

NIST 800-63-1 Overview

Tim Polk

Computer Security Division

NIST ITL

OMB 04-04, E-Authentication Guidance for Federal Agencies, (12/16/2003)

- 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
- Agencies classify electronic transactions according to potential consequences of an auth error
- NIST tasked with developing complementary technical guidance

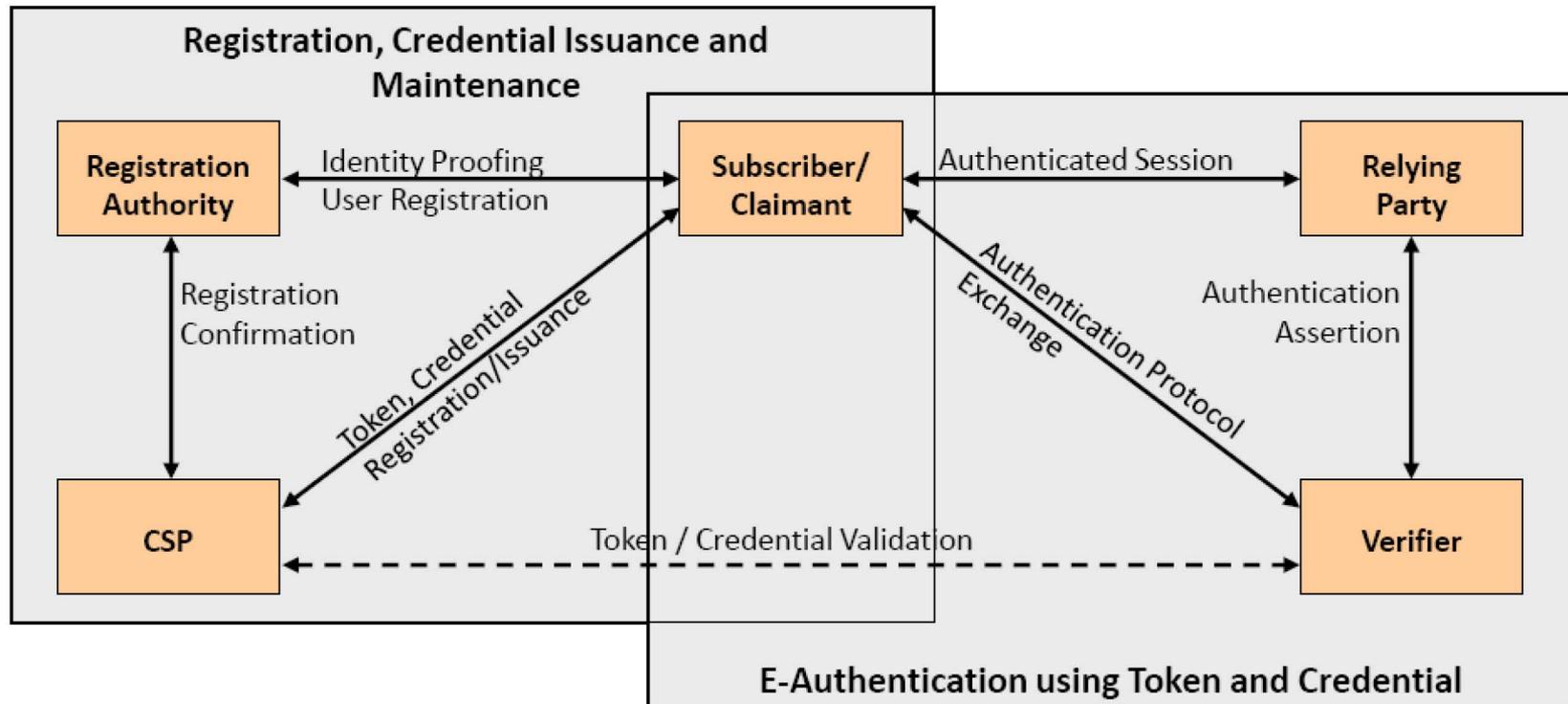
SP 800-63/63-1

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

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



NOTES: The Players:

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

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

What's New in -1? What's Missing?

- What's New
 - Authentication Technologies
 - New types, generalized support for combinations, and more detail on assertions and lifecycle
 - Derived Credentials
 - Leveraging existing credentials to issue new credentials without identity proofing
 - FICAM-managed Assessment
 - Separate identity and attribute providers
- What's Missing
 - KBA
 - Remote biometrics

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