

What is a Digital Signature?




A Review of PKI
Technology and Practical
Application.

Digital Signature

- Allows an individual to sign, seal or notarize a document electronically.
- Allows anyone looking at the electronic document to verify:
 - The identity of the signature owner
 - Whether or not the document has been altered since it was signed.
- This is done using the Public Key Infrastructure.


Examples of a Digital Signature

Can be personalized to include an image of your seal or hand written signature.



Steve Palmer

Digitally signed by Steve Palmer
DN: c=US, st=Florida, l=Tallahassee, ou=Growth Management, o=City of Tallahassee, cn=Steve Palmer, email=steven.palmer@talgov.com
Date: 2009.10.30 16:01:28 -04'00'



Paula D. Burn
Commission # DD530199
Expires March 31, 2010
Bonded Troy Firm - Insurance, Inc. 800-989-7918

Digitally signed by Paula D. Burn
DN: cn=Paula D. Burn, c=US, o=National Notary Association, ou=9d205234eb73d2d29caa7c13aa03f106ae2908de
Date: 2009.11.04 10:45:09 -05'00'

Signature of Notary

Public Key Infrastructure (PKI)

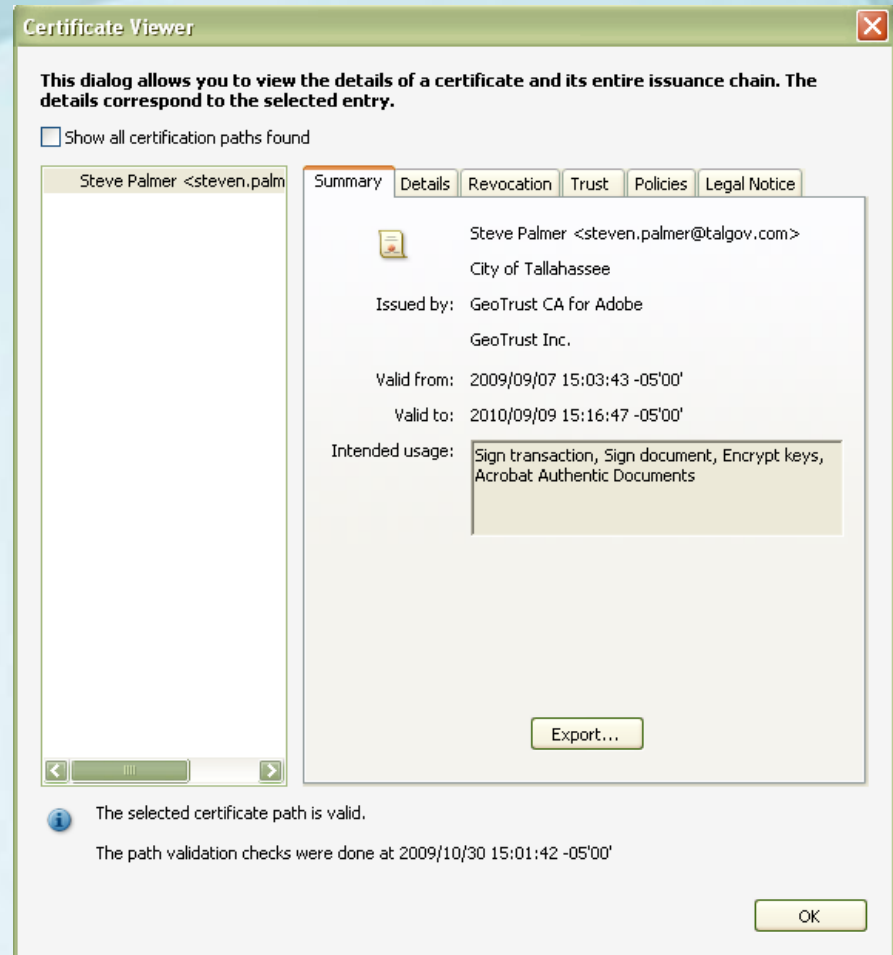
- Is defined as a set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke digital certificates.

