Hierodiction Software

Secure Key Manager (SKM)

Verifier (VFY), Base System Security (BSS)

What is Hierodiction SKM 2.0?

Hierodiction Secure Key Manager 2.0 offers secure generation, storage and retrieval of cryptographic keys. The SKM Manager comprises of: (a) The SKM Server, implemented as a Web Service; and (b) The SKM Requestor, the client that communicates with the SKM Server. The SKM Requestor includes a set of library functions, invoking the SKM Web service, which may seamlessly integrate with your own .net applications. In addition, the Requestor comes with a powerful cryptographic library that enables your custom applications to have quick and easy access to cryptographic functions; and an easy to use interface (Requestor Client Software) that enables one to create cryptographic key pairs for data encryption.

The SKM Server offers the following services:

(a) RequestKey() generates a cryptographic key pair in the SKM. The public key is communicated to the Requestor, however, the private key remains unknown due to the fact that it is not actually stored anywhere but is quasi "forgotten" by the SKM. The private key can only be reconstructed by an authorized requestor. Even complete control over the SKM Key Server will not enable one to read any private key stored therein.

(b) ActivateKey() reconstructs the private key and retrieves it from the SKM server.

The Verifier (VFY):

An extension to the SKM, which produces a second digital signature on voting rights in addition to the election server. An independent watchdog authority providing additional safeguards in the election process would typically run the Verifier and thus monitor the elections.

Benefits

High Security Storage: Due to the fact that the private key is not actually stored anywhere as such, even total physical control over the SKM Server will not enable one to retrieve private keys.

Flexible: SKM currently supports RSA key sizes between 512 and 2048 bit. Future upgrades will support key sizes beyond 2048 bit. The key size can be flexibly chosen upon request. Hence, the SKM can easily support incremental encryption in teams. The port of the Web service can be flexibly adjusted according to your firewall specifications.

Platform-independent: Keys can be made available in Microsoft's Crypto Provider or in Java Big Integer format.

Manageable: Easy-to-use menu-based customizing of SKM Server and Requestor.

Robust: Emergency recovery procedure.

Auditable: Tamper-proof encrypted logging in SKM Server and Requestor.

Scalable: AES 256 bit encryption of SKM Server database content for SAN support.

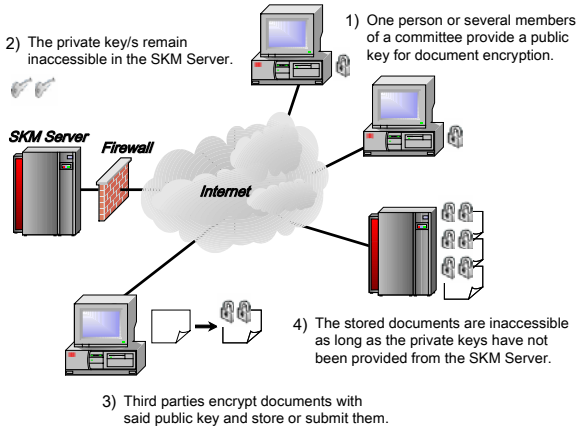
Secure Communications: Data exchange between the Requestors and the SKM Server is encrypted and authenticated using 1024 bit RSA keys. Only the requestor originally requesting key generation may retrieve its private key.

Productive: Hierodiction SKM is more than just a Secure Key Manager. The SKM Requestor ships with a well-documented and powerful cryptographic library, enabling programmers to produce stable and secure cryptographic functions. The functionality includes RSA for encryption and signature, blind signature, zero-knowledge proof, AES, hexadecimal and Big Integer conversion, Random Prime generation and verification, SHA-1, key conversion between Microsoft Crypto Provider and Java Big Integer Mathematics, …

Available interfaces are documented in detail and examples of standard cryptographic scenarios are explained to help your programmers make full use of its powerful functionality.

Contact: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at

Application Scenario I: Document Management in Organizations

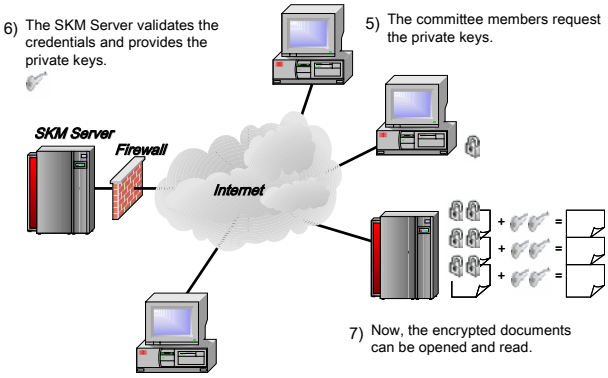


This scenario is a standard situation in many business processes, whether it be in the public sector, banking or legal information systems. Let us explore the electronic submission of tenders (Electronic Procurement) as an example:

The committee members responsible for the tender generate key pairs in the SKM Server, where the public key is made available to potential bidders and the private key remains unknown to be later reconstructed by the SKM Server (Steps 1 and 2). Bidders submitting their tenders use the public keys to encrypt their tender documents.

