Important notice:

Microsec already has two root certificates included in Mozilla root store. The “Microsec e-Szigno Root CA 2009” is still in the root store with active status. The first root certificate “Microsec e-Szigno Root CA” expired in 2017. To replace it Microsec created a new root “e-Szigno Root CA 2017” and the whole new CA hierarchy based on ECC in 2017. It has near the same CA hierarchy as the presently active CA hierarchy. The only differences are the use of ECC algorithms in the full certification chain and the setup of a new subordinate CA dedicated to the issuance of TSA certificates.
The new CA hierarchy was audited by TÜViT first in 2017 and later in 2018.

Table of Contents

General information about CA's associated organization

CA Company Name	MICROSEC Micro Software Engineering & Consulting Private Limited Company by Shares
Company website	https://e-szigno.hu/en/ https://www.microsec.hu/en/
Organizational type	Private organization
Primary market / customer base	Based on its already existing PKI services Microsec started its eIDAS conformant qualified trust services among the firsts companies in Europe in 2016. Microsec offers certification services, time stamps and archiving (preservation) services for natural and legal persons. Microsec has special contracts with the Hungarian Lawyers and Attorneys who are its most important customers but Microsec issues certificates for governmental users, banks, insurance companies and others too. The services are available for anybody, Microsec has some customers from other EU member states too. Microsec focuses its operation into Hungary but plans to expand its business to other countries in Europe in the following years.
Impact to Mozilla Users	Microsec is a relatively small company but responds quickly to the changes in the legislation or in the user requirements, offers very flexible services. It has to fulfil special European and Hungarian requirements and it can be guaranteed only if Microsec has its root certificates directly included in the root stores.
Inclusion in other major browsers	Microsec already has two root certificates included in Mozilla root store. The first root certificate expired in 2017. To replace it Microsec created a new root and the whole new CA hierarchy based on ECC in 2017. The new hierarchy was audited by TÜViT first in 2017 and later in 2018 again. Mozilla (https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport) Microsoft (https://social.technet.microsoft.com/wiki/contents/articles/31634.microsoft-trusted-root-certificate-program-participants.aspx#Participants_list) Apple (https://support.apple.com/en-us/HT208125)
CA Primary Point of Contact (POC)	Full name: Dr. Sándor Szőke Direct E-mail address: sandor.szoke@microsec.com Phone number (mobile): +36 30 932-7718 CA Email Alias: info@e-szigno.hu CA Phone Number: +36 1 505-4444 Title / Department: Deputy Director of Trust Services

Technical information about each root certificate

Important notice: only specifying here the new root certificate object of this request. Information already registered for the “Microsec e-Szigno Root CA 2009” shall be kept as already recorded by Mozilla.

Certificate Name	e-Szigno Root CA 2017
Certificate Issuer Field	CN = e-Szigno Root CA 2017 2.5.4.97 = VATHU-23584497 O = Microsec Ltd. L = Budapest C = HU
Certificate Summary	Microsec issues several types of certificates under the same root but using dedicated subordinate CA-s for different certificate types. Microsec had two main reason to set up this new CA hierarchy: - the present root will expire in 2029 so Microsec is not able to issue TSA certificates under this root with 12 years validity - The present hierarchy uses mainly RSA2048 keys which may not be suitable for longer periods. The new CA hierarchy uses ECC256 keys which expected to be suitable for longer time
Root Cert URL	http://www.e-szigno.hu/rootca2017.crt
SHA-1 Fingerprint	89 d4 83 03 4f 9e 9a 48 80 5f 72 37 d4 a9 a6 ef cb 7c 1f d1
Valid from (YYYY-MM-DD)	2017-08-22
Valid to (YYYY-MM-DD)	2042-08-22
Certificate Version	v3
Certificate signature algorithm	ECDSA with SHA-256
Signing key parameters	ECC NIST Curve P-256
Test Website URL (SSL)	Valid: https:/ec3sslca2017-valid.e-szigno.hu/ Expired: https:/ec3sslca2017-expired.e-szigno.hu/ Revoked: https:/ec3sslca2017-revoked.e-szigno.hu/
Example Certificate (non-SSL)	TLS certificates are issued in this CA hierarchy, test sites are given in the point above.

