



Identity, Credential, and Access Management

The Need for Device Authentication and Verification

February 24, 2010

Tim Baldrige

AWG Co-Chair

Office of the CIO

NASA

tim.baldrige@nasa.gov



Introduction

- Today, we as consumers
 - Enjoy the convenience of wide acceptance of card based purchasing
 - Expect privacy in transactions
 - Expect only authorized transactions
- These are core principals of comprehensive security
 - Availability
 - Confidentiality
 - Integrity



The Problem...

- In the open...
We must protect against actions which will do harm
- In a card (or token) based transaction both the card and the terminal must have effective countermeasures to threats against C.I.A.
- This is true for Logical Access Control, including Information Assurance and Confidentiality, and Physical Access Control



Today...

- In the Federal community we have PIV and PIV-I is emerging where
 - Contact based Logical Access uses a PKI based mutual authentication
 - Contactless based Physical Access uses a free read CHUID and in very few places PKI/asymmetric or symmetric authentication
- FIPS 201 and SP 800-73 define PIN protected and free read data elements on PIV (and PIV-I).
 - Nefarious entities may attempt to skim free read data from PIV
 - Imposter terminals may attempt to trick individuals in to entering their PIN, thereby increasing the attack surface.



The Gap ...

- The current standard and technology for PIV is based on the requirement of a terminal authenticating the card.
- The countermeasure against “leaking” information is for the card to authenticate the terminal.



Identity, Credential, and Access Management

The Solution...

