NIST Special Publication 800-63-1

Elaine Newton & Ray Perlner

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

Scope

- Technical framework for remote authentication
  - registration & identity proofing
  - token types
  - token and credential management
  - authentication protocols

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

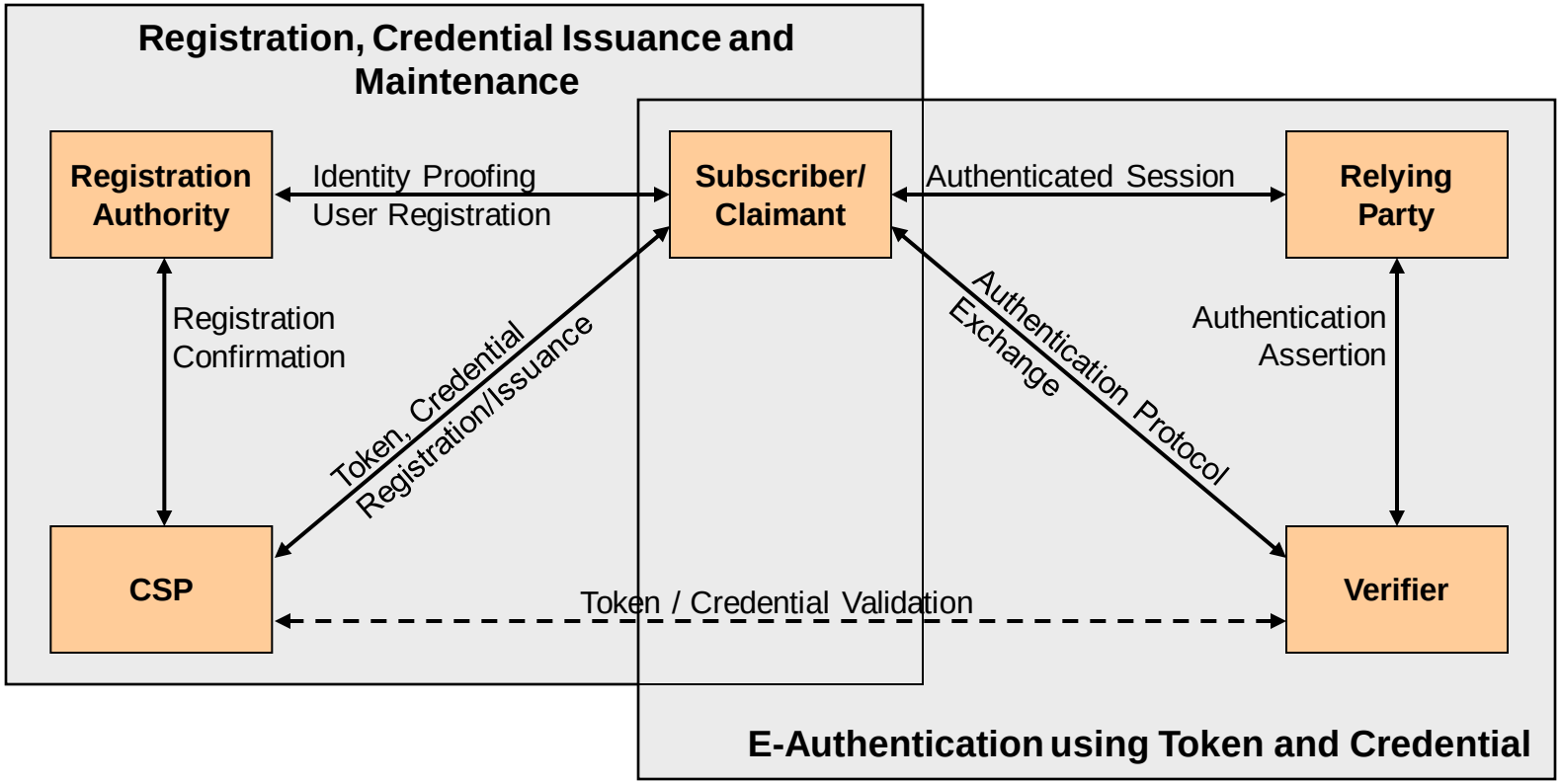
- It's Fantastic
  - Finally, a basis to compare mechanisms!
- It's Too Prescriptive
  - What about bingo cards?
  - What about remote biometrics?
  - What about knowledge based authentication?
  - What about combinations of tokens?

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?

