MicroCA

Certificate Issuing and Certificate Lifecycle Management (CA) System

MicroCA is a web-based, platform and browser independent X.509 certificate issuing and certificate lifecycle management system that provides full CA functionality. MicroCA can issue certificates and supports all certificate status change operations (suspend, release from suspension, revoke, renew). It provides information about the status of certificates (valid, suspended, revoked, expired) by providing revocation lists (CRL) and online certificate status responses (OCSP).

The main functions of the system are:

- Certificate management
    - X.509 compliant certificate issuance based on a certificate request (PKCS#10, SPKAC) or a previous X.509 certificate. DN data in certificates can be configured freely.

- The extensions to be included in the certificate can be specified using certificate profiles. The editable certificate profiles can be used to define any extension and can be used to create any ASN1 structure.
- Multiple ways to specify certificate validity:
  - Default validity period based on certificate profile.
  - Specify any validity period within the validity range specified in the profile.
  - Specify future validity
  - Specify the validity (up to 10 minutes) of a short term certificate for issuing OCSP Responder certificates compliant with RFC 6960 OCSP standard.
- Web server certificate issuance:
  - EV certificate profiles support
  - Issuing PSD2 qualified web server and seal certificates
  - Support for Google Transparency log servers
  - CAA record-based domain verification
  - IANA list based master domain verification
  - International (non-ASCII) domain support (Punycode)
- Key quality checking: weak key detection, key uniqueness checking.
- Unique identifier in certificates (Permanent Identifier - RFC 4043
- Publication of certificates to external public LDAP (OpenLDAP) database (public certificate store). Publication can be specified per certificate.
- Support for SCEP (Simple Certificate Enrollment Protocoll)

- CA key management

  - Multi CA operation, i.e. management of multiple CA keys within one CA application, the type of keys can be specified separately.
  - Supported provider key types:
    - RSA, usable key size: 2048, 3072, 4096 bits
    - 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)

    - Hash algorithms used in signatures: SHA256, SHA384, SHA512
    - Protection of the provider keys:
        - software
        - hardware: **H**ardware **S**ecurity **M**odule (nCipher, Thales Luna, Utimaco). Keys protected by operator cards according to K of N policy
        - PKCS11
    - Multi-level certificate hierarchy (offline Root, Sub CA)
- Revocation services
    - Certificate suspension, release from suspension, revocation.
    - In case of certificate status change, automatic generation of revocation list in a delayed manner only for the affected CA.
    - Delayed revocation list generation
    - Retention/removal of expired certificates from revocation lists
    - ExpiredCertsOnCRL extension support for revocation lists
    - Support for OCSP (RFC 6960)
    - CRL support (RFC 5280), deltaCRL not supported.
    - CRL synchronization to external public server, no direct connection from the Internet to MicroCA, so practically complete disconnection from the Internet is supported.
- Authentication and access control:
    - Logon with X.509 authentication certificate (EC, RSA). On logon, certificate revocation check and privilege check

    - o Dual control on certificate issuance, only certificate issuance with appropriate privileges allowed.
- Logging: electronically signed and time-stamped (RFC 3161) XML log files (audit log)
- Redundancy, HA operation, active and passive nodes, also for operator card protected service keys.
- Interfaces:
    - webes user (RA, Admin) interface
    - REST API
    - Command line

Supported platforms:

- OS: Linux (preferred: Oracle Linux, Red Hat, CentOS)
- Database support: MySQL, MariaDB, PostgreSQL, Oracle
- Webserver: Apache 2.4.x

MicroRA

Registration and client management software for CA systems

MicroRA is a web-based, platform- and browser-independent case management system designed to support processes related to the authentication service.

The main features of the system are:

- Registration of enrolling clients and their organizations and tracking of their entire lifecycle related to the certification service.
- -Registering smart card and certificate data
- Suspension, release from suspension, revocation, status query and download of certificates are all available via MicroRA for supported CA applications
- Provision of input data for card production and certificate issuance (also in bulk)
- Printing of PUC code documents

- MQ-based asynchronous communication with public customer portal, i.e. no direct inward connection from the Internet.
- Processing certificate requests in XML and signed eAkta format.
- Management of services related to the authentication service including their billing information.
- Registering cost owners and providing input data for billing
- Automatic generation of documents for the certification service related to the clients (certificate request form, hand-over declarations, contracts)
- Attachment of electronic documents for each client, organisation, etc.
- Transmission of notification e-mails to clients
- Role-based rights management
- Cluster mode support
- Encrypted data backup, GDPR compliance. Selective deletion of client data by dropping the decryption key associated with the client (so that the data for that client is essentially deleted from the backups).

