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

NIST SP 800-63-1

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

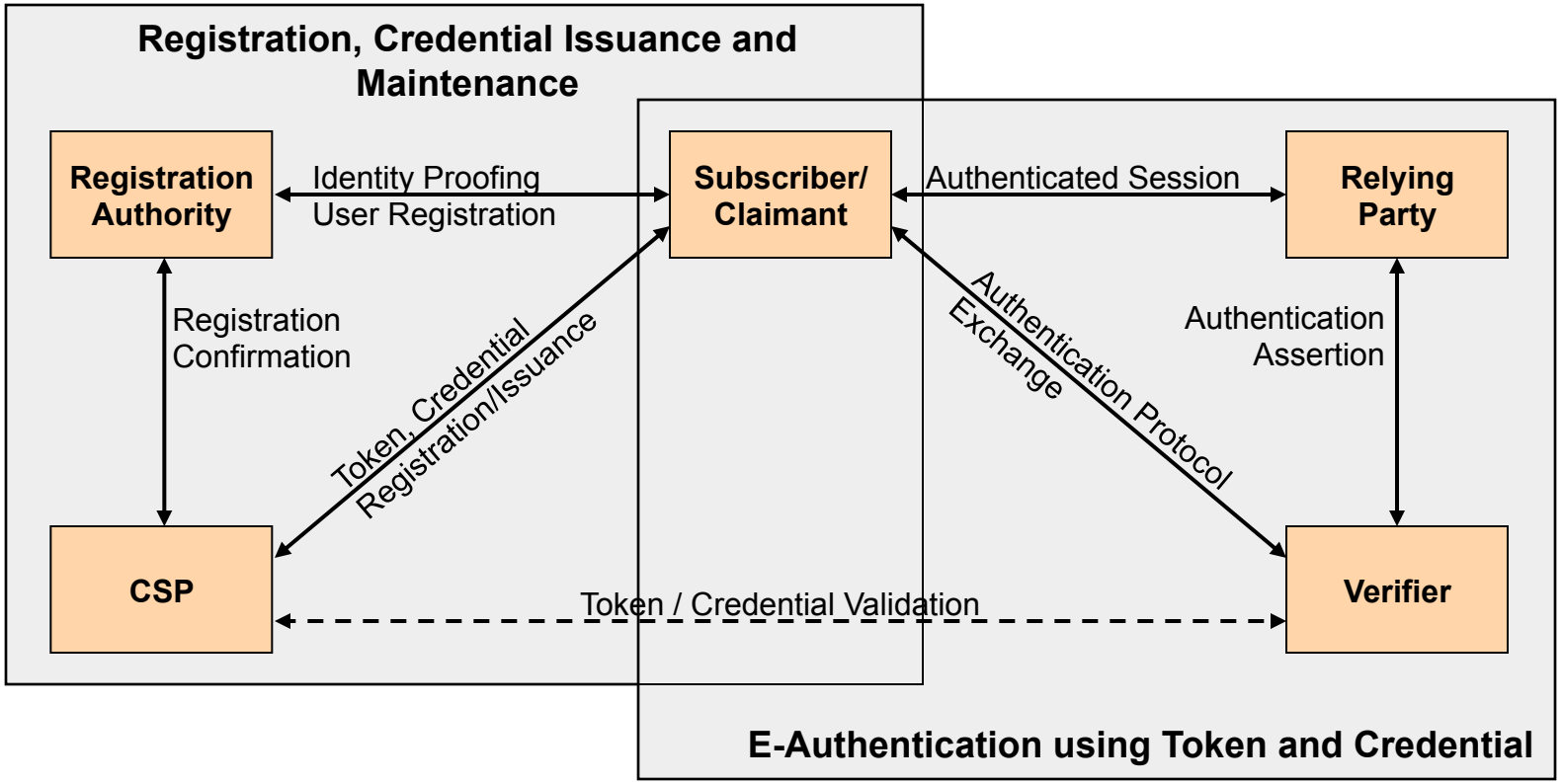
- It's Fantastic
  - Finally, a basis to compare mechanisms!
- It's Too Prescriptive
  - What about bingo cards?
  - What about remote biometrics?
  - What about knowledge based authentication?
  - What about combinations of tokens?