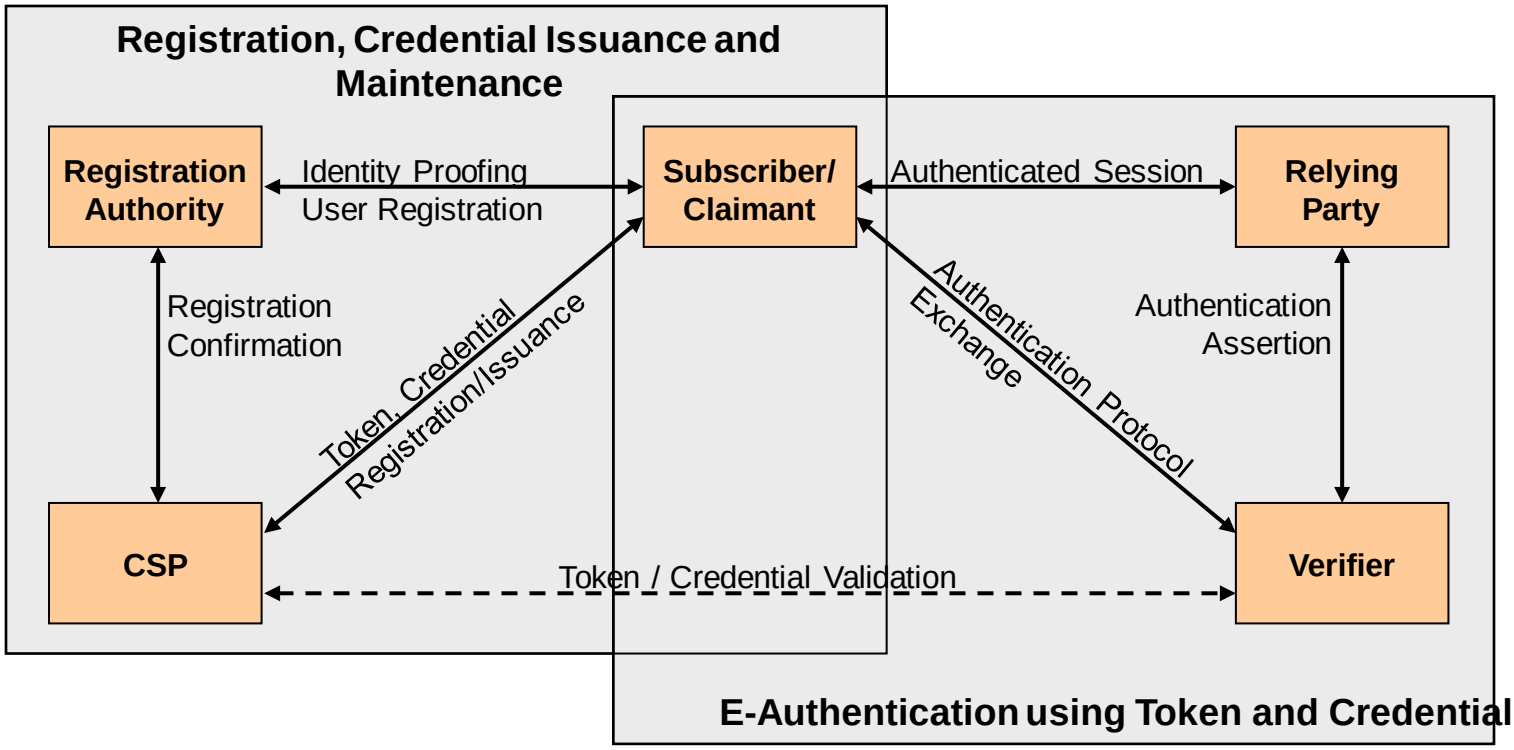
SPECIFICS BY SECTION

The 800-63-1 E-Authentication Model



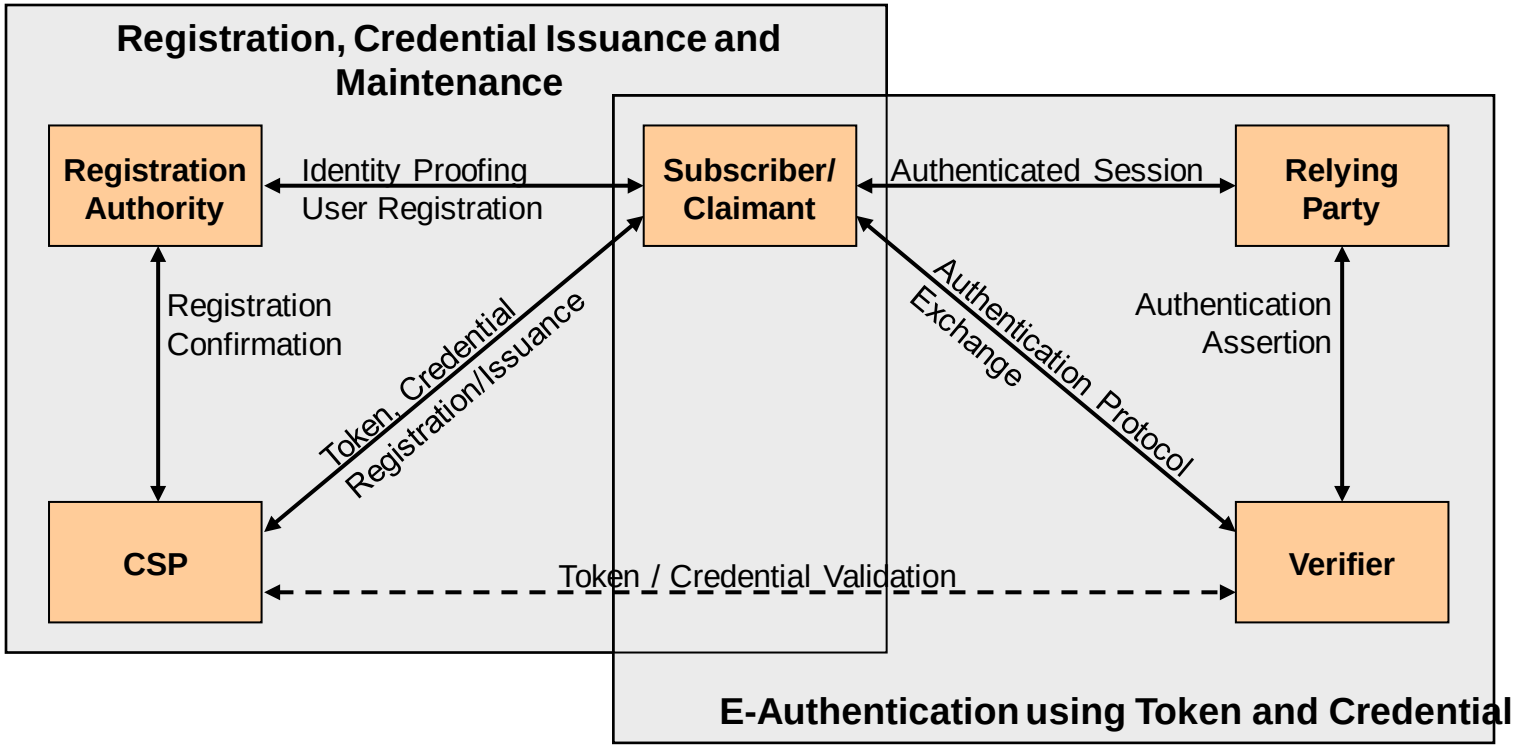
The Players (1 of 2)

- 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



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



Calculating the Overall Authentication Assurance Level

- Overall AL is the low watermark of the ALs for each of the components (i.e., the likely target for the attacker)
  - Registration and identity proofing
  - The token (or combination of tokens)
  - Binding between the identity proofing and the token(s), if done separately
  - Authentication protocols
  - Token and credential management processes
  - Authentication assertions (if used)
- There is no such thing as AL 2.5, 3.25, etc. according to 800-63-1 (or 800-63).

GETTING STARTED: REGISTRATION & ISSUANCE

Registration and Issuance Threats

Registration	Impersonation of claimed identity
	Repudiation of registration
Issuance	Disclosure
	Tampering
	Unauthorized issuance

Names Used in Credentials

- Verified Name (Level 3 and above)
  - RA has determined that the name is officially associated with a real person and the Subscriber is the person who is entitled to use that identity
- Pseudonym
  - RA has not verified the Subscriber's name, or the name is known to differ from the official name
    - At Level 2, this can be used but
      - The RA or CSP must retain actual identity and
      - The credential must be be distinguishable.

Proofing by Level (1 of 3)

[See Table 3 for details.]

Level 2 - In Person

- Uses government picture ID (e.g., driver's license or Passport)
  - Compares pic; records data
- Credentials are
  - issued via associated phone number or email address in records Or
  - issued and notice is sent to a confirmed address of record Or
  - issued in a manner that confirms the claimed address.

Level 2 - Remote

- Inspects both a gov't ID number and a financial or utility account number. Verifies one.
  - Confirms data is consistent w/ applicant supplied-data
- Credentials are
  - issued via associated physical address , phone number, or email address of the Applicant in records Or
  - issued and notice is sent to a confirmed address of record.

Proofing by Level (2 of 3)

[See Table 3 for details.]

Level 3 - In Person

- Verifies government picture ID (e.g., driver's license or Passport)
  - Confirms data; compares pic; & records ID number
- Credentials are
  - issued via associated phone number while recording voice of the Applicant (or using equivalent means for the level of non-repudiation) Or
  - issued and notice is sent to a confirmed address of record Or
  - issued in a manner that confirms the claimed address.

Level 3 - Remote

- Verifies government ID number and a financial or utility account number
  - Confirms data is consistent w/ applicant supplied-data
- Credentials are
  - issued via associated physical address or phone number of the Applicant in records. For the latter, the CSP records the voice of the Applicant (or uses equivalent means for the level of non-repudiation).

Proofing by Level (3 of 3)

[See Table 3 for details.]

Level 4 - In Person

- Verifies (primary) government picture ID (e.g., driver's license or Passport)
  - Confirms data; compares pic; & records ID number
- Either
  - Inspects a secondary government ID and confirms that identifying data is consistent with the primary ID

    OR
  - Verifies financial account number and confirms data is consistent with application.
- RA records a current biometric (e.g., photo or fingerprints) to ensure that Applicant cannot repudiate application.
- Credentials are issued in a manner that confirms the address of record.

Level 4 - Remote

- Not Applicable

Is this the same Applicant? (1 of 2)

- Registration, identity proofing, token creation/issuance, and credential issuance are can be broken up into separate physical encounters or electronic transactions.
  - Level 1 – No specific requirement but an effort should be made to uniquely identify and track applicants.

Is this the same Applicant? (2 of 2)

Physical

Level 2 – Temporary secret as specified for Level 2 Electronic transactions;

Or biometric characteristic recorded during a prior encounter.

Level 3 – A secret as specified for Level 3 Electronic transactions, but temporary secrets can not be reused;

Or biometric characteristic recorded during a prior encounter.

Level 4 – Biometric characteristic recorded during a prior encounter.

Electronic

Level 2 – Temporary secret either established during a prior encounter or sent to the Applicant's phone number, email, or physical address.

Level 3 – Temporary secret either established during a prior encounter or sent to the Applicant's physical address of record.

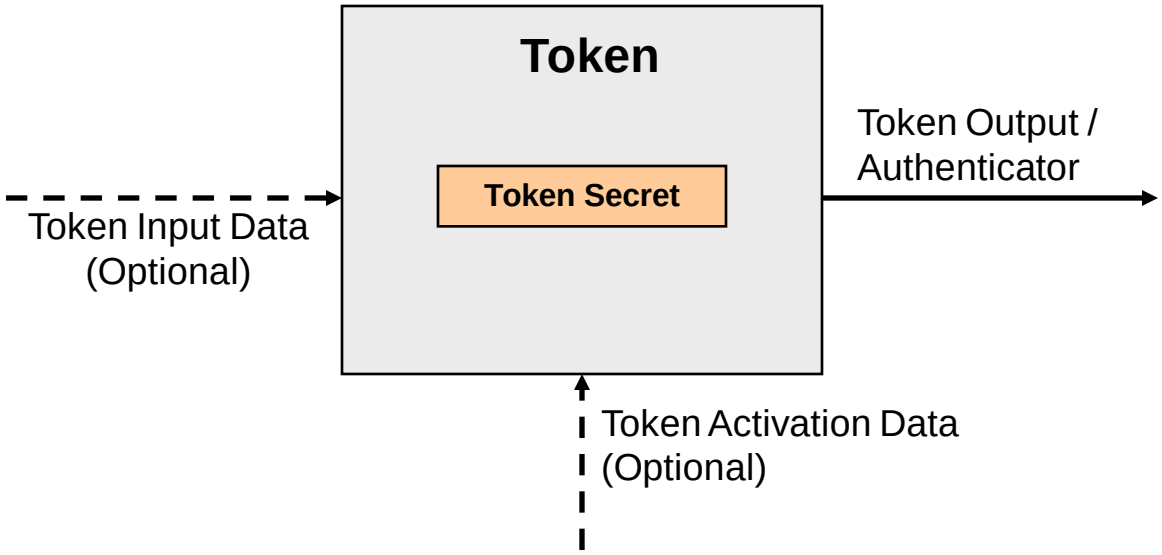
Or permanent secret issued within a protected session.