MicroRA can easily handle tens of thousands of customers, thanks to the fact that many of the functions (e.g. service pick-up, document printing) can be performed on a group of customers at once (bulk changes). The server-side component of the system is based on a PostgreSQL database, communication is handled by an Apache web server, while the substantive work is done by a PHP interpreter. On the client side, only a browser is required to run.

Supported platforms:

- OS: Linux (preferred: Oracle Linux, Red Hat, CentOS)
- Database support: PostgreSQL

Supported CA applications:

- Microsec MicroCA application
- EJBCA CA application

MicroTSA

Timestamp application

MicroTSA is a standard (RFC 3161, ETSI EN 319421 and ETSI EN 319422) timestamping software that can receive timestamp requests and issue timestamps via HTTP or HTTPS using username-password or certificate-based authentication over HTTPS or a unique URL.

MicroTSA application features:

- Apache web server executable module (mod_tsa)
- Compliant with the RFC 3161 timestamp standard
- Supported key types: RSA (1024 (not recommended), 2048, 3072, 4096 bits), ECDSA (NIST-P-126/256/384/512 bits)
- Protection of the provider keys:
    - software
    - hardware: Hardware Security Module (nCipher, Thales Luna, Utimaco). Keys protected by operator cards according to K of N policy
    - other HSMs via PKCS11
- Supported impression algorithms: SHA-1(not recommended), SHA-256, SHA-384, SHA-512
- Hashes in the request can be enabled separately.
- It is optionally configurable to include the hashes in the request (if enabled) in the response, or a different one.
- ESSCertID is generated with SHA-256 impression building algorithm conforming to RFC 5816
- Supported protocols: HTTP, HTTPS (TLS1.2, TLS1.3)
- For the timestamp certificate:
    - Compliance with X509 standard
    - Certificate signing with RSA or ECDSA algorithm
- Support the inclusion of the eIDAS OrganizationIdentifier field in the timestamp certificate DN
- QCStatements support
- Verification of the private key usage period (PrivateKeyUsagePeriod) in the certificate. If expired, it refuses to sign with the key, even if the certificate is still valid.
- In terms of logging, the following information is stored in the Apache web server's own log (MicroTSA audit log):
    - Source IP address
    - User name (Basic authentication)
    - Timestamp request/response time
    - Timestamp request ID (id)

- Timestamp serial number (TST/serial)
- Nonce value in timestamp request (TS REQ/Nonce)
- Type of hash in the incoming timestamp request and the hash itself (TS REQ /msg_imprint)
- Type of the hash in the timestamp response and the hash itself (TS RESP/digest)
- Type of the hash of the timestamp signing certificate and the hash itself (TS RESP/ sig_cert_hash)
- Type of the signature in the time stamp response (RSA-SHA256/ecdsa-with-SHA256) and the signature value itself
- Size of the timestamp response in bytes
- Time taken to generate the timestamp response

Example:

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

- Authentication: an arbitrary authentication layer can be added in front of the Apache web server running MicroTSA using any firewall element. However, MicroTSA supports the following types of authentications using an Apache web server:
  - http Basic authentication (based on htpasswd file or LDAP database)
  - Certificate-based authentication:
    - with SSLRequire rules
    - SSLFakeBasic authentication (SSLFakepasswd file, LDAP database)
  - Unique url based authentication backed to basic authentication.
- Scalability:
  - In the case of Apache web server running MicroTSA, higher performance can be achieved locally by increasing the number of child processes depending on the capacity of the HSM.
  - It is possible to set up multiple virtual machines (nodes) running MicroTSA behind a LoadBalancer proxy web application (e.g. Apache), the number of which can be arbitrarily increased depending on the capacity of the associated HSM devices.
  - In case of multiple MicroTSA nodes, care must be taken that either each node has its own timestamp key and certificate, or if signing with the same key, each node distributes timestamps from a different range of serial numbers.
- Performance: with a two-node MicroTSA system using a two-node nShield XC Solo Base HSM device pair, up to 600-700 timestamps per second can be issued (RSA 3072-bit or NIST-P-256 key).

