John B.
Harris

DIGITALLY
SIGNED

SIGNiX™

Technology
Frequently Asked Questions
Last updated June 26, 2012

Common Technology Questions

What kind of electronic signature does SIGNiX produce?

SIGNiX uses a specific type of electronic signature known as a "digital" signature. Digital signatures are based on Public Key Infrastructure (PKI), a powerful technology that alleviates online fraud. PKI cuts fraud by several methods, including authenticating the signer and making the signed record tamper-evident.

Is this technology proprietary to SIGNiX?

The identification of the signatory and the process by which SIGNiX creates and provides access to the digital signing credential is a patented process. However, the digital signatures that are produced by SIGNiX products are standards-based, stored in the PDF produced by the system, and can be independently verified outside of the SIGNiX environment.

The signatures are produced according to ISO 32000-1 (PDF), and include cryptographic elements that are also standards-based (x.509, RSA, DSA, SHA and others).

Document consumers (signatories and viewers) need not refer back to SIGNiX for verification of the signatures because each individual signature or initial action is a digital signature and those signatures are fully resident in the PDF itself.

E-signature services that don't utilize digital signatures for each signing event require document recipients to check with their proprietary service to validate individual signatures, meaning if the service goes out of business or is shut down, those signed documents may be put into question.

SIGNiX does keep a detailed audit log, however, for evidentiary purposes. This audit log is also available as part of the signing process, and can be provided in XML and PDF versions.

What is a digital signature? How is one created?

A digital signature is a document fingerprint (a.k.a. hash), encrypted with a PKI private key.

A digital signature is created as follows: The contents of the document being signed are used to create a very long number, called a hash code, which is unique for that document and similar to a fingerprint. The hash code is encrypted using the signer's private key. The resulting encrypted hash is a digital signature.

The owners of private keys are required by the rules of PKI to maintain the secrecy of their private key so that only they can make their digital signature. According to these rules, the key owner can be held responsible for any use of their private key.

In SIGNiX, certificates and private keys are managed automatically by the SIGNiX solution. The private keys are stored in *encrypted form within a secured system. The key owner authorizes use of their private key by entering their signing credentials into a dialog during an online document signing ceremony.*

The key owner may be held responsible for any digital signature created in this way. If a user knows or suspects that their signing credentials have been compromised, they must go to the SIGNiX web site as soon as possible at https://www.SIGNiX.net, log in, and change their signing credentials, or notify SIGNiX or an administrator immediately.

Digital signatures are usually accompanied by the digital certificate of the signer, which is a public version of the signing credentials that is used to verify signatures as well as verify the authenticity of the credentials themselves.

What is signature verification? How does it work? Why should I do it? How do I do it?

When you receive a signed electronic document, the certificate accompanying the signature identifies who signed. But why should anyone trust what the certificate says? Both the document and the signer's certificate are electronic records. Electronic records are easily altered. How can you be sure that the document you have was actually signed by the person identified in the certificate and that no changes have been made to the document? Signature verification provides this assurance.

With a simple digital signature, signature verification software takes the signer's public key from the certificate and uses it to decrypt the digital signature and recover the original hash code. It then computes a new hash of the signed document and compares the new hash to the decrypted original. If they match, the verification succeeds…otherwise it fails.

SIGNiX uses a more sophisticated digital signature algorithm, known as DSA, which achieves the same effect without allowing decryption of the original hash. DSA signatures have the interesting property that they do not reveal the hash of the original document if a new hash doesn't match.

Successful verification indicates that the public key in the certificate is correct, since an incorrect public key would not cause the digital signature to produce a matching hash. Successful verification also indicates the document has not changed since signing—if the document had changed, then the new hash would not match the one in the signature. If the signature itself had been changed, it again would not produce a matching hash.

In order to verify that the person identified in the certificate is the actual owner of the public key, verification software must check the integrity of the signer's certificate. There are several questions that must be answered to verify a certificate, including the following:

- *Is the certificate unaltered since being issued?*
- *Is the issuer trustworthy?*

A certificate is an electronic record with its own digital signature. Each certificate is signed by the Certification Authority that issued it. The verifier confirms the validity of the certificate by verifying this signature. In order to do this verification, the verifier uses the public key from a certificate belonging to the issuing CA.

The verification process is then repeated on the issuer's certificate and again on any certificates above it. If this chain eventually leads to a "trusted root" certificate that is already known to the verification software as being trustworthy, then the verifier considers the signer identification in the original certificate to be valid, otherwise it does not.

The verifier must also check that the signature was created at a time when all of the certificates in the verification chain were within their valid usage period and none of *them had been revoked. For SIGNiX signatures, the signing time is indicated by a reliable timestamp placed on the signature by a Timestamp Authority immediately after the signature was created.*

In documents signed by SIGNiX, the PDF viewer is normally configured to automatically verify signatures whenever a document is viewed.