CRLs	CRL URLs: http://rootca2017-crl1.e-szigno.hu/rootca2017.crl http://rootca2017-crl2.e-szigno.hu/rootca2017.crl http://rootca2017-crl3.e-szigno.hu/rootca2017.crl The value of the nextUpdate field is equal to 25 hours + thisUpdate. New CRL is issued maximum 24 hours after the last CRL issuance, but within 1 hour after the change of a revocation status. The details are written in the CPS in the sections 4.10 Certificate Status Services and 7.2 CRL Profile
OCSP	OCSP URLs: http://rootca2017-ocsp1.e-szigno.hu http://rootca2017-ocsp2.e-szigno.hu http://rootca2017-ocsp3.e-szigno.hu Microsec typically issues a new OCSP response for each OCSP request, which contains the actual revocation status information. Microsec includes the nextUpdate field in the OCSP response any may use the OCSP stapling too. The value of the nextUpdate field is equal to 12 hours + thisUpdate. New OCSP is issued maximum 6 hours after the last OCSP issuance. The details are written in the CPS in the sections 4.10 Certificate Status Services and 7.3 OCSP Profile
Request Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	DV: supported OV: supported IV: supported EV: supported (new service)
EV Policy OID(s)	2.23.140.1.1. 0.4.0.194112.1.4. 1.3.6.1.4.1.21528.2.1.1.171.2.8 (last characters depend on the CP version)

CA Hierarchy information for each root certificate

CA Hierarchy	Each Microsec hierarchy is available in our CPS at **1.3.1 Certification Authorities.** Also you can find a detailed graph about the CA hierarchy at https://e-szigno.hu/en/pki-services/ca-certificates.html . Latest, ECC based hierarchy: • "e-Szigno Root CA 2017" – Root certification unit, that issues ECC based Certificates for the Certification Units of the Trust Service Provider. This Certification Unit has a self certified (ECC based) certificate. • "e-Szigno Qualified TSA CA 2017" issues Certificates for Time Stamping Authorities. • "e-Szigno Qualified CA 2017" issues Qualified Certificates for electronic signature for natural persons on Qualified Electronic Signature Creation Device excluding pseudonym. • "e-Szigno Qualified Organization CA 2017" issues Qualified Certificates for electronic seal for legal persons on Qualified Electronic Seal Creation Device. • "e-Szigno Qualified TLS CA 2018" issues Qualified Website Authentication Certificates. • "e-Szigno Qualified QCP CA 2017" issues Certificates according to certificate policies that do not require that the private key belonging to the Certificate shall reside inside of a Qualified Electronic Signature/Seal Creation Device. Doesn't issue pseudonymous Certificates. • "e-Szigno Qualified Pseudonymous CA 2017" issues pseudonymous qualified Certificates. • "e-Szigno Class3 CA 2017" issues other than Codesigning Certificates to natural and legal persons exclusively according to the III. certification class. This unit does not issue pseudonymous Certificates. • "e-Szigno Class3 CodeSigning CA 2017" issues Codesigning Certificates to natural and legal persons exclusively according to the III. certification class. This unit does not issue pseudonymous Certificates. • "e-Szigno Class2 CA 2017" issues other than Codesigning Certificates to natural and legal persons exclusively according to the II. certification class. This unit does not issue pseudonymous Certificates. • "e-Szigno Class2 CodeSigning CA 2017" issues Codesigning Certificates to natural and legal persons exclusively according to the II. certification

	class. This unit does not issue pseudonymous Certificates. • "e-Szigno Pseudonymous CA 2017" issues pseudonymous Certificates to natural persons exclusively according to the II. and III. certification class. • "e-Szigno Online SSL CA 2017" issues only not qualified Website Authentication Certificates automatically. Certified by "e-Szigno Root CA 2017". • "e-Szigno Class3 SSL CA 2017" issues only Website Authentication Certificates and Certificates for networking authentication exclusively according to the III. certification class. • "e-Szigno Class2 SSL CA 2017" issues only Website Authentication Certificates and Certificates for networking authentication exclusively according to the II. certification class. • OCSP responders; every Certification Unit with ECC based Certificate certifies dedicated OCSP responder unit, which gives responses regarding the revocation status of the Certificates issued by the given certification unit. The OCSP responder unit's name contains the "OCSP Responder" text besides the given certification unit name. The "OCSPSigning" extended key usage is present in the OCSP responder Certificates. The aforementioned units have ECC based Certificates. Each issued enduser certificate is based on ECC-256 or RSA with at least 2048 bit key length.
Sub CAs Operated by 3rd Parties	No 3rd parties.
Cross-Signing	Not used.
Technical Constraints or Audits of Third-Party Issuers	There is no 3rd party Issuer in this CA hierarchy.

