

The Strength of User Vs. System Signing

Imagine if everyone had a key to your safe - **Would you still use it?**

If your banker could sign money transfers on your behalf - **Would you allow it?**

Although the answers to these questions are quite obvious, people tend to be more forgiving of the same security lapses with regards to how they sign documentation, even though their personal or company's fortune could be at stake.

This document discusses two digital signature approaches for signing documents or transactions: **User Signing** (or user keys) vs. **System Signing** (or system keys). This paper is designed to provide you with a clear differentiation between the two terms and provide you with the necessary tools for making educated decisions for your organization's digital signature needs.

What are digital signatures?

If we look at paper documents, signatures are the most common legal way to ensure the intent and accountability of the signer. With a track record of hundreds of years, signatures are still the most popular (and legal) method used in business today. That said, history also documents hundreds of thousands of stories of successful signature forgeries.

"A digital signature is a fingerprint, uniquely identifying both the document and the singer."

Today, more and more organizations and businesses are trying to cut the use of paper altogether (and its associated high costs) and complete business processes electronically. Digital signatures take the concept of the traditional paper-based signature into the digital realm, by adding a digital "fingerprint" as a signature to a document. This unique fingerprint distinctively identifies both the document and the signer.

Digital signatures offer your company high security, state-of-the-art technology to ensure:

Data integrity - Any changes made to the document after it is signed are clearly indicated and the signature is consequently invalidated.

Non-repudiation - Each signature is uniquely linked to the signer & document.

What is User Signing and System Signing?

"With system signing, two users can produce the same signature."

With **User Signing**, similar to a physical (wet) signature on paper, each user has a unique signature. This is accomplished by using a private key to create the signature. With User Signing, any two users who sign a document will produce a different signature because each signature is created by the corresponding user's unique private key.

With **System Signing**, all users **utilize the same key** for signing documents. In this scenario, two users signing the same document will produce the exact same signature (assuming time difference is not a factor) because all signatures are using the same key.

The Pitfall of System Signing

Naturally, having all signatures done by one system key introduces a **repudiation problem**. With one signing key used by all users in an organization, a user may deny signing a document. Moreover, proving a signature belongs to a specific individual becomes exceptionally challenging, as all signatures appear the same.

An example of the above scenario would be a doctor that has used a system signing solution to sign a medical report prior to an operation. Later, a malpractice suit was filed involving the signed document. The "signed" document is used to prove that the doctor had been aware of certain problems leading to the malpractice... The doctor can, rightfully or not, repudiate signing the medical report, claiming it isn't his signature and anyone who has had access to the system could have signed it. Of course, if user signing had been used instead of system signing, the doctor could not repudiate his signature, since he was the only one with access to his signing key.

System signing makes sense when a system level operation is being made (e.g. eCommerce transaction that needs to be signed), where no specific user is tied to the process. Another example of sensible system signing would be signing scanned documents as part of the scanning process, in order to ensure a scanned image is identical to the original.

So, why are there system-signing based solutions?

There is no question among legal and security experts that user signing is a far superior solution to system signing, and that user signing should be selected over the use of system signing, whenever possible.

So the question is why do some companies select system signing based solutions instead? The answer is that they either do not know the difference, or don't have the infrastructure on-site to support user signing. At the time, system signing seemed like the easiest answer.

Until CoSign® was developed, user signing required a robust infrastructure that created and managed multiple keys, and renewed the keys upon certificate expiration. While this type of key management was the source for the uniqueness and greater security of user signing, it also added complexity. Because of its simplicity, system signing only needs to manage a single key.

CoSign enjoys the best of both worlds and has a patented design to remove the complexity and operational overhead costs associated with user signing. By providing an easy-to-deploy user signing solution with virtually zero IT management, CoSign is a superior solution over any system based signing solution.

Summary

No one should use a safe that multiple individuals have a key to. System signing based solutions should be avoided to prevent the significant problems that can arise from repudiation issues. Instead, a solution that is easy-to-deploy, verifies signer authenticity, and requires virtually zero-management should be implemented. The CoSign digital signature solution is designed to accomplish all of these things, for a significantly lower cost than a consumer will pay for other digital signature solutions.