Inhalt

1Information checklist for CAs applying for inclusion in Mozilla

1.1 General information about the associated organization of the CA

1.1.1 Company Name

Atos

1.1.2 Website URL

https://pki.atos.net/TrustedRoot/

1.1.3 Organizational type

Private Corporation

1.1.4 Primark Market / Customer Base

Atos Trustcenter acts in Europe, but also has international customers.
The PKI-Services are offered to the Public, with no restrictions to user groups.

1.1.5 Impact to Mozilla Users

Client-CA

- Digitally sign messages or files to confirm the authorship and enable to verify if the signed messages or files have not been changed or corrupted.
- Digitally encrypt messages or files to keep them confidential.
- Usage in client authentication tools for secure identification and authorization.

SSL-CA

- Authentication of a domain name and encryption of the communication channel to a webserver.

CodeSigning-CA

- Confirm the author of software.
- Enable to confirm that the software has not been changed or corrupted.

1.1.6 CA Contact Information

CA Email Alias:

gmde-trustcenter@atos.net

CA Phone Number:
+49 5931 805 0

Title / Department:
Atos Trustcenter

1.2 Technical information about each root certificate

1.2.1 Certificate Name

Atos TrustedRoot 2011
CN=Atos TrustedRoot 2011, O=Atos, C=DE

1.2.2 Certificate Issuer

CN=Atos TrustedRoot 2011, O=Atos, C=DE

1.2.3 Certificate Summary

The hierarchy of the Atos TrustedRoot consists of one Root, which issues three types of CAs for different purposes:

1. AO SSL Server CA
2. AO Client CA
3. AO CodeSigning CA

1.2.4 Root Cert URL

https://pki.atos.net/certs/Atos_TrustedRoot_2011.pem
https://pki.atos.net/certs/Atos_TrustedRoot_2011.cer

1.2.5 SHA1 Fingerprint

2b b1 f5 3e 55 0c 1d c5 f1 d4 e6 b7 6a 46 4b 55 06 02 ac 21

1.2.6 Valid From

2011-07-07

1.2.7 Valid To

2031-01-01

1.2.8 Certificate Version

V3

1.2.9 Certificate Signature Algorithm

sha256RSA

1.2.10 Signing key parameters

2048 bit

1.2.11 Test Website URL (SSL)

https://pki.atos.net:7081/

1.2.12 Example Certificate (non-SSL)

As attachment

1.2.13 CRL URL

https://pki.atos.net/crl/Atos_TrustedRoot_CA_2011.crl
The ‘nextUpdate’ field will be set to issue time + 1 day in the CRLs.

The CRLs will be reissued when the old one is about to expire. The CRL Overlap Time is set to 10 minutes so that a new CRL will be issued after 23h50m.
The test to import our CRLs into the Firefox browser was successfully.

1.2.14 OCSP URL

http://pki-ocsp.atos.net

1.2.15 Requested Trust Bits

- Websites (SSL/TLS)
- Email (S/MIME)
- CodeSigning

1.2.16 SSL Validation Type

The following levels of SSL validation are used for certificates within this root's hierarchy:

- DV
- OV

1.2.17 EV Policy OID(s)

EV certificates are not issued.

1.3 CA Hierarchy information for each root certificate

1.3.1 CA Hierarchy

- RootCA: Atos TrustedRoot 2011 (CN=Atos TrustedRoot 2011, O=Atos, C=DE)
    - SubCA: Atos TrustedRoot Client-CA 2011
        - CN=Atos TrustedRoot Client-CA 2011, O=Atos, C=DE
    - SubCA: Atos TrustedRoot Server-CA 2011
        - CN=Atos TrustedRoot Server-CA 2011, O=Atos, C=DE
    - SubCA: Atos TrustedRoot CodeSigning-CA 2011
        - CN=Atos TrustedRoot CodeSigning-CA 2011, O=Atos, C=DE

All subordinate CAs are internally-operated.

1.3.2 Externally Operated SubCAs

All SubCAs are internally.

1.3.3 Cross-Signing

No Cross-Signing.

1.3.4 Technical Constraints or Audits of Third-Party Issuers

No Third-Party Issuer.