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

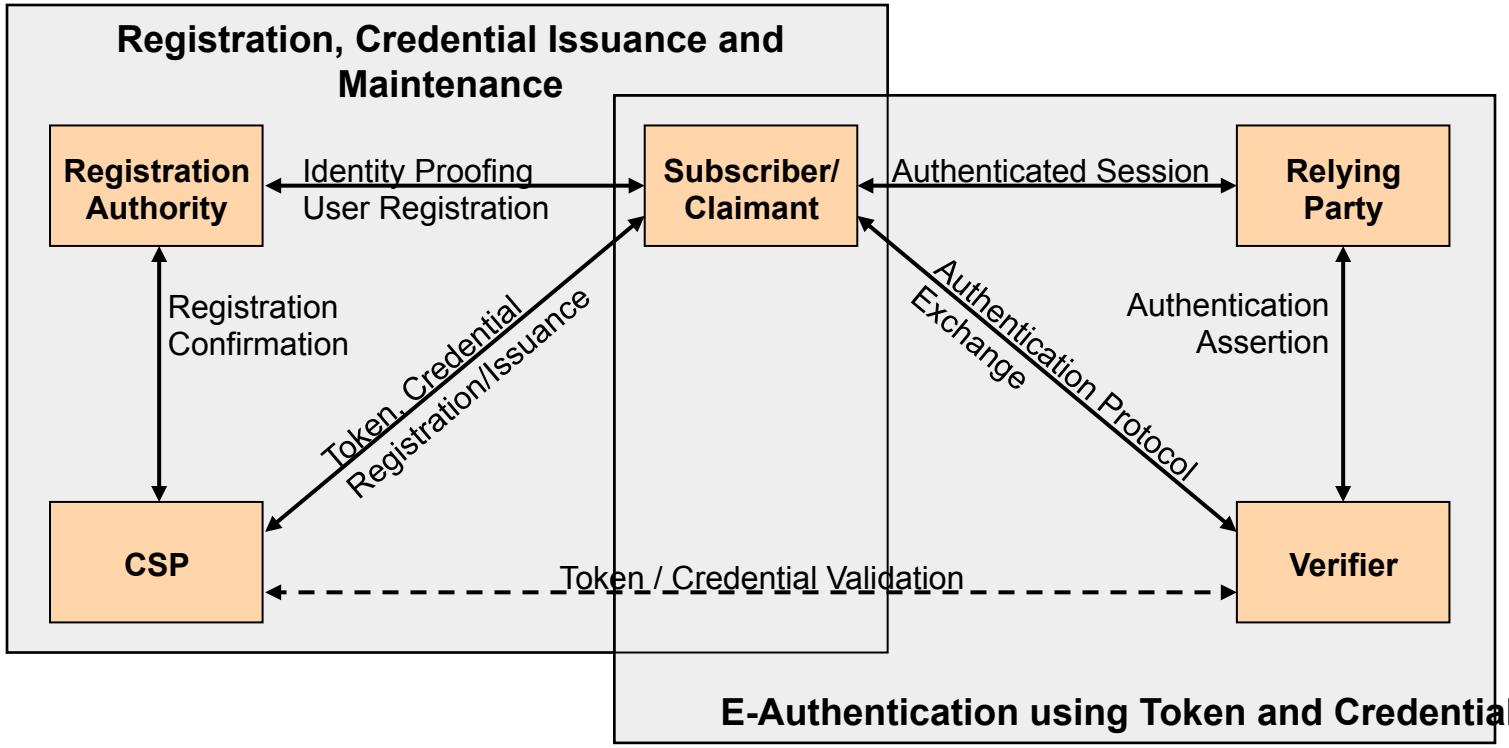


NIST SP 800-63-1

SECTION FOUR

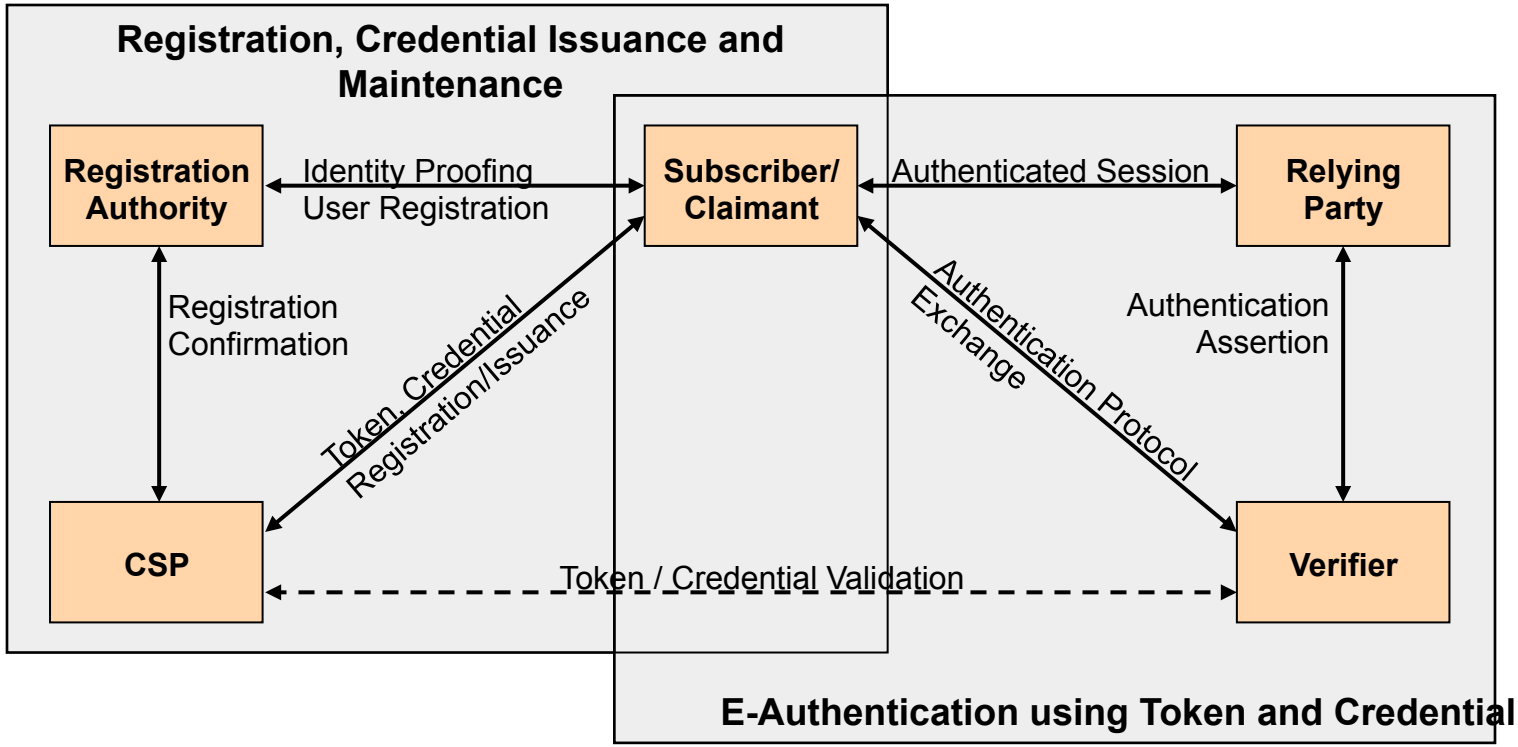
The Players (1 of 2)

- 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

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?