Take Two

- Leveraging existing credentials to issue derived credentials is permitted
  - 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

TOKENS AND THEIR MANAGEMENT

Tokens: The model



- This is a bit much for passwords, but it's needed for things like OTP tokens and PKI

Tokens: Factors

- Something you know
- Something you have
- Something you are

Token types

- Something you know
  - Memorized Secret token
  - Pre-Registered Knowledge Token
- Something you have
  - Look up Secret token
  - Out of Band Token
  - Single factor One-Time Password Device
  - Single-factor Cryptographic Device
- Multifactor tokens (have&are / have&know)
  - Multifactor Software Cryptographic Token
  - Multifactor One-Time Password Device
  - Multifactor Cryptographic Device

Tokens: Requirements per Assurance level

- Level 1:
  - At least one secret based token (have or know)
  - Low entropy authenticators (e.g. passwords) require a throttling mechanism
- Level 2:
  - Passwords etc. need more entropy
- Level 3:
  - Multifactor authentication
    - Effectively something you have plus another factor
- Level 4:
  - Hardware token based on approved cryptography
    - FIPS 140-2 Level 2 with Level 3 physical security

What is a credential

- Binds a representation of a token to a verified name
- Private Credentials
  - Token representation reveals token secret (e.g. password)
- Public Credentials
  - Token representation does not reveal token secret (e.g. public key)
- Weakly Bound Credentials
  - Still looks valid if it has been modified (e.g. password database)
- Strongly Bound Credentials
  - Contains a cryptographic checksum demonstrating integrity and source authenticity. (e.g. certificate)

Token and Credential Management Activities

- Credential Storage
  - CSP stores and protects credential records
- Token and Credential Verification Services
  - CSP assists Verifier to facilitate user authentication process
- Token and Credential Renewal/Reissuance
  - CSP issues the Subscriber new credentials with a later expiration date
  - In Renewal CSP also issues a new token
- Token and Credential Revocation and Destruction
  - CSP renders a token invalid by distributing revocation information to Verifiers and/or collecting and destroying the token.
- Records Retention
  - CSP maintains information collected by the RA during ID-proofing
- Security Controls
  - CSP Implements appropriate SP 800-53 controls

Credential Storage Requirements

- Level 1
  - No Plaintext Passwords
  - Access controls required for secrets
- Level 2
  - Access controls, Approved Encryption
  - Passwords are hashed with a variable salt
- Level 3
  - Encryption module for shared secret files must be FIPS 140-2 level 2 or higher
- Level 4
  - Same as level 3

Token and Credential Verification Services Requirements

- Level 1
  - Long term secrets should not be shared unless absolutely necessary
- Level 2
  - Cryptographic Protection required for weakly bound or private credentials
- Level 3
  - Long term secrets are not shared with third parties
  - CSP provides revocation info
- Level 4
  - Same as level 3

Token and Credential Renewal/Reissuance Requirements

- Level 1 - No Stipulation
- Level 2
  - Use unexpired token in level appropriate authentication process
  - Approved Cryptography and protected sessions are required
  - Passwords must be re-issued not renewed (i.e a new password must be chosen)
- Level 3
  - Use unexpired token in level appropriate authentication process
  - Approved Cryptography and protected sessions are required
- Level 4
  - Use unexpired token in level appropriate authentication process
  - Approved Cryptography, protected sessions, and keys bound to the authentication process are required

Token and Credential Revocation and Destruction Requirements

- Level 1
  - No Stipulation
- Level 2
  - Revoke or Destroy within 72 hours
- Level 3
  - Revoke or Destroy within 24 hours
- Level 4
  - Revoke within 24 hours
  - Should destroy token within 48 hours

Records Retention Requirements

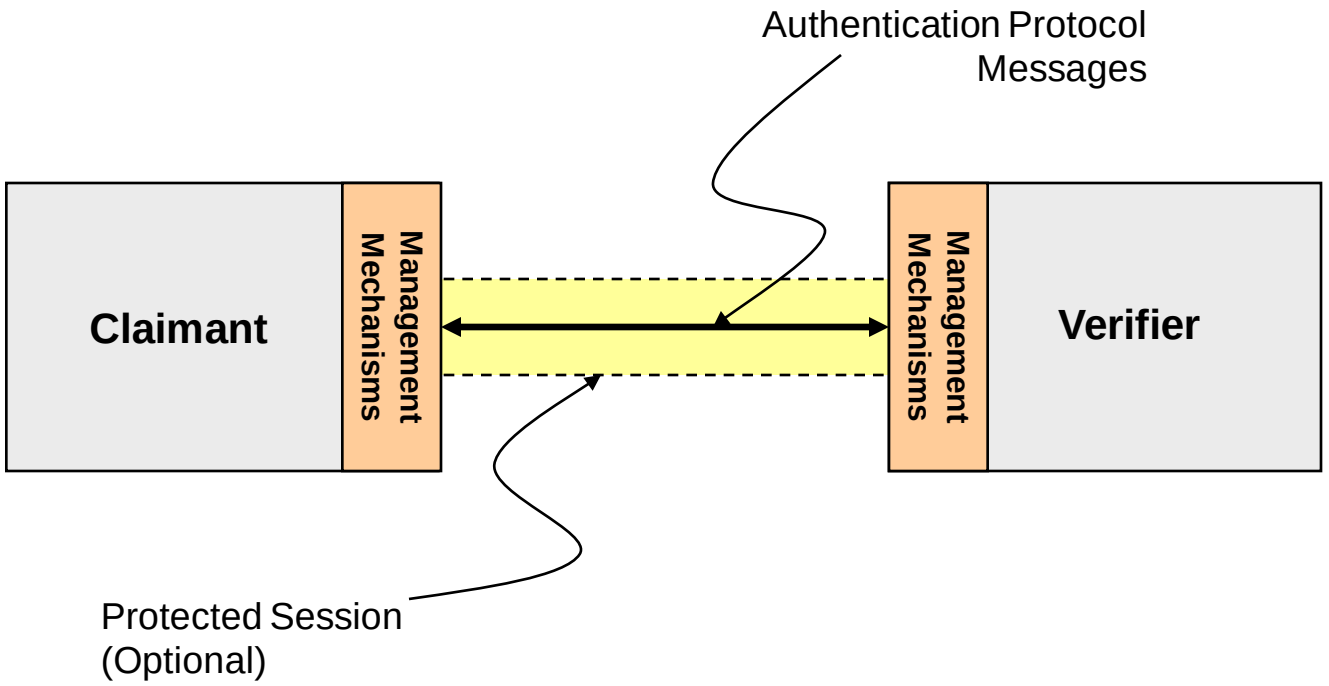
- Level 1
  - No Stipulation
- Level 2
  - Retain registration, history, and status (including revocation) records for 7 years 6 months after expiration
- Level 3
  - Same as level 2
- Level 4
  - Retain registration, history, and status (including revocation) records for 10 years 6 months after expiration

Security Controls Requirements

- Level 1
  - No Stipulation
- Level 2
  - SP 800-53 low baseline
- Level 3
  - SP 800-53 moderate
- Level 4
  - SP 800-53 moderate

A PLAN COMES TOGETHER: THE AUTHENTICATION PROCESS AND ASSERTIONS

Authentication Process Model



Authentication Threats and Resistance

- **Online Guessing**
  - Guidelines are provided for throttling mechanisms (when applicable)
- **Phishing/Pharming (Verifier Impersonation)**
  - What the user doesn't know, can't be phished
  - OTP protocols protect long term token secrets, but not short term token authenticators.
  - If you're using a password, it can be phished
- **Eavesdropping**
  - Includes offline dictionary attacks but not active attacks
- **Replay**
  - Timestamps, packet numbers and challenge response protocols protect against replay
- **Session Hijacking**
  - The authentication process must be linked to keys that protect later sensitive transactions
  - Effective defense requires CSRF and XSS protection
- **Man in the Middle**
  - Relying on a human to check a certificate or verify use of a secure protocol provides *weak resistance*
  - Cryptographic protocols like client-authenticated TLS provide *strong resistance*

Required Authentication Protocol Threat Resistance per AL (from Table 11)

