Validation Authority

HIGHLIGHTS

Reliably verify the status of digital certificates

Entrust Validation Authority provides evidential value and greater efficiency in the verification of the status of the digital certificates.

Validation Authority is designed to:

- Provide reliable information on the status of a digital certificate
- Process information from one or multiple CAs using CRLs or CA database
- Facilitate integration with corporate information systems
- Reduce installation and maintenance costs

KEY FEATURES & BENEFITS

Reliability and control

- Emergency mechanism activates when connection to the database is lost, ensuring the integrity of the registered data and that no information is lost
- Supports selecting automatic events (which are assigned different levels of severity) and defining manual events (for registering actions that occur outside the application)

Efficiency for large infrastructures

- Facilitates managing large volumes of certificates via the certificate database or LDAP CRL retrieval
- Quickly and efficiently processes certificate status changes, which provides for OCSP responses that are fast and accurate
- Supports high availability and scalable architectures
- Kubernetes-based virtual appliance provides for easy install, upgrade, monitoring, and modern architecture

Learn more about Validation Authority at entrust.com

Validation Authority

HOW IT WORKS

Functionality

- Store information on the status of certificates generated by one or more CAs
- Respond to requests (from users or service providers) for information on the status of digital certificates used in the signing of electronic transactions
- Respond to requests (from either the user's browser or the web server if OCSP stapling is used) for information on the status of digital certificates used when a web server protects the communication via TLS/SSL
- Guarantee the non-repudiation of the responses digitally signed by the Validation Authority, and specify the date and status (valid, revoked, suspended, or unknown) of the certificate
- Redirect, if necessary, the requests to an external OCSP responder that can provide an authoritative response for certain certificates
- Generate event logs so operators can monitor the system status, its security, and to what extent the corporate specifications are being met
- Keep track of and limit each client's use of the OCSP service; Validation Authority assigns a service usage quota or restricts use for a specific time period (i.e. billing)

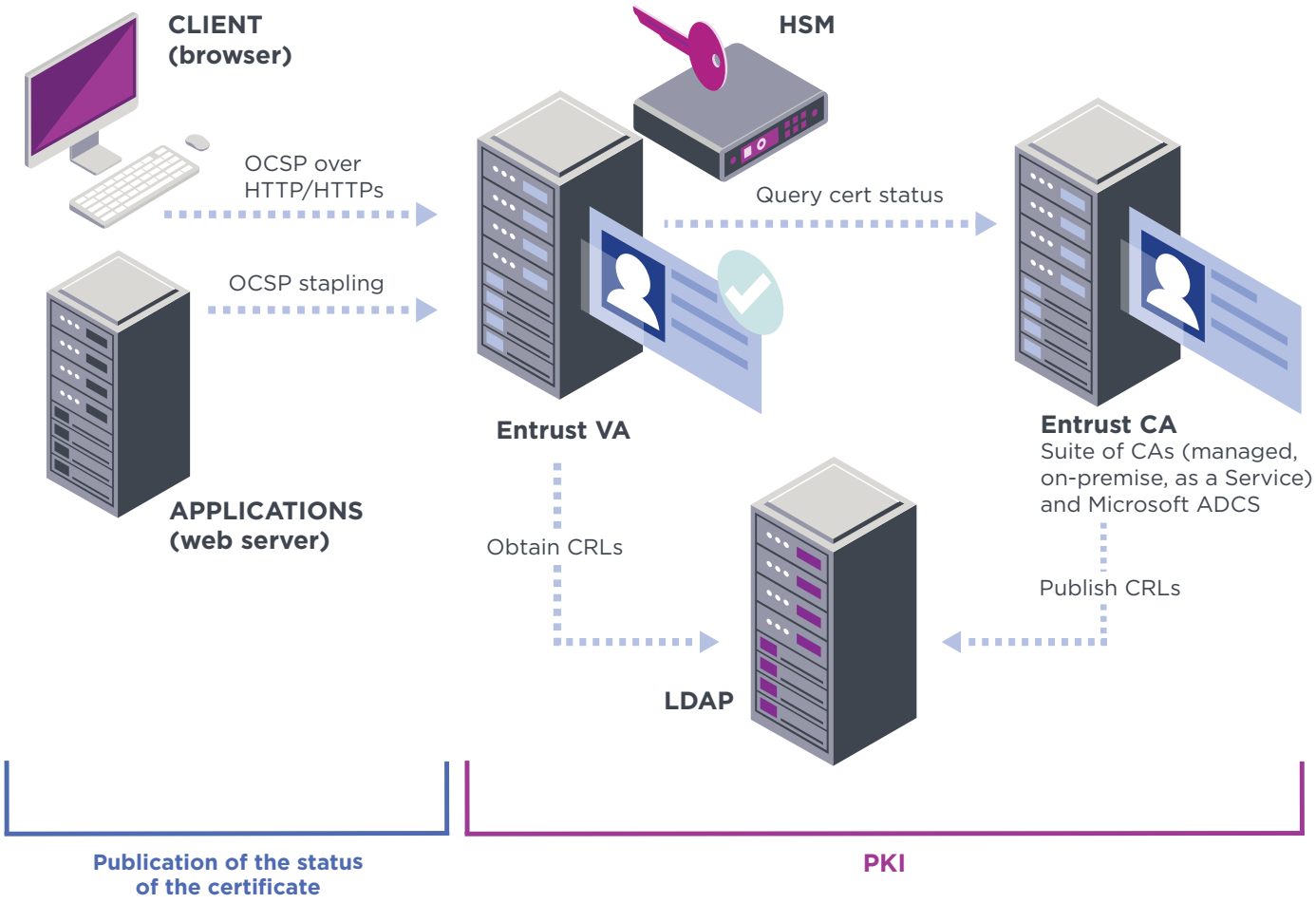
Architecture

The figure below illustrates the general architecture of Validation Authority and how it interacts with network components (applications or users) under the IETF OCSP standards. Validation Authority can operate with an HSM and requires access to a database and a network time source (not shown in the figure).

Depending on the configuration of the certificate status update system, Validation Authority connects regularly to the CA or downloads CRLs from an LDAP directory or a web server.

Validation Authority

Architecture (continued)



Learn more about Validation Authority at entrust.com

Validation Authority

TECHNICAL SPECIFICATIONS

Online validation protocol: OCSP as per IETF RFC2560 and RFC 6960; support of OCSP Stapling (IETF RFC 6066 and RFC 6961)

Cryptographic devices: RSA PKCS #11

Connectivity: SQL, LDAP, HTTP/HTTPS, REST

Update mechanism: ITU-T X509v3 CRL, queries to the CA

Support for multiple CA solutions: Yes

Event monitoring: Grafana dashboards and Loki log display

SYSTEM REQUIREMENTS

Operating systems: Entrust Deployment Manager on Linux

Database systems: Postgres, Oracle, Microsoft SQL Server

Optional HSM: Entrust nShield®, Thales, (contact us to find out which models are supported)

Time source: Operating system time synchronized with an external source

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223