CCADB Case 00001692

Case Information

CA Owner	Microsec Ltd.
Subject	Microsec Root Inclusion Request 2024-01 for "e-Szigno TLS Root CA 2023"
Case Record Type	Root Inclusion Request
Root Stores Applying To	Apple;Mozilla;Google Chrome

Case Information - Apple

Values & Benefits Statement	https://static.e-szigno.hu/docs/Apple--Values&Benefits_Statement--2025-11-28.pdf
CA Lifecycle Management	https://static.e-szigno.hu/docs/Apple--CA_Lifecycle_Management--2025-11.pdf
Linting	https://static.e-szigno.hu/docs/Apple--Linting--2025-11-28.pdf
Customer and Change Management	https://static.e-szigno.hu/docs/Apple--Customer_and_Change_Management--2025-11.pdf

Case Information - Google Chrome

Chrome Root Program Policy Agreement	True

Case Information - Mozilla

Value Statement Link (Mozilla)	https://bugzilla.mozilla.org/attachment.cgi?id=9372747 (https://bugzilla.mozilla.org/attachment.cgi?id=9372747)
Bugzilla Bug (link)	https://bugzilla.mozilla.org/show_bug.cgi?id=1873057 (https://bugzilla.mozilla.org/show_bug.cgi?id=1873057)

CA Owner Information

Company Website	https://e-szigno.hu/en/ (https://e-szigno.hu/en/)
Organizational Type	Private Corporation
Geographic Focus	Hungary, Europe
Primary Market / Customer Base	Microsec issues certificates for governmental users, banks, insurance companies, and general public.
Document Repository	https://e-szigno.hu/documents-and-policies (https://e-szigno.hu/documents-and-policies)
Document Repository Description	All services have CP and CPS documents and for several services Microsec has Disclosure Statement, which is an abstract of the CPS. In case of multipurpose roots "Microsec e-Szigno Root CA 2009" and "e-Szigno Root CA 2017", several type of certificates are issued under each of the root CAs, but from different subordinate CAs. The details can be found in each CPS document in chapter 1.3.1. All of the listed documents are relevant for each multipurpose root CA. According to the new Root Program requirements, Microsec created dedicated Root hierarchies for TLS, S/MIME and CodeSigning. For the DV and OV type of TLS certificates the following service is relevant: • eIDAS conform Certificate for Website Authentication For the EV certificates the following service is relevant: • eIDAS conform Qualified Certificate for Website Authentication The domain validation rules and other TLS related regulations can be found in these CPS documents.
Recognized CAA Domains	e-szigno.hu
Problem Reporting Mechanism	info@e-szigno.hu, https://e-szigno.hu/security-events-report
CA Address	Ángel Sanz Briz út 13. Graphisoft Park Southern Area, Building C, Budapest, Hungary, H-1033
CA Email Alias 1	ccadb_contact@microsec.hu

List of all 'Included' Root Certificates

CERTIFICATE SUBJECT COMMON NAME / CCADB NAME	SHA-256 FINGERPRINT	INCLUDED IN ROOT STORES
e-Szigno Root CA 2017	BEB00B30839B9BC32C32E4447905950641F26421B15ED089198B518AE2EA1B99	Google Chrome; Microsoft; Mozilla
e-Szigno TLS Root CA 2023	B49141502D00663D740F2E7EC340C52800962666121A36D09CF7DD2B90384FB4	Microsoft
Microsec e-Szigno Root CA 2009	3C5F81FEA5FAB82C64BFA2EAECAFCDE8E077FC8620A7CAE537163DF36EDBF378	Apple; Google Chrome; Microsoft; Mozilla

e-Szigno TLS Root CA 2023

Root Case Number: R00004174
Root Stores Applying To: Apple;Mozilla;Google Chrome

Certificate Information

Root Certificate Status	Apple: Not Included; Google Chrome: Not Included; Microsoft: Included; Mozilla: Not Yet Included
Explanation and Role	This root is dedicated to issuing exclusively TLS certificates, as required by several Root Programs.
Root Certificate Download URL	https://www.e-szigno.hu/tlsrootca2023.crt
crt.sh URL	https://crt.sh/?q=B49141502D00663D740F2E7EC340C52800962666121A36D09CF7DD2B90384FB4 (https://crt.sh/?q=B49141502D00663D740F2E7EC340C52800962666121A36D09CF7DD2B90384FB4)