1.4 Verification Policies and Practices

1.4.1 1. Documentation

https://pki.atos.net/TrustedRoot/

This CPS describes the organization, the processes and the security level of all Public Key Infrastructure (PKI) services provided by the Atos Trusted CA. It is intended that this CPS covers the requirements as specified by the ETSI specification TS 102 042 "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates". The structure of this CPS is equivalent to the structure of RFC3647. The RFC3647 suggests an optional Certificate Policy document (CP). A CP is not implemented for the Atos Trusted CA because all relevant information are part of this CPS.

1.4.2 Audits

Audit Type: ETSI TS 102 042 v2.1.2 (2010-04)
Auditor: DQS Holding GmbH
Auditor Website: https://de.dqs-ul.com
URL to Audit Report and Management's Assertions:
https://de.dqs-ul.com/kunden/kundendatenbank.html?aoemydqs%5Bcompany_no%5D=334220&aoemydqs%5Baction%5D=singleView&cHash=c086db2a2cd03a17407d1f2712ab2dd4

1.4.3 SSL Verification Procedures

See chapter 4.2 (Initial identity validation / page 17ff) at Atos Trustcenter CPS.

After the request was created by a customer, an email will be send to the email address given in the certificate. The email contains a system generated one-time-password, which the customer has to use to activate the certificate request.

Work instructions for RA employee:

- Check Identification

#	STEP	CHECK
1	Is the requester a natural or juristic person	Is the requester a natural or juristic person? If it is a natural person go to step 2, otherwise to step 5.
2	Check for a valid representation	Is the requester a representation of the juristic person (organisation), is the authority available If yes, go to step 3, otherwise to step 11.
3	Analysis of a juristic person	Does the juristic person exists? (Check the Commercial Registry) If yes, go to step 4, otherwise to step 11.
4	Check authority for representation	On - first request of an applicant or - an unknown representations or - an abnormal bulk of certificate requests or

		- variations of the ‚normal' day-to-day business or - a request for a high-profile domain name the RA-employee have to obtain a re-insurance from the issuer of the authority. Is the requester authorized to do the request? If yes, go to step 5, otherwise to step 11.
5	Check the person	Check the identity card of the requester. Go to step 8.
6	Check validity date of identity card	Is the identity card valid? If yes, go to step 9, otherwise to step 11.
7	Check the adress	Is there a valid address on the identity card (Check against telephone directory, Google Maps etc.)? If yes, go to step 10, otherwise to step 11.
8	Check the personal data	Does the identity of the requester consistent with the information in the formular? If yes, go to step 1 in table 'check certificate request', otherwise to step 11.
9	Abort	You have to cancel he request.

- Check certificate request

#	STEP	CHECK
1	Check Top Level Domain-Name	Is there a Top Level Domain-Name given in the request ? If yes, go to step 2, otherwise to step 9.
2	Check Top Level Domain-Registration	Is the Top Level Domain registered at DENIC (www.denic.de) or IANA (www.iana.com)? If yes, go to step 3, otherwise to step 9.
3	Check Organisation Name	Does the organization name of Domain-Registration match the given one in the certificate request? If yes, go to step 4, otherwise to step 9.
4	Check Commercial Registry	Is the organization with the given information (Name, Address, etc.) registered in the Commercial Registry? If yes, go to step 5, otherwise to step 9.
5	Check contact information	Are the requests contact information valid? If yes, go to step 6, otherwise to step 9.
6	Check email address	Does the email adress' domain name match the requested domain name? If yes, go to step 7, otherwise to step 9.
7	Check SAN	Are all DNS names given in SAN? If yes, go to step 8, otherwise to step 9.
8	Save data	Save all the data and accept the request.
9	Abort	You have to cancel he request.

1.4.4 Email Address Verification Procedures

See chapter 4.2 (Initial identity validation / page 17ff) at Atos Trustcenter CPS.

After register a new account at the Website an email with a system generated one-time-password will be send to the given mail address. The customer has to activate the service with this password. After this procedure the customer could create certificate request for this email address only.

Look also at the table 'Check Identification' in section SSL Verification Procedures to identify the requester.

1.4.5 Code Signing Subscriber Verification Procedures

See chapter 4.2 (Initial identity validation / page 17ff) at Atos Trustcenter CPS.

Look at section SSL Verification Procedures

1.4.6 Multi-factor Authentication

The RA system for certificate issuance is protected twice. First the system is accessible from a DMZ in the Atos intranet only, so that only Employees of Atos Trustcenter have network access. The other protection is a multi-factor authentication with hardware token for Atos Trustcenter employees (RA), so only specified persons could login to the RA system to cause issuance of certificates.

1.4.7 Network Security

See chapter 7 (Technical security controls / page 37ff) at Atos Trustcenter CPS.

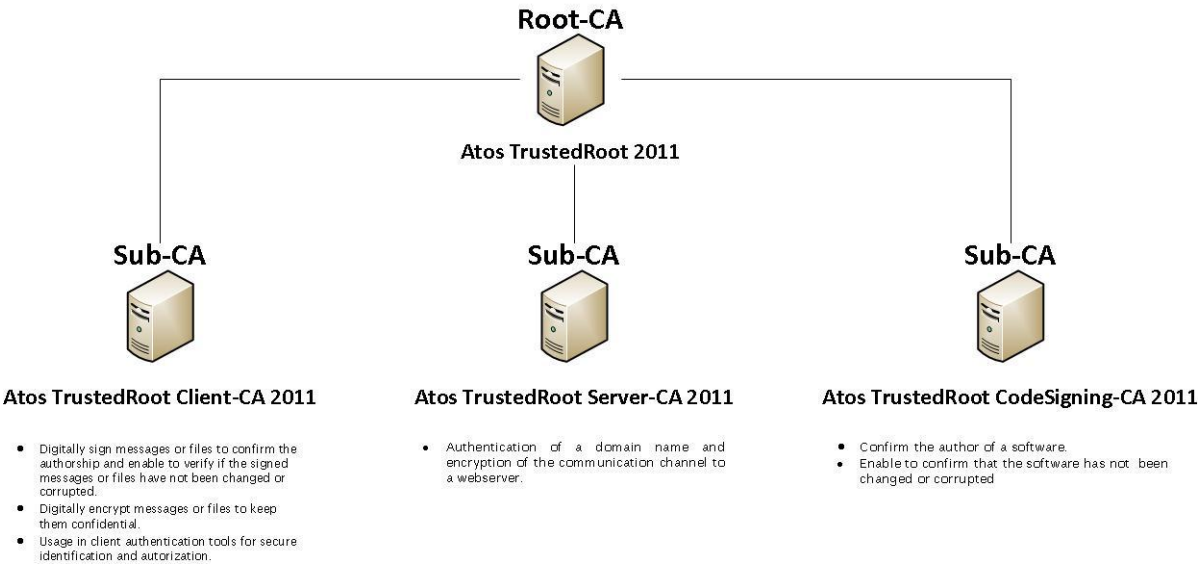
1.5 Response to Mozilla's CA Recommended Practices

1.5.1 Publicly Available CP and CPS

CPS is can be downloaded from the CAs website.
https://pki.atos.net/TrustedRoot/

This CPS describes the organization, the processes and the security level of all Public Key Infrastructure (PKI) services provided by the Atos Trusted CA. It is intended that this CPS covers the requirements as specified by the ETSI specification TS 102 042 “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”. The structure of this CPS is equivalent to the structure of RFC3647. The RFC3647 suggests an optional Certificate Policy document (CP). A CP is not implemented for the Atos Trusted CA because all relevant information are part of this CPS.

1.5.2 CA Hierarchy



1.5.3 Audit Criteria

The Atos Trustcenter was evaluated against the ETSI specification TS 102 042 “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”.

The documents of the auditor are available at:
https://de.dqs-ul.com/kunden/kundendatenbank.html?aoemydqs%5Bcompany_no%5D=334220&aoemydqs%5Baction%5D=singleView&cHash=c086db2a2cd03a17407d1f2712ab2dd4

1.5.4 Document Handling of IDNs in CP/CPS

Look at table ‘Check identification’ in section 1.5.6

1.5.5 Revocation of Compromised Certificates

See chapter 5.9 (Certificate revocation and suspension / page 26f / item 121) at Atos Trustcenter CPS.