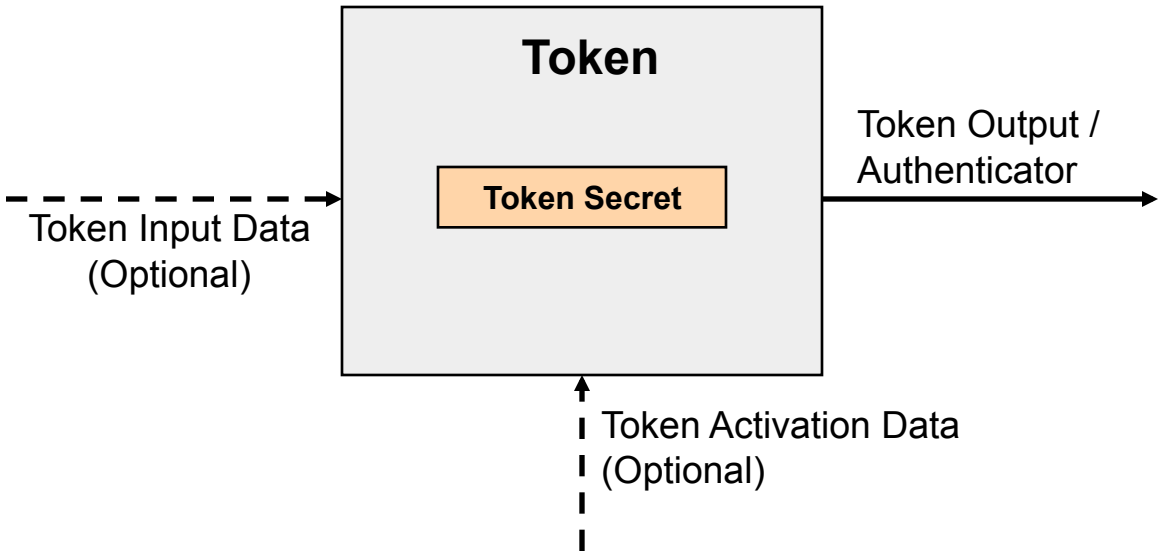
- Functions broken up into separate physical encounters or electronic transactions.
  - Registration,
  - Identity proofing,
  - Token creation/issuance, and
  - Credential issuance.
- Requirements exists for binding by AL
  - Level 1 – No specific requirement but an effort should be made to uniquely identify and track applicants.
  - Other Levels' requirements are based on secrets and/or biometrics.

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
- Model is based on PKI certificates but also includes things like password database entries

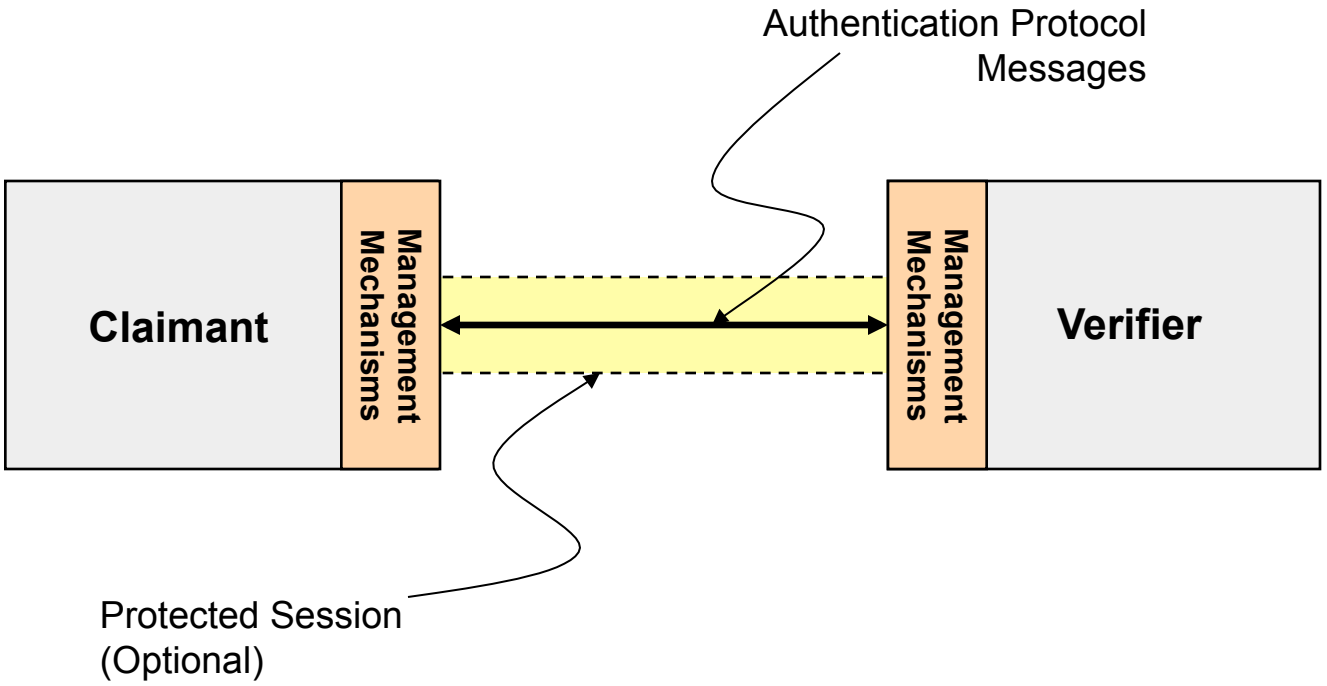
Token and Credential Management Activities

(Requirements are given for each category – See Document for Details.)

- 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

A PLAN COMES TOGETHER: THE AUTHENTICATION PROCESS AND ASSERTIONS

Authentication Process Model



Authentication process requirements per assurance level

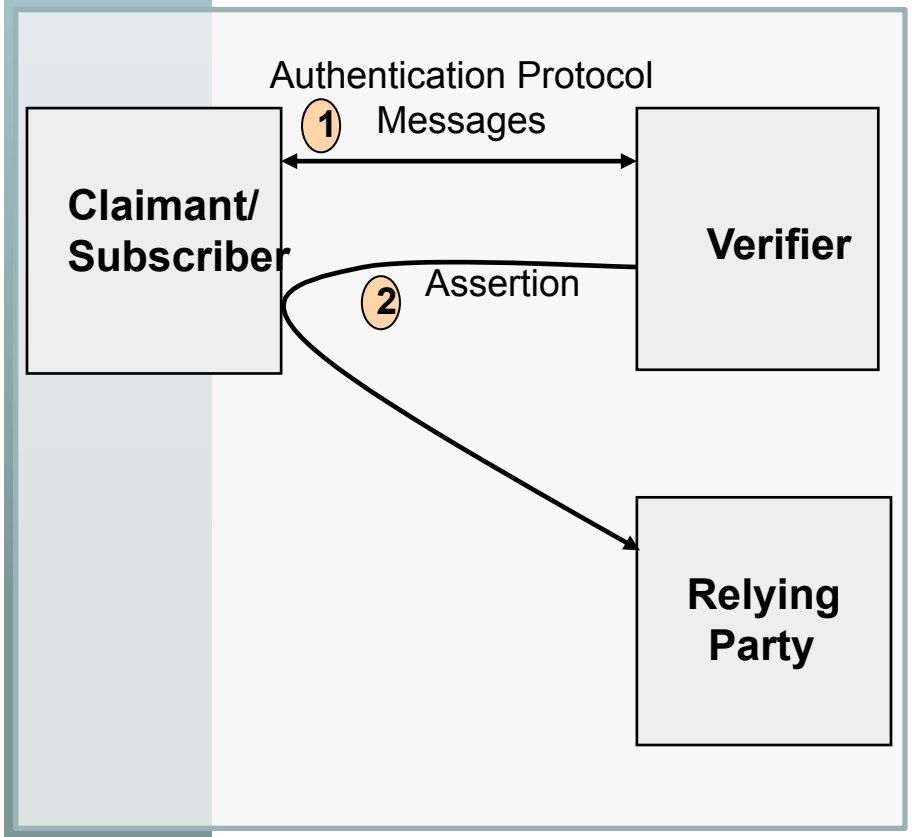
- Level 1
  - Protects against replay and online guessing attacks
  - Offline dictionary attacks are ok, but not plaintext passwords
- Level 2
  - Protects against session highjacking, eavesdropping, MITM (weakly)
  - Approved cryptography required
  - Highest level that allows password-only authentication
- 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

