EVIDEN
an atos business

Atos Trustcenter

Server Certificates + Code Signing Certificates

Version 1.5

26.04.2023

Content

1 Introduction

The Atos Trustcenter covers the whole bandwidth of PKI-services. They range from registration and certification to deployment and publication of the certificates via directories. The certificates can be deployed according to the imposed requirements on smartcard, USB-stick, MicroSD card or as software certificate.

The Trustcenter team also offers consulting and implementation projects using its experiences from the PKI-Projects that the team itself operates.

Flexibility and the possibility of dwelling on the customers' demands are the special strong points of Atos' Trustcenter, whose base is formed by the continuously self-developed software products – e.g. certification, management of certificates and request tracing – which can flexibly be adapted to the customer's needs.

2 The Atos Trustcenter Portfolio

The Atos Trustcenter renders all certification services from a single source.

- End-user, SSL Server certificates, Code Signing certificates (internally or publicly trusted)
- Smartcard/USB-token/MicroSD card or software solution
- Directory services (LDAP, OCSP)
- Certificate management via SCEP, REST or ACME
- Web based registration service and request tracing
- Revocation services (CRL)
- Helpdesk, training
- PKI conception & consulting
- Evaluation and product testing
  (e.g. CA- & Directory-products as well as client products)

The Trustcenter systems are operated in ISO27001-certified data center of Atos in Germany. In addition the Trustcenter operates an ETSI certified TrustedRoot CA which is trusted by default in the products of all major browser vendors.

According to the customer demands selected task areas may remain at the customer, e.g. managing of the registration service. It is also possible to issue CA-certificates.

Atos Trustcenter has implemented different PKI infrastructures. Organizational workflows for the request processing were defined and documented in operational manuals and descriptions of proceedings.

The administrative tasks are taken care of with the help of modern, database-driven software. Besides the registration of requests they also include the pre and post verification of the request data and the certification contents together with a signature verification.

Via web-based request tracing the customer may check the request's actual status and download the certificate.

3 TrustedRoot PKI

3.1 Atos TrustedRoot CA

Beside customer specific PKI services, Eviden operates an ETSI certified Trusted-Root CA, the "Atos TrustedRoot CA", which is publicly being recognized as trusted by the major browser vendors.

The TrustedRoot CA is used to issue the following kinds of certificates to Eviden customers:

- Client certificates to sign or encrypt content or to authenticate a user
- Server certificates to authenticate systems and to establish secure end-to-end connection
- Codesigning certificates to sign software components

3.2 TrustedRoot Hierarchy

The different types of certificates are issued by some subordinate CAs of the Atos Trusted Root CA:

- The "Atos TrustedRoot Client-CA" issues User Certificates (SMIME/Auth/DocSigning).
- The "Atos TrustedRoot Server CA" issues SSL/TLS Server Certificates.
- The "Atos TrustedRoot CodeSigning CA" issues Code Signing Certificates.

The following picture depicts the hierarchy of the Atos TrustedRoot CA and its subordinate CAs.

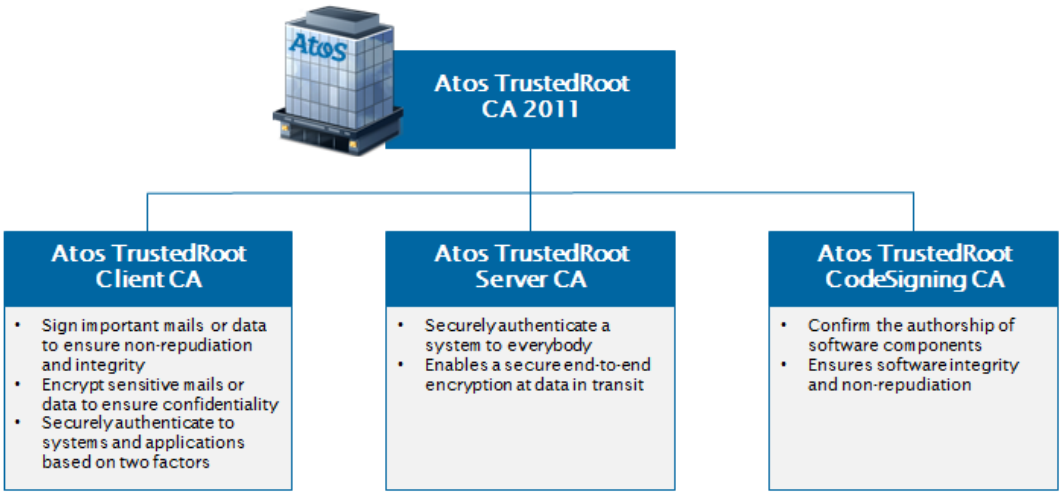

Figure 1: TrustedRoot CA Hierarchy

Eviden also operates a non TrustedRoot CA designed and operated in a similar fashion which is used to issue certificates for non-public / company-internal usage. In addition, it is possible to define customer specific Issuing Cas.

3.3 PKI-Portal

To request and manage the different kinds of certificates, the Atos Trustcenter provides a web-based portal (“PKI-Portal”) for its customers. Based on the role of a user, the portal enables users to request, approve, download, install, revoke or manage own certificates in a self-service.

3.4 Browser integration

The Atos TrustedRoot CA is accepted as “Trusted Root” by the most common following certstores / browser vendors:

- Microsoft / Windows / Internet Explorer
- Mozilla / Linux / Firefox
- Google / Android / Chrome

This acceptance process is in progress at Apple, Adobe and Oracle.

The Atos Trustcenter is certified regarding ETSI EN 319 401 + 411 and all “Trusted Root” activities are in line with this standard.

4 PKI Service for Server Certificates

The Atos Trustcenter offers a service to its customer for requesting server certificates signed by the Atos TrustedRoot CA respectively its subordinate Cas. The following sections describe this service in more detail.

4.1 Initial registration

The PKI service for server certificates is provided using the PKI-Portal of the Atos Trustcenter. Registered users are able to requests certificates for registered domains of the customers. These admin users, domains and the customers tenant itself have to be registered and configured in the portal, prior to usage.

The initial registration and tenant configuration comprises the following steps:

- the customer has to be registered:
  - he has to sign the subscriber agreement
  - the customers identity has to be verified
  - a new tenant is configured in the PKI portal
- the customers domains have to be registered:
  - the ownership of each domain is checked
  - the domains are configured in the PKI portal
- admin users have to be configured:
  - the identity of each user is checked

New domains and/or admin users may be added at any time later on.

4.2 Request process overview

As soon as the initial tenant configuration has been done, authorized users may request server certificates for registered domains of the customer using the PKI-Portal. If the domain has already been registered and verified successfully, the certificates will be issued immediately.

The default process to request a server certificate comprises the following steps (see picture below):

1. A user in need of a certificate creates a certificate request and sends it to some privileged user. This is a customer specific process, e.g. by mail.
2. The privileged admin user approves the request and triggers the certification process using the PKI-Portal.
3. The request is checked and afterwards the certificate is issued immediately.
4. A link pointing to a download page for the new certificate is send to the contact person (as mentioned in the request filed by the admin user).
5. Admin users are always able to view and manage all certificates (e.g. to revoke certificates) or to check the status of a request

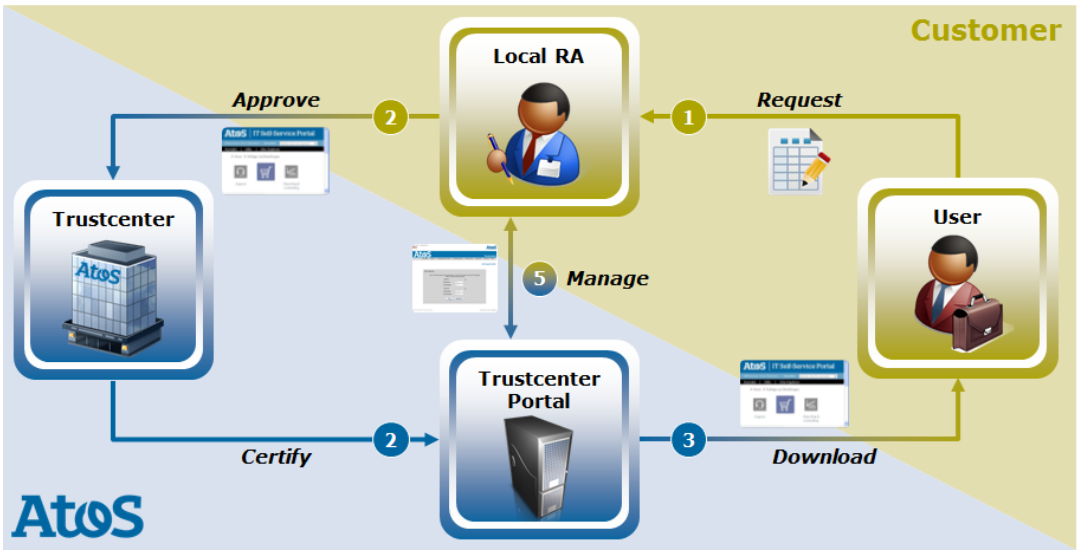

Figure 2: Request process

All processes within the PKI portal may be adapted according to customer needs.

4.3 Certificates and Validity

The following types of server certificates may be requested using the PKI portal:

- Standard server certificates
  (class 1; domain-validated; only one domain; no wildcards)
- Premium server certificates
  (class 2; domain and organization validated; only one domain; no wildcards)
- Multi-Domain certificates
  (Premium certificates with multiple SAN entries)
- Wildcard certificates
  (Premium certificates containing a wildcard in the domain name)

The validity of the publicly trusted certificates is up to 1 year.

4.4 PKI-Portal

The Atos Trustcenter operates for its customers the multitenant PKI-Portal (HTML Based GUI Web pages). The PKI-Portal has the URL https://pki.atos.net/standard

The PKI-Portal is the central tool used for request processing, status tracking, certificate management and source for help and support.

The following sections describe the default roles, workflows and feature of the SSL/TLS server certificate functionality of the PKI portal. All features may be adopted to meet the specific requirements or a customer. Beside server certificates, the portal might also be used to request User, Codesigning or other kinds of certificates. These features are not in scope of this document.

4.4.1 Roles

By default, the following roles are distinguished in the PKI-Portal for server certificates:

- Local RA: Certificates can be applied for via self-service; they can be installed and administrated.
- RA ("Registration Authority") Interface: Co-workers of the Trustcenter in the RA role adopt the configuration of domains and Local RA admin users; they may also fulfil administrative duties and responsibilities.
- RO ("Registration Officer") Interface: Users in the RO role are able to create and deactivate Local RA admin user accounts or to change their rights.

Customer specific adaptions and additional roles may be added according to customer requirements.

4.4.2 Standard workflows

The following functions are available for Local RA admin users within the PKI-Portal:

- Login with username and password
- Certificate management:
  - File a server certificate request
  - Request a renewal of a certificate
  - Download of a certificate
  - Revoke a certificate
- Overview / list of certificate requests / issued certificates
  - searchable and filterable by different attributes, e.g. the expiration date
- Various reports regarding the amount of valid certificates
  - absolute number of certificates, by domain, by certificate type, etc.
- Domain / user management
  - List of registered users
  - List of registered domains
- Help and Support Pages
  - Portal User Guide
  - FAQs and How-To's on certificate request handling
- Download page
  - TrustedRoot CA Certificates
  - Revocation List (CRL)

In case of customer specific requirements these may be implemented into specific PKI-workflows.

4.4.3 Multi-tenant functionality support

The PKI-Portal provides multi-tenancy functionality. Each customer uses the standard processes, default settings and given layout, but within its own tenant definition by default.

In case of customer specific requirements regarding processes, settings or layout these may be implemented based on change requests (CR).

Examples for specific requirements are:

- adaption of the request process,
- additional views or reports,
- certificate profiles or validity may be adapted,
- additional certificate types (User-, SSL-, Codesigning-, Machine certificate) that may be requested by users can be added.

4.4.1 Certificate Request Format

To request a Server Certificate a private key and the corresponding Certificate Signing Request (CSR) has to be generated on the target server by the responsible server administrator. The CSR also includes the target domain name and – if applicable – the organization info.

It has to be ensured, that the CSR meets some important requirements:

- the key length must be 2048 Bit,
- the domain name(s) must be included as a Subject Alternative Name (SAN) attribute,
- the distinguished name attributes must meet the customers definition (see below).

Support on how to generate a Certificate Signing Request can be found on the support pages of the Trustcenter portal.

The CSR must contain the following information:

- The “Organization (O)” field must exactly contain the customer’s company name.
- Other Parameters like “Country Code (C)”, “State (S)” and “Location (L) “should be filled in according to the site where the company resides.
- The Common Name (CN) must contain exactly one entry that is one of the values contained in the Certificate’s subjectAltName extension.

After receiving the CSR file from an applicant, the Local RA admin users will create a new certificate request and paste the request data (in base64 encoded PKCS#10 format) into the corresponding field of the form (see picture below). The request will then automatically be checked and the certificate will be issued immediately.

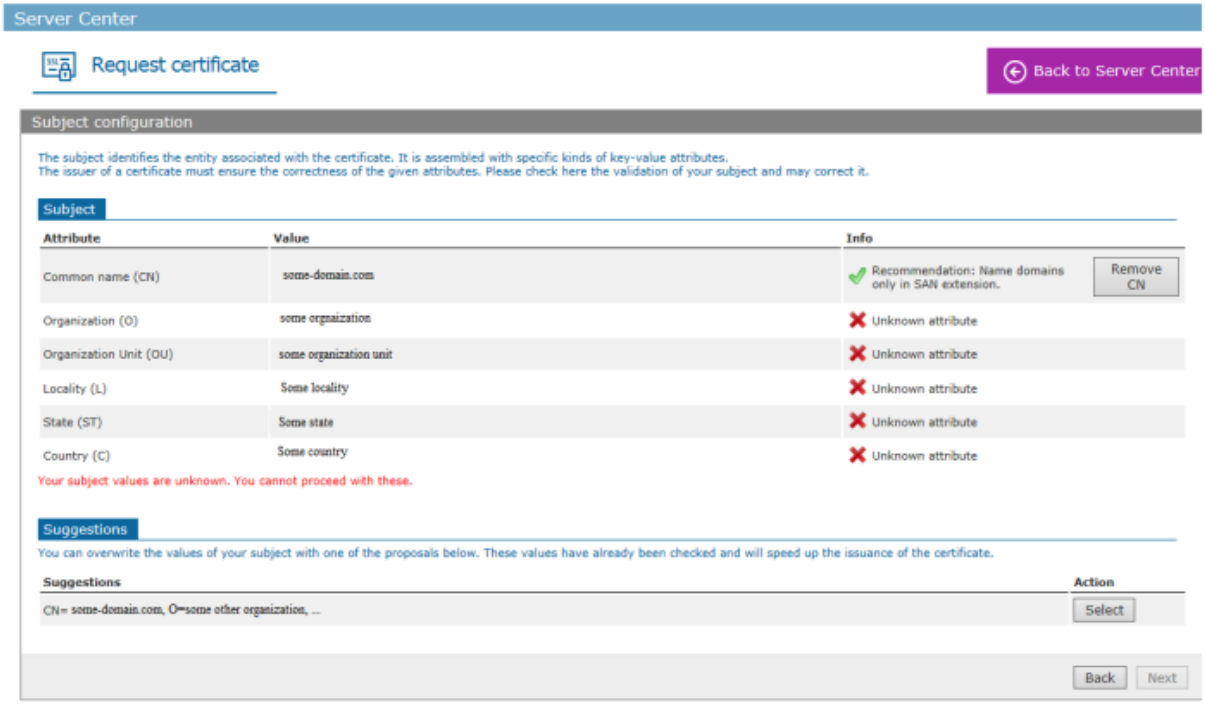

Figure 3: Request checks

4.4.2 E-mail notifications

Users are informed on the creation of a certificate via e-mail. The mail contains a link to a page where the user may download the new certificate. The download page also contains information on the installation of the certificate in different kinds of webservers. The details of this process may be adopted to conform to the needs of the customer.

Prior to the certificate's expiration date, the user will be informed by mail about the expiration. These mails are sent out 3 month and again 2 weeks before expiration.

4.4.3 Help and Support Pages

The PKI-Portal also contains various user support documentation. It is an efficient way to find information and troubleshoot PKI-Portal, subscriber enrollment or other issues:

- Each page of the portal contains an information box containing a small usage description of the page being currently displayed
- A user guide is available from the menu
- A support website providing detailed information and troubleshooting material on certificate request generation and installation for various webservers

The support website includes:

- An FAQ list with answers on frequently asked questions,
- How-To guides,
- Product white papers,
- A searchable knowledge base.

4.5 Certificate status services

The certificates are made available for download by an internet-based LDAP-service. Revocation Lists (CRLs) can be accessed via the PKI-Portal and the CRL distribution points (CDP) as stated in the certificates. In addition, the Atos Trustcenter is running an internet-based OCSP-service.

5 Service Level

By default, the service level of the PKI-Services of the Trustcenter are defined as:

CA-Services:

- Production of certificates (“production time”) will be on working days from 8 to 17 h (Mo – Fr, excluding public holidays in Germany).
- The CA-Service will be available for 99,5%, related to the production time.

CRL-Services (Provision of Certificate Revocation Lists (CRL) via HTTP and LDAP):

- CRLs will be online 7 days, 24 hours per day (“online time”).
- CRLs will be available for 99,5%, related to the online time.

OCSP-Services (Online Certificate Status Service via HTTP):

- OCSP will be online 7 days, 24 hours per day (“online time”).
- OCSP will be available for 99,5%, related to the online time.

PKI Portal:

- HTML Based GUI Web pages
- PKI Portal will be online 7 day, 24 hours per day (“online time”).
- PKI Portal will be available for 99,5%, related to the online time.

Support:

- Support by the Atos Trustcenter Team (see “Support”) will be at “production time”.

The Trustcenter team will – from time to time and with advance notice - perform maintenance tasks on the Trustcenter systems which may have influence on “production time” and “online time”, but which do not influence the SLA.

6 Support

This section describes the support approach. The support is delivered by a “First-Level-Support” and a “Second-Level-Support”. The “First-Level-Support” is provided by the customer’s helpdesk, the “Second-Level-Support” is provided by Atos Trustcenter.

Tasks of the “First-Level-Support” are:

- Direct customer contact, e.g. via email or phone
- Use training material and FAQs to solve problems
- Contact Second-Level-Support in case of issues which cannot be solved

Tasks of the “Second-Level-Support” are:

- Provide training material and FAQs for users and First-Level-Support
- Assist First-Level-Support in case of issues which cannot be solved by the First-Level-Support

Atos Trustcenter will deliver the Second-Level-Support on working days (Mo – Fr, excluding public holiday in Germany), from 8 to 17 h.

The “Second-Level-Support” is not able to cover the following issues:

- Support any applications at customer’s site which uses the issued certificates (e.g. Mail clients or Webservers)
- Support the generation of certificate requests (e.g. in Webservers)

These tasks have to be covered by other support groups and/or the application responsible.

7 Pricing

The following pricing information is non-binding and exclusive of VAT and/or taxes.

The general terms and conditions of Atos Information Technology GmbH shall apply to all services provided by Eviden.

7.1 Server certificates

7.1.1 Trusted Root CA

The following prices apply per valid certificate:

Type	1y	6m	3m
Standard server certificate (One domain, domain-validated)	83, - €	50, - €	30, - €
Multi-domain server certificate (server certificate with multiple domains, up to twenty-five domains, domain-validated)	83, - € + 45, - per domain	50, - € + 28, - per domain	30, - € + 17, - per domain
Wildcard server certificate (server certificate with wildcard domains, domain-validated)	375, - €	225, - €	135, - €
Premium server certificate (One domain, domain- and organization-validated)	110, - €	66, - €	40, - €
Premium Multi-domain server certificate (Premium server certificate with multiple domains, up to twenty-five domains, domain- and organization-validated)	110, - € + 60, - per domain	66, - € + 35, - € per domain	40, - € + 22, - € per domain
Premium Wildcard server certificate (Premium server certificate with wildcard domains, domain- and organization-validated)	495, - €	297, - €	179, - €

The price will be charged after issuance of the certificate.

7.1.2 Internal Root CA

The following prices apply per valid certificate:

Type	3y	2y	1y	6m	3m
Standard server certificate (One domain)	144, - €	90, - €	56, - €	34, - €	20, - €
Multi-domain server certificate (With multiple domains)	144, - € + 79, - per domain	90, - € + 49, - per domain	56, - € + 31, - per domain	34, - € + 19, - per domain	20, - € + 11, - per domain
Wildcard server certificate (Up to twenty-five domains)	1320, - €	528, - €	330, - €	198, - €	120, - €

The total price for a fixed (predefined) amount of certificates will be charged on a monthly base.

7.2 Code Signing certificates

7.2.1 Trusted Root CA

The following prices apply per requested certificate:

Type	3y	2y	1y
Code Signing certificates: (Organization validated)	495, - €	385, - €	220, - €

The price will be charged after issuance of the certificate.

7.2.2 Internal Root CA

The following prices apply per requested certificate:

Type	3y	2y	1y
Code Signing certificates:	312, - €	242, - €	138, - €

The price will be charged after issuance of the certificate.