- Supported operating systems:
  - CentOS Linux 6.x/7.x/8.x
  - Red Hat Enterprise Linux (RHEL) 6+
  - Oracle Linux (preferred)
  - Solaris (SPARC)
- Other software components developed by Microsec to complement MicroTSA:
  - MicroTSC DB: Timestamp counter application and database. The application can asynchronously parse Apache web server logs to sort timestamp data by user into a database where timestamp consumption data can be searched. With an additional add-on component, the consumption data can be made available to customers with the same authentication data used to query the timestamp. This module can also generate graphical consumption statistics for a specified time interval.
- Prepaid module: with this module, it is possible to add timestamp users and to assign individual time stamp quantities per user to be consumed. When a prepaid amount is approached, the user will receive an email notification or, when the prepaid amount is reached, the timestamp will be disabled for that user. This module can be used with LDAP-based authentication.
- Performance tester application: the Microsec tsflow application is available on Windows platform and is an excellent tool to test the performance of a timestamp service.
- For more details see: https://e-szigno.hu/idobelyeg-performancia-teszt

MicroOCSP

Online certificate status information application

The MicroOCSP is a standard (RFC 6960) OCSP response issuance application that provides online query of the status of certificates issued by an unlimited number of CAs. MicroOCSP is part of the MicroCA application but can also be purchased separately. The MicroOCSP application is written in native code and is therefore capable of much higher response performance compared to Java-based OCSP solutions. It also supports the use of short term OCSP responder certificates (valid up to 10 minutes) as recommended by the relevant OCSP standard for OCSP-NOCHECK extensions.

MicroOCSP application features:

- Native daemon application, accessible on the HTTP port specified in the configuration by setting the amount of child processes according to the performance requirements.
- A proxy application (e.g.: Apache 2.4.x) must be used to connect to the outside world, with which load balancing operation scaling can be implemented by configuring multiple MicroOCSP servers. Performance up to 400 bps per node

- Compliant with the RFC 6960 OCSP protocol standard
- Supported key types: RSA (1024 (not recommended), 2048, 3072, 4096 bit), ECDSA (NIST-P-126/256/384/512 bit)
- Supported key storage devices:
    - software
    - nCipher / nShield HSM models, K of N operator card mode of operation
    - other HSMs via PKCS11
- Supported hash algorithms: SHA-1(not recommended), SHA-256, SHA-384, SHA-512
- Supported protocols: HTTP or HTTPS (TLS1.2, TLS1.3) via web server
- For OCSP responder certificate:
    - Compliance with X509 standard
    - Certificate signing with RSA or ECDSA algorithm.
    - Support the inclusion of the EIDAS OrganizationIdentifier field in the OCSP responder certificate DN.
    - Include OCSP NOCHECK extension in the certificate
    - Support for short expiry (up to 10 minutes) OCSP responder certificates for the same key. New certificate can be automatically reloaded before expiry.
- Logging the following information to syslog:
    - Source IP address
    - OCSP request ID (id)
    - OCSP request/response time
    - OCSP request certificate hexadecimal serial number
    - Short name of the issuer of the certificate in the OCSP request as defined in the OCSP configuration, if the issuer is an unknown CA to the OCSP responder, then 'unknown CA'
    - nonce value in the OCSP request
    - Certificate revocation status (VALID, REVOKED)
- Communication - HTTP based.
- OCSP response signing algorithm:
    - RSA, usable key size: 2048, 3072, 4096 bits
    - 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

- Tracing algorithms used in OCSP responses:

    - SHA256, SHA384, SHA512
- MultiCA support - response to certificates issued by multiple CAs, unlimited number of CAs supported.
- Can be a source of data for OCSP responses:
    - MicroCA MySQL database
    - File database (index)
    - revocation list (CRL). It is recommended that the CRL is generated event-driven, i.e. for each certificate status change, and that expired certificates are not removed from the CRL.
- Supported operating systems:
    - CentOS Linux 6.x/7.x/8.x
    - Red Hat Enterprise Linux (RHEL) 6+
    - Oracle Linux (preferred)
    - Solaris (SPARC)
- Database support: MySQL, PostgreSQL, Oracle

Supported CA applications:

- Microsec MicroCA application.
- Any CA application via CRL
- Any CA application when creating a suitable database structure via replication.

MicroSCEP

Certificate management application

With MicroSCEP, it is possible to conveniently supply certificates to devices supporting the SCEP protocol. MicroSCEP requires the use of MicroRA registration software and a CA application that supports automatic certificate issuance based on PKCS10 certificate requests and certificate data.

