ADSS Web RA Server

Digital Identity Management

ADSS Web RA Server is a comprehensive registration and vetting platform that enables Enterprises, Governments and Trust Service providers to deliver customizable enrolment and onboarding to issue digital certificates to people devices and applications from ADSS Server based CA's and 3rd party CA's

Enrollment and Vetting Overview

Digital certificates provide individuals, organisations, applications, and devices with trustworthy digital identities for use within the digital world. However, in order for a digital identity to be afforded any level of trust, the person, application or device must undergo a vetting process in order to establish that the entity enrolling is who they claim to be.

In the digital world there are different levels of assurance that can be placed in a digital identity and the transaction being performed, low, medium and high assurance levels.

Low assurance identities can be provisioned by simply and automatically by providing an email address or other electronic means to check that the holder of the identity exists and has access to the email address, in order to place higher levels of assurance in an identity, more robust checks into an identity must be taken in order to ensure the entity is who they claim to be.

In order for PKI Registration Authorities, need to be able to gather all of the information needed to help them check and vet entities who are enrolling, this ranges from organizational vetting to prove you are the company representative and own a domain name for a TLS certificate, through to, vetting an individual for the issuance of an AATL or even Qualified certificate to support trusted and legally enforceable digital signatures.

Ascertia's ADSS Web RA Server is uniquely positioned to provide Enterprises, Governments and Trust Service providers with a comprehensive and flexible platform upon which they can build enrolment and vetting workflow to digitally onboard individuals, organisations, applications, and devices for high trust use cases.

Key Features

- **Flexible Certificate Support**: Web RA Supports a range of certificate types:

  SSL / TLS Server Certificates
  - DV, OV and EV SSL Certificates
  - Compliance with CAB Forum specifications

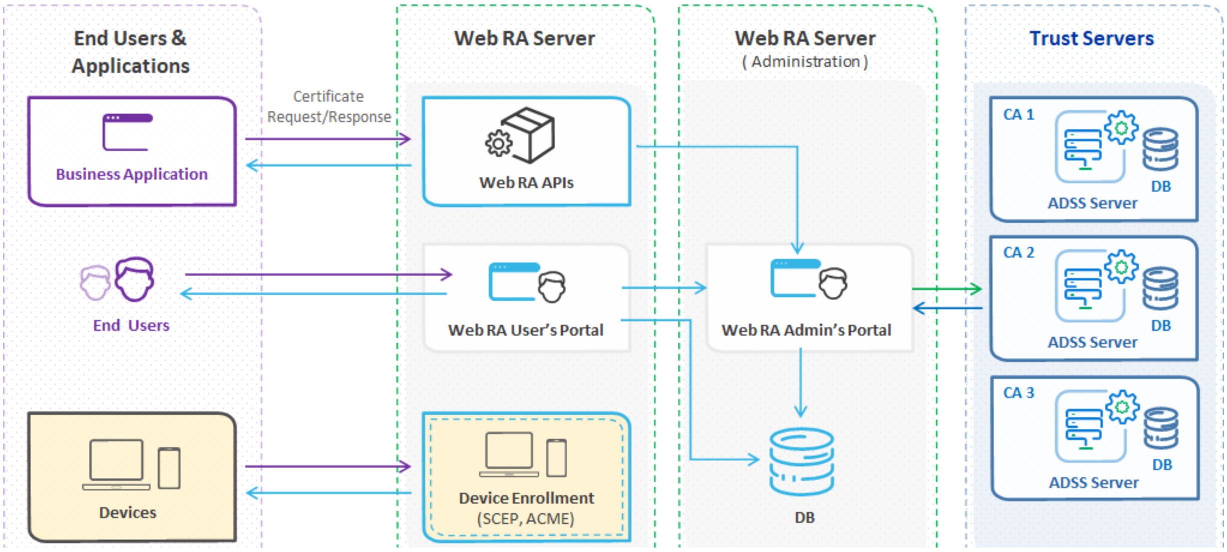
  SSL / TLS and S/MIME Client Certificates
  - on smart cards/tokens
  - via PFX / PKCS#12 files

  Digital Signature Certificates
  - for Bulk Signing
  - for remote signing
  - for local signing using smartcards/tokens
- **Interoperability**: Tested with Microsoft Active Directory Certificate Services, Entrust Security Manager, Primekey EJBCA, and other CA's
- **Flexible Enrolment and Vetting**: Includes support for:
  - Dynamic Vetting Forms
  - using a drag & drop based form designer
  - simply configurations to define multiple certificate request types
  - full review and approval features
- **Device Enrolment: Web RA Server supports device enrolment via**
  - SCEP protocol - gutmann-scep-14
  - CMPv2 – RFC 4210, 4211 & 3GPP
  - EST - RFC 7030
  - ACME – RFC 8738
  - Windows Native Certificate Enrolment

ADSS OCSP Server Architecture

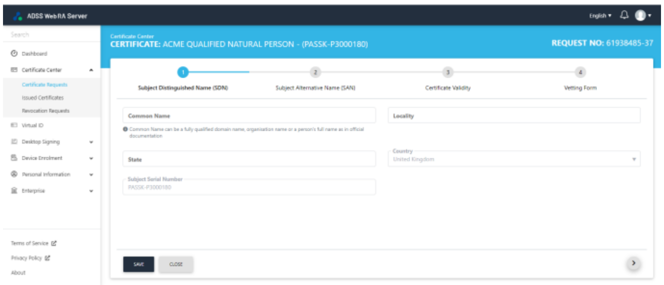
Managing digital certificates effectively is a key requirement for any IT security team. ADSS Web RA does this quickly, simply and securely. Authorised security administrators can monitor, review and approve certificate issuance requests, renew certificates before they expire and revoke certificates from one intuitive secure web-browser interface. ADSS Web RA provides automatic notifications of these time-critical events.

