

Instructions or techniques allowing the online notary public's electronic notarial certificate to be read and authenticated:

SIGNiX uses a specific type of electronic signature known as a "digital signature." The digital signatures that are produced by our system are standards-based and aren't proprietary. Digital signatures use coded messages that are unique to both the document and to the signer, and this protects the document against tampering.

Our digital signatures can be independently verified without checking back with SIGNiX's system because the supporting legal evidence has been embedded into the PDFs directly.

SIGNiX's signatures can be verified using free PDF viewing software like Adobe Reader.

When opening the PDF, Adobe should display a blue banner at the top, or should have a "Validate" button to use, and each signature can be clicked on for additional details.

The signatures are produced according to ISO 32000-1 (PDF), and include cryptographic standards, including x.509, RSA, DSA and SHA. Also included is the digital certificate, which is an electronic record containing a user's public key. Digital certificates are used to identify who a key pair belongs to, and they also declare limits on when and how the private key can be used.

Certificates are issued and managed by Certification Authorities (CAs), who are called "authorities" because they vouch for the validity of the information in the certificates they issue. CAs also maintain repositories of published certificates and certificate revocation lists. SIGNiX is authorized as an official Certification Authority and also uses other broadly trusted CAs.

All of our certificates are in X.509 version 3 format and are signed using 2048-bit keys.

To perform a verification on a signed document and its digital certificate, 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 trusted by the verification software, then the verifier considers the signer identification in the original certificate to be valid.

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a time when all of the certificates in the verification chain were within their valid usage period and none of them had been revoked.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 trusted Timestamp Authority immediately after the signature was created.