1.5.6 Verifying Domain Name Ownership

Look at section SSL Verification Procedures

1.5.7 Verifying Email Address Control

Look at section Email Address Verification Procedures

1.5.8 Verifying Identity of Code Signing Certificate Subscriber

Look at section Code Signing Subscriber Verification Procedures

1.5.9 DNS names go in SAN

See work instructions for certificate request (point 7) in section SSL Verification Procedures

1.5.10 Domain owned by a Natural Person

See work instructions for check identification in section SSL Verification Procedures

1.5.11 OCSP

The OCSP services launches on port 80 at pki-ocsp.atos.net.
URL: http://pki-ocsp.atos.net
The service was tested in Firefox successfully without errors.

1.6 Response to Mozilla's list of Potentially Problematic Practices

1.6.1 Long-lived DV certificates

The Atos Trustcenter actually only creates or accepts certificates with a duration of one or two years.

1.6.2 Wildcard DV SSL certificates

For wildcard certificates, the RA employee gets a hint before he can do the issuance of the certificate. The employees are instructed to accept only wildcard SSL certificates to subscribers whose actual identity has been validated with organizational validation (OV).

1.6.3 Email Address Prefixes for DV Certs

For domain-validated SSL certificates we now use an email challenge-response mechanism to verify that the SSL certificate subscriber owns/controls the domain to be included in the certificate.
We limit the set of verification addresses to the set given in your Problematic Practices:

- admin@domain
- administrator@domain
- webmaster@domain
- hostmaster@domain
- postmaster@domain
- Plus any address listed in the technical or administrative contact field of the domain's WHOIS record, regardless of the addresses' domains.

1.6.4 Delegation of Domain / Email validation to third parties

The Atos Trustcenter doesn't delegate domain or email validation to third parties.

1.6.5 Issuing end entity certificates directly from roots

Certificates are only issued by the SubCAs.

1.6.6 Allowing external entities to operate subordinate CAs

The Atos Trustcenter doesn't allow external entities to operate as a subordinate CA.

1.6.7 Distributing generated private keys in PKCS#12 files

The CA only generates the key pairs for encryption certificates.
After generating the key pairs the user can download the P12-File from our web service. The user have to login with his username and password, which he has defined at his registration. Our web service only interacts over https and the P12-File is protected with the users password.

1.6.8 Certificates referencing hostnames or private IP addresses

If a SSL certificate request contains an IP address or a not resolvable hostname, the RA employee gets a hint and he is instructed to check the addresses manually.
Like described in your Problematic Practices the IP address belongs to the provided field in the Subject Alternative Names extension.

1.6.9 Issuing SSL Certificates for Internal Domains

If a SSL certificate request which contains not allowed TLDs or null characters in the Common Name and subjectAlternativeName the RA employee gets a hint before he can do the issuance of the certificate.

Further there is an automatic check against allowed TLDs that are eligible to be used for domains in certificates issued within your CA hierarchy

1.6.10 OCSP Responses signed by a certificate under a different root

The OCSP response will be signed by a certificate of a SubCA of our RootCA and was tested with the Firefox web browser successfully.

1.6.11 CRL with critical CIDP Extension Generic names for CAs

The Atos Trustcenter creates full CRLs and doesn't put critical CIDP extensions into it

1.6.12 Generic names for CAs

The common name (CN) of the RootCA and SubCAs contains our company name and a hint to his responsibility.

- CN=Atos TrustedRoot 2011
    - CN=Atos TrustedRoot Client-CA 2011
    - CN=Atos TrustedRoot Server-CA 2011
    - CN=Atos TrustedRoot CodeSigning-CA 2011

All certificates contains our company name in organization (o).

- O=Atos

1.6.13 Lack of Communication with End Users

Our Atos Trustcenter is always contactable by email (gmde-trustcenter@atos.net) for everyone.
We accept and act upon every complaints.