It works with supported CA applications by default, can be easily integrated with other CA applications, supports Load Balance mode.

MicroSCEP application features:

- Upstream proxy application (e.g.: Apache 2.4.x) must be used to connect to the outside world, with which Load Balance operation can be scaled by configuring multiple MicroSCEP servers.
- Compliant with the RFC 8894 SCEP protocol standard
- SCEP communication signing algorithm:
    - RSA, usable key size: 2048, 3072, 4096 bits

    - 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
- Supported key storage devices:
    - software
    - nCipher / nShield HSM models, K of N operator card mode
    - other HSMs via PKCS11
- Supported hash algorithms:
  SHA-1(not recommended), SHA-256, SHA-384, SHA-512
- Supported protocols: HTTP or HTTPS (TLS1.2, TLS1.3) via web server.
- Managed certificates - X.509, RFC 5280 format
- Supported certificate requests - PKCS#10
- Supported operating systems:
    - CentOS Linux 6.x/7.x/8.x
    - Red Hat Enterprise Linux (RHEL) 6+
    - Oracle Linux (preferred)
    - Solaris (SPARC)

Supported CA applications

- Microsec MicroCA application
- EJBCA CA application

Supported clients

- Apple iOS - last 5 major versions (factory iOS SCEP client)
- e-Szignó Certmanager
- SSCEP application
- AutoSCEP application
- JSCEP application

MicroAC

Attribute certificate issuing application

The MicroAC application enables the issuance of attribute certificates for X.509 compliant signing, authentication and encryption certificates according to RFC 5755, ETSI TS 119471 and ETSI 119472.

With the issued attribute certificates, an organization may, for example, verify the role of the signatory when signing, or other attributes of the signatory. With this solution, it is no longer necessary to indicate the role in the certificates issued by the CA. The organization certifying the role can make its own decisions about the role of its employee (certify, modify, revoke) without modifying or revoking the X.509 certificate.

Integration with other registry applications can be undertaken by agreement.

MicroAC application features:

- Certificates: in X.509 and RFC 5755 format
- Certificate requests: in RFC 5755 request format with signing certificate.
- Supported holder (references to signing certificates) types:
  - Signatory certificate imprint
  - DN in the signing certificate (Adobe compatibility)
- Communication - HTTP and HTTPS based.
- The algorithm that signs the attribute:
  - RSA, usable key size: 2048, 3072, 4096 bits
  - 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
- Hash algorithms used in attribute certificates:
  - SHA256, SHA384, SHA512
- Role matching via REST API and from Windows AD (based on group membership)
- Supported keystore tools:
  - Software

    - nCipher / nShield HSM models, K of N operator card mode of operation
    - other HSMs via PKCS11
- Supported operating systems:
    - CentOS Linux 6.x/7.x/8.x
    - Red Hat Enterprise Linux (RHEL) 6+
    - Oracle Linux (preferred)
- Supported attribute databases:
    - Microsec MicroRA
    - Easy to integrate with attribute databases with XML interface.
    - Windows AD (integration required)
- Supported clients
    - Microsec e-Signature client
    - Microsec e-Signature SDK
    - Adobe Acrobat/Reader

MicroCardPerso

Bulk key generation application

MicroCardPerso is a universal key generation and certificate enrollment application that allows both electronic and - if the necessary equipment is available - visual personalization of cards and tokens with PKCS#11 interface. Electronic impersonation means the generation and submission of keys and associated PKCS#10 requests to MicroRA.

MicroCardPerso supports both electronic and visual mass card and token impersonation. It can be easily integrated with card manufacturing equipment supporting the Windows operating system.

The MicroCardPerso application complies with the following major standards, recommendations, and protocols:

- Support for HTTP and HTTPS protocols when connecting to the MicroRA application. Direct CA communication is possible (integration required)
- Support for certificate and username/password based authentication
- Supported key algorithm (must be supported by the hardware device):
    - RSA, usable key size: 2048, 3072, 4096 bits
    - 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

Supported key storage hardware devices:

- Bit4Id Touch & Sign 2048 (eSB) card (SSCD)
- Gemalto Classic TPC IM CC (eSG) card/token (SSCD)
- Gemalto IDPrime MD 840 and IDPrime MD 3840 (QSCD)
- Gemalto IDPrime MD 940 and IDPrime MD 3940 (QSCD)
- Gemalto IDPrime MD 940B and IDPrime MD 3940B (QSCD)
- Integration with other hardware devices supporting the PKCS#11 standard is possible.

