TrustedX: The Custody of Signed Documents

This article outlines strategic aspects of TrustedX's electronic signature platform related to archiving and preserving e-signatures over time.

Archiving is the long-term storage of documents, e-signatures and associated metadata in repositories. Custody entails guaranteeing the preservation of signatures to maintain their probative value over a given period of time.

TrustedX's custody module implements the document repository interactions required for archiving documents and signatures and managing signature metadata. Signatures are preserved in accordance with the *AdES standards from the European Telecommunications Standards Institute (ETSI).

In terms of repository support, TrustedX's flexible architecture allows adopting a range of implementation strategies. Archiving can be implemented on an external database managed by the platform, based on fixed content storage systems and/or integrated in DMS/ECM content managers using a customized plug-in.

Signature Preservation and Mobility

Verifying signatures entails checking the integrity of the document and obtaining evidence guaranteeing that the digital certificates were valid at the time of signing, i.e., that they had not been not revoked. So this process can be performed after the digital certificates have expired, this evidence must be archived and preserved.

Certificate status information is obtained online via a connection with the certification service provider (CSP) that issued the certificates. This information must be protected cryptographically to assure the signature's integrity over time.

Probative information is lost owing to the passage of time (valid evidence becomes invalid after a certain date) but also possibly owing to the mobility of the signed document (in implementations with a designated evidence store separate from the signature store, the evidence is only valid in the file system).

Safelayer Secure Communications S.A., manufacturer of multi-factor authentication, PKI authentication and e-signature solutions - c/ Basauri, 17 Edif. Valrealty Edif. B Pl. Baja Izq. 28023 Madrid - World Trade Center (Edif. S-4), Moll de Barcelona S/N 08039 Barcelona - +34 917080480 – Safelayer.com

SAFELAYER

The solution to the problem of preserving signatures is set out in RFC 3126/5126 from the Internet Engineering Task Force's (IETF). The CAdES, XAdES and PAdES standards from the ETSI, which TrustedX supports, currently adopt the IETF's initial proposal and define the long-term signature formats and how to preserve certificate evidence over time.

Standardization and document orientation are essential characteristics of the ETSI standards, and the evidences providing the probative value are maintained in the signatures regardless of the repository where they are archived. This approach completely dissociates the document from the repositories and allows verifying the signatures with third-party tools or simply migrating the documents to other systems without loss of the probative value.

Repositories for E-signed Documents

Inherent in archiving electronically signed documents is the organizing and managing of these documents and their properties or metadata, the associated workflows, content and format conversion, and, in particular, aspects related to information searches. Other archiving requirements may include the storage and content integrity guarantee functions offered by some storage systems.

For instance, content managers provide a specialized document management experience by natively providing a graphical administration console and management tools. The option to integrate the TrustedX signature platform in an existing corporate system makes it possible to use these resources instead of having to enter them from a specific repository designated for this purpose, which results in cost savings in staff training and maintenance and the automation of signature management.

This facility is standard in DMS/ECM content management or storage systems and therefore forms part of many common document custody system scenarios. In these scenarios, however, this functionality is difficult to implement using other types of repositories, such as databases.

TrustedX implements archiving (sending documents for custody), status verification (checking the status of one or more documents), document retrieval (retrieving signed documents that can be verified by third parties), deletion (deleting documents) and verification (checking document signatures). Regardless of the repository type, these functions are common and include:

- Content managers. TrustedX has integration mechanisms for using a corporate content manager. In this case, a specific connector for searching for documents and a mechanism for accessing documents based on lightweight clients such as HTTP/WebDAV must be developed.

- External database (future relases). In this scenario, TrustedX supports archiving in Oracle databases, which store and maintain the signed documents and signature metadata.

- Storage Systems[1]. Allows using the corporate storage infrastructure for archiving documents via connectors. Supports EMC Centera storage systems.

In terms of the technical standards of the repository connection, TrustedX supports JDBC for database (Oracle) or accessibility via HTTP/WebDAV (e.g., Alfresco or Documentum). To support fixed content storage systems, such as EMC Centera, connectors for the API's of these devices are supplied. In all cases, TrustedX supports configuring service policies for archiving with different repositories and/or with different properties.

[1] *Option available only through some Safelayer partners. Contact Safelayer for further information.*