Example of a Certificate

Name, Email Address and company affiliation of signature owner

CA that issued the Certificate

Additional details like public key and date stamp can be found under the Details tab.

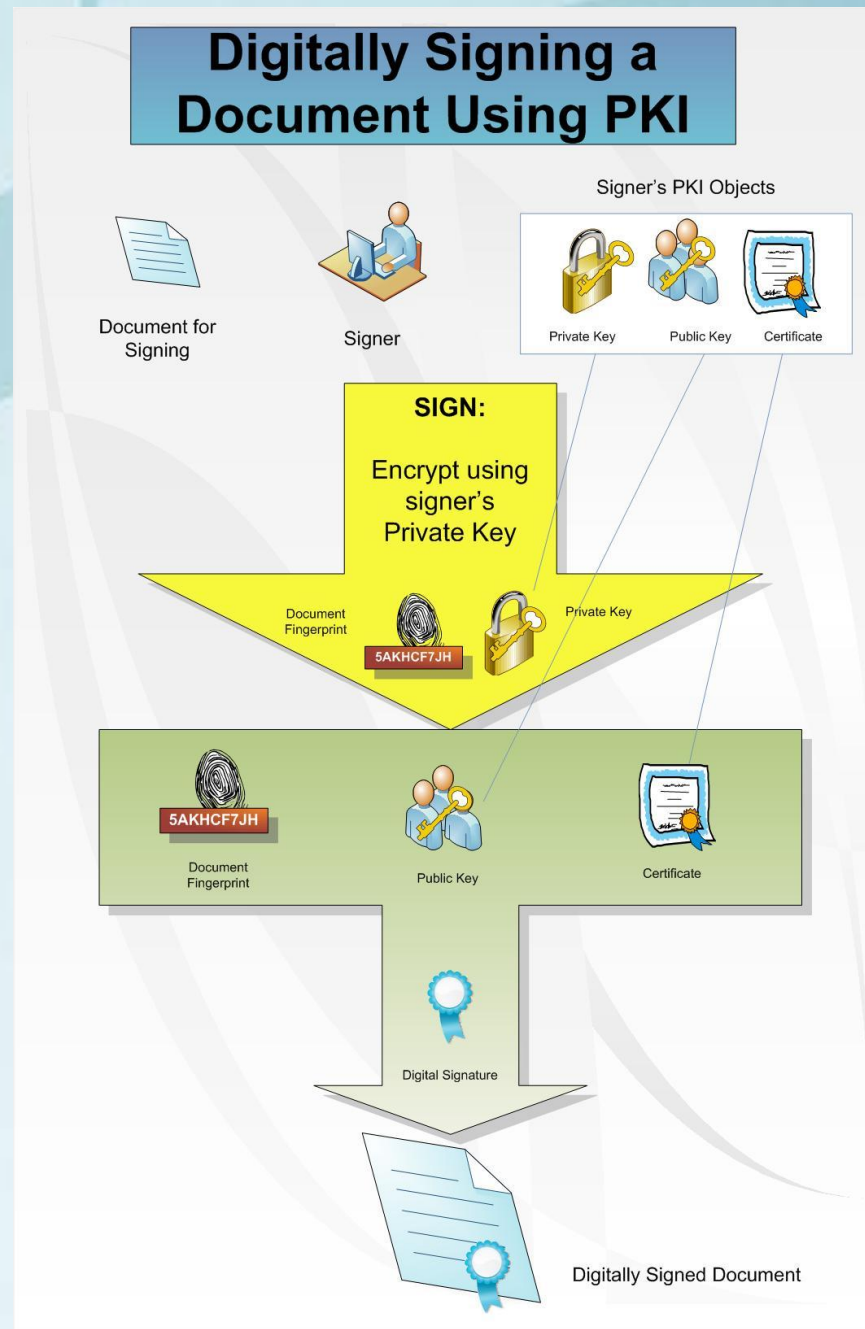


Certificate Authority (CA)

- Defined as an entity that issues digital certificates for use by other parties.
- Also known as a “Trusted Third Party”
- Responsible for verifying the identity of an individual that they issue a digital certificate to.
- Examples of CAs:
 - GeoTrust
 - IdentTrust
 - Global Sign
 - Chosen Security
- For a complete list of CAs recognized by the City of Tallahassee for issuing digital signatures please contact 891-7078.

