vSEC:ID® Server

Do you want to add digital signature security to your organization's work flows? The vSEC:ID Server is an easy to integrate software solution that enables PKI operations such as digital signature generation, signature verification, encryption, decryption and certificate validation.

Digital Signatures – a Cornerstone for Secure Transactions

Digital signatures enable organizations to put trust in their IT infrastructure because of the cryptographic certainty that they guarantee. Characteristics for digital signatures include:

- Most important security feature for on-line transactions;
- Electronic equivalent to a written signatures;
- Secure, reliable and legally binding in most regions;
- Industry standard for creating proof of an electronic transaction.

Overview of vSEC:ID® Server

The vSEC:ID Server is a standalone server application that can be used independently or in conjunction with other products from Versatile Security.

The vSEC:ID Server performs the cryptographic operations required to verify the digital signatures made on the client side and validates the digital certificates used. The vSEC:ID server has many interfaces which makes it easy to integrate into any web application. The application interfaces include HTTP, XML and a Java™ SDK. The server component can also interact with back-end components such as HSMs through standard interfaces (PKCS#11).

The server component can perform all standard PKI operations such as sign, encrypt, decrypt, verify and validate certificates along with OCSP and CRL checking.

The vSEC:ID Server can be involved in all the companies work flows which require strong authentication, confidentiality and non-repudiation.

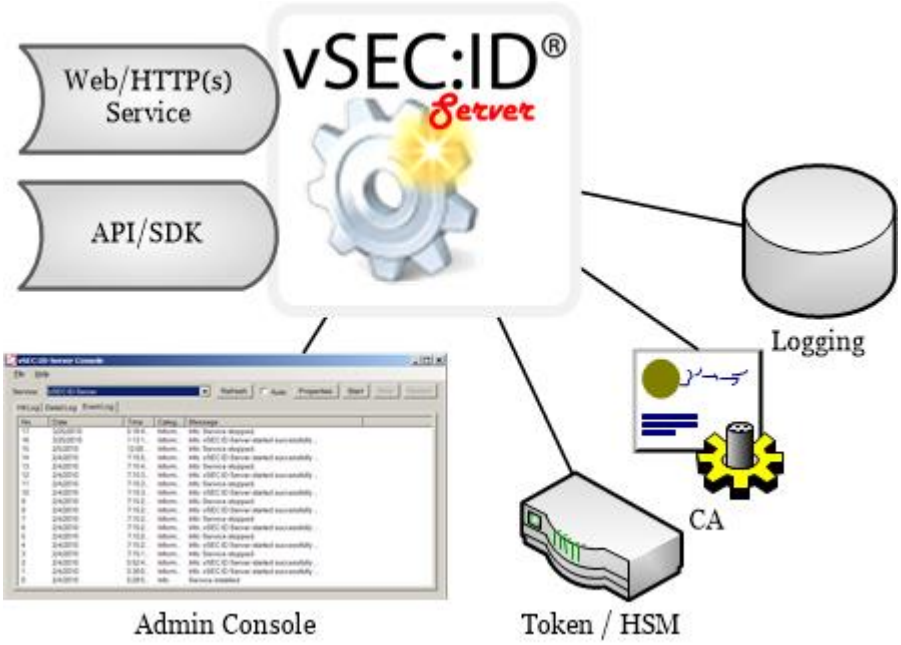

Figure 1: vSEC:ID® Server interfaces

vSEC:ID Server Use-Case

Figure 2: vSEC:ID® Server example – Digital Signature Verification

Technical Specifications

Operating Systems

- MS Windows Server
  - 2003, 2008 & 2008 R2 (32bit & 64bit)

Functionality

- Verify, sign, encrypt, decrypt PKCS#7 and XML based signatures and envelopes
- Additional: verify and translate (PKCS#1, WAP SignedContent), verify certificate (X509, WTLS), timestamp (data, signature)
- Cryptographic backend services: OCSP, TSA
- Long term signature support : CAdES
- HTTP(s) XML and Key/Value interface
- XML WebServices (in connection with MS-IIS)
- SDK available in two packages:
  - DLL: To be used from native applications such as C/C++
  - JAR: A Java package to be used from Java based applications
- Windows Service
- Management and configuration console
- Hit log and detail log
- Optional: RDBMS reporting, certificate retrieval (RDBMS, HTTP, LDAP), receipt server

Cryptography

- PKCS#11 based HSM for private keys
- Optional all cryptographic algorithm can be used directly from PKCS#11 (FIPS 140 compliant)

Performance

- Highly scalable (depending on number and speed of CPU cores)
- Cryptography performance scalable with PKCS#11 HSM (hardware security modules)

Standards Compliancy

- RFC1157/RFC1441: A Simple Network Management Protocol (SNMPv1 and SNMPv2)
- RFC1777/RFC3494: Lightweight Directory Access Protocol (LDAPv1 and LDAPv2)
- RFC1945/RFC2616: Hypertext Transfer Protocol - HTTP/1.0 and HTTP/1.1 (partial)
- RFC2559: Internet X.509 Public Key Infrastructure - Operational Protocols - LDAPv2
- RFC2560: Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol - OCSP
- RFC3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)
- RFC3275: XML-Signature Syntax and Processing
- RFC5126: Electronic Signature Formats for long term electronic signatures (CAdES)
- RFC5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile
- RFC5652: Cryptographic Message Syntax (CMS)
- Public Key Cryptography Standards (PKCS) (important are: PKCS#1, PKCS#7, PKCS#8, PKCS#11, PKCS#12)
- W3C: XML-Signature Syntax and Processing, XML-Encryption Syntax and Processing, Decryption Transform for XML Signature
- Wireless Application Protocol (e.g. WAP-161-WMLScriptCrypto, WAP-211-WAPCert, WAP-217-WPKI)
- Identrus Operating Rules and System Documentation Release 1.6 (e.g. IT-PKI, IT-DSMSSP, IT-OCSPCR)

versatile SECURITY