Note: document encryption and possible document concatenation with SHA-1 hashing can easily be implemented with the ready-made functions of the SKM Requestor Crypto Library (Steps 3 and 4).

When the submission period expires, the committee members request their private keys from the SKM Server. Only the person or application originally requesting the key generation may retrieve the key (Steps 5 to 6). Once all private keys have been provided, the encrypted bids are opened (Step 7).



Application Scenario II: Electronic Voting (e-voting)

A similar scenario is used in e-voting

The Secure Key Manager is responsible for providing the security necessary to prevent the tampering of votes. This is achieved by encrypting the ballot sheet with the public keys of the election committee members *before* the ballot sheet is submitted to the election server (Steps 3 and 4). In doing so, neither the system administration of the Election Server nor any single committee member is able to manipulate the ballots.

In using the SKM, each committee member requests generation of a private/public key pair and a public key is issued to each member. The private key remains unknown. The only person to request its reconstruction is the committee member who requested its generation and each committee member has to expressly reconstruct the respective private key.

After vote casting has been terminated, the members of the election committee retrieve their respective keys and jointly provide the information necessary to open the ballot (Steps 5 to 7 above).

Majority Decisions in a Committee

In either scenario, majority decisions may be implemented. For example, 3 out of 5 committee members may access a document or may open an electronic ballot box.

The defined quorum may not be altered later and may not be manipulated, for instance, by a database administrator manually changing the database content.

The Verifier (VFY)

An essential issue in e-voting is the lack of server observability by independent authorities. EVOTE supports independent election monitoring by a range of means – one of them authenticating the voter's election token that is used to cast a vote with a second digital signature. This is done by the Verifier.

This enables an independent watchdog authority to check the work of the election server itself because after vote casting finished all votes submitted must be associated with a token bearing this second signature.

Also, the list of voters for whom such a second signature was issued must be identical to the list of active voters in the voter roll. The Verifier functionality was included in the SKM, however, due to the modular, Web-based concept of Hierodiction systems SKM and Verifier may also be run separately.

Independent election monitoring creates trust and auditability; it increases the accountability and transparency of the election system with respect to the authorities that are politically and legally responsible for conducting the elections.

Base System Security (BSS)

„Is this really the election server?"

„Was the software configuration altered during the election?"

Valid questions that may be asked in an election and that have to be answered satisfactorily. Servers are unobservable per se and it is a prime concern in electronic voting to **strengthen the trust in electronic voting**.

BSS enables to monitor the election server's software configuration from a secure server that is not managed by the election server administration.

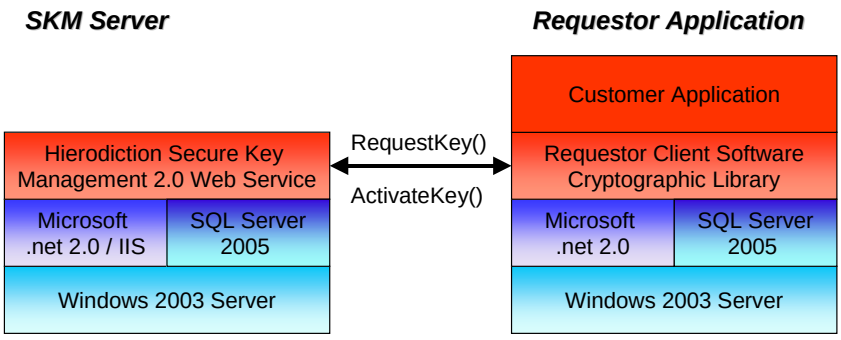
The **integrity of the software configuration is continuously ascertained**, manipulations in the software used are detected and signalled, whereupon an independent monitoring authority may initiate the appropriate actions.

BSS may also monitor a SKM/VFY installation or, in fact, an arbitrary software installation.

System Environment

The SKM/VFY and the BSS services are based on widely supported industry standards and where there is sufficient qualified staff available.

Due to its Web-based architecture the SKM service easily integrates in many application environments, providing the SOAP standard is adhered to. The SKM crypto library also supports the ready conversion between Java key formats and those used in the Microsoft .net environment.



Contact: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at