Building Trust and Security
Adventures in Access Management on Campus and in the Cloud

October 30, 2014
Building Trust and Security: Adventures in Access Management on Campus and in the Cloud

Moderated by Steve Devoti, University of Wisconsin-Madison

- Adventure #1: Ann West, Internet2 InCommon
- Adventure #2: Mary Dunker, Virginia Tech
- Adventure #3: Renee Shuey, Penn State
Adventure #2
Achieving Security Through InCommon Silver

MARY DUNKER, VIRGINIA TECH
dunker@vt.edu
THE SETTING

Identity Assurance Profiles
Bronze and Silver
2. All personnel with login access to IdMS Operations infrastructure elements must use access Credentials as least as strong as the strongest Credential issued by the IDPO.
4.2.3 CREDENTIAL TECHNOLOGY

ALTERNATIVE MEANS for meeting criteria

x.509 personal digital certificate on SafeNet eToken
THE PLOT

All personnel with login access to the following Virginia Tech applications and servers use a credential at least as strong as the personal digital certificate on an eToken.

- Token Administration System
- EJBCA (PKI)
- Directory Administration Tool
- Person Registry database server
- Shibboleth server
- CAS server
- LDAP server
THE PLOT (WITH VILLAIN)

Fall, 2013, Admin Password Compromise in Windows Active Directory Child Domain
THE SAFE HOUSE

IdMS Operations
Infrastructure Elements
SECURITY IS BEING ABLE TO SLEEP AT NIGHT.
Virginia Tech Multi Factor Authentication Working Group will recommend plans to implement multi-factor one-time password technology for critical applications and servers.

The Adventure continues…