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

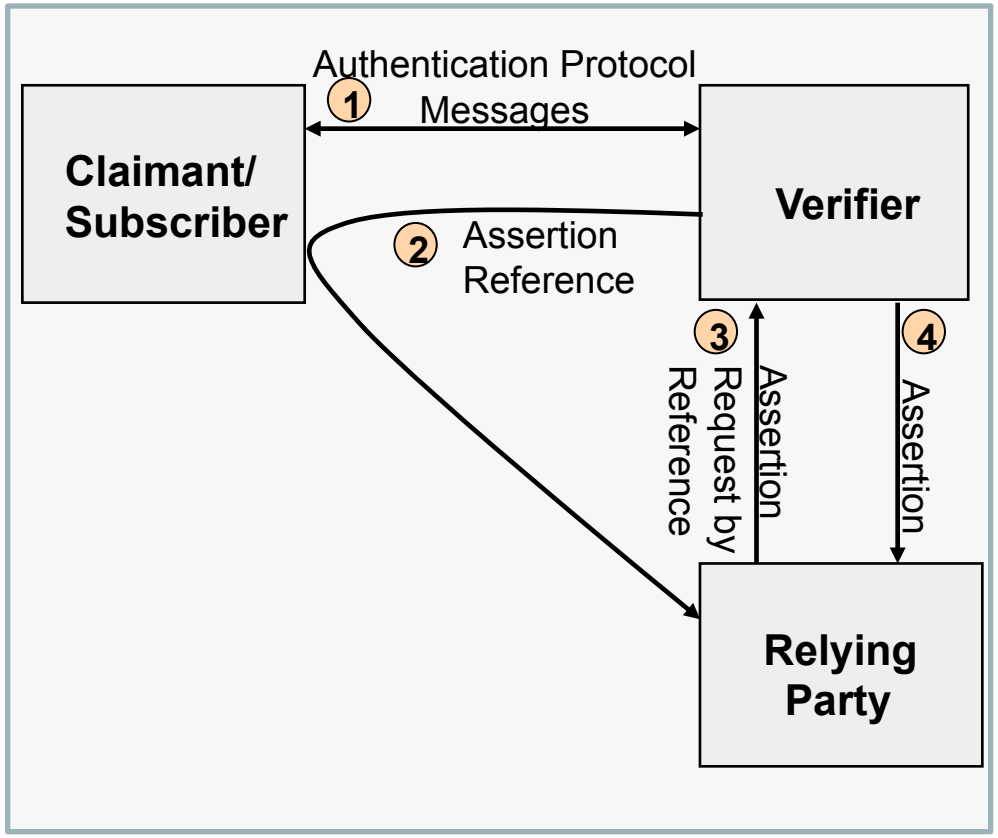
Authentication Process Attacks/Threats	Level 1	Level 2	Level 3	Level 4
Online guessing				
Replay				
Session hijacking				
Eavesdropping				
Phishing/pharming (verifier impersonation)				
Man in the middle				
Denial of service/flooding				

Assertion Models

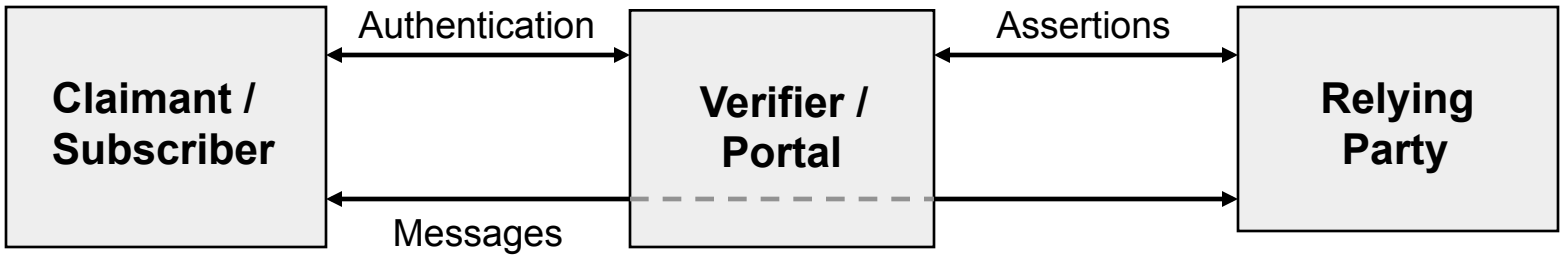
Direct Model



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

Assertion requirement highlights

- At most levels, Assertions must contain
  - Subscriber Name
  - Intended RP
  - Level of Assurance
  - Timestamp / Validity period
- Approved crypto required everywhere from Level 2 up
  - For SAML and cookies this means TLS at both Verifier and RP
- Password based Kerberos is vulnerable to dictionary attack
  - This means you can't use it at level 2 and above
- Level 3 introduces 30 minute timeout (even for SSO)
- Level 4 requires holder of key assertions or Kerberos
- Non-Kerberos protocols protect against repudiation-type threats at levels 3 and 4.

Assertion Threats

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

NIST SP 800-63-1

SECTION NINE

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				

TAKE AWAYS & FREQUENTLY ASKED QUESTIONS

What's New?

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

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

NIST SP 800-63-1

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?: 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