Hierodiction Software

Secure Document Store (SDS)

What is Hierodiction SDS 1.0?

In many organisations and applications, documents are to be deposited in a secure document store with the following typical requirements:

(a) Depositing of arbitrary document types (MS Office, pdf, Visio, database files etc.). These files may also be rather large.

(b) Documents are to be deposited encrypted to protect them from manipulation.

(c) Once deposited, documents are to be "frozen", ie, they should not be modified or erased.

(d) Access is to be controlled by various mechanisms: Password, system encryption, asymmetric encryption or access should be restricted to a joint group or a quorum thereof (committee decisions).

(e) Manipulation protected logging of depositing and (in some scenarios) of retrieving the files deposited.

(f) File signature.

Hierodiction SDS fulfils these requirements and provides an auditable file store for critical processes, such as elections or public administration processes.

Benefits

Self-commitment of the depositor: The depositor of the documents does not have the opportunity to alter or erase documents undetected. On deposit in the document store, an unalterable timestamp is stored with the document. SDS hence enables the depositor to prove that a certain document contained certain content at a certain point in time.

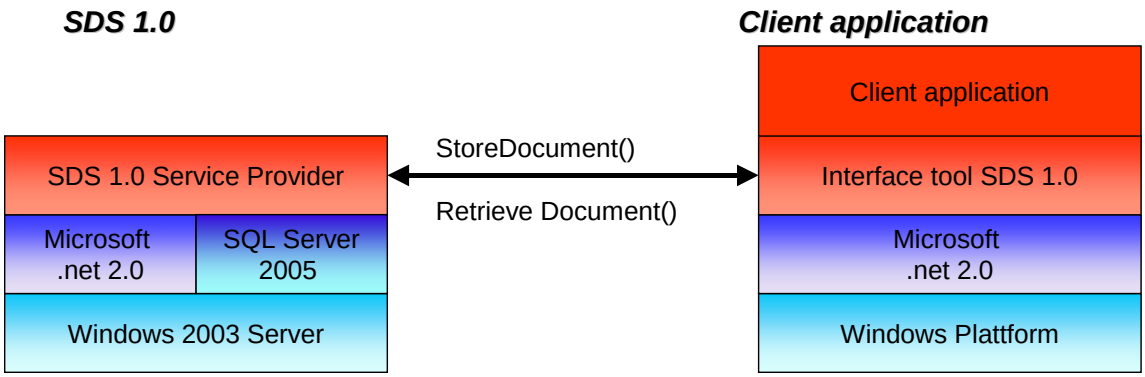
Flexible: SDS supports several cryptographic procedures: AES (system or password), RSA with one key pair or group/quorum decisions (the latter only in conjunction with Hierodiction SKM). It hence enables a large range of application scenarios.

Simple Administration: SDS offers a standard Web service to user applications and can easily be integrated in other applications.

Auditable: Manipulation-protected, encrypted logging with Hierodiction LGG (included in SDS).

Productive: SDS comes with tools facilitating its integration with third-party applications.

SDS is based on the standard Microsoft platform, which enjoys broad industry support.



Contact: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at
All rights reserved. Errors reserved. The text may reference patents or patents pending. April 2010

Application Scenario: E-Voting

EVOTE supports election committees in preparing, monitoring and counting elections or referenda. Its data is encrypted and protected from manipulation by multiple layers of security (s. description of EVOTE and LGG).

However, apart from formatted data a large number of documents are produced in the course of an election:

(a) Minutes and transcripts

(b) Load files

(c) Tables and analyses

(d) Applications, motions and notices

These documents are a non-technical, however material part of documenting and processing an election. SDS enables the secure deposit of such artefacts.

As from SP4 of Release 1 SDS is integrated in EVOTE.

Election Committee

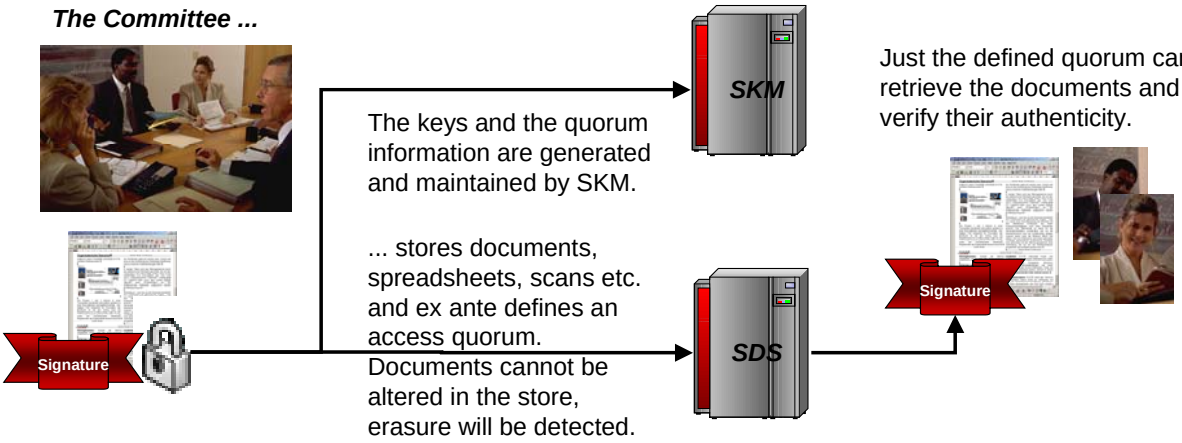
SDS saves EVOTE users to implement a separate document store, which may be expensive and burdensome.

Application Scenario: Document Management in Committees *

In many business or public administration processes, documents are produced which should be stored in a secure and authenticated manner and should only be accessible to the **group in its entirety** or a pre-defined and **unalterable quorum** thereof. Examples include sensitive personal data, files in public procurement or security-sensitive plans or documents.

Only the defined quorum may access the documents.

The deposit of documents and (optionally) every access are logged in LGG. SDS is integrated in the Intrusion Detection Cockpit of LGG which causes an application alarm when encountering suspicious system activities.



* This scenario also requires the quorum and key management in SKM.

Microsoft, Windows, MS Office, Visio, SQL Server and .net are trademarks of Microsoft Corporation. RSA is a trademark of RSA Security Inc. AES is a standard of NIST. Hierodiction is a trademark of Hierodiction Software GmbH.

Contact: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at
All rights reserved. Errors reserved. The text may reference patents or patents pending. April 2010