Will the validity of the digital signatures outlast the certificate expiration date? In other words, how do I verify a signature years later?

Yes. Each signature's digital certificate is verified at the time of signing, and that 'revocation status is embedded into the PDF document to provide signature validity over the long-term. This so-called 'long-term validation' or LTV allows the signatures to remain valid in a PDF, even after the certificates have long since expired, assuming the certificates were *valid at the time of signing.*

What is the difference between a digital signature and a digitized signature?

Digital signatures should not be confused with digitized signatures. A digitized signature is a graphical representation of a handwritten signature. Digitized signatures are typically obtained through means of an electronic signature pad, or by scanning a handwritten signature from a paper document. Obviously, digitized signatures by themselves cannot be used to verify digital transactions, since they can be easily forged.

Can digital signatures be easily forged?

No. The type of cryptosystem and the length of the keys determine how difficult it is to forge a digital signature. SIGNiX maximizes security of signatures by using the U.S government standard Digital Signature System (DSS), with extremely large 2048-bit keys.

Without knowing the user's private key, it is impossible to forge their digital signature. This makes creation of a digital signature more secure than a paper-based ink signature, as long as access to the private key is strictly controlled.

The key owner may be held responsible for any digital signature created by someone with knowledge of their signing credentials. If a user knows or suspects that their signing credentials have been compromised, they should notify SIGNiX directly or go to the SIGNiX web site as soon as possible at https://www.SIGNiX.net, log in, and change their credentials.

What is a timestamp? What are they used for? How do I know that a signer signed at a particular time?

A timestamp is a digitally signed record that associates a reliable time with some other record. Timestamps can be used to demonstrate that the other record existed in a specific form at the indicated time.

SIGNiX timestamps user's electronic signatures in order to reliably record the time at which the signature was created. SIGNiX uses the SIGNiX Timestamp Authority to create these timestamps.

What is a Timestamp Authority?

A Timestamp Authority is a service that records the time of an event (a timestamp) based on time sources that are not from the signer's computer, and thus not as subject to manipulation.

SIGNiX uses the SIGNiX Timestamp Authority. SIGNiX timestamps are digitally signed using DSS with a 2048-bit key and are in PKIX Time-Stamp Protocol (RFC 3161) format. Also, as SIGNiX can use certificates from other Certificate Authorities, SIGNiX can leverage their timestamping services as well.

What is a digital certificate?

A digital certificate is an electronic record containing a user's public key. The main purpose of a certificate is to identify whom a key pair belongs to. Certificates also declare limits on when and how the private key can be used.

Certificates are issued and managed by Certification Authorities (CAs), who vouch for the accuracy of the information they contain.

Since certificates are electronic records, they can be easily tampered with. For this reason, certificates are digitally signed by their issuer. Verifying the signature on the certificate confirms who issued the certificate and indicates whether the information in the certificate has remained unaltered.

SIGNiX uses certificates issued by the SIGNiX Certification Authority and also other broadly trusted CAs, including Symantec. All SIGNiX certificates are in X.509 version 3 format. SIGNiX certificates are signed using 2048-bit keys.

Do my users need to carry a smart card or USB token with them to sign documents? I thought PKI required these devices?

SIGNiX provides the power, assurance, reliability, and integrity of digital signatures without the hassle of additional hardware devices. Users simply authenticate and click to sign their documents, and SIGNiX handles all of the keys, certificates and technology behind the scenes. Users need only bring themselves (or a mobile phone, if you choose that form of authentication).

How does a user identify and authenticate him or herself to the system? What types of user authentication do you offer?

SIGNiX offers several levels of user authentication to best match the level of risk associated with the transaction itself. These are described below in ascending order of strength.

- *Basic: Email-only authentication. Proves a user has access to a specific email address.*
- *Sponsored / Pass-thru: Leverages authentication provided by an integrated partner's system.*
- *SMS / Text Message: Sends a text message with a one-time password to a user's mobile. Proves a user has access to an email address and a specific mobile device.*
- *Identity Vetting / Know Your Customer (KYC): Confirms specific information about a user, such as social security number, date of birth, etc. Proves that a user not only has an email address but also possesses more privileged information.*
- *Knowledge-Based Authentication (KBA): Asks the user very specific questions about past residences, possessions, and transactions. Proves that a user not only has access to an email address but also possesses significantly privileged information.*

Do you create the signing certificates / credentials for each user? Or do I need to do that?

SIGNiX takes care of all of the key and certificate creation for you so that you don't have to.

Can SIGNiX work with a certificate authority (CA) that we request?

Yes, SIGNiX can work with certificates from other Certificate Authorities if requested. Contact SIGNiX for more details on this.

What is a Certification Authority (CA)?

Certification Authorities issue and manage digital certificates. CAs are called authorities because they vouch for the accuracy of the information in the certificates they issue.