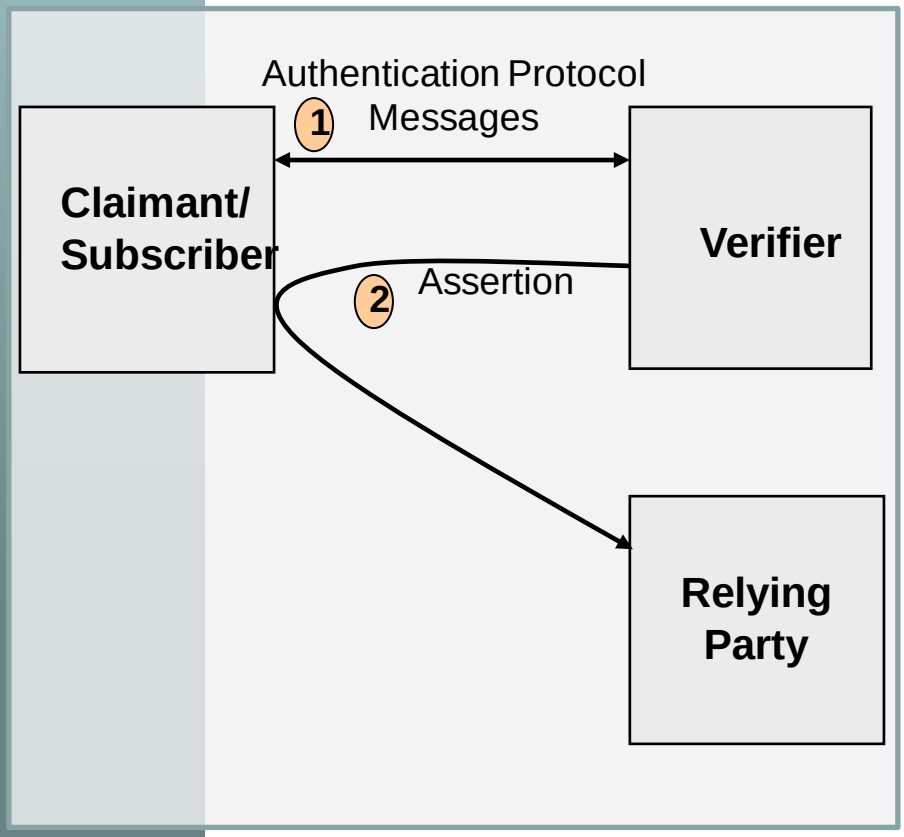
Authentication Process Attacks/Threats	Level 1	Level 2	Level 3	Level 4
Online guessing				
Replay				
Session hijacking				
Eavesdropping				
Phishing/pharming (verifier impersonation)				
Man in the middle				
Denial of service/flooding				

Authentication process requirements per assurance level

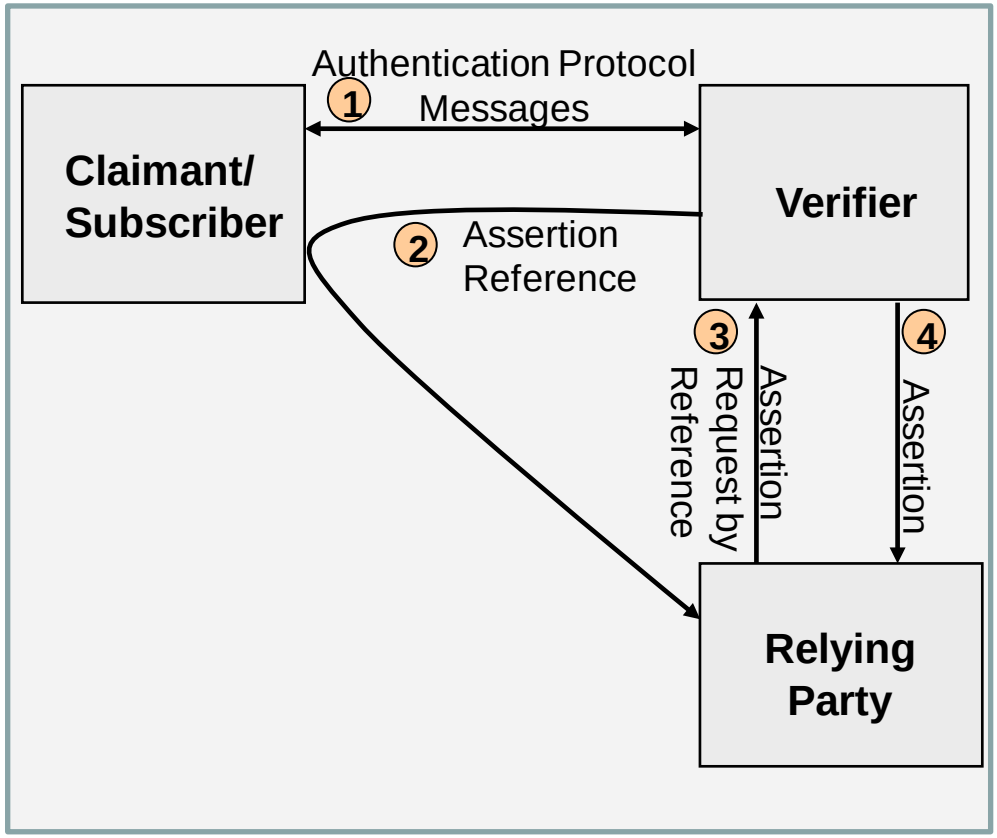
- Level 1
  - Protects against replay and online guessing attacks
  - Offline dictionary attacks are ok, but not plaintext passwords
- Level 2
  - Protects against session highjacking, eavesdropping, MITM (weakly)
  - Approved cryptography required
  - Highest level that allows password-only authentication
- Level 3
  - Two-Factor authentication required
  - Protects long term secrets against phishing
- Level 4
  - Strongly protects against MITM
  - Protects long and short term secrets against phishing

