MicroCA

Tanúsítványkibocsátó és tanúsítvány életciklus menedzsment (CA) rendszer

A MicroCA egy webalapú, platform és böngésző független X.509 tanúsítványkibocsátó és tanúsítvány életciklus menedzsment rendszer, mellyel teljes körű CA funkcionalitás valósítható meg. A MicroCA képes tanúsítványok kibocsátására, valamint támogatja a tanúsítvány állapot megváltoztatására irányuló összes műveletet (felfüggesztés, visszaállítás, visszavonás, megújítás). A tanúsítványok aktuális állapotáról (érvényes, felfüggesztett, visszavont, lejárt) visszavonási listák (CRL) és online tanúsítvány-állapot válaszok (OCSP) szolgáltatásával nyújt információt.

A rendszer fő funkciói:

- Tanúsítvány menedzsment
    - X.509 szabványnak megfelelő tanúsítvány kibocsátás tanúsítvány kérelem (PKCS#10, SPKAC), illetve korábbi X.509-es tanúsítvány alapján. A tanúsítványokba kerülő DN adatok tetszőlegesen konfigurálhatóak.
    - A tanúsítványba kerülő kiterjesztések tanúsítvány profilok segítségével adhatóak meg. A szerkeszthető tanúsítvány profilok bármilyen kiterjesztés definiálására alkalmasak, tetszőleges ASN1 struktúra hozható velük létre.
    - Tanúsítványok érvényességének megadása többféleképpen:
        - Alapértelmezett érvényességi idő tanúsítvány profil alapján.

        - Tetszőleges érvényességi idő megadása, profilban szereplő érvényességi tartományon belül.
        - Jövőbeli érvényesség megadása
        - Rövidlejáratú tanúsítvány érvényességi (akár 10 perc) megadása RFC 6960 OCSP szabványnak megfelelő OCSP Responder tanúsítványok kibocsátásához.
    - Webszerver tanúsítvány kibocsátás:
        - EV tanúsítvány profilok támogatása
        - PSD2-es minősített webszerver és bélyegző tanúsítványok kibocsátása
        - Google Transparency logszerverek támogatása
        - CAA rekord alapú domain ellenőrzés
        - IANA lista alapján engedélyezett fődomének ellenőrzése
        - Ékezetes domain-ek támogatása (Punycode)
    - EIDAS szerinti minősített (webszerver, aláírói, bélyegző, időbélyegző) tanúsítványok kibocsátásának támogatása
    - Kulcsminőség ellenőrzés: gyenge kulcsok kiszűrése, kulcsok egyediségének ellenőrzése.
    - Egyedi azonosító a tanúsítványokban (Permanent Identifier - RFC 4043
    - Tanúsítványok külső nyilvános LDAP (OpenLDAP) adatbázisba (publikus tanúsítványtár). A publikálás tanúsítványonként megadható.
    - SCEP (Simple Certificate Enrollment Protocoll) támogatása

- CA szolgáltatói kulcsok kezelése

    - Multi CA működés, azaz egy CA alkalmazáson belül több CA szolgáltatói kulcs kezelése, a szolgáltatói kulcsok típusa külön megadható.
    - Támogatott szolgáltatói kulcstípusok:
        - RSA, használható kulcsméret: 2048, 3072, 4096 bit

        - EC: (secp112r2 secp128r1 secp128r2 secp160k1 secp160r1 secp160r2 secp192k1 secp224k1 secp224r1 secp256k1 secp384r1 secp521r1 prime192v1 prime192v2 prime192v3 prime239v1 prime239v2 prime239v3 prime256v1 sect113r1 sect113r2 sect131r1 sect131r2 sect163k1 sect163r1 sect163r2 sect193r1 sect193r2 sect233k1 sect233r1 sect239k1 sect283k1 sect283r1 sect409k1 sect409r1 sect571k1 sect571r1 c2pnb163v1 c2pnb163v2 c2pnb163v3 c2pnb176v1 c2tnb191v1 c2tnb191v2 c2tnb191v3 c2pnb208w1 c2tnb239v1 c2tnb239v2 c2tnb239v3 c2pnb272w1 c2pnb304w1 c2tnb359v1 c2pnb368w1 c2tnb431r1 brainpoolP160r1 brainpoolP160t1 brainpoolP192r1 brainpoolP192t1 brainpoolP224r1 brainpoolP224t1 brainpoolP256r1 brainpoolP256t1 brainpoolP320r1 brainpoolP320t1 brainpoolP384r1 brainpoolP384t1 brainpoolP512r1 brainpoolP512t1)
    - Az aláírásokban használt lenyomatképző algoritmusok: SHA256, SHA384, SHA512
    - Szolgáltatói kulcsok védelme:

        - szoftveres
        - hardveres: **H**ardware **S**ecurity **M**odule (nCipher, Thales Luna, Utimaco). Operátori kártyákkal védett kulcsok K of N policy szerint.
        - PKCS11
    - Több szintű tanúsítvány hierarchia kialakítása (offline Root, Sub CA)

- Visszavonási szolgáltatások
    - Tanúsítványok felfüggesztés, visszaállítás, visszavonása.
    - Tanúsítvány állapot változás esetén automatikus visszavonási lista generálás késleltetett módon kizárólag az érintett tanúsítványkiadó egység esetén.
    - Időzített visszavonási lista generálás
    - Lejárt tanúsítványok megtartása/levétele a visszavonási listákról
    - ExpiredCertsOnCRL kiterjesztés támogatása visszavonási listák esetén
    - OCSP támogatása (RFC 6960)
    - CRL támogatása (RFC 5280), deltaCRL nem támogatott.
    - CRL kiszinkronizálás külső publikus kiszolgálóra, nincsen az internet irányából a MicroCA felé közvetlen kapcsolat, így gyakorlatilag az internetről való teljes leválasztás támogatott.

- Autentikáció és jogosultságkezelés:
    - Bejelentkezés X.509-es autentikációs tanúsítvánnyal (EC, RSA). Bejelentkezéskor tanúsítvány visszavonás ellenőrzés, továbbá jogosultság ellenőrzés
    - Dual control a tanúsítványok kibocsátásakor, csak megfelelő jogosultsággal engedélyezett a tanúsítvány kibocsátás.

- Naplózás: elektronikusan aláírt és időbélyegzett (RFC 3161) XML naplóállományok (audit log)

  Redundancia biztosítása, HA működés, aktív és passzív node, operátori kártyával védett szolgáltatói kulcsok esetén is.
- Interfészek:
    - webes felhasználói (RA, Admin) felület
    - REST API
    - Parancssori vezérlési lehetőség

Támogatott platformok:

- OS: Linux (preferált: Oracle Linux, Red Hat, CentOS)
- Adatbázis támogatás: MySQL, MariaDB, PostgreSQL, Oracle
- Webszerver: Apache 2.4.x

MicroRA

Regisztrációs és ügyfélnyilvántartó szoftver CA rendszerekhez

A MicroRA egy webalapú, platform és böngésző független ügyviteli rendszer, amely a hitelesítés szolgáltatáshoz kapcsolódó folyamatok támogatására hivatott.

A rendszer fő funkciói:

- A tanúsítványigénylő ügyfelek és szervezeteik nyilvántartása, és a hitelesítés szolgáltatáshoz kapcsolódó teljes életciklusuk követése
- Intelligens kártyák és tanúsítványok adatainak nyilvántartása
- A tanúsítványok felfüggesztése, visszavonása, visszaállítása, státuszának lekérdezése, valamint letöltése egyaránt elérhető a MicroRA-n keresztül a támogatott CA alkalmazások esetében
- Kártyagyártáshoz, valamint tanúsítványkibocsátáshoz szükséges bemeneti adatok szolgáltatása (tömegesen is)
- PUK levelek nyomtatása
- Publikus ügyfélportállal történő MQ alapú aszinkron kommunikáció, azaz az internet irányából nincsen közvetlen befelé irányuló kapcsolat.
- XML és aláírt e-akta formátumú tanúsítványigénylések feldolgozása
- Hitelesítés szolgáltatáshoz kapcsolódó szolgáltatások kezelése a számlázásukhoz szükséges információkkal együtt
- Költségviselők nyilvántartása, és a számlázáshoz szükséges bemeneti adatok szolgáltatása
- Hitelesítés szolgáltatáshoz szükséges iratok automatikus generálása az ügyfelekhez kapcsolódóan (tanúsítványkérelem adatlap, átvételi nyilatkozatok, szerződések)
- Elektronikus dokumentumok csatolása az egyes ügyfelekhez, szervezetekhez stb.
- Értesítő e-mailek továbbítása az ügyfelek részére
- Szerepkör alapú jogosultságkezelés
- Cluster üzemmód támogatása
- Titkosított adatmentés, GDPR megfelelés. Szelektív ügyféladat törlési lehetőség az adott ügyfélhez tartozó dekódoló kulcs eldobásával (így a mentésekből is lényegében törlésre kerül az adott ügyfélre vonatkozó adat).