Certificate Data Extracted from PEM

Subject	CN=e-Szigno TLS Root CA 2023; O=Microsec Ltd.; L=Budapest; C=HU; OrganizationIdentifier=VATHU-23584497
Issuer	CN=e-Szigno TLS Root CA 2023; O=Microsec Ltd.; L=Budapest; C=HU; OrganizationIdentifier=VATHU-23584497
Valid From (GMT)	2023/07/17
Valid To (GMT)	2038/07/17
Certificate Serial Number	00E86F187BD6396B984A49980A
SHA-1 Fingerprint	6F9AD5D5DFE82CEBBE3707EE4F4F52582941D1FE
SHA-256 Fingerprint	B49141502D00663D740F2E7EC340C52800962666121A36D09CF7DD2B90384FB4
Signature Hash Algorithm	ecdsaWithSHA512
Public Key Algorithm	EC secp521r1
SPKI SHA256	47487900A1BEB9EE08CCBC1116A8EC55F454B638994319F051B984023CED6423
Subject + SPKI SHA256	C7409B514E0E5C75D667813CFF982EE939A2BB216E00C5BA89374A9DB31F7E95

Key Generation

Key Generation Date	2023/06/07
Key Generation Audit Report Date	2023/06/07
Key Generation Audit Report	https://bugzilla.mozilla.org/attachment.cgi?id=9371119 (https://bugzilla.mozilla.org/attachment.cgi?id=9371119)

Pertaining to Certificates Issued by this CA

Full CRL Issued By This CA	http://crl.e-szigno.hu/tlsrootca2023.crl (http://crl.e-szigno.hu/tlsrootca2023.crl)
JSON Array of Partitioned CRLs	

CA Hierarchy Information

Cross-Signed by another Root Cert?	No
Cross Signed by Another CA Operator?	No
Has Externally Operated SubCAs?	No
CP/CPS allows Ext Operated SubCAs?	No
Has External Registration Authorities?	No
CP/CPS allows External RAs?	No
Description of PKI Hierarchy	The hierachy contains the following Subordinate CA units: - e-Szigno Qualified TLS CA 2023 for issuing exclusively EV and QWAC certificates - e-Szigno OV TLS CA 2023 for issuing exclusively OV and IV certificates - e-Szigno DV TLS CA 2023 for issuing exclusively DV certificates
Intended Use Case(s) Served	Server Authentication (TLS) 1.3.6.1.5.5.7.3.1;Client Authentication 1.3.6.1.5.5.7.3.2
CA/B Forum Certificate Policy Identifier	extended-validation 2.23.140.1.1;domain-validated 2.23.140.1.2.1;organization-validated 2.23.140.1.2.2
TLS Certificate Domain Validation Method	3.2.2.4.7 DNS Change;3.2.2.4.18 Agreed-Upon Change to Website v2;3.2.2.4.19 Agreed-Upon Change to Website - ACME;3.2.2.5.1 Agreed-Upon Change to Website;3.2.2.5.3 Reverse Address Lookup

Test Websites

Test Website - Valid	https://eqtlsca2023-valid.e-szigno.hu (https://eqtlsca2023-valid.e-szigno.hu)
Test Website - Expired	https://eqtlsca2023-expired.e-szigno.hu (https://eqtlsca2023-expired.e-szigno.hu)
Test Website - Revoked	https://eqtlsca2023-revoked.e-szigno.hu (https://eqtlsca2023-revoked.e-szigno.hu)

