



The Strength of User vs. System Signing

Imagine if everyone had a key to your safe.

Would you still buy it?

Imagine if your banker would sign money transfers on your behalf.

Would you allow it?



Although the answers to these questions are quite obvious, when talking about digital signatures, people tend to be more forgiving, even though their personal or company's fortunes could depend on this security.

This document discusses two approaches to digital signatures: **User Signing** (or user keys) vs. **System Signing** (or System keys) for signing documents or transactions. This document is designed to provide you with a clear differentiation between the two terms and give you the tools for making the right decision for your organization.

>>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. However, history is also loaded with stories of successful forgeries of these signatures....

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

Fast forwarding to today, more and more organizations and businesses are trying to cut the use of paper altogether (and its associated high cost) 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. A digital signature is a unique fingerprint, distinctively identifying both the document and the singer.

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 **User signing**, similar to a physical (wet) signature on paper, each user has a unique signature. This is accomplished by a private key used for creating 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 are **using the same key** for signing documents. In this case, 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.

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

>>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 repudiate signing a document, and how can one prove otherwise when all signatures look the same? Any user could have created that signature.

For example, a doctor used a system signing solution to sign a medical report prior to an operation. Later, there was a malpractice suit 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 couldn't 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 (natural person) is tied to the process. Another example would be signing scanned documents as part of the scanning process 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, if 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 the easy way out.

User Signing vs. System Signing

User signing requires a robust infrastructure that creates & manages multiple keys, and renews the keys upon certificate expiration. While this key management is the source for the uniqueness and greater security of user signing, it also adds complexity. Because of its simplicity, system signing only needs to manage a single key.

CoSign enjoys both worlds and has a patented design to remove 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.

To conclude, one should not buy a safe, which has the same key for all owners; system signing based solutions should be avoided to prevent repudiation problems while choosing a solution that is easy-to-deploy with virtually zero-management.



For more information please contact sales@arx.com or visit www.arx.com

Your comments and feedback are welcome