A MicroRA rendszer segítségével könnyedén kezelhető több tízezres ügyfélkör is, köszönhetően annak, hogy a funkciók jelentős része (pl. szolgáltatások felvétele, iratok nyomtatása) az ügyfelek egy csoportjára egyszerre is végrehajtható. A rendszer szerver oldali komponense PostgreSQL adatbázison alapszik, a kommunikáció Apache webszerver segítségével történik, míg az érdemi munkát PHP interpreter végzi. Kliens oldalon csupán egy böngészőprogram futtatására van szükség.

Támogatott platformok:

- OS: Linux (preferált: Oracle Linux, Red Hat, CentOS)
- Adatbázis támogatás: PostgreSQL

Támogatott CA alkalmazások

- Microsec MicroCA alkalmazás
- EJBCA CA alkalmazás

MicroTSA

Időbélyegző alkalmazás

A MicroTSA szabványos (RFC 3161, ETSI EN 319421 és ETSI EN 319422) időbélyegek létrehozására alkalmas szoftver, mely felhasználónév-jelszó vagy tanúsítvány alapú autentikációval HTTPS protokollon vagy egyedi URL-en HTTP vagy HTTPS protokollon keresztül képes időbélyeg-kérések fogadására és időbélyegek kibocsátására.

A MicroTSA alkalmazás jellemzői:

- Apache webszerver alatt futtatható modul (mod_tsa)
- Megfelel az RFC 3161 időbélyeg szabványnak
- Támogatott kulcstípusok: RSA (1024(nem ajánlott) 2048, 3072, 4096 bit), ECDSA (NIST-P-126/256/384/512 bit)
- Támogatott kulcstároló eszközök:
  - szoftveres
  - nCipher / nShield HSM modellek, K of N operátori kártyás működési mód
  - PKCS11-en keresztül más HSM-ek
- Támogatott lenyomatképző algoritmusok: SHA-1(nem javasolt), SHA-256, SHA-384, SHA-512
- A kérésben szereplő lenyomatokat külön lehet engedélyezni.
- Tetszőlegesen konfigurálható, hogy a kérésben szereplő lenyomat (amennyiben engedélyezett) szerepeljen a válaszban, vagy attól eltérő.
- ESSCertID SHA-256 lenyomatképző algoritmussal készül megfelelve az RFC 5816 szabványnak
- Támogatott protokollok: HTTP, HTTPS (TLS1.2, TLS1.3)
- Az időbélyegző tanúsítványát tekintve:
  - X509-es szabványnak való megfelelés
  - Tanúsítvány aláírása RSA vagy ECDSA algoritmussal

    - Támogatja az EIDAS szerinti OrganizationIdentifier mező szerepeltetését az időbélyegző tanúsítvány DN-ben
    - QCStatements támogatás
    - A tanúsítványban szereplő magánkulcs használati idejének (PrivateKeyUsagePeriod) ellenőrzése. Ha az lejárt, nem hajlandó aláírni a kulccsal, még akkor sem, ha a tanúsítvány még érvényes.
- Naplózást tekintve az Apache webszerver saját naplójába kerülnek az alábbi információk (MicroTSA audit log):
    - Forrás IP cím
    - Felhasználónév (Basic autentikáció)
    - Időbélyeg kérés/válasz időpontja
    - Időbélyeg kérés azonosítója (id)
    - Időbélyeg sorozatszáma (TST/serial)
    - Időbélyeg kérésben szereplő Nonce érték (TS REQ/Nonce)
    - Bejövő időbélyeg kérésben szereplő lenyomat típusa és maga a lenyomat (TS REQ /msg_imprint)
    - Időbélyeg válaszban szereplő lenyomat típusa és maga a lenyomat (TS RESP/digest)
    - Időbélyeg aláíró tanúsítvány lenyomatának típusa és maga a lenyomat (TS RESP/ sig_cert_hash)
    - Időbélyeg válaszban szereplő aláírás típusa (RSA-SHA256/ecdsa-with-SHA256) és maga az aláírás értéke
    - Időbélyeg válasz mérete byte-ban
    - Időbélyeg válasz generálásának időtartama

Minta:

10.48.160.2 teszt [17/Mar/2022:00:01:08 +0100] [id:YjJsNJvkcM-CI@Hp2L@pPAAAAAM] TST: Granted (serial: 01011F8C) |TS REQ: [nonce: DC9F640A65D7FC7F] [msg_imprint: sha256:903d53fdd7e0db481a672c1adc557646512bacf7873ce7c6b3f1cb630099b183]| |TS RESP: [digest: sha256:b7a216f9f74307261101429ba8e2f0a9deef6efd1d4b4a0166420835e94d0d91] [sig_cert_hash: sha256:c214bee7f3521699a57ddce81518f14b9fb00f61a3ca0748c7ba33aebbc536e4] [signature: ecdsa-with-SHA256:3045022002d6520c418e1620a81a045f0b3515323a7242bdf5ed3b7505d103b7f8cbf6a8022100e40427ef76747caf8eb2cb0a29df7fec95b27cabe9baa6d465295ab492692085]| - 2204 1120us

- Autentikáció: A MicroTSA-t futtató Apache webszerver elé tetszőleges autentikációs réteg beépíthető bármilyen tűzfalelemmel. Ugyanakkor Apache webszerver segítségével az alábbi autentikációs típusokat támogatja a MicroTSA:
    - http Basic autentikációs (htpasswd fájl vagy LDAP adatbázis alapján)
    - Tanúsítvány alapú autentikáció:
        - SSLRequire szabályokkal
        - SSLFakeBasic autentikáció (SSLFakepasswd fájl, ldap adatbázis)
    - Egyedi url alapú autentikáció basic autentikációra visszavezetve.
- Skálázhatóság:
    - A MicroTSA-t futtató Apache webszerver estén a gyerek processzek számának növelésével lokálisan lehet nagyobb performanciát elérni a HSM kapacitásának függvényében.
    - Lehetőség van több MicroTSA alkalmazást futtató virtuális gépet (node-ot) LoadBalancer proxy webalkalmazás (pl.: Apache) mögé beállítani, ezek száma

tetszőlegesen növelhető a kapcsolódó HSM eszközök kapacitásának függvényében.
    - Több MicroTSA node esetén ügyelnünk kell arra, hogy vagy minden node-nak saját időbélyegző kulcsa és tanúsítványa legyen, vagy ha ugyanazzal a kulccsal írnak alá, akkor eltérő sorozatszám tartományból osszanak az egyes node-ok időbélyegeket.
- Performancia: Egy két darabból álló nShield XC Solo Base HSM eszközpárt használó két node-os MicroTSA rendszerrel akár 600-700 db/másodperc időbélyeget lehet kiadni (RSA 3072 bites, vagy NIST-P-256-os kulccsal.
- Támogatott operációs rendszerek:
    - CentOS Linux 6.x/7.x/8.x
    - Red Hat Enterprise Linux (RHEL) 6+
    - Oracle Linux (preferált)
    - Solaris (SPARC)
- MicroTSA működését kiegészítő egyéb Microsec által fejlesztett szoftver komponensek:
    - MicroTSC DB: Időbélyeg számláló alkalmazás és adatbázis. Az alkalmazás az Apache webszerver naplóit aszinkron módon elemezve képes az időbélyegző adatokat felhasználók szerint adatbázisba rendezni, amiben az időbélyeg fogyasztási adatok kereshetővé válnak. További plusz kiegészítő komponens segítségével a fogyasztási adatok az ügyfelek számára is elérhetővé válnak ugyanazokkal az autentikációs adatokkal, melyekkel az időbélyeget is le lehet kérdezni. Ez a modul grafikonos fogyasztási statisztikákat is tud készíteni megadott időintervallumra.
    - Prepaid modul: Ezzel a modullal lehetőség van időbélyeg felhasználókat felvenni, és felhasználónként külön-külön lefogyasztható időbélyeg mennyiségeket a felhasználóhoz hozzárendelni. A lefogyasztható mennyiség megközelítésekor a felhasználónak e-mail értesítést küld, illetve a beállított mennyiség elérésekor letiltja az időbélyegzést az adott felhasználó számára. Ez a modul LDAP alapú autentikáció esetén használható.
    - Perfomancia tesztelő alkalmazás: Windows platformon elérhető a Microsec tsflow alkalmazás, mely kiválóan alkalmas egy időbélyeg szolgáltatás teljesítményének tesztelésére
        - Bővebb leírás itt: https://e-szigno.hu/idobelyeg-performancia-teszt

MicroOCSP

Online tanúsítvány-állapot információs alkalmazás

A MicroOCSP szabványos (RFC 6960) OCSP válaszok kibocsátására szolgáló alkalmazás, mely korlátlan számú CA által kibocsátott tanúsítvány aktuális státuszának lekérdezését biztosítja online módon. A MicroOCSP része a MicroCA alkalmazásnak, de önállóan is megvásárolható. A MicroOCSP alkalmazás natív kódban írt szoftver, ezért jóval nagyobb válaszadási teljesítményre képes a Java alapú OCSP megoldásokhoz képest. Támogatja a vonatkozó OCSP szabvány által javasolt a rövid lejáratú (akár 10 percig érvényes) OCSP válaszadói tanúsítványok használatát is OCSP-NOCHECK kiterjesztés esetén.