Test Results

Revocation Tested	TESTED, OK
CA/Browser Forum Lint Test	TESTED, OK
EV Tested	NOT APPLICABLE

Audit Statements

Audit Firm	Hunguard
Audit Firm Location	Hungary

Standard Audit

Standard Audit	https://www.hunguard.hu/wp-content/uploads/2025/12/Attestation_letter_011_standard_v10_ds.pdf (https://www.hunguard.hu/wp-content/uploads/2025/12/Attestation_letter_011_standard_v10_ds.pdf)
Type	ETSI EN 319 411
Statement Date	2025/12/05
Period Start Date	2024/09/10
Period End Date	2025/09/09

BR Audit

BR Audit	https://www.hunguard.hu/wp-content/uploads/2025/12/Attestation_letter_011_TLS-BR_v10_ds.pdf (https://www.hunguard.hu/wp-content/uploads/2025/12/Attestation_letter_011_TLS-BR_v10_ds.pdf)
Type	ETSI EN 319 411
Statement Date	2025/12/05
Period Start Date	2024/09/10
Period End Date	2025/09/09

EV Audit

EV Audit	https://www.hunguard.hu/wp-content/uploads/2025/12/Attestation_letter_011_TLS-EV_v10_ds.pdf (https://www.hunguard.hu/wp-content/uploads/2025/12/Attestation_letter_011_TLS-EV_v10_ds.pdf)
Type	ETSI EN 319 411
Statement Date	2025/12/05
Period Start Date	2024/09/10
Period End Date	2025/09/09

Non-Audit Documents

Document Type	CP/CPS
Document Link	https://static.e-szigno.hu/docs/hrsz--all--ssl--EN--v3.18.pdf
Effective Date	2025/12/22
Associated Trust Bits	Server Authentication;OCSP Signing
Version	
Policy Identifiers	0.4.0.194112.1.4; 0.4.0.2042.1.6; 0.4.0.2042.1.7; 2.23.140.1.1; 2.23.140.1.2.1; 2.23.140.1.2.2
Comments	Covers only dedicated TLS roots. Dedicated TLS roots issue only website authentication certificates with serverAuth EKU only.

Document Type	MD/AsciiDoc CP/CPS
Document Link	https://github.com/microsec/regulations/releases/download/v3.18/hrsz--all--ssl--EN.md
Effective Date	2025/12/22
Associated Trust Bits	Server Authentication;OCSP Signing
Version	
Policy Identifiers	0.4.0.194112.1.4; 0.4.0.2042.1.6; 0.4.0.2042.1.7; 2.23.140.1.1; 2.23.140.1.2.1; 2.23.140.1.2.2
Comments	Covers only dedicated TLS roots. Dedicated TLS roots issue only website authentication certificates with serverAuth EKU only.

Document Type	Self-Assessment
Document Link	https://docs.google.com/spreadsheets/d/1FBSiOGKDORmX31AQCc9J5j7C7vN0XLTLJ_8XOD0Wa_o/edit?gid=207711376#gid=207711376
Effective Date	2025/12/01
Associated Trust Bits	
Version	
Policy Identifiers	
Comments	

Application Information - Apple

Apple Certificate Request Status	
Replacing a Certificate?	False
SHA-256 Hash of the Cert being Replaced	
Certificate Replacement Date	
CA Owner Operating?	Yes
Apple Trust Bits	serverAuth
Apple EV Enabled	False
Apple EV Policy OID(s)	
Apple Applied Constraints	

Application Information - Google Chrome

Replacing an existing Cert in CRS?	False
SHA-256 Hash of the Cert being Replaced	
Removal date for existing cert from CRS	
Does the CA Owner operate this CA?	Yes
EV Treatment Requested?	

Application Information - Mozilla

Mozilla Certificate Request Status	Pending Approval
Mozilla Trust Bits	Websites
Mozilla EV Policy OID	
Mozilla Applied Constraints	