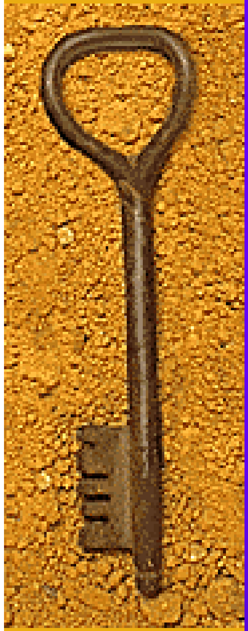
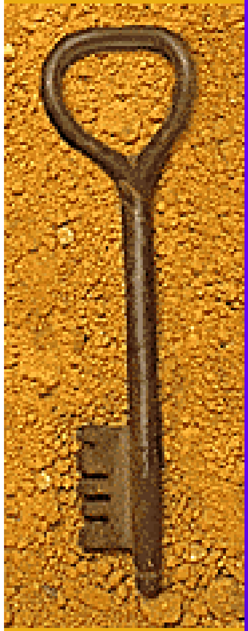
e-Authentication Guidance

Bill Burr
NIST
william.burr@nist.gov
301-975-2914



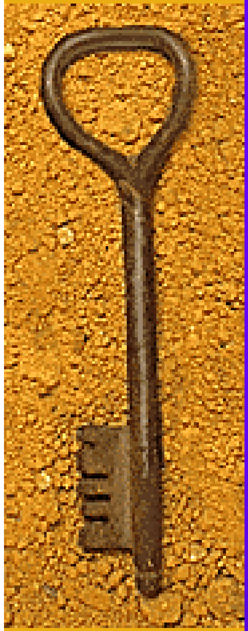
E-Authentication Tech Guidance

- Will Be NIST Recommendation
- Puts technical flesh on OMB generated e-Authentication policy guidance
  - Federal Register announcement pending
  - Four levels of assurance
  - Defined in terms of the possible risks and consequences of authentication error
- Disclaimer: everything is subject to change
  - I don't control the policy about risks/assurance levels
  - I reserve the right to change my mind on the things I do control



Assurance levels

- OMB guidance defines 4 assurance levels
- Assurance level needed determined by consequences of authentication error
  - Inconvenience
  - Financial loss
  - Distress
  - Standing or reputation
  - Harm to agency programs or reputation
  - Civil or criminