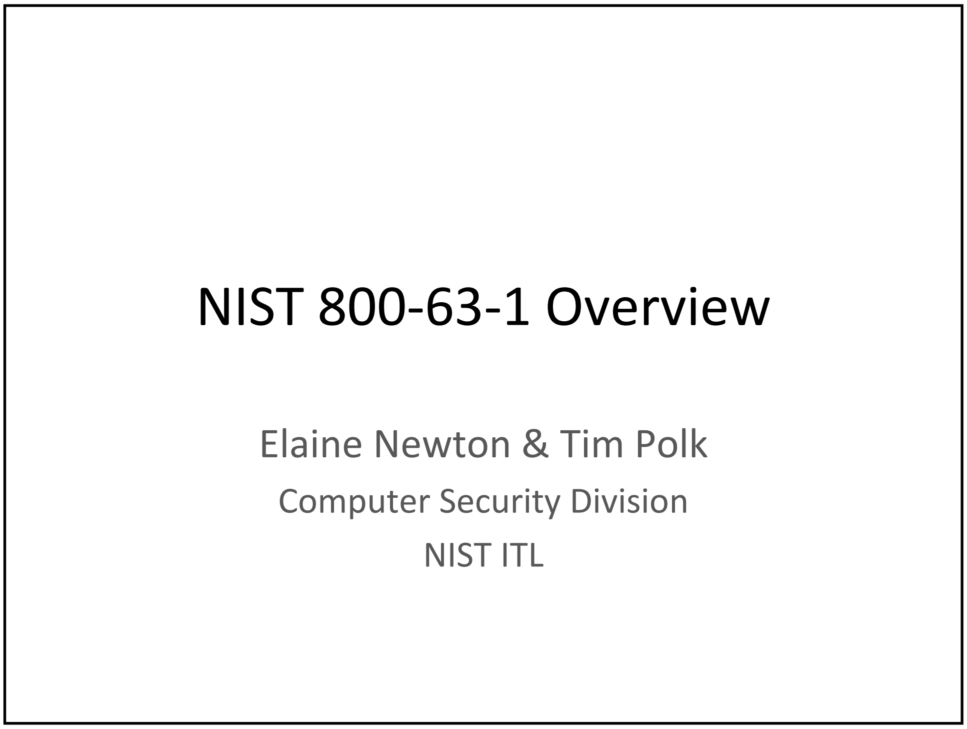
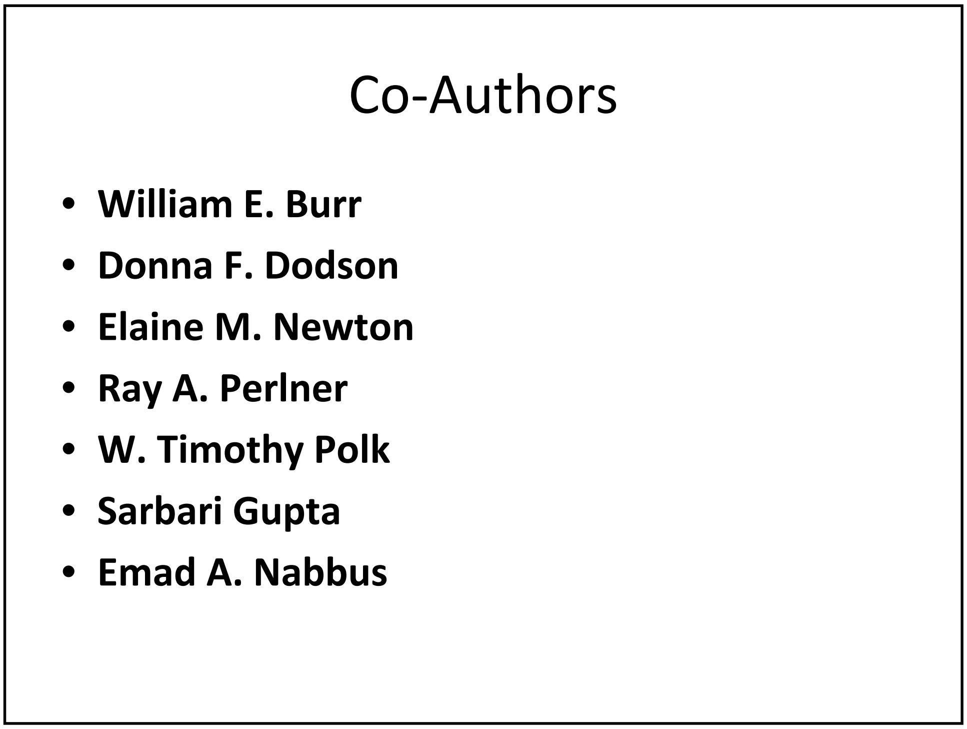


NIST 800-63-1 Overview

Elaine Newton & Tim Polk

Computer Security Division

NIST ITL



Co-Authors

- **William E. Burr**
- **Donna F. Dodson**
- **Elaine M. Newton**
- **Ray A. Perlner**
- **W. Timothy Polk**
- **Sarbari Gupta**
- **Emad A. Nabbus**

SP 800-63-1

- Scope: technical authentication framework for remote authentication
  - registration & identity proofing
  - token types
  - authentication protocols
  - token and credential management

OMB Memorandum 04-04

- E-Authentication Guidance for Federal Agencies (12/16/2003)
  - Agencies classify electronic transactions into four levels of authentication assurance according to the potential consequences of an authentication error
  - NIST develops complementary authentication technical guidance to help agencies identify appropriate technologies
  - Agencies req’d to begin implementation in 90 days after NIST issues guidance

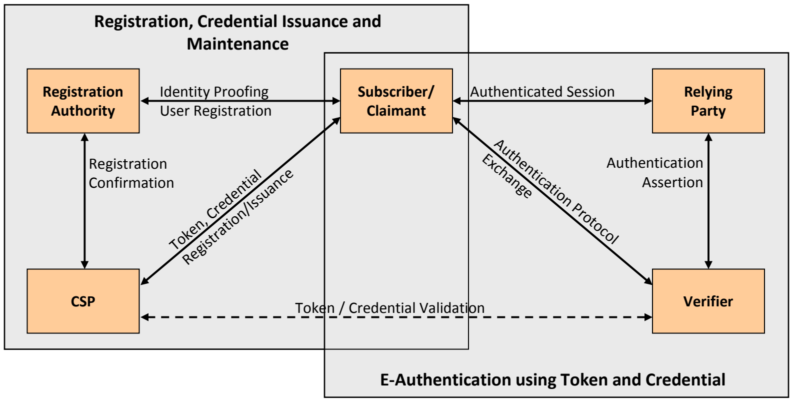
Why Levels of Assurance?

- OMB 04-04
  - Describes 4 assurance levels, with qualitative degrees of confidence in the asserted identity's validity:
    - Level 1 = Little or no confidence
    - Level 2 = Some confidence
    - Level 3: High confidence
    - Level 4: Very high confidence
  - NIST Special Publication 800-63-1
    - Technical requirements for remote authentication over an open network in response to OMB 04-04
    - Revision to SP 800-63 (published in 2006)
- Security Commensurate with Need
- One Size Does Not Fit All!

Rewind: The Response to 800-63

- It's Fantastic
  - Finally, a basis to compare mechanisms!
- It's Too Prescriptive
  - What about bingo cards?
  - What about remote biometrics?
  - What about knowledge based authentication?
  - What about combinations of tokens?

Figure 1: The 800-63-1 E-Authentication Model



Registration, Credential Issuance and Maintenance

Registration Authority

Identity Proofing
User Registration

Subscriber/ Claimant

Authenticated Session

Relying Party

Registration Confirmation

Token, Credential Registration/Issuance

Authentication Protocol Exchange

Authentication Assertion

CSP

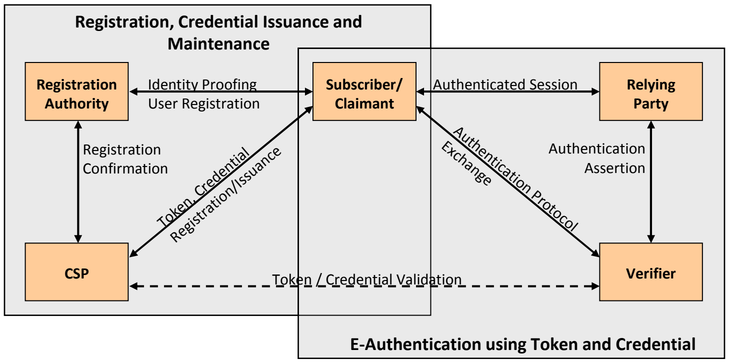
Token / Credential Validation

Verifier

E-Authentication using Token and Credential

The Players (1 of 2)

- Token: is a secret, or holds a secret used in a remote authentication protocol
- Subscriber: A party whose identity or name (and possibly other attributes) is known to some authority
- Credential Service Provider (CSP): A trusted authority who issues identity or attribute tokens



Registration, Credential Issuance and Maintenance

Registration Authority

Identity Proofing
User Registration

Subscriber/ Claimant

Authenticated Session

Relying Party

Registration Confirmation

Token, Credential Registration/Issuance

Authentication Protocol Exchange

Authentication Assertion

CSP

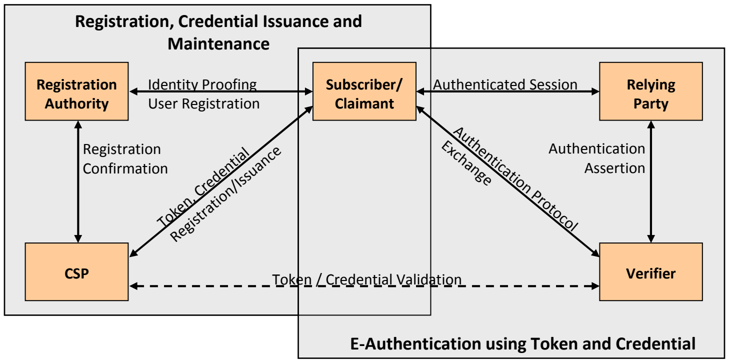
Token / Credential Validation

Verifier

E-Authentication using Token and Credential

The Players (2 of 2)

- Registration Authority (RA): registers a person with some CSP
- Relying party: relies on claimant's identity or attributes
- Verifier: verifies claimant's identity


Registration, Credential Issuance and Maintenance
Registration Authority
Identity Proofing
User Registration
Subscriber/ Claimant
Authenticated Session
Relying Party
Registration Confirmation
Token, Credential Registration/Issuance
Authentication Protocol Exchange
Authentication Assertion
CSP
Token / Credential Validation
Verifier
E-Authentication using Token and Credential

Level 1 Authentication

- Single factor: typically a password
- Can't send password in the clear
  - May still be vulnerable to eavesdroppers
- Moderate password guessing difficulty requirements

Level 2 Authentication

- Single factor: typically a password, but several additional options
  - Must block eavesdroppers (e.g., password tunneled through TLS)
  - Fairly strong password guessing difficulty requirements
  - May fall to main-in-the middle attacks, social engineering & phishing attacks

Level 3 Authentication

- 2 factors, typically a key encrypted under a password (soft token)
- Must resist eavesdroppers
- May be vulnerable to man-in-the-middle attacks (e.g. phishing & decoy websites), but must not divulge authentication key

Level 4 Authentication

- 2 factors: “hard token” unlocked by a password or biometric
- Must resist eavesdroppers
- Must resist man-in-the-middle attacks
- Critical data transfer must be authenticated with a key bound to authentication

Tokens

- Passwords
- Out of Band Tokens
- Soft Cryptographic Tokens
- One Time Password Devices
- Hard Cryptographic Tokens

Response to Draft(s) of 800-63-1

- When will we see another revision?!
- What about all the techniques we see used more and more?
  - What about knowledge-based authentication?
  - What about biometrics?
- How can this be done cheaper and faster, especially for those with PIV cards?
- How Does This Relate to NSTIC?

What’s New?

- Authentication Technologies
- Derived Credentials
- FICAM-managed Assessment
- Clarified Scope

What’s New?: Authentication Technologies

- Recognition of more types of tokens, including pre-registered knowledge token, lookup secret token, out-of-band token, as well as some terminology changes for more conventional token types;
- General support for tokens in combination;
- Detailed requirements for assertion protocols and Kerberos;
- Simplification of guidelines for password entropy and throttling; and
- More comprehensive lifecycle with new section on token and credential management.

What’s New?: Derived Credentials

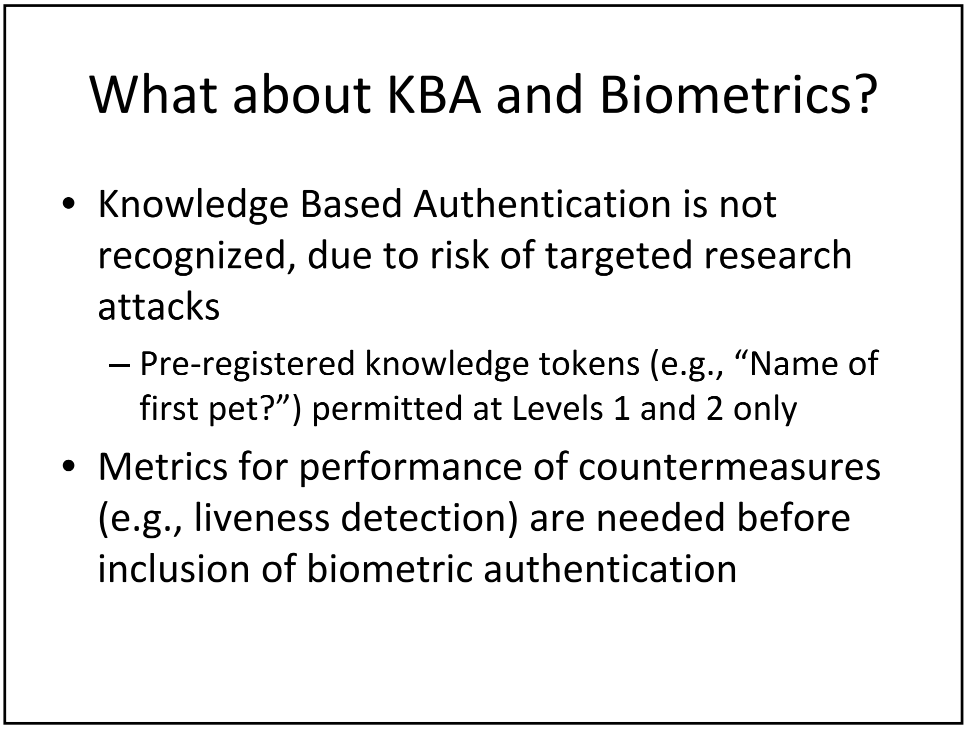
- New guidelines that permit leveraging existing credentials to issue derived credentials
  - – Assurance level for derived credentials from the same CSP cannot exceed the assurance level associated with the original credential
    - proof of possession and control of the original token may be substituted for repeating identity proofing
  - – Assurance level for derived credentials from a different CSP must be less than the assurance level associated with the original credential
    - Special case allows issuance of new Level 4 credentials if CSP can collect and verify a biometric

What’s New?: Assessing Conformance

- SP 800-63 is silent regarding conformance processes
- Acceptance of third party credentials created a demand for assessment of CSPs
  - No NIST-managed conformance assessments
  - Assessing systems through the Federal Chief Information Officer Council’s Trust Framework Provider Adoption Process (TFPAP)

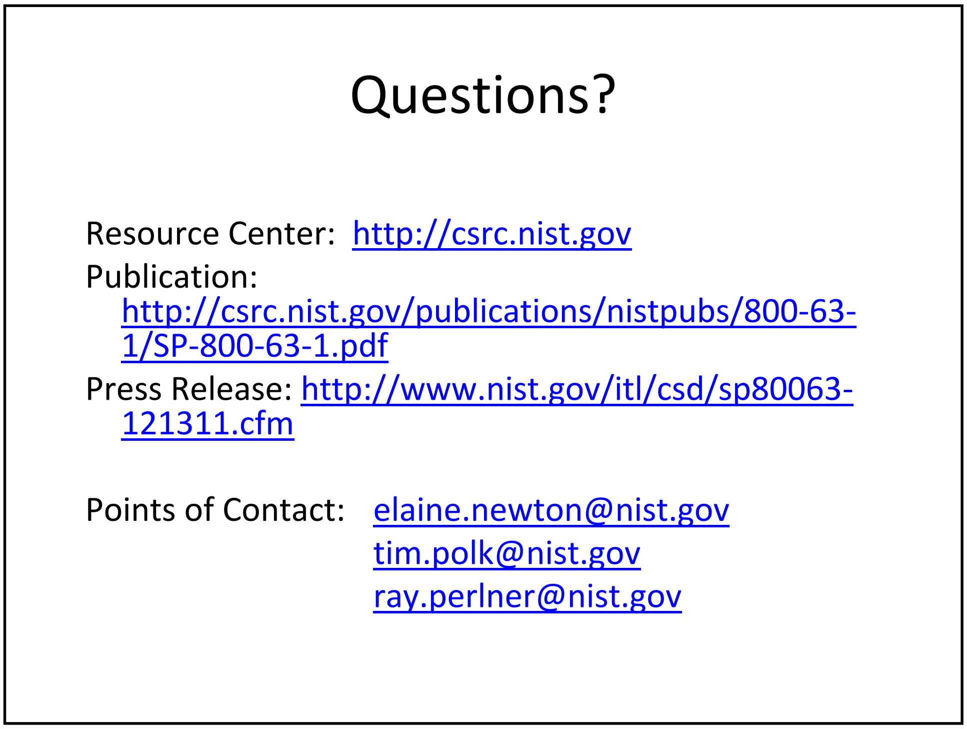
What’s New?: Clarified Scope

- Emphasis that the document is aimed at Federal IT systems;
  - Informs but does not restrict the development of standards or guidelines to support NSTIC
- Recognition of different models, including a broader e-authentication model (in contrast to the simpler model common among Federal IT systems shown in Figure 1) and an additional assertion model, the Proxy Model, presented in Figure 6.
  - Pre-positioning for adoption of future NSTIC standards and guideline development



What about KBA and Biometrics?

- Knowledge Based Authentication is not recognized, due to risk of targeted research attacks
  - Pre-registered knowledge tokens (e.g., “Name of first pet?”) permitted at Levels 1 and 2 only
- Metrics for performance of countermeasures (e.g., liveness detection) are needed before inclusion of biometric authentication



Questions?

Resource Center: http://csrc.nist.gov

Publication:
http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

Press Release: http://www.nist.gov/itl/csd/sp80063-121311.cfm

Points of Contact: elaine.newton@nist.gov
tim.polk@nist.gov
ray.perlner@nist.gov