|  |  |
| --- | --- |
| *Trust Elevation Method:* | Digital Certificates (X.509 PKI). Although digital certificates are most often used as primary credentials for authentication, encryption and/or signing, there is no intrinsic reason they cannot be used as secondary assertions of identity. |
| Questions: |  |
| Which party is performing the method? Include details of multiple parties and attestation where appropriate. | Digital certificates are issued by Certification Authorities to computer code, subscribers, groups, and devices. |
| How does the method improve trust? | A secondary credential can reinforce the identity assertion(s) of the primary credential or assertion. |
| How does the method address the threat of eavesdropping? | n/a |
| How does the method address the threat of online guessing? | The cryptographic technology of the digital certificate minimizes the threat of online guessing, though a lightweight key pair with obsolete hash algorithm is vulnerable to cracking. |
| How does the method address the threat of replay attack? | * Session tokens – can serve as session tokens * OTP – can utilize digital certificates * Nonce with message authentication code (MAC) * Timestamping – strengthens timestamping substantially |
| How does the method address the threat of man in the middle?   * Man in the browser * Boy in the browser * Man in the mobile | * PKI based mutual authentication * PKI based encryption |
| How does the method address the threat of spoofing and masquerading?   * SMS spoofing * IP address spoofing * CallerID spoofing | Digital certificate technology is a credential-based method and does not address these threats |
| Are there implementation requirements for improving trust? If so, what are they and why are they necessary? | The trustworthiness of cryptographic technology is very sensitive to implementation practices. Rather than describe implementation requirements, refer to the documentation of the Federal PKI Policy Authority through [www.idmanagement.gov](http://www.idmanagement.gov) . |
| How does the method address the threat of theft | The private key is protected by a password, biometric or nonce. |
| How does the method address the threat of phishing?   * Phishing * Spear Phishing (Whaling) * Clone Phishing | Digital certificate technology is a credential-based method and does not address these threats |
| How does the method address the threat of credential duplication? | Each certificate contains one or more unique private-public key pairs based on proven cryptographic technologies. |
| How does the method address the threat of session hijacking? | Digital certificate technology is a credential-based method and does not address these threats |
| Are there privacy and/or confidentiality issues engaged when using the method, such as user consent for attribute release/exchange? Are there reasonable solutions for potential privacy impacts? | The concerns are the same as for any other credential-based alternative. |
| What are the usability issues when using the method? Are there reasonable solutions for potential usability impacts? | Software applications are only now reliably enabled to use PKI for authentication and signing. Operating systems are now PKI-aware and there are evolving implementation options for the basic technology that make it more user-friendly. That said, the process of engaging a digital certificate for any of its functions should require validation, which requires infrastructure to discover the path to the issuer’s directory service and software to deliver the answer in a way the application can use. |