ADSS Web RA is a front-end registration authority application that harnesses the power of ADSS CA Server to directly issue and manage the lifecycle of certificates. ADSS Web RA provides an intuitive user experience for administrators and end users, administrators can easily build enrolment workflow for certificate enrolment for end user certificates or server certificate enrolment based on PKCS#10 certificate signing requests. ADSS Web RA Server provides organisations with a delegated administration model, this enables organisations and service providers to segregate certificate administration into separate enterprises which can be managed separately.



Putting you in control

Organisations are provided with full control over the user experience, ADSS Web RA provides the ability to fully brand the user interface, create service plans, easily create vetting forms and create subscriber agreements.



Certificate Center
CERTIFICATE: ACME QUALIFIED NATURAL PERSON - (PASSK-P3000180) REQUEST NO: 61938485-37

Subject Distinguished Name (SDN) | Subject Alternative Name (SAN) | Certificate Validity | Vetting Form

Common Name

Common Name can be a fully qualified domain name, organisation name or a person's full name as in official documentation

Locality

State

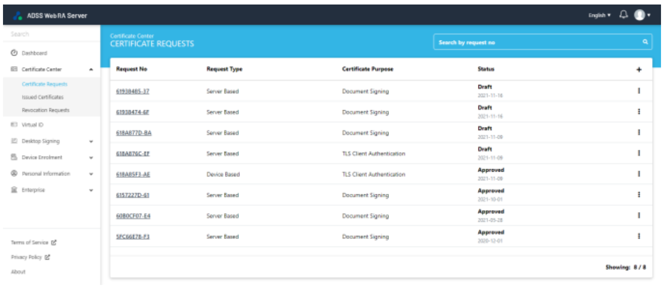
Country: United Kingdom

Subject Serial Number: PASSK-P3000180

Flexible Certificate Lifecycle Management

ADSS Web RA enables developers the ability to integrate certificate issuance programmatically by exposing a Rest API, this enables the easy integration of certificate lifecycle management into business applications.

ADSS Web RA also provides industry standard enrolment protocols, these enable device and application integrations. Organizations can seamlessly issue and manage certificates using market standard protocols like SCEP.



Certificate Center
CERTIFICATE REQUESTS

Request No	Request Type	Certificate Purpose	Status
61938485-37	Server Based	Document Signing	Draft 2021-11-16
61938474-6F	Server Based	Document Signing	Draft 2021-11-16
618A877D-BA	Server Based	Document Signing	Draft 2021-11-09
618A876C-EF	Server Based	TLS Client Authentication	Draft 2021-11-09
618A85F3-AE	Device Based	TLS Client Authentication	Approved 2021-11-09
6157227D-61	Server Based	Document Signing	Approved 2021-10-01
60B0CF07-E4	Server Based	Document Signing	Approved 2021-05-28
5FC66E78-F3	Server Based	Document Signing	Approved 2020-12-01

Showing: 8 / 8

Centralizing Certificate Management: Organisations strive for a centralised and consistent certificate management platform, ADSS Web RA can be deployed to provide certificate lifecycle management for a single instance of ADSS Server or provide administration and lifecycle management across a number of ADSS CA Servers, this helps organisations deliver a consistent user and administrative experience and reduces inconsistencies in certificate management.

Management Control and Reporting: Detailed role-based access controls make it easy to give staff the rights they need, for instance allowing help-desk staff to access log information so they can help customers whilst ensuring that they cannot view or change any configuration data.

ADSS Web RA Server is an advanced registration and vetting tool that supports multiple CAs, role based operator access controls and high availability configurations.

Secure web-based management is provided as standard together with advanced management configuration options and detailed reporting.

Supported Operating Systems:

Microsoft Server 2019, 2016

Supported Databases:

Microsoft SQL Server 2019, 2017

Supported Security Modules – via ADSS Server

Thales Luna and Protect Server
Entrust nShield
Utimaco SS & CS CP5
Microsoft Azure Key Vault
Amazon AWS Cloud HSM (Linux Only)

M Hathaway

×

Mike Hathaway | Chief Product Officer

About Ascertia

Ascertia provides digital trust for people, devices, data and documents for everybody from individuals to Enterprises and Governments. Ascertia's PKI and digital signature technologies serve a global customer base and partner network via direct and indirect sales channels.

For more info

info@ascertia.com

www.ascertia.com