A MicroOCSP alkalmazás jellemzői:

- Natív démon alkalmazás, mely a konfigurációban megadott HTTP porton érhető el a performancia igényeknek megfelelő mennyiségű gyerekprocessz beállításával.
- Előtét proxy alkalmazás (pl.: Apache 2.4.x) segítségével kell a külvilággal való kapcsolatot megvalósítani, mellyel a Load Balance működéssel skálázás is megvalósítható több MicroOCSP szerver beállításával. Performancia node-onként akár 400 db/sec
- Megfelel az RFC 6960 OCSP protokoll szabványnak
- Támogatott kulcstípusok: RSA (1024(nem ajánlott) 2048, 3072, 4096 bit), ECDSA (NIST-P-126/256/384/512 bit)
- Támogatott kulcstároló eszközök:
    - szoftveres
    - nCipher / nShield HSM modellek, K of N operátori kártyás működési mód
    - PKCS11-en keresztül más HSM-ek
- Támogatott lenyomatképző algoritmusok: SHA-1(nem javasolt), SHA-256, SHA-384, SHA-512
- Támogatott protokollok: HTTP, illetve előtét webszerveren keresztül HTTPS (TLS1.2, TLS1.3)
- Az OCSP válaszadói tanúsítványát tekintve:
    - X509-es szabványnak való megfelelés
    - Tanúsítvány aláírása RSA vagy ECDSA algoritmussal
    - Támogatja az EIDAS szerinti OrganizationIdentifier mező szerepeltetését az OCSP válaszadói tanúsítvány DN-ben
    - OCSP NOCHECK kiterjesztés feltüntetése a tanúsítványban
    - Rövid lejáratú (akár 10 perc) OCSP válaszadói tanúsítványok támogatása ugyanahhoz a kulcshoz. A lejárat előtt automatikusan újra lehet tölteni az új tanúsítványt.
- Naplózást tekintve a syslogba kerülnek az alábbi információk:
    - Forrás IP cím
    - OCSP kérés azonosítója (id)
    - OCSP kérés/válasz időpontja
    - OCSP kérésben szereplő tanúsítvány hexadecimális sorozatszáma
    - OCSP kérésben szereplő tanúsítvány kibocsátójának OCSP konfigurációban meghatározott rövid neve, amennyiben az OCSP válaszadó számára ismertelen CA a kibocsátó, akkor „unknown CA"
    - OCSP kérelemben szereplő nonce érték
    - Tanúsítvány visszavonási állapota (VALID, REVOKED)
- Kommunikáció – HTTP alapon
- Az OCSP választ aláíró algoritmus:
- RSA, használható kulcsméret: 2048, 3072, 4096 bit
- EC: (secp112r2 secp128r1 secp128r2 secp160k1 secp160r1 secp160r2 secp192k1 secp224k1 secp224r1 secp256k1 secp384r1 secp521r1 prime192v1 prime192v2 prime192v3 prime239v1 prime239v2 prime239v3 prime256v1 sect113r1 sect113r2 sect131r1 sect131r2 sect163k1 sect163r1 sect163r2 sect193r1 sect193r2 sect233k1

sect233r1 sect239k1 sect283k1 sect283r1 sect409k1 sect409r1 sect571k1 sect571r1 c2pnb163v1 c2pnb163v2 c2pnb163v3 c2pnb176v1 c2tnb191v1 c2tnb191v2 c2tnb191v3 c2pnb208w1 c2tnb239v1 c2tnb239v2 c2tnb239v3 c2pnb272w1 c2pnb304w1 c2tnb359v1 c2pnb368w1 c2tnb431r1 brainpoolP160r1 brainpoolP160t1 brainpoolP192r1 brainpoolP192t1 brainpoolP224r1 brainpoolP224t1 brainpoolP256r1 brainpoolP256t1 brainpoolP320r1 brainpoolP320t1 brainpoolP384r1 brainpoolP384t1 brainpoolP512r1 brainpoolP512t1

