Web RA Release Notes

This document provides a high-level description of the new features offered in each version of Web RA. Only the main features in each release are identified.

Web RA v2.1.0.0 April 2020

- Installation wizard supported to install or uninstall Web RA for seamless and smooth deployment that includes fresh, upgrade, load balancing, installation with existing DB using Windows authentication and SQL Server User both
- GDPR user management compliance added to Web RA Administration.
- Access control implemented to have dual control in order to approve certificate generation, renewal and revocation requests by an approval manager and Enterprise RAO (Registration Authority Operators)
- PFX generation supported for the user to export the required PFX file if allowed by an Administrator
- Bulk registration supported for the Simple Certificate Enrollment Protocol (SCEP) using a CSV file
- Changes done for certificate renewal and revocation for Virtual ID, Desktop Remote Signing and device enrollment
- Password challenge is now configurable for device enrollment, using three options none, fixed or random password
- Compatibility with mobile interface now supported
- User interface improvements done for the admin and web interfaces
- Signup can be restricted on user portal by an Administrator

Web RA v2.0.0.0 January 2019

- An authorized operator who can be an administrator or an Enterprise RAO (Registration Authority Operators) has a separate interface to manage the certificate management service, protected by SSL and password authentication
- Administrators can configure connectors, profiles and service plans to operate the service including SMTP servers and SMS OTP gateways
- Administrators can add subscriber agreements for each type of certificate request
- Administrators can create dynamic vetting forms with various types of questions and different type of input fields for end users to fill in the required information
- Google CAPTCHA is implemented to secure sensitive user forms from automated attacks
- Administrator RAOs or Enterprise RAOs are able to review and approve pending certificate requests if the vetting is turned on
- An OEM version of ADSS Server is used to handle all certificate requests, harnessing the power of ADSS server and certificate generation features, working with one or more external CAs
- ADSS CSP is a service that allows to sign the documents using a desktop Application VCSP. The Web RA enables end users to enrol them to use CSP services with the desktop application.
- Remote authorization enrolment can be configured from Web RA
- Web RA now supports the SCEP protocol for device and application certificate enrolment
- Web RA administrator interface can also be used for face to face registration and enrolment
- Administrators can enroll Enterprise RAOs from administrative portal. End users can also enrol themselves in the Web RA via the user’s portal and activate their account using the link sent to their email address

- Suitably authorised Enterprise RAOs can add or invite enterprise members individually or in bulk
- One Enterprise RAO can manage requests from more then one enterprise and their members, adding multi-tenancy support to the application
- Application contains a detailed account and access control management from administrator's portal. Application can have many administrators all with different roles and rights and can vet requests from only allowed list of enterprises.
- Web RA can be deployed in a load balanced environment to support high volume requests and throughput
- Terminated Service Provider (TSP) can be maintained as a list, where Web RA administrators can receive requests to manage the certificates on behalf of a terminated service provider. Mainly these operations involve revoking a certificate
- User portal now supports both password and OTP based login authentications
- One user can become part of multiple enterprises and request certificates using the enterprise allowed profiles
- Detailed audit logs are maintained on both administrator's and user's portal
- Domain verification for DV, OV and EV SSL certificates supported in Web RA using TXT records or by uploading a file with verifiable content
- Support of rest based APIs for certificate management is available via secure API keys created for enterprises