

Update on PAIWG

Setting the Priorities for Interoperability

Tim Baldrige
December 2, 2008

Organization

- PAIIWG Facilitates Industry and Government Communication
- Involved Government Personnel Recognize Issues
- Identification of Root Authority and Scope
 - Executive Order 12977, Amended 13286
 - HSPD-7, HSPD-12 and HSPD-24,
 - OMB Memos M04-04 & M05-24
 - RTCA DO-230B

Purpose

- Define options for interoperable numbering schemas for both Federal and non-Federal issuing authorities suitable for physical access control and related identity applications
- Determine and define options for protocols providing a high level of assurance for physical access control systems that meet Government interoperability and performance requirements
- Define options for contactless access control protocols that meet privacy and security requirements of the Government

Next Steps

- Submission of a Interagency Security Committee project proposal
- Convene PAIWG for work on PIV Identifier Model

Questions

Tim.Baldrige@nasa.gov

BACKUP

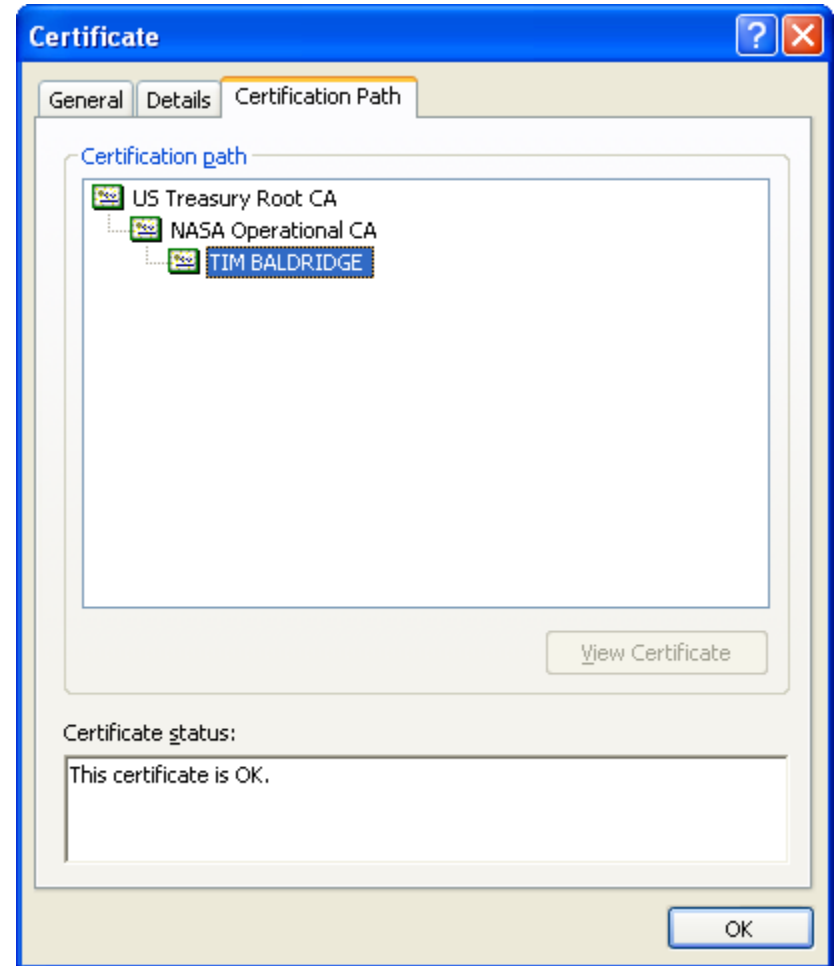
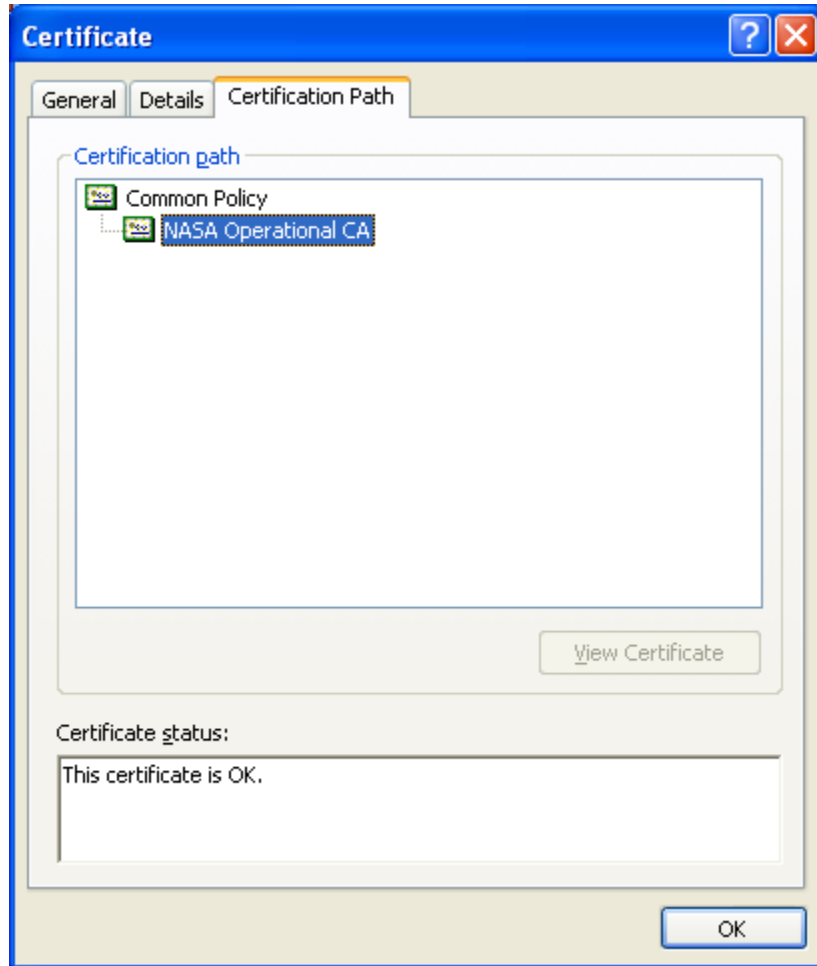
Topics

- Trust Anchor
- Cryptographic Soundness
- Card Authentication Key
- CAK PACS Issues
- 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

Card Authentication Certificate Enabled PACS Readers

- Challenge Is To PKI Enable Legacy PACS Door Readers
- Legacy - Two Step Mechanism
 - Enroll PIV Card With Full PKI To Head-end.
 - Hash Of Cert Or Public Key With FASC-N To Panel
- Next Generation - Full PKI Revocation Check At Each Access Point.
- SCVP vs OCSP vs CRL Checking

CAK PACS Issues

- Card Readers On The “Attack” Side Must Allow Bi-directional Communication
- Card Readers On The “Attack” Side Must NOT Contain Persistent PACS Level Secret or Private Keys
- Card-to-Reader Communication Must Not Reveal Identity Prior to the Card Validation of the Authenticity of the Reader

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

Device Identification Verification

- Secure Computing Environment for PACS
 - Must Identify PACS Devices.
 - Readers
 - Door Controllers
 - Panels / Local System Redundancy
 - Numbering of PACS
 - Registration of PACS Identifier on PIV Card by PCI
 - PACS DIV relates to PACS Crypto – PLAID
 - Security Technology
 - HSM, SAM, SIM