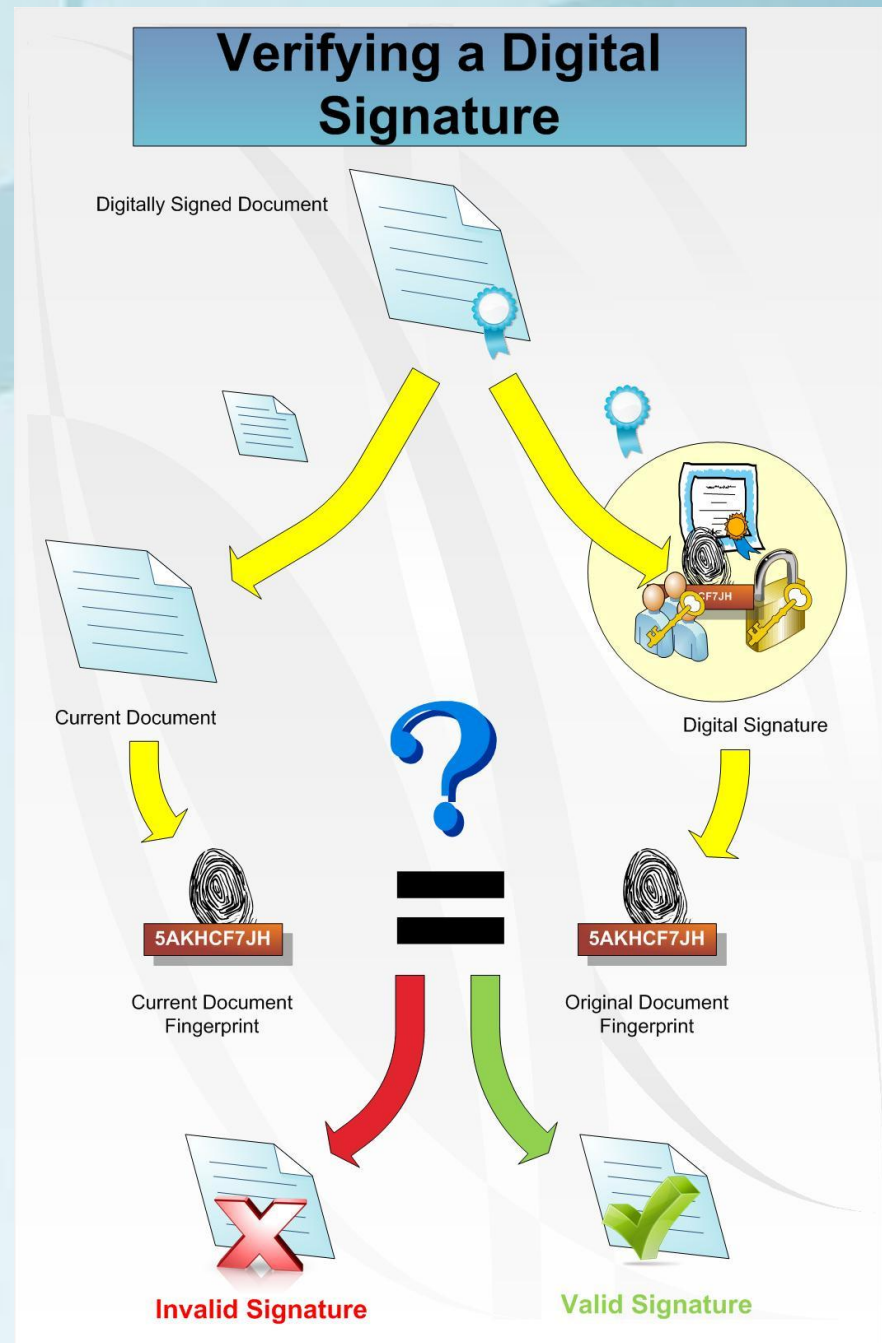
Digital Signature Technology: Signing

- Public Key Infrastructure or PKI is the technology used in digital signature process.
- It is made up of both a public key which is visible to everyone and a private key which is not.
- During the signing process a document fingerprint is hash encrypted using the signer's private key.
- The hash encrypted fingerprint, along with the signer's public key and the signer's certificate from a 3rd Party Certificate Authority(CA) are elements in the digital signature.



Digital Signature Technology: Verifying

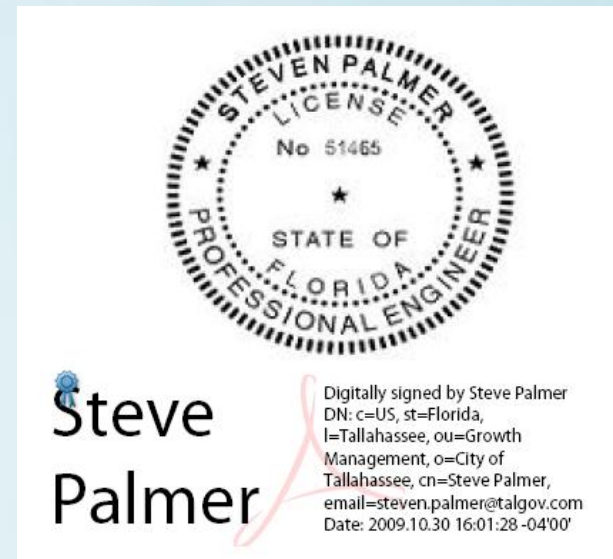
- The signature can be easily verified as being valid by checking the certificate. If the document has been altered or if there is possibly an issue with the certificate the certificate ribbon will often display an “x” or caution sign.
- When a signature is verified by PDF viewer, the viewer checks the current documents and it’s document fingerprint against the decrypted document fingerprint stored in the signature. If the two match, the document is valid. If the two do not match, the document has been altered and is no longer valid.



Buying and Using a Digital Signature

- Our customers can find information and links to our trusted 3rd Party Certificate Authorities on our web site.
- Cost of digital signature certificates varies greatly starting at about \$60.00 a year and goes up.
- Certificate Authorities should have at least a NIST level 3 for verifying the signer's identity.