Assertion Models

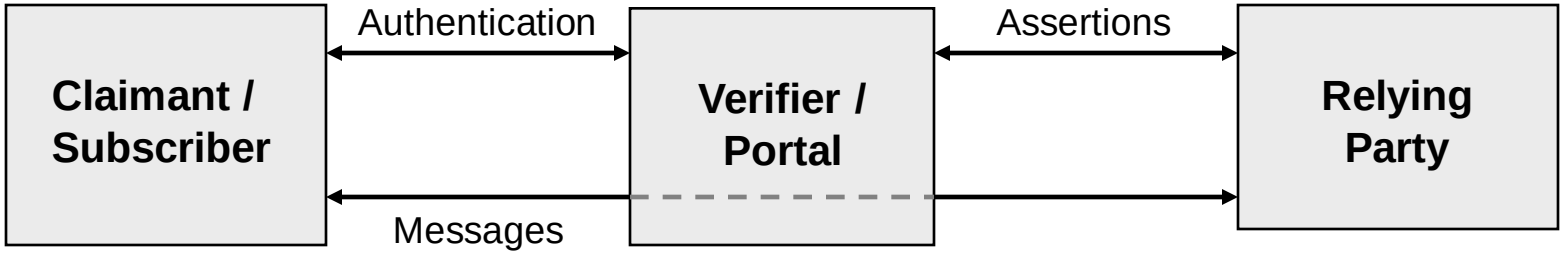
Direct Model



Indirect model



Proxy Model



- This model is added for completeness. Most of the requirements concern the first two models.

Assertion Types

- SAML assertions
- Kerberos Tickets
- HTTP cookies
  - These are the most common mechanism for keeping an HTTPS session open
  - In such cases Verifier and RP are the same entity

Secondary Authenticators

- The subscriber must prove to the RP that he or she is the subject of the assertion.
- This is accomplished by proving knowledge of a temporary secret (secondary authenticator) provided by the Verifier
  - Direct model (bearer assertions): Secondary authenticator is signed assertion
  - Indirect model (bearer assertions): Secondary authenticator is assertion reference
  - Kerberos: Secondary authenticator is session key
  - Holder of Key Assertion (direct or indirect model): Secondary authenticator is Subscriber's long term token secret.
- Secondary Authenticators must be hard to forge and cryptographically protected if/when transmitted.

Assertion Threats

- Assertion Threats
  - Manufacture/Modification
  - Disclosure
  - Repudiation by Verifier
  - Repudiation by Subscriber
  - Redirect
  - Reuse
- Secondary Authenticator Threats
  - Manufacture
  - Capture
- Binding Threats
  - Assertion Substitution

Required Threat Resistance per AL (from Table 12)

Threat	Level 1	Level 2	Level 3	Level 4
Assertion manufacture/modification				
Assertion disclosure				
Assertion repudiation by Verifier				
Assertion repudiation by Subscriber				
Assertion redirect				
Assertion reuse				
Secondary authenticator manufacture				
Secondary authenticator capture				
Assertion substitution				

Assertion requirements per assurance level

- Level 1 (and above)
  - Assertions specify the desired security level
  - Secondary authenticators are hard to forge
    - i.e. cryptographic checksum or 64-bits of entropy
  - Assertions are single use and expire if not used within time limit
    - Single Domain: 12 hours, Cross Domain: 5 minutes
  - Communications between Verifier and RP are cryptographically protected
- Level 2
  - Assertions explicitly or implicitly identify intended RP
  - Approved Cryptography Required Everywhere
    - This means you can't use a user chosen password as a Kerberos key.
  - Any Secondary Authenticators must be obtained and used securely by the Subscriber.
    - This Usually means TLS at both the Verifier and RP
- Level 3
  - Assertions are signed (except Kerberos tickets, which use symmetric key MAC)
  - Automatic logout after 30 minutes of inactivity
    - This Usually means single domain assertions expire faster (30 min instead of 12 hrs)
- Level 4
  - Holder of Key assertions and Kerberos only

TAKE AWAYS & FREQUENTLY ASKED QUESTIONS

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

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 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

What's New?: Derived Credentials

- New guidelines that permit leveraging existing credentials to issue derived credentials
  - Derived credentials from the ***same*** CSP cannot exceed the assurance level associated with the original credential
  - 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

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: ray.perlner@nist.gov
elaine.newton@nist.gov
tim.polk@nist.gov