor éppen a rendszer helyes működése miatt derül fény egy rendellenességre. Pl.: üres bemenő könyvtárat kellene feldolgozni, vagy dokumentumot ellenőrzésre kapott a rendszer és ezen ez elbukott. Tehát a megkezdett folyamat végigvihető csak rendellenesnek ítélt végeredménnyel zárult le.

8.1.1.4 ERROR szint

Amennyiben egyértelműen hiba következett be a rendszer működésében és a megkezdett feldolgozási ágon a folyamat nem folytatható tovább.

8.1.2 log4j.properties

log4j.properties

```
log4j.appender.LOGFILE.layout.ConversionPattern=[%-5p] %d [%t] %l %x - %m%n
log4j.logger.hu.microsec=DEBUG, LOGFILE
log4j.appender.LOGFILE.Append=true
log4j.rootLogger=INFO, LOGFILE
log4j.appender.LOGFILE.DatePattern='-'yyyy-MM-dd'.log'
log4j.appender.LOGFILE.layout=org.apache.log4j.PatternLayout
log4j.additivity.hu.microsec=false
log4j.appender.LOGFILE=org.apache.log4j.DailyRollingFileAppender
log4j.appender.LOGFILE.File=./base/logs/websevice
```

8.1.3 log4j-monitor.properties

log4j-monitor.properties

```
log4j.appender.LOGFILE.layout.ConversionPattern=[%-5p] %d [%t] %l %x - %m%n
log4j.logger.hu.microsec=DEBUG, LOGFILE
log4j.appender.LOGFILE.Append=true
log4j.rootLogger=INFO, LOGFILE
log4j.appender.LOGFILE.DatePattern='-'yyyy-MM-dd'.log'
log4j.appender.LOGFILE.layout=org.apache.log4j.PatternLayout
log4j.additivity.hu.microsec=false
log4j.appender.LOGFILE=org.apache.log4j.DailyRollingFileAppender
log4j.appender.LOGFILE.File=./base/logs/websevice-monitor
```

8.2 Auditnaplózás

A feldolgozási folyamatban résztvevő dokumentumokról és könyvtárakról ad egyértelműen pozitív vagy negatív feldolgozási státuszt egyetlen egyszer. A naplózott adatokból egyértelműen beazonosítható a dokumentum vagy könyvtár, helye, profilja, prioritása, időpontja és státusza.

Ebből a naplóból deríthető ki legkönnyebben, hogy egy dokumentum vagy könyvtár feldolgozása el sem volt kezdhető, vagy nem volt továbbküldhető vagy sikeres volt.

Az audit napló alapértelmezésben fájl alapú és a műszaki naplóba íródik a feldolgozási lépések közé INFO szinten. Konfigurációs fájlban azonban előírható az adatbázis alapú naplózás, ekkor megszűnik a fájl alapú kiírás. Az adatbázisba naplózásnál nincs lehetőség naplózási szintet állítani, azaz minden esetben a pozitív vagy negatív besorolás kiírásra kerül.

Az adatbázis alapú naplót a PKI Monitorozó rendszerrel lehet legkönnyebben kezelni.

9 A PKI rendszer működéséhez szükséges URL-ek a tűzfal konfigurációs beállításokhoz

9.1.1 Időbélyegzés

<https://btsa.e-szigno.hu/>*

9.1.2 Tanúsítványok

<http://www.e-szigno.hu/>*

<http://www.netlock.hu/index.cgi>

<http://nqca.mavinformatika.hu/cer/>*

<http://qca.mavinformatika.hu/cer/>*

<http://hiteles.mavinformatika.hu/cer/>*

9.1.3 OCSP kérés

<http://rootocsp2009.e-szigno.hu>

<http://qocsp2009.e-szigno.hu>

<http://a3ocsp2009.e-szigno.hu>

<http://a2ocsp2009.e-szigno.hu>

<http://sslocsp.e-szigno.hu>

<http://www.netlock.hu/ocsp.cgi>

9.1.4 CRL letöltés

http://crl.e-szigno.hu/*

http://www.e-szigno.hu/*

<http://www.netlock.hu/index.cgi>

http://trust-sign.mavinformatika.hu/CA/*

http://qca.mavinformatika.hu/crl/*

http://nqca.mavinformatika.hu/crl/*

http://www.trust-sign.hu/CA/*

9.1.5 Teszt időbélyegzés

https://bteszt.e-szigno.hu/*

9.1.6 Teszt tanúsítványok

https://srv.e-szigno.hu/*

9.1.7 Teszt OCSP kérés

http://teszt.e-szigno.hu/*

http://bteszt.e-szigno.hu/*

9.1.8 Teszt CRL letöltés:

http://teszt.e-szigno.hu/*

http://bteszt.e-szigno.hu/*

http://tesztca.mavinformatika.hu/crl/*

9.1.9 IP címek

Ezek változhatnak.

a2ocsp2009.e-szigno.hu	193.42.222.125
a3ocsp2009.e-szigno.hu	193.42.222.125
bteszt.e-szigno.hu	193.42.222.29
btsa.e-szigno.hu	193.42.222.109
crl.e-szigno.hu	193.42.222.125
hiteles.mavinformatika.hu	193.68.41.238
nqca.mavinformatika.hu	193.68.41.42

qca.mavinformatika.hu	193.68.41.50
qocsp2009.e-szigno.hu	193.42.222.125
rootocsp2009.e-szigno.hu	193.42.222.125
srv.e-szigno.hu	193.42.222.22
ssllocsp.e-szigno.hu	193.42.222.125
teszt.e-szigno.hu	193.42.222.26
tesztca.mavinformatika.hu	193.68.41.62
trust-sign.mavinformatika.hu	193.68.41.42
www.e-szigno.hu	193.42.222.99
www.netlock.hu	194.149.14.22
www.trust-sign.hu	193.68.41.143