Verification Policies and Practices

Documentation	All public documents are available at: https://e-szigno.hu/en/pki-services/certificate-policies-general-terms-and-conditions/ Direct links to the actual CP & CPS: https://www.e-szigno.hu/docs/hr--fok--ssl--EN--v2.8.pdf https://www.e-szigno.hu/docs/szsz--fok--ssl--EN--v2.8.pdf The CPS is in the RFC3647 structure so any required information can be found at the corresponding section.
Audits	Audit type: ETSI EN 319 411 Auditor: TÜViT - TÜV Informationstechnik GmbH Auditor website: https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/en/AA2018121301_Microsec-eSzignoRoot-CA-2009_nonEV-CAs_s.pdf
SSL Verification Procedures	Before issuing a certificate Microsec validates the identity of the natural person, the organization (in case of OV certificates) and the authorization or control of using the requested domain. The general rules are described in the CPS in section **3.2 Initial Identity Validation.** The domain validation methods are described in section **3.2.2.2 Validation of Domain Authorization or Control**
Email Address Verification Procedures	In those certificates, where the email address may be included the CPS contains a statement in the following section: **4.2.2 Approval or Rejection of Certificate Applications** **…** If the Subject requests a Certificate containing an email address, the Service Provider verifies the email address to be indicated in the Certificate. It ascertains that the email address exists and verifies that it is the Subject's email address indeed. This statement can be found for example in the following document: https://www.e-szigno.hu/docs/szsz--fok--uni--EN--v2.8.pdf The typical email validation works as follows: When the Subscriber requests the certificate through our web form at first he shall select the type of the certificate and he shall enter his email address to be included in the certificate. Microsec sends a one time URL with limited time validity to this email address and the Subscriber shall continue the application process by using this link. Microsec includes only that email address into the certificate which were tested this way. The email validation is made in addition to the other validation processes, it does not replace any of them.
Code Signing Subscriber Verification Procedures	Not applicable.

Multi-factor Authentication	Microsec uses procedural controls as described in the **section 5.2** of the CPS Microsec manages trusted roles and only the employees of Microsec may have access to the critical systems and applications. Microsec uses dual control and separation of the duties, so one person is not able to make the critical operations alone (like certificate issuance). Each employee has a VPN certificate on a secure QSCD smartcard, and they can access the IT systems only after the PKI based authentication which request also the knowledge of the PIN code.
Network Security	Microsec follows the requirement of the Network and Certificate System Security Requirements maintained by the CABF. The main requirements are published in the CPS in the section **6.7 Network security Controls,** the details are given in the internal documents of Microsec. Microsec has an ISO 27001 IT security certificate, which is refreshed yearly.

Baseline Requirements Self Assessment

The latest version of the BR Self Assessment is attached in a separate document.

Response to Mozilla's CA Required or Recommended Practices

Publicly Available CP and CPS	Microsec supplies the complete Certification Policy (CP) and Certification Practice Statement (CPS) documents containing sufficient information to determine whether and how the CA complies with the Mozilla policy requirements. The CP/CPS documents are publicly available from the official web site of Microsec from the following link: https://e-szigno.hu/en/pki-services/certificate-policies-general-terms-and-conditions/ Direct links: CP & CPS: https://www.e-szigno.hu/docs/hr--fok--ssl--EN--v2.8.pdf https://www.e-szigno.hu/docs/szsz--fok--ssl--EN--v2.8.pdf The CPS document clearly indicates in the section 1.3.1 in subsection "Certification Units" which root and intermediate certificates and policies shall be applied to. The documents are available in digitally signed PDF format. The CP/CPS is available in Hungarian and English version. The Hungarian version may be authoritative (as that's the working language of the CA) but the CA is responsible for ensuring that the translation is not materially different from the authoritative version of the document. The CP/CPS documents are structured according to the RFC3647.
CP/CPS Revision Table	The CP/CPS documents are reviewed at least yearly and the revision is clearly indicated in the document by increasing the version number even if no other changes were made. Every CP/CPS document has a Revision Table on page 3.
CAA Domains listed in CP/CPS	Microsec checks the content of the CAA records as described in the section **4.2.2 Approval or Rejection of Certificate Applications** of the CPS. Microsec issues the requested certificate only if the CAA record is clear or it contains the following value: www.e-szigno.hu