- Signatures should be able to be applied using a PDF authoring software such as Adobe Acrobat.
- The digital signature should have the capability to incorporate an image of the signer's signature or seal.
- Training on how to apply a digital signature will be provided by the Certificate Authority.

The screenshot shows the Talgov.com website for the City of Tallahassee. The header includes the Talgov.com logo and navigation tabs for Residents, Businesses, Government, Visitors, Students, Your Own Utilities, and E-Services. The main content area is titled "Digital Signature Certificate Authorities" and contains a dropdown menu for "Transactions" and a text block explaining that the City is reviewing its policy on Electronic Signature, Electronic Seals and Electronic Notary to bring that policy inline with the method of electronic seals adopted by the Board of Engineers. It references Chapter 61G15-23.003 of the Laws and Rules of the Florida Board of Engineers. Below this, there is a section for "Other Growth Management Areas" with a list of links including Growth Management Home, Applications and Forms, Residential Permits, Permitting Process, City Fast Tracking Initiative, City Projects, Online Permitting, Fee Schedule, Land Development Process, Building Inspection, and Concurrency. To the right, there is a "Related Links" section with links for City Projects, Online Permitting, Development, Construction, Licenses and Permits, and Permits and Regulations. A "Share This" section with a Facebook icon is also present.





Question??