ADSS Web RA Server

Digital Identity Management

Managing digital certificates effectively is a key requirement for any IT security team. ADSS Web RA Server (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 secure web-browser interface. Web RA provides automatic notifications of these time-critical events.

Web RA is a front-end registration authority application that harnesses the power of ADSS CA Server (or other CAs) to directly issue and manage the lifecycle of certificates. 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. 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, Web RA provides the ability to fully brand the user interface, create service plans, easily create vetting forms and create subscriber agreements.

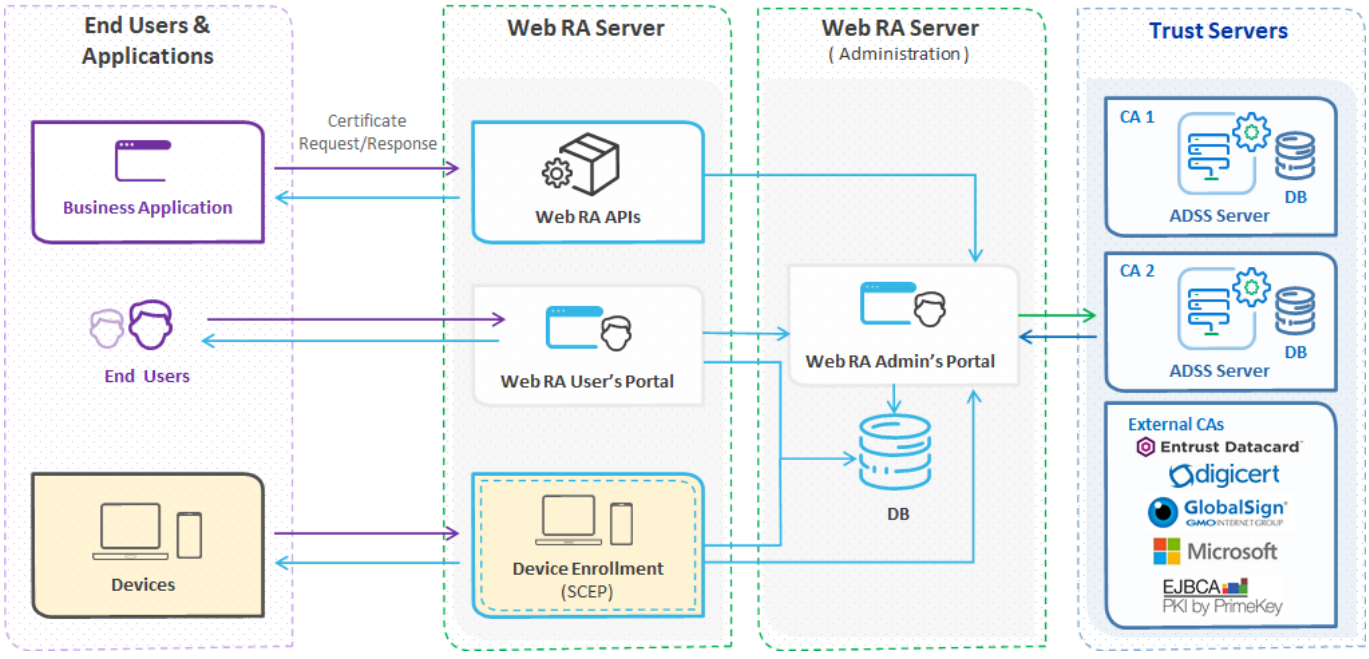
Flexible Certificate Lifecycle Management

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.

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 such as SCEP.

Centralising Certificate Management

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



Key features for ADSS Web RA:

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

Remote Qualified Signature Creation Device
- Ascertia ADSS Server SAM Appliance

Digital Signature Certificates
- for Bulk Signing
- for remote signing via Ascertia Virtual CSP
- for local signing using smartcards/tokens
- via PFX / PKCS#12 files

Integrated with Ascertia SigningHub
- Register Users
- Register Mobile devices for remote signing

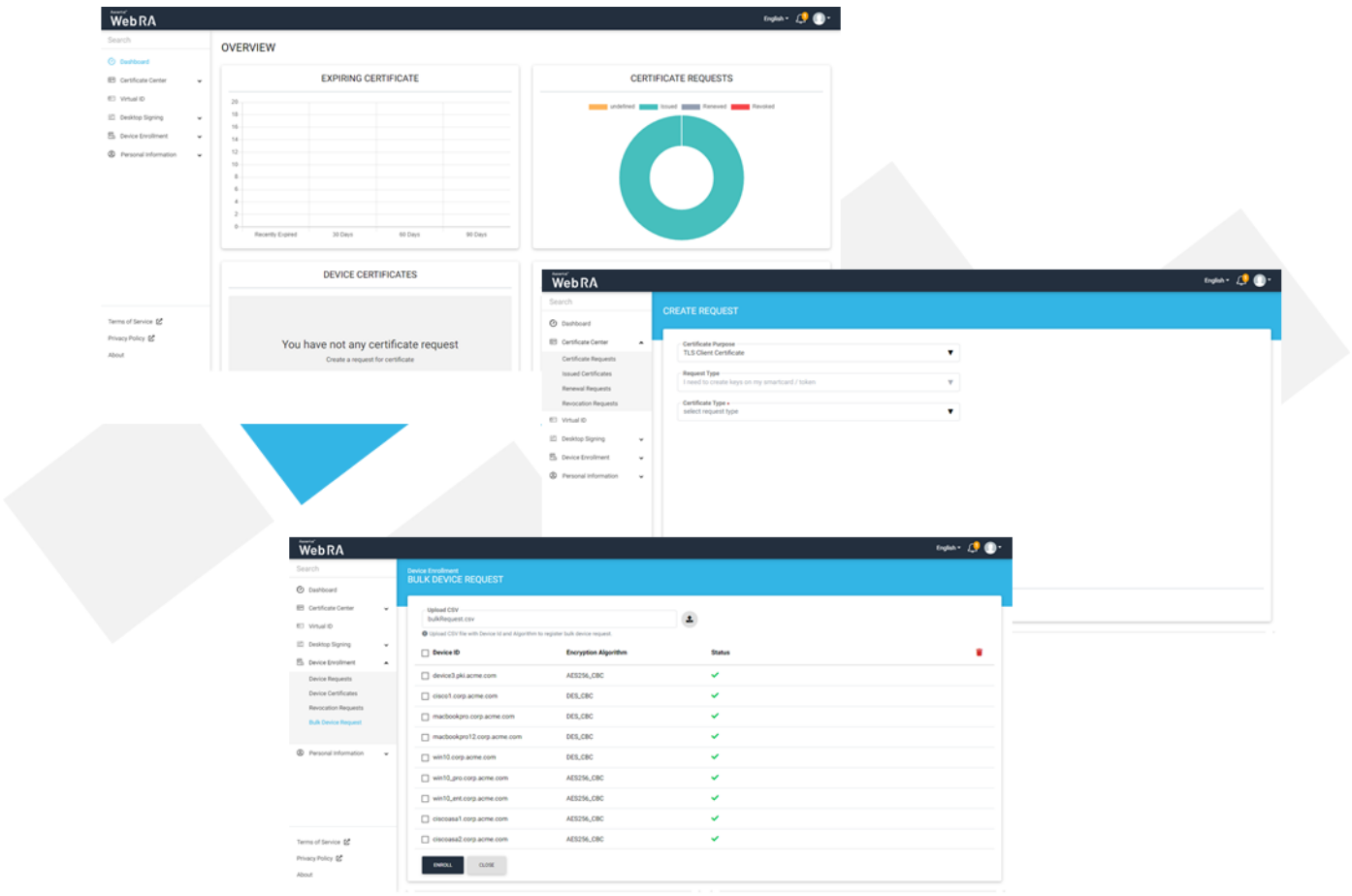
Device Enrolment
- Using SCEP and ACME protocols

Know Your Customer
- Dynamic Vetting Forms
- using a drag & drop based form designer
- simply configurations to define multiple certificate request types
- full review and approval features

Face to Face enrolment
- issuance of certificates by security administrators

APIs for Business Applications
- Rest APIs to control certificate issuance and management

Enterprise Management and Enrolment
- Enables an organisation to managing their own users



Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 203 633 1177
40 Occam Road, Guildford, Surrey, GU2 7YG, UK

Signed by: Mike Hathaway
Signed at: 2020-07-17 09:32:28 +00:00
Reason: I approve this document

M Hathaway