Hardware Token Assurance for UCTrust

David Walker
Office of the President
University of California
David.Walker @ ucop.edu

Overview

- eAuthentication Context
  - OMB M-04-04 (and FIPS PUB 199)
  - NIST 800-63
- Implications for UCTrust
- Next Steps?

OMB M-04-04 Criteria for Required Assurance Level

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information (FIPS PUB 199)	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

FIPS PUB 199 Confidentiality Impact Descriptions

	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

(FIPS 199 also describes impacts for *Integrity* and *Availability*)

NIST 800-63 (Selected) Criteria for Assurance Implementation

	Assurance Level Requirements			
	1	**2**	**3**	**4**
Hard crypto token (FIPS 140-2 Level 2)	x	x	x	x
1-time password device (FIPS 140-2 Level 1)	x	x	x	
Soft crypto token (FIPS 140-2 Level 1)	x	x	x	
Passwords & PINs	x	x		
Assertions acceptable	x	x	x	
Remote registration acceptable	x	x	x	
Number of ID's required	0	1	1	2

Implications for UCTrust

- Level 3
  - New UCTrust Assurance profile, layered on *UCTrust Basic* (*UCTrust TwoFactor*?)
- Level 4
  - New UCTrust Assurance profile, layered on *UCTrust Basic* (and new Level 3 profile?)
  - A class of applications that do not use Shibboleth, and/or a "Level 4 Shibboleth" profile.

Next Steps?

- What are the use cases?
- How do existing UC hardware tokens fit in?
- Potential activities
  - Define UCTrust assurance profiles
  - RFP for tokens (at different levels?)