BR Commitment to Comply statement in CP/CPS	The CPS contains the required statement in the section **1.2.1 Certificate Policies**: The Trust Service Provider conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org url. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.
Audit Criteria	ETSI EN 319 411-1 V1.2.2 (2018-04)
Complete Audit History	Microsec already has two roots included in the CCADB (one has been expired) which are regularly audited. The new root CA was set up in 2017 and was audited in 2017 and 2018. Booth audit reports are accessible on the web page of the auditor (TÜViT) and the web page of Microsec too, and they were attached to the Mozilla **Bug 1445364** Microsec new (ECC) Root Inclusion Request
Revocation of Compromised Certificates	In the CPS: **4.9.1 Circumstances for Revocation**
Verifying Domain Name Ownership	In the CPS: **3.2.2 Authentication of an Organization Identity or a Domain**
Baseline Requirements	The CPS describes which domain validation methods are used in the section **3.2.2.2 Validation of Domain Authorization or Control**
WHOIS	WHOIS information is used to obtain basic contact information about the domain owner, but this information will be verified later (or before) and further validation methods are used too.
Email Challenge-Response	Microsec uses the constructed email for the checking of the control over the requested domain as described in the CPS in section **3.2.2.2.4 Constructed Email to Domain Contact (BR 3.2.2.4.4)**

Verifying Email Address Control	In those certificates, where the email address may be included the CPS contains a statement in the following section: **4.2.2 Approval or Rejection of Certificate Applications …** If the Subject requests a Certificate containing an email address, the Service Provider verifies the email address to be indicated in the Certificate. It ascertains that the email address exists and verifies that it is the Subject's email address indeed. This statement can be found for example in the following document: https://www.e-szigno.hu/docs/szsz--fok--uni--EN--v2.8.pdf The typical email validation works as follows: When the Subscriber requests the certificate through the web form at first he shall select the type of the certificate and then he shall enter his email address to be included in the certificate. Microsec sends a one time URL with limited time validity to this email address and the Subscriber shall continue the application process by using this link. Microsec includes only that email address into the certificate which was tested this way.

DNS names go in SAN	In the CPS: **3.1.1 Types of Names** **Denomination of the Subject** … • Common Name (CN) – OID: 2.5.4.3 The name of the Subject This field contains a single IP address or FQDN that is one of the values contained in the Certificate's "Subject Alternative Names" extension. Always filled out. Only that domain name or IP address is indicated that exists and legally used by the Applicant. … **Subject Alternative Names** A "Subject Alternative Names" field is not listed as a critical extension in the Certificate. The content will be filled as follows. The "Subject Alternative Names" field always contain at least one entry. Each entry is either a "dNSName" containing the Fully-Qualified Domain Name or an "iPAddress" containing the IP address of a server. The Trust Service Provider confirms that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. The "Subject Alternative Names" field shall not contain a Reserved IP Address or Internal Name. The "dNSName" field shall not contain domain name containing underscore ("_") character. Wildcard FQDNs are permitted.

OCSP	- The OCSP service of Microsec is available through HTTP on standard port 80. - The OCSP URI-s are listed in the certificates. - Microsec supports the GET method. - OCSP response contains “good” only if the certificate was issued by that CA. - Microsec typically issues a new OCSP response for each OCSP request, which contains the actual revocation status information. Microsec includes the nextUpdate field in the OCSP response any may use the OCSP stapling too. The value of the nextUpdate field is equal to 12 hours + thisUpdate. New OCSP is issued maximum 6 hours after the last OCSP issuance. The maximum expiration time is 10 days. - Microsec issues OCSP responder certificates by using SHA-256 . - OCSP service is conform to RFC6960. The details are written in the CPS in the sections **4.10 Certificate Status Services and** **7.3 OCSP Profile**
Network Security Controls	Microsec follows the requirement of the Network and Certificate System Security Requirements maintained by the CABF. Microsec checks at least 3% of the issued TLS certificates quarterly. The main requirements are published in the CPS in the section **6.7 Network security Controls,** the details are given in the internal documents of Microsec. Microsec has an ISO 27001 IT security certificate, which is refreshed yearly.
CA Hierarchy	Microsec has an active root with multiple subordinate CA-s which issue different type of enduser certificates by using different policies. The new CA hierarchy was set up in 2017 because the present root certificate will expire in 2029. The new – ECC based – CA hierarchy is near the same as the present – RSA based – hierarchy. Please refer to the previous section, which includes a textual description of the hierarchy in the CPS. Also you can find a detailed graph about the CA hierarchy at https://e-szigno.hu/en/pki-services/ca-certificates.html .

