Bugzilla ID: 711366
Bugzilla Summary: Add Atos Trustcenter CA cert to trusted root CA cert list

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Atos
Website URL	https://pki.atos.net/TrustedRoot/
Organizational type	Private Corporation
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.
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.
CA Contact Information	CA Email Alias: gmde-trustcenter@atos.net CA Phone Number: +49 5931 805 0 Title / Department: Atos Trustcenter

Technical information about each root certificate

Certificate Name	Atos TrustedRoot 2011
Certificate Issuer Field	CN=Atos TrustedRoot 2011, O=Atos, C=DE
Certificate Summary	This root signs three types of internally-operated intermediate certificates for issuing SSL server, client, and code signing certificates.
Root Cert URL	https://pki.atos.net/certs/Atos_TrustedRoot_2011.cer
SHA1 Fingerprint	2B:B1:F5:3E:55:0C:1D:C5:F1:D4:E6:B7:6A:46:4B:55:06:02:AC:21
Valid From	2011-07-07
Valid To	2030-12-31
Certificate Version	3
Cert Signature Algorithm	sha256RSA
Signing key parameters	2048 bits
Test Website URL	https://pki.atos.net:7081/

CRL URL	https://pki.atos.net/crl/Atos_TrustedRoot_CA_2011.crl http://pki.atos.net/crl/Atos_TrustedRoot_Server_CA_2011.crl (NextUpdate: 24 hours) CPS section 3.3: CRLs are published at least every 24 hours.
OCSP URL	http://pki-ocsp.atos.net
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV
EV Policy OID(s)	Not EV

CA Hierarchy information for each root certificate

CA Hierarchy	Currently the internally-operated subCAs are: - Atos TrustedRoot Client - CA 2011 - Atos TrustedRoot Client - CA 2012 - Atos TrustedRoot Server - CA 2011 - Atos TrustedRoot CodeSigning - CA 2011
Externally Operated SubCAs	None
Cross-Signing	None
Technical Constraints on Third-party Issuers	No third-party issuers Comment #8: No RA is issuing certificates on behalf of Atos Trusted Root and it is not intended to do this in the future. RAs are only be used to register subscribers but not to issue certificates. For this Atos Trusted Root will perform the following steps: 1) The RA will have a signed contract with Atos. Part of this contract is the CPS in the then-current version, corresponding Work-instructions and Security Requirements. 2) The RA has to agree to act according to the paragraphs of this documents. 3) Periodic audits by Atos Trusted Root will be done to verify that. 4) Those audits will be scheduled in the list Periodical Checks (in German: "Regelmäßige Prüfungen"), which is an attachment to the IT security concept of Atos Trusted Root.

Verification Policies and Practices

Policy Documentation	CPS (English): https://pki.atos.net/EJPKI-WebFrontend/Public/TrustedRoot/Download?File=AtosTrustedCA_CPS_v1.5.pdf Subscriber Agreement: https://bugzilla.mozilla.org/attachment.cgi?id=582228
Audits	Audit Type: ETSI TS 102 042 v2.1.2 (2010-04) Auditor: DQS Holding GmbH, https://de.dqs-ul.com ETSI Certificate: https://de.dqs-ul.com/kunden/kundendatenbank.html?aoemydqs%5Bcompany_no%5D=334220&aoemydqs%5Baction%5D=singleView&cHash=c086db2a2cd03a17407d1f2712ab2dd4 (2011.04.14) Statement of recent surveillance audit: https://bugzilla.mozilla.org/attachment.cgi?id=635650 (06.06.2012) Comment #8: Annual audits are requirements which derive directly from the ETSI-certification. Therefore they are not explicitly mentioned in the CPS. Annual audits (internal and external) are scheduled in the list Periodical Checks (in German: "Regelmäßige Prüfungen"), which is an attachment to the IT security concept of Atos Trusted Root.

Organization Verification Procedures	CPS chapter 4.2: The identity of an applicant is verified for the different CAs with different evidences: · [SSL-CA]: AO collects the necessary evidences for the verification of the subject's identity, requesting an AO SSL Server CA certificate. More details see statement 77. · [Client-CA]: AO collects the necessary evidences either directly for the verification of the subject's identity, requesting an AO Client CA certificate. Alternatively there exists a registration authority authorized by the CA and operating according to a contractual agreement which is offered to a specific group of subscribers. The registration authority collects the evidences for the verification of the subject's identity belonging to this group of subscribers. More details see statements 69, 73, 74 and 75. · [CodeSigning-CA]: AO collects the necessary evidences for the verification of the subject's identity, requesting an AO CodeSigning CA certificate. More details see statement 76.
SSL Verification Procedures	CPS chapter 4.2, statement 77: A legal entity, represented by a device or system, which requests a certificate is identified and authenticated for the first time via the subject's name of the certificate: - The device or system possesses an Internet Domain name, and a registration as Top Level Domain (which can be found for Germany with www.denic.de or international with www.iana.com), where the registered full name of the legal entity is registered and this matches the subject's full name. - The legal's entity full name matches the subject's name in the certificate. - The existence of the legal entity is evident from an excerpt from the commercial register (certificate of registration, in Germany: Handelsregisterauszug). Atos_ca_Information_v1.1.pdf: 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. 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
Email Address Verification Procedures	CPS chapter 4.2, statements 69, 73, 74, 75. Statement 75: In addition to the personal identification and authentication a representative has to provide: - Evidence that he or she is authorized by the legal entity to request a certificate (the name of the person is included in the certificate as the subject) for it - Evidence of the existence of the legal entity in form of -- an excerpt from the commercial register (certificate of registration, in Germany: Handelsregisterauszug), or -- a registration of a Top Level Domain (which can be found for Germany with www.denic.de or international with www.iana.com) Atos_ca_Information_v1.1.pdf: 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 CPS section 3.1: Upon generation, the subscriber gets a notice via email, that the complete and accurate certificate is issued and can be downloaded by the subscriber.

Code Signing Subscriber Verification Procedures	CPS chapter 4.2: AO collects the necessary evidences for the verification of the subject's identity, requesting an AO CodeSigning CA certificate. More details see statement 76. Statement 76: A legal entity requesting a certificate is identified and authenticated for the first time via the subject's name of the certificate: - The legal's entity full name matches the subject's name in the certificate. - The existence of the legal entity in form is evident with either -- an excerpt from the commercial register (certificate of registration, in Germany: Handelsregisterauszug), or -- a registration as Top Level Domain (which can be found for Germany with www.denic.de or international with www.iana.com), where the registered full name of the legal entity is registered and it matches the subject's full name. Question: Where does it say how it is verified that the certificate subscriber is authorized by the organization to request the code signing certificate? Comment #8: This is part of the work instruction document for our trustcenter employees that handles the identification procedure. It is the same procedure like SSL certificate request check, described in our "information checklist" (section 1.4.2 table 1 & 2 / especially table 1 step 2).
Work instructions for RA employee	Check Identification: 1 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 address. 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: 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.
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.
Network Security	See CPS chapter 7, Technical security controls.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	Yes
CA Hierarchy	Yes
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	Look at table "Check identification" in CPS section 1.5.6. Comment #8: We are on implmenting a new IDN check in our pki portal. At a new SSL certification request the system will generate the punycode (RFC 3492) of the requested domain name. While the trustcenter employee checks the reuqest, he has to type the domain name into an input textfield (copy&paste is not allowed/available). The punycode of this input will be generated too and compared with the first code. On mismatch the trustcenter employee gets a hint and has to check the domain name manually in detail, because there could be an issue of homographic spoofing.
Revocation of Compromised Certificates	See chapter 5.9 (Certificate revocation and suspension / page 26f / item 121) at Atos Trustcenter CPS.
Verifying Domain Name Ownership	Yes. See above.
Verifying Email Address Control	Yes. See above.
Verifying Identity of Code Signing Certificate Subscriber	Yes. See above.
DNS names go in SAN	Yes. See above.
Domain owned by a Natural Person	Yes. See above.
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.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	The Atos Trustcenter actually only creates or accepts certificates with a duration of one or two years.
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).

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.
Delegation of Domain / Email validation to third parties	CPS section 2.2.2: The registration authority performs the identification and authentication of end certificate applicants. Subordinate organizations within or a dedicated group of authorized employees of a larger organization can act as RAs for the CA serving the entire organization, but RAs may also be external to the CA. CPS section 4.2: AO collects the necessary evidences either directly for the verification of the subject's identity, requesting an AO Client CA certificate. Alternatively there exists a registration authority authorized by the CA and operating according to a contractual agreement which is offered to a specific group of subscribers. The registration authority collects the evidences for the verification of the subject's identity belonging to this group of subscribers. More details see statements 69, 73, 74 and 75. … Alternatively – if there is a contract for a group of subscribers, of which the specific subject is a member of - the subject appears in person at the appropriate registration authority. An employee of the registration authority assures in written or electronic form that the subject requesting a certificate has the claimed identity. In this case the evidence is checked indirectly against a physical person.
Issuing end entity certificates directly from roots	Certificates are only issued by the SubCAs.
Allowing external entities to operate subordinate CAs	The Atos Trustcenter doesn't allow external entities to operate as a subordinate CA.
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.
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.
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

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.
CRL with critical CIDP Extension	The Atos Trustcenter creates full CRLs and doesn't put critical CIDP extensions into it
Generic names for CAs	The common name (CN) of the RootCA and SubCAs contains our company name and a hint to his responsibility.
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.