Supported platforms:

- OS: Windows - current supported version

Supported CA applications:

- Microsec MicroCA application.
- EJBCA CA application

Supported card manufacturing equipment:

- Zebra ZXP Series 7

For other types we can undertake the integration.

e-Szignó Certmanager

Certmanager is a client application that runs on Windows and macOS (beta) operating systems to sign with and manage your keys stored in a software, smart card, stored key service.

Other significant features of the application include:

- Software/card certificate enrollment using SCEP protocol,
- card certificate, pin code management and unlocking,
- automatic installation of renewed certificates from the provider's certificate store for both software and card certificates

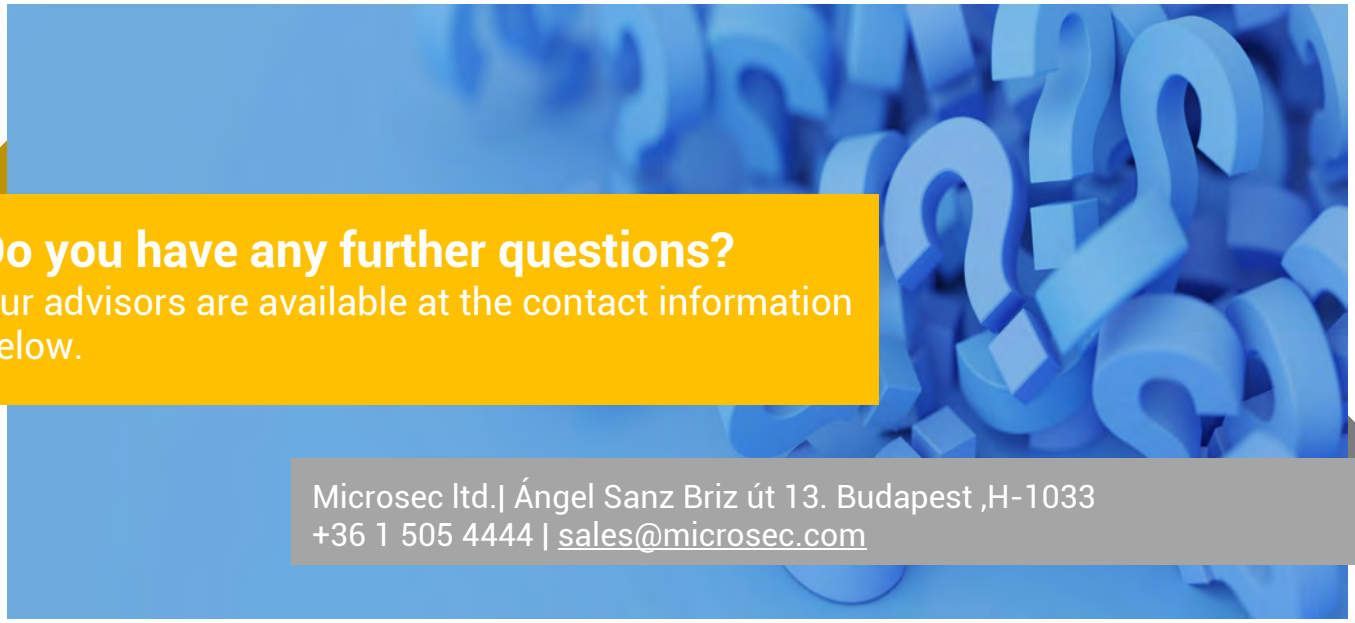
- make stored key signature available from Windows CSP/KSP signature-enabled applications.
- automatic enrolment of certificates into Windows/Mac OSX certificate store

Supported key storage hardware devices:

- Bit4Id Touch & Sign 2048 (eSB) card (SSCD)
- Gemalto Classic TPC IM CC (eSG) card/token (SSCD)
- Gemalto IDPrime MD 840 and IDPrime MD 3840 (QSCD)
- Gemalto IDPrime MD 940 and IDPrime MD 3940 (QSCD)
- Gemalto IDPrime MD 940B and IDPrime MD 3940B (QSCD)
- Qualified remote key storage device (RQSCD)
- We can integrate with other hardware devices supporting PKCS#11 standard.

Supported operating systems:

- Windows 10+
- MacOSX (beta)



Do you have any further questions?

Our advisors are available at the contact information below.

Microsec ltd.| Ángel Sanz Briz út 13. Budapest ,H-1033
+36 1 505 4444 | sales@microsec.com