PAIIWG at ASIS

Tim Baldridge

September 16, 2008

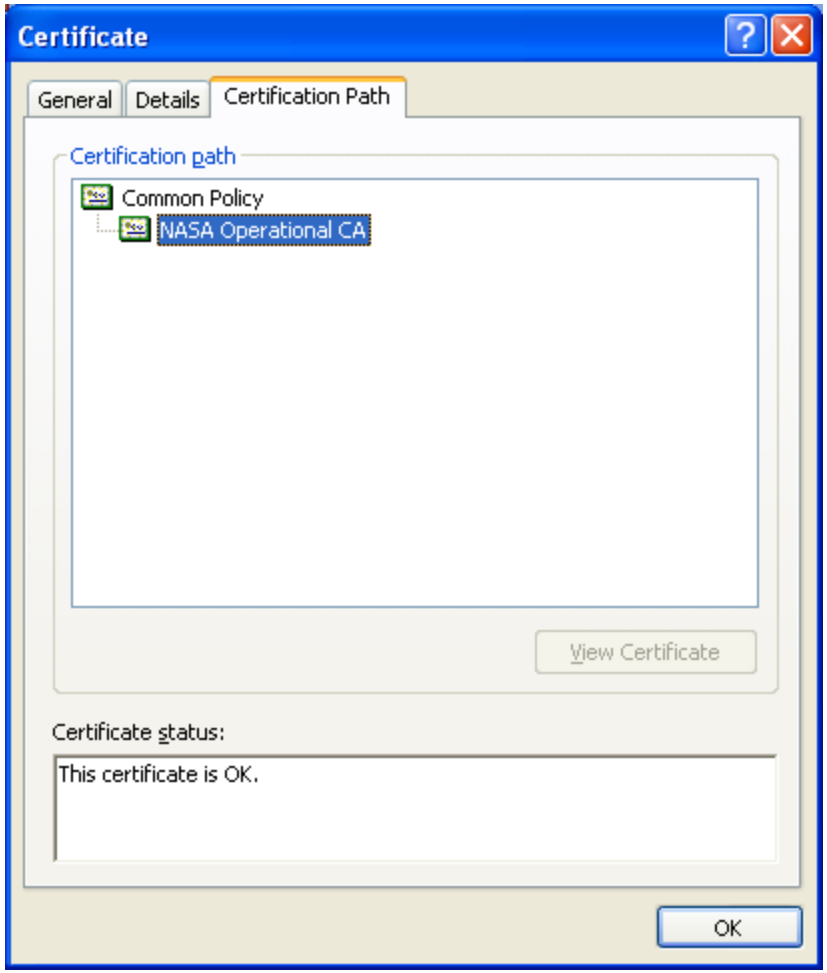
Topics

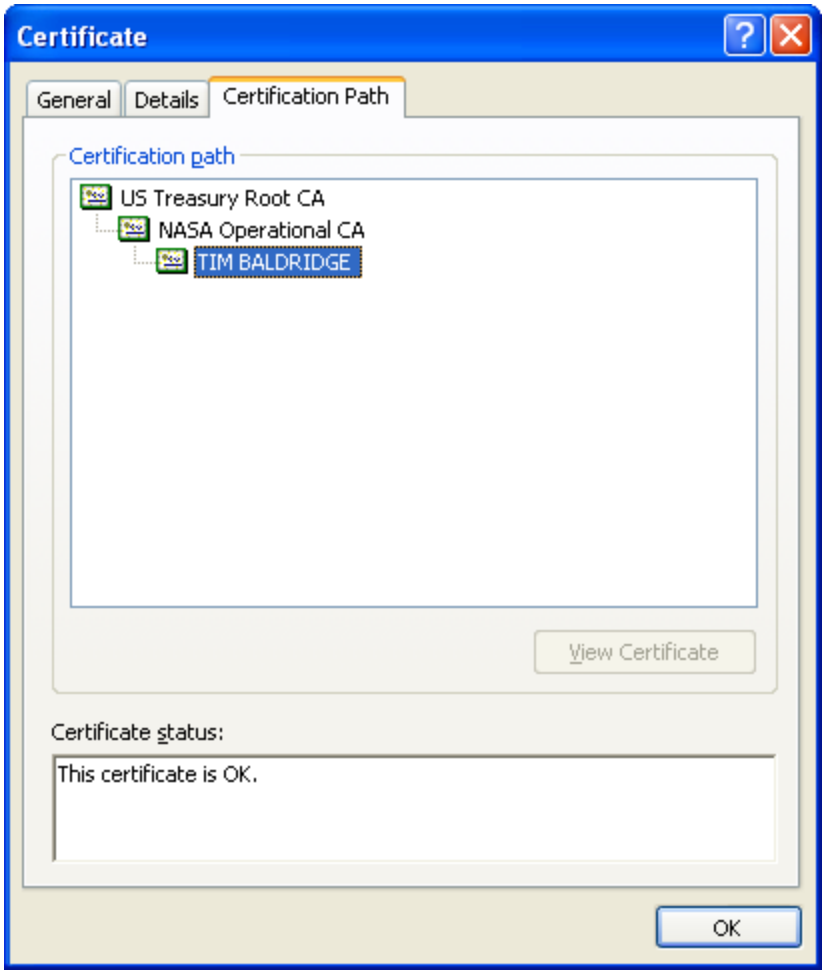
- Trust Anchor
- Cryptographic Soundness
- Card Authentication Key
- PIV Identifier Model

Trust Anchor

- What is it?
  - A self-signed root certificate that a relying party accepts as authoritative
- PIV Cards
  - Common Policy (Root CA)
- PIV Interoperable Cards
  - Federal Bridge (Root CA)
- PIV Compatible Cards
  - ?? (Root CA)

Example PIV Trust Chain





Cryptographic Soundness

- A Qualitative Description of Business and Technical Practices Which Insure Integrity And Confidentiality
- Keying materials
  - What is the Key Use
  - Chain of Custody in Key Distribution
  - Who has control
  - How many entities possess a key

Card Authentication Key

- Asymmetric
  - PKI Based Infrastructure Exists
  - Uncommon in PACS Applications
  - Policy Enforced Unique Key per Card
- Symmetric
  - Faster algorithm
  - No Enterprise Key Management Infrastructure
  - Typical Deployment Uses Only a Few System-wide Keys Across a Card Population

PIV Identifier Model

- ISSUE
  - How to Extend Numbering to Non-Federal PIV Interoperable Card Issuers
  - Both Legacy And New PACS Must Enroll Cards to Enable Efficient Recognition at Point-of-Access
  - In The CHUID the GUID is Intended for this Purpose but Remains Inadequately Defined