Certification Authorities also maintain repositories of published certificates and certificate revocation lists.

SIGNiX uses the SIGNiX Certification Authority and also other broadly trusted CAs, including Symantec. A user gets a SIGNiX certificate by registering for a SIGNiX digital identity. The SIGNiX certificate and CRL repository is available at https://www.SIGNiX.net/pki.jsp.

What is certificate revocation? When should I revoke my certificate? How do I do it?

Certificate revocation makes the corresponding private key no longer useful for creating digital signatures. Signature verifiers that check certificate revocation lists will not verify digital signatures created after revocation of the associated certificate.

A key owner must revoke their certificate if they know or seriously suspect that their private key has been compromised—meaning that it could be used to create unauthorized digital signatures.

In the SIGNiX solution, certificates and private keys are managed automatically by SIGNiX. The private keys are stored in encrypted form within a secured system. An end-user does not normally need to revoke keys within this system. Nevertheless, if a user with a digital identity wants to ensure that the certificate associated with the account has been revoked, they should perform the account recovery procedure on their digital identity account. Recovering signing credentials causes revocation of the subscriber's existing certificate and re-issuance of a new certificate with a new key pair.

Users with a digital identity authorize use of their private key using their signing credentials. Users are responsible for maintaining the secrecy of their signing credentials. Users may be held responsible for any use of the corresponding private key when this use occurs under the direction of a user that has been properly authenticated using these credentials. If a user knows or suspects that their signing credentials have been compromised, they must immediately go to the SIGNiX web site at https://www.SIGNiX.net, log in, and change their signing credentials, and notify SIGNiX or an administrator immediately.

What is the normal lifetime of a certificate? What happens when a certificate expires?

Since the risk of compromise of a key increases over time, Certification Authorities place a limit on the useful lifetime of each private key. The normal lifetime of a private key is determined by the validity period of the corresponding certificate. Signature verifiers will not verify digital signatures created after expiration of the associated certificate.

Generally, SIGNiX-generated end-user certificates expire after 2 years.

Certificates provided by SIGNiX Certificate Authority partners typically have expiration dates requested by the client, and may vary from the two year lifetime described above.

Security and Compliance

Is your datacenter SAS-70 certified?

Yes, the datacenter hosting the SIGNiX services is actually SSAE-16 SOC1 certified, which is the updated and current standard, and it features physical and *logical security controls exceeding industry requirements.*

How do users choose to sign multiple signature fields at once, with a single click?

Although this capability is possible within the SIGNiX solution, it is disabled by default because specific industries and applications deem this capability unacceptable due to security and/or regulatory concerns.

How does SIGNiX protect the signing credentials / keys?

All private keys are stored in an HSM according to cryptography best practices and standards. The generation of the private keys and their association with identities is tied to a SIGNiX patented process wherein credentials are accessed by a combination of user PIN and information stored by SIGNiX.

Additional detail can be provided under NDA. Please contact SIGNiX for more information.

Is an audit log generated that includes information on each transaction?

Yes, a comprehensive audit log is created as the document(s) move through the process, with each action carefully tracked.

Note that due to the use of digital signatures on the document, the signed PDF(s) also includes information about each signature so that a viewer of the document can see explicit details about when and how each signature and initial step was taken.

Is the audit log secured in any way against tampering?

Yes, the audit log is digitally signed to provide tamper-evidence.

Does SIGNiX store the audit log record?

Yes. We track and store a detailed list of transaction details. This information can also be downloaded as a PDF alongside the signed document(s) and is available as XML content that can be imported into your own systems of record.

Do you store documents?

Although SIGNiX can readily be used as a storage service for documents, it is neither necessary nor recommended in most cases. SIGNiX recognizes that users have widely varying requirements for the storage of customer transactions and information and would prefer to take on the responsibility for storing those documents alongside other documents they already manage for their business. SIGNiX does keep a copy of the audit trail for evidentiary purposes, but this information is not publicly accessible from SIGNiX.

What is the Retention Policy for SIGNiX stored documents?

ESIGN requires retention and availability for the life of the agreement so SIGNiX keeps documents until such time as the customer has stored a copy and requested shredding (destruction) of the document possessed by SIGNiX.

How does SIGNiX destroy documents when they are no longer needed?

SIGNiX electronically shreds documents according to DOD standard 5220.22-M.

What happens if SIGNiX goes out of business?

Because SIGNiX signs documents with digital signatures in compliance with industry standards, such as PDF, you can be assured that your documents will be capable of independent verification within PDF viewers that fully support the ISO

32000-1 (PDF) standard. This means that you do not need to rely on servers that SIGNiX controls simply to check the validity of SIGNiX-signed documents in your possession, unlike other eSignature services.

Moreover, SIGNiX provides the documents directly to customers to store in their own systems, rather than keeping them. (See above) Customers have the ability to maintain these signed files independently of SIGNiX.