Document Handling of IDNs in CP/CPS	Microsec supports the usage of IDN, because the Hungarian alphabet contains special characters too. Microsec uses Punycode or/and UTF8 encoding in case of these special characters depending on the requirements of the used certificate field. As part of the validation process Microsec converts all the requested domain to Punycode and checks the malicious domain values.
Usage of Appropriate Constraints	Microsec issues several types of enduser certificates under the same root but by using separate subordinate CAs. Nor the root CA neither the intermediate CAs contain EKU values. Microsec requests to set booth the serverAuth and the emailProtection EKUs in the CCADB.
Pre-Issuance Linting	Presently Microsec uses Post-Issuance Linting to reduce the number of misissuance events. All the issued TLS certificates are checked manually by using cablint before the publication of the certificate. In the near future Microsec plans to introduce the pre-issuance linting for all the TLS certificates.

Response to Mozilla's list of Forbidden or Problematic Practices

Long-lived Certificates	Microsec issues TLS certificates with two years validity. The CPS limits the validity to 825 days according to the BR: **6.3.2 Certificate Operational Periods and Key Pair Usage Periods** **End-User Certificates** subhead
Non-Standard Email Address Prefixes for DV certs	Microsec uses only the standard email adresses with the local parts which are listed in the BR section 3.2.2.4. See in the CPS: **3.2.2.2.4 Constructed Email to Domain Contact (BR 3.2.2.4.4)**
Issuing End Entity Certificates Directly From Roots	Microsec issues only OCSP and TSA certificates from the present root CA, but will issue only OCSP certificate from the new root CA. See the details in the CPS: **6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)**
Distributing Generated Private Keys in PKCS#12 Files	Microsec never generates the private key for the TLS certificates and never distributes the keys and TLS certificates in PKCS#12 files. About the key pair generation and delivery you can read more in the CPS: **6.1 Key Pair Generation and Installation**
Certificates Referencing Local Names or Private IP Addresses	Microsec never issues TLS certificates for Reserved IP Address or Internal Names. See the regulation in the CPS: **3.1.1 Types of Names** **Subject Alternative Names** subhead
Issuing SSL Certificates for .int Domains	Microsec issues Certificates only for those top level domains which can be found on the actual IANA Root Zone Database. See the regulation in the CPS: **3.2.2.2 Validation of Domain Authorization or Control**
OCSP Responses Signed by a Certificate Under a Different Root	Microsec provides OCSP service according to the RFC 6960 "authorized responder" principle, so its every certification unit certifies separately an OCSP responder, which provides information on the revocation status of the Certificates issued by that certification unit. See the details in the CPS: **4.10.1 Operational Characteristics** **Online Certificate Status Protocol (OCSP)**
Issuance of SHA-1 Certificates	Microsec doesn't issue SSL certificates using SHA-1 and there is no any valid enduser certificate using SHA-1.
Delegation of Domain / Email Validation to Third Parties	Microsec doesn't delegate any activity to 3rd parties related to the validation during the TLS certificate issuance.

Allowing External Entities to Operate Subordinate CAs	Presently Microsec doesn't allow any external entities to operate subordinate CAs which can be chained up to the Microsec root CA. If it will happen in the future, the same requirements will be applied for those CAs as the CAs operated by Microsec itself. This include the regular audit and the publication of those CAs in the CCADB too.
Generic Names for CAs	Every CA has a well distinguishable name which contains the "e-Szigno" brand name. The certificates contain the name of the company in the "O" field and the VAT number in the "OrgID" field, so Microsec can be easily identified. Seethe details in the CPS: **3.1 Naming** **3.1.1 Types of Names** **3.1.2 Need for Names to be Meaningful**
Lack of Communication With End Users	Microsec can be contacted by the Subscribers in many ways and there are several communication possibilities also for third parties who are not the customers of Microsec. The received information or incident report is processed the same way and does not depend on the legal status of the Sender.
Backdating the notBefore Date	Microsec ensures that the accuracy of its internal time source within 1 sec comparing to the official UTC time. The system time is synchronized to the UTC time at least 4 times a day. Microsec never backdates the certificates, the notBefore time is never earlier than the actual time. See in the CPS: **5.5.5 Requirements for Time-stamping of Records**
Issuer Encoding in CRL	The encoding of the Issuer field in the CRL is byte-for-byte equivalent with the encoding of the Issuer in the certificate by using the exact same string types and field contents.