Horus Vericert

Improve and centralize the validation of public key certificates

Public key certificates allow applications to integrate security services such as user authentication, non-repudiation of transactions, or confidentiality of data exchanges. The validity of these certificates needs to be verified at the time of their use and after their use, in the case of non-repudiation and data confidentiality. Atos, a European actor in IS security, provides **vericert**, a complete solution based upon customized validation policies to validate electronic certificates.

Politics validation

A public key certificate is validated according to a validation policy, which is a set of rules. Validation policies cover various cases with different levels of complexity. The validation of a given certificate demands at least:

- a certification path to a Certification Authority (CA)
- a validation policy

Once the certification path constructed, the validity of each certificate belonging to it must be checked through CRLs (Certificate Revocation Lists) or OCSP responses (On-line Certificate Status Protocol).

Additional constraints may be defined in the validation policy, such as accepted certification policies, length of the certification path or relevant key usages.

Vericert, a centralized service for validating electronic certificates

One or more validation policies can be defined in order to fulfill the needs of different applications. As a central point for the administration of accepted CAs and revocation information, vericert provides a simpler, consistent and powerful way of validating certificates.

When validating a certificate at the current time, vericert collects the required certificates, CRLs and/or OCSP responses, and hands them to the requester. Information collected in order to reply to a request can be re-used, partially or not, for another request. This improves the time of response and reduces the load on the network.

When validating a certificate at a time in the past, elements already collected (certificates, CRLs and/or OCSP responses) must be provided by the requester, and then, they are checked by vericert.

A European leader in integrated security

Atos has built up a unique body of expertise in information systems security, bringing together know-how in consulting and systems integration and an in-depth understanding of corporate security technologies.

SÉCURITÉ CERTIFICATION SÉCURITÉ CERTIFICATION

Certified Products CSPN
ANSSI-CSPN-2014/10

vericert version 2.1.2

Trusted partner for your **Digital Journey**

Atos

A PKI-enabling solution for secure applications

Vericert is managed through the use of customized web interfaces, allowing remote management from personal computers using standard web browsers.

When a certificate validation with regards to a validation policy is required, **vericert** is accessible via a web interface (web service) using HTTP or HTTPS (SSL). Responses can be signed.

When solely querying the revocation status of a certificate, **vericert** is accessible via the OCSP protocol (RFC 6960).

Vericert supports the following functional components

- A certificate storage used to securely store CA certificates
- A CRL storage used to cache CRLs obtained from predefined CRL distribution points or using CRL distribution points (CRLDP) extensions, if present in certificates
- An OCSP client to get the revocation status of certificates
- An OCSP server to provide the revocation status of certificates
- The upload of the European TSL (« Trusted Service List ») to get the trusted certificate authorities

Vericert supports the following functional optional component

- A Hardware Security Module (HSM) for the protection of the private keys used to sign validation responses or OCSP responses
- Vericert supports different kinds of HSMs, either provided by Atos or by third parties

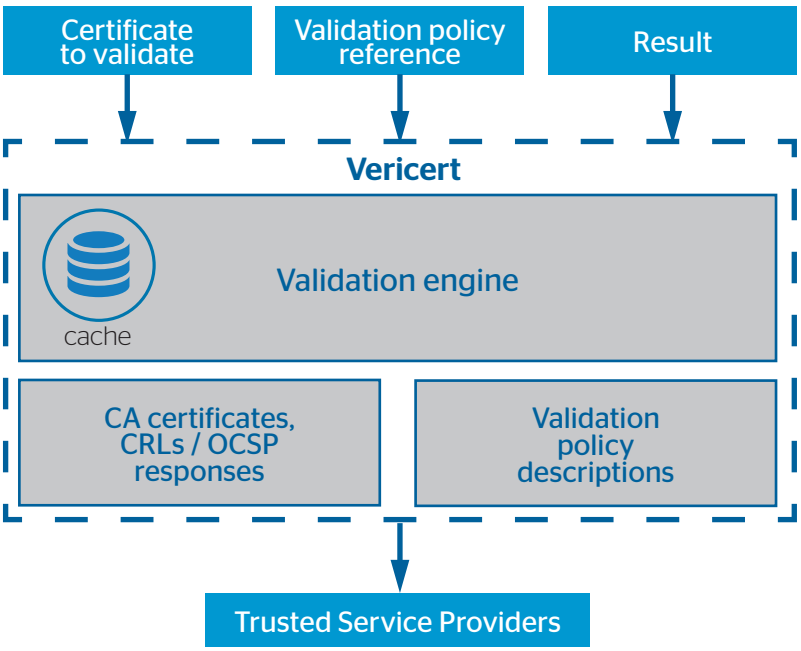
Validation policy customization

Using a web interface, it is possible to enter:

- trusted self-signed certificates
- certification path constituents
- OIDs (Object Identifiers) for Certification Policies (CPs)
- key usage values
- extended key usage values as defined in RFC 5280

Norms and standards for interfaces and protocols

- Certificate format compliance with ITU-T X.509v3 and RFC 5280
- Revocation information compliance with ITU-T X.509v3 CRL and OCSP Protocol (RFC 6960)
- SOAP 1.1 et WSDL 1.1 for the validation of certificates against a validation policy
- RFC 6960 for the revocation status of certificates
- Connectivity: HTTP, LDAP and HTTPS
- TSL v5 (ETSI TS 119 612 V2.2.1)



Find out more about us
https://atos.net/en/products/cyber-security/digital-identities/cryptographic-data-preparation-device

© Atos August 2018 - All trademarks are the property of their respective owners. Atos, the Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Bull, Canopy, equensWorldline, Unify, Worldline and Zero Email are registered trademarks of the Atos group. Atos reserves the right to modify this document at any time without notice. Some offerings or parts of offerings described in this document may not be available locally. Please contact your local Atos office for information regarding the offerings available in your country. This document does not represent a contractual commitment.

CT_180813_LPM_Fs_Horus_Vericert_en3