- Az OCSP válaszokban használt lenyomatképző algoritmusok:
  - SHA256, SHA384, SHA512
- MultiCA támogatás – válaszadás több CA által kibocsátott tanúsítványokra, a támogatott CA-k darabszámának nincsen felső korlátja
- OCSP válaszok adatainak forrása lehet:
  - MicroCA MySQL adatbázis
  - fájl adatbázis (index)
  - visszavonási lista (CRL). Javasolt, hogy a CRL eseményvezérelten generálódjon, azaz minden tanúsítványállapotváltozás esetén, továbbá a lejárt tanúsítványok ne kerüljenek le a CRL-ről.
- Támogatott operációs rendszerek:
  - CentOS Linux 6.x/7.x/8.x
  - Red Hat Enterprise Linux (RHEL) 6+
  - Oracle Linux (preferált)
  - Solaris (SPARC)
- Adatbázis támogatás: MySQL, PostgreSQL, Oracle

Támogatott CA alkalmazások:

- Microsec MicroCA alkalmazás
- CRL-en keresztül bármilyen CA alkalmazás
- Megfelelő adatbázis struktúra létrehozásakor replikációval szintén bármilyen CA alkalmazás

MicroSCEP

Tanúsítvány menedzsment alkalmazás

A MicroSCEP segítségével lehetőség van arra, hogy az SCEP protokollt támogató eszközök kényelmesen kerüljenek ellátásra tanúsítványokkal. A MicroSCEP használatához szükséges a MicroRA nyilvántartó szoftver használata, valamint olyan CA alkalmazás, mely támogatja a PKCS10-es tanúsítványkérelmek és tanúsítványadatok alapján történő automatikus tanúsítvány kibocsátást.
A támogatott CA alkalmazásokkal alapértelmezetten együtt működik, más CA alkalmazáshoz könnyen illeszthető, támogatja a Load Balance üzemmódot.

A MicroSCEP alkalmazás jellemzői:

- Előtét proxy alkalmazás (pl.: Apache 2.4.x) segítségével kell a külvilággal való kapcsolatot megvalósítani, mellyel a Load Balance működéssel skálázás is megvalósítható több MicroSCEP szerver beállításával.
- Megfelel az RFC 8894 SCEP protokoll szabványnak
- RSA, használható kulcsméret: 2048, 3072, 4096 bit
- EC: (secp112r2 secp128r1 secp128r2 secp160k1 secp160r1 secp160r2 secp192k1 secp224k1 secp224r1 secp256k1 secp384r1 secp521r1 prime192v1 prime192v2 prime192v3 prime239v1 prime239v2 prime239v3 prime256v1 sect113r1 sect113r2 sect131r1 sect131r2 sect163k1 sect163r1 sect163r2 sect193r1 sect193r2 sect233k1 sect233r1 sect239k1 sect283k1 sect283r1 sect409k1 sect409r1 sect571k1 sect571r1 c2pnb163v1 c2pnb163v2 c2pnb163v3 c2pnb176v1 c2tnb191v1 c2tnb191v2 c2tnb191v3 c2pnb208w1 c2tnb239v1 c2tnb239v2 c2tnb239v3 c2pnb272w1 c2pnb304w1 c2tnb359v1 c2pnb368w1 c2tnb431r1 brainpoolP160r1 brainpoolP160t1 brainpoolP192r1 brainpoolP192t1 brainpoolP224r1 brainpoolP224t1 brainpoolP256r1 brainpoolP256t1 brainpoolP320r1 brainpoolP320t1 brainpoolP384r1 brainpoolP384t1 brainpoolP512r1 brainpoolP512t1
- Támogatott kulcstároló eszközök:
  - szoftveres
  - nCipher / nShield HSM modellek, K of N operátori kártyás működési mód
  - PKCS11-en keresztül más HSM-ek
- Támogatott lenyomatképző algoritmusok: SHA-1(nem javasolt), SHA-256, SHA-384, SHA-512
- Támogatott protokollok: HTTP, illetve előtét webszerveren keresztül HTTPS (TLS1.2, TLS1.3)
- Kezelhető tanúsítványok - X.509, RFC 5280 szerinti formátumú
- Támogatott tanúsítvány kérelmek - PKCS#10
- Támogatott operációs rendszerek:
  - CentOS Linux 6.x/7.x/8.x
  - Red Hat Enterprise Linux (RHEL) 6+
  - Oracle Linux (preferált)
  - Solaris (SPARC)

Támogatott CA alkalmazások

- Microsec MicroCA alkalmazás
- EJBCA CA alkalmazás

Támogatott kliensek

- Apple iOS – utolsó 5 főverzió (gyári iOS SCEP kliens)
- MeT – Microsec tanúsítvány kezelő
- SSCEP alkalmazás
- AutoSCEP alkalmazás
- JSCEP alkalmazás

MicroAC

Attribútum tanúsítvány kibocsátó alkalmazás

A MicroAC alkalmazással lehetőség van X.509 szabványnak megfelelő aláírói, autentikációs és titkosító tanúsítványokhoz tartozó az RFC 5755, az ETSI TS 119471 és az ETSI 119472 szerinti attribútum tanúsítványok kibocsátására.

