

# Multi-factor Authentication Considerations for InCommon Silver



Mary Dunker – Virginia Tech

dunker@vt.edu

InCommon Confab

April 26, 2012



# Disclaimer

- All opinions expressed in this presentation are strictly my own. IdPs should perform due diligence in justifying their management assertions when applying for InCommon Silver certification.

# Multi-factor for Silver

- Community approach
- Virginia Tech's approach
- Your approach?



# Our Goal



# Our Guidance

InCommon®

## Identity Assurance Profiles Bronze and Silver

9 May 2011  
Version 1.1

# Why Multi-factor?

- Deficiencies in meeting some aspect of requirement
- Handing out “something you have” creates opportunity to strengthen process
- Multi-factor can strengthen authentication security



# Our Problem

## 4.2.3 CREDENTIAL TECHNOLOGY

These InCommon IAPs are based on use of “shared Authentication Secret” forms of identity Credentials. If other Credentials are used to authenticate the Subject to the IdP, they must meet or exceed the effect of these requirements.

# CIC Silver Collaboration

- University of Chicago
- University of Illinois
- Indiana University
- University of Iowa
- University of Michigan
- Michigan State University
- University of Washington (partner)
- University of Minnesota
- Ohio State University
- Pennsylvania State University
- Purdue University
- University of Wisconsin-Madison
- Virginia Tech (partner)





# Community Approach

Review sections of IAP unique to multi-factor.

- 4.2.3.1 Credential Unique Identifier
- 4.2.3.2 Resistance to Guessing Authentication Secret
- 4.2.3.3 Strong Resistance to Guessing Authentication Secret
- 4.2.3.4 Stored Authentication Secrets
- 4.2.3.5 Protected Authentication Secrets



# Community Approach

Criteria: Describe how to “meet or exceed” requirements using MF.  
Guidance from NIST 800-63.

Examples:

- Single factor token = *something you have* and must be used in conjunction with another factor – *something you know*
- Multi-factor token = *something you have* that requires activation with another factor



# Types of Tokens

Out-of band token

One time password token

Digital certificate

Cryptographic token

Vendor security specifications




# Single-factor Token Combination

Question: Must both factors meet all requirements?

Consensus: At least one factor must “meet or exceed.” Consider whether factor that does not meet requirements strengthens or weakens security.





# Multi-factor (integrated) Token Considerations

How is device activated?

How is the “shared  
Authentication Secret” stored  
and protected?

Does “activation password”  
meet Silver?

# Community Resource: Multi-factor Considerations

- Examples
  - Single factor combination
  - Multi-factor token
- Sample Management Assertions for multi-factor token requiring activation
- FAQ

<https://spaces.internet2.edu/display/InCAssurance/Multi-factor+Considerations>

# Virginia Tech's Approach

- Digital Certificate on USB hardware token (SafeNet 64K USB eToken Pro)
- Central Authentication Service
- Shibboleth



# Virginia Tech's Approach

Personal Digital Certificate (PDC)  
with “bronze” and “silver” object  
identifiers (OID)





# Virginia Tech's Approach

... on USB hardware token  
(SafeNet 64K USB eToken Pro)  
issued in-person



# Integration

- x.509 authentication in CAS login handler
- CAS sees bronze or silver OID
- CAS passes information to Shib
- Shib asserts Bronze or Silver Identity Assertion Qualifier

# Why?

- Userid/password process lacked identity proofing step
- Scope analysis (during CIC collaboration) showed Silver likely to only be required by services that employees use – not students.
- PDCs on eTokens already issued in-person, to employees
- Existing policy documents for PKI helped with audit

# Your Approach

- Who is planning to use multi-factor for InCommon Silver?
- What kinds of MF devices are you using?
- How's it going?

<https://spaces.internet2.edu/display/InCAssurance/Community+Contributions>