

# Security Considerations for a Technical Framework to Support E- Prescribing

---

Donna F Dodson

National Institute of Standards and Technology

[donna.dodson@nist.gov](mailto:donna.dodson@nist.gov)

# Business Requirements

---

- Laws and regulations
  - Policies
  - Risk Management
    - Assets
    - Threats
    - Vulnerabilities
    - Security Controls
- SP 800-30, Risk Management Guide for Information Systems**

# Some Definitions

---

- ❑ Authentication – The process of establishing confidence in user identities.
- ❑ Access Control –The process of granting or denying specific requests for obtaining and using information and related information processing services
- ❑ Electronic Signature - An electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.
- ❑ Digital Signature – A class of electronic signatures based on cryptography to provide authentication of the signer, message integrity and non-repudiation.
- ❑ Confidentiality –The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.
- ❑ Integrity – The property that sensitive information has not been modified or deleted in an unauthorized and undetected manner.

# Authentication Framework

---

	Local	Remote
Human		<b>SP 800-63, Electronic Authentication Guidance</b>
Device		

# NIST SP 800-63

---

- Companion to OMB M04-04 Policy Guidance for e-authentication
  - Agencies classify electronic transactions into four levels related to authentication assurance according to the potential consequences of an authentication error
  - Consider: privacy, inconvenience, damage to reputation, financial loss or agency liability, harm to agencies and programs, unauthorized release of sensitive information, personal safety, civil or criminal violations

# NIST SP 800-63

---

- Technical authentication framework for remote e-authentication
- Establishes technical requirements for four levels of M04-04 for
  - Registration and Identity Proofing
  - Tokens
  - Token and Credential Management
  - Authentication Protocols
  - Assertions

# Four Levels of SP 800-63

---

## □ Level 1

- 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

---

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

# Level 3

---

- ❑ Two 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

---

- ❑ Two 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

# Factoring other security requirements

---

- Properties required for signatures – are there levels of signatures like levels of authentication?
- Is there a need for confidentiality or integrity?
- Are there compensating controls within the system?