

SERVER-MANAGED VS. CLIENT-MANAGED DIGITAL SIGNATURES

Who We Are

Since 1995, Kyberpass has been helping organizations overcome the challenges of building and deploying high-trust applications for corporate enterprises. Kyberpass recognized two very important issues. First, building high-trust applications should not be a one-off integration of a series of security technologies done on a custom basis for a specific customer. Rather it should be a highly integrated, re-useable platform, which hides the details and complexity of the underlying technologies. Second, trust is only as good as the underlying party providing the trust. For this reason, Kyberpass was one of the first companies to recognize and implement the Identrus business integration solution. Identrus banks are trusted third parties (TTPs), which underpin the entire trust infrastructure.

The Issue

Both server-managed and client-managed digital signatures are valid processes when applying electronic signatures to documents or other business objects. However, regulatory and business requirements may favor one method over the other. The primary issue is whether the signing process needs to be centralized (server-managed) or distributed (client-managed). Server-managed signing controls the business process from a single corporate vantage point, allowing operational system checks to enforce permitted sequencing of steps and events. Client-managed signing puts the control in the hands of the signer (client) and relies on the client to follow a given set of rules and processes.

Legal Enforceability

Digital signatures have long been recognized as a viable identity solution for electronic transactions. Given the proper structure, a digital signature is the legal equivalent of a wet signature in a paper-based system. A significant amount of legislation has been passed allowing the use of electronic signatures, including digital signatures.

However, to achieve legal enforceability certain rules must be followed. Some of these rules include:

- A supporting infrastructure mostly external to the record itself
- Strongly integrating digital signatures with application work flows and data storage
- Strong authorization controls for signatories integrated in to application workflows
- Use of trusted time stamps
- Trustworthy and tamper evident audit trails
- Verification of the authenticity and good standing of the signatory at the time of signing by the organization making the validation request to a TTP

Client-Managed Signing

For client-managed signing, as is typical of the Adobe Plug-in for Acrobat and other third party plug-ins, the following applies:

- The signing action is loosely integrated with, or out of control of, the host application
- Signing is solely at the direction of the user
- PDF hashing, time-stamping (from the local PC time clock), reason for signing, signature assembly into the signed PDF all happen locally on the desktop
- Signer (not the organization) may verify himself by making a direct validation (OCSP) check to the TTP and the receipt of this in some way must be integrated into the signature
- Onus is on the recipient of the signed document to verify the signer's identity by making direct validation (OCSP) checks to the TTP, or to somehow extract the signer's self-validation receipt and verify it

- Onus is on the recipient to accept the purported "trusted" signing time
- Loose coupling of the signed and validated PDF to the application server is at the discretion of the signer

While all these components of the signing process are convenient for user-to-user exchanges, they may not meet the strict (e.g. legal) requirements of a corporate policy.

Server-Managed Signing

Server-managed signing takes the signing process up a level and provides for the following:

- PDF (and other business objects) are signed under full control of the Web application within the browser environment
- PDF objects typically remain on the application server, and are just rendered to the desktop
- Users must obtain authorization from the application to sign an object
- Using the Kyberpass PDF Crypto Service the object is prepared for signing, time stamped with a trusted (server) time stamp, and a hash is generated for signing
- Under application control the signature is validated by a TTP and the user's identity is verified and authenticated in real-time via an OCSP check by the *organization*
- The validation response is securely logged on the server
- The PDF Crypto Service assembles the signed PDF and returns it to the application for storage

In a server-managed signing environment, authentication of users and signing policies and procedures can be controlled from a central point. This will improve overall business process and maintain consistency.

Summary

The following chart summarizes the differences between server-managed and client-managed signing:

Item	Client-Managed	Server-Managed
Enforces sequencing of steps & events	No	Yes
Ensures signer is authorized to sign	No	Yes
Verifies authenticity and standing of signer at time of signing	Partial	Yes
Trusted time stamp	No	Yes
Trustworthy and tamper evident audit trail	No	Yes
Computer systems readily available for audit & validation	No	Yes
Ensures a legally binding equivalent	Partial	Yes
Closely coupled to web application	No	Yes
Browser based	No	Yes
Bandwidth requirement (for PDF)	High	Low
Application integration costs	None	Low
Server costs	None	Moderate to High
Client per seat costs	Moderate	Low

Corporate Headquarters: Kyberpass Corporation
1111 Prince of Wales Drive, Ottawa, Ontario, Canada K2C 3T2

Tel 800.845.1140
Direct 613.727.6556
Fax 613.727.8238

www.kyberpass.com

All rights reserved. Kyberpass is a registered trademark. All other names and brands are the property of their respective owners.