A kiadott attribútum tanúsítványokkal valamely szervezet igazolhatja például aláíráskor az aláíró szerepkörét, illetve az aláíró egyéb attribútumait. A megoldással nincsen szükség a továbbiakban a szerepkör feltüntetésére a hitelesítés szolgáltató által kibocsátott tanúsítványokban. A szerepkört igazoló szervezet saját hatáskörben rendelkezhet a munkavállalója szerepköreiről (igazolhatja, módosíthatja, visszavonhatja) az X.509-es tanúsítvány módosítása, illetve visszavonása nélkül.

Egyéb nyilvántartó alkalmazásokhoz az integráció megállapodás szerint vállalható.

A MicroAC alkalmazás jellemzői:

- Tanúsítványok: X.509 és RFC 5755 szerinti formátumban
- Tanúsítvány kérelmek: RFC 5755 kérelem formátumban, aláíró tanúsítvánnyal.
- Támogatott holder (aláírói tanúsítványra mutató referenciák) típusok:
    - Aláírói tanúsítvány lenyomata
    - Aláírói tanúsítványban szereplő DN (Adobe kompatibilitás)
- Kommunikáció - HTTP és HTTPS alapon
- Az attribútumot aláíró algoritmus:
    - RSA, használható kulcsméret: 2048, 3072, 4096 bit
    - EC: (secp112r2 secp128r1 secp128r2 secp160k1 secp160r1 secp160r2 secp192k1 secp224k1 secp224r1 secp256k1 secp384r1 secp521r1 prime192v1 prime192v2 prime192v3 prime239v1 prime239v2 prime239v3 prime256v1 sect113r1 sect113r2 sect131r1 sect131r2 sect163k1 sect163r1 sect163r2 sect193r1 sect193r2 sect233k1 sect233r1 sect239k1 sect283k1 sect283r1 sect409k1 sect409r1 sect571k1 sect571r1 c2pnb163v1 c2pnb163v2 c2pnb163v3 c2pnb176v1 c2tnb191v1 c2tnb191v2 c2tnb191v3 c2pnb208w1 c2tnb239v1 c2tnb239v2 c2tnb239v3 c2pnb272w1 c2pnb304w1 c2tnb359v1 c2pnb368w1 c2tnb431r1 brainpoolP160r1 brainpoolP160t1 brainpoolP192r1 brainpoolP192t1 brainpoolP224r1 brainpoolP224t1 brainpoolP256r1 brainpoolP256t1 brainpoolP320r1 brainpoolP320t1 brainpoolP384r1 brainpoolP384t1 brainpoolP512r1 brainpoolP512t1
- Az attribútumokban használt lenyomatképző algoritmusok:
    - SHA256, SHA384, SHA512
- Szerepkör egyeztetés REST API-n és Windows AD-ból (csoporttagság alapján)
- Támogatott kulcstároló eszközök:

    - szoftveres
    - nCipher / nShield HSM modellek, K of N operátori kártyás működési mód
    - PKCS11-en keresztül más HSM-ek
- Támogatott operációs rendszerek:
    - CentOS Linux 6.x/7.x/8.x
    - Red Hat Enterprise Linux (RHEL) 6+
    - Oracle Linux (preferált)
- Támogatott attribútum adatbázisok:
    - Microsec MicroRA
    - XML interfésszel rendelkező attribútum adatbázisokhoz könnyen illeszthető.
    - Windows AD (integráció szükséges)
- Támogatott kliensek
    - Microsec e-Szignó kliens
    - Microsec e-Szignó SDK
    - Adobe Acrobat/Reader

MicroCardPerso

Tömeges kulcsgeneráló alkalmazás

A MicroCardPerso egy univerzális kulcsgeneráló és tanúsítványigénylő alkalmazás, mellyel lehetőség van PKCS#11 interfésszel rendelkező kártyák és tokenek elektronikus és -szükséges berendezés megléte esetén- vizuális megszemélyesítésre egyaránt. Az elektronikus megszemélyesítés a kulcsok és azokhoz tartozó PKCS#10 kérelmek legenerálását, valamint MicroRA rendszerbe való beküldését jelenti.

A MicroCardPerso támogatja a tömeges kártya és token elektronikus és vizuális megszemélyesítést is. Könnyen integrálható a Windows operációs rendszert támogató kártyagyártó berendezésekhez.

A MicroCardPerso alkalmazás az alábbi főbb szabványoknak, ajánlásoknak és protokolloknak felel meg:

- HTTP és HTTPS protokollok támogatása a MicroRA alkalmazáshoz történő kapcsolódáskor. Közvetlen CA kommunikáció is lehetséges (integráció szükséges)
- Tanúsítvány, illetve felhasználónév/jelszó alapú autentikáció támogatása
- Támogatott kulcs algoritmus (a hardvereszköznek is támogatnia kell):

- RSA, használható kulcsméret: 2048, 3072, 4096 bit
- EC: (secp112r2 secp128r1 secp128r2 secp160k1 secp160r1 secp160r2 secp192k1 secp224k1 secp224r1 secp256k1 secp384r1 secp521r1 prime192v1 prime192v2 prime192v3 prime239v1 prime239v2 prime239v3 prime256v1 sect113r1 sect113r2 sect131r1 sect131r2 sect163k1 sect163r1 sect163r2 sect193r1 sect193r2 sect233k1 sect233r1 sect239k1 sect283k1 sect283r1 sect409k1 sect409r1 sect571k1 sect571r1 c2pnb163v1 c2pnb163v2 c2pnb163v3 c2pnb176v1 c2tnb191v1 c2tnb191v2 c2tnb191v3 c2pnb208w1 c2tnb239v1 c2tnb239v2 c2tnb239v3 c2pnb272w1 c2pnb304w1 c2tnb359v1 c2pnb368w1 c2tnb431r1 brainpoolP160r1 brainpoolP160t1 brainpoolP192r1 brainpoolP192t1 brainpoolP224r1 brainpoolP224t1 brainpoolP256r1 brainpoolP256t1 brainpoolP320r1 brainpoolP320t1 brainpoolP384r1 brainpoolP384t1 brainpoolP512r1 brainpoolP512t1

Támogatott kulcstároló hardvereszközök:

- Bit4Id Touch & Sign 2048 (eSB) kártya (SSCD)
- Gemalto Classic TPC IM CC (eSG) kártya/token (SSCD)
- Gemalto IDPrime MD 840 és IDPrime MD 3840 (QSCD)
- Gemalto IDPrime MD 940 és IDPrime MD 3940 (QSCD)
- Gemalto IDPrime MD 940B és IDPrime MD 3940B (QSCD)
- Egyéb PKCS#11 szabványt támogató hardvereszközhöz vállaljuk az integrációt.

Támogatott platformok:

- OS: Windows - aktuális támogatott verzió

Támogatott CA alkalmazások:

- Microsec MicroCA alkalmazás
- EJBCA CA alkalmazás

Támogatott kártyagyártó berendezések:

- Zebra ZXP Series 7
- Más típusokhoz az integrációt vállaljuk.

Microsec e-Szignó Tanúsítványkezelő

A MeT egy Windows és macOS (béta) operációs rendszeren futó kliens alkalmazás mellyel a szoftveresen, chipkártyán, tárolt kulcsos szolgáltatásban található kulcsait használhatja aláírásra, illetve kezelheti.

További jelentős funkciói az alkalmazásnak:

- SCEP protokollal történő szoftveres/kártyás tanúsítvány igénylés,
- kártya tanúsítvány, pin kód kezelés és feloldás,
- megújított tanúsítvány automatikus telepítése szolgáltató tanúsítványtárából mind szoftveres mind kártyás tanúsítványok esetén
- tárolt kulcsos aláírás elérhetővé tétele Windows CSP/KSP alapú aláírásra képes alkalmazásokból
- tanúsítványok automatikus regisztrációja a Windows/Mac OSX tanúsítványtárába

Támogatott kulcstároló hardvereszközök:

- Bit4Id Touch & Sign 2048 (eSB) kártya (SSCD)
- Gemalto Classic TPC IM CC (eSG) kártya/token (SSCD)
- Gemalto IDPrime MD 840 és IDPrime MD 3840 (QSCD)
- Gemalto IDPrime MD 940 és IDPrime MD 3940 (QSCD)
- Gemalto IDPrime MD 940B és IDPrime MD 3940B (QSCD)
- Minősített távoli kulcstároló eszköz (RQSCD)
- Egyéb PKCS#11 szabványt támogató hardvereszközhöz vállaljuk az integrációt.

Támogatott operációs rendszerek:

- Windows 10+
- macOS (béta)

További kérdései vannak?

Tanácsadóink a lenti elérhetőségeken állnak rendelkezésére.

1033 Budapest, Ángel Sanz Briz út 13.
+36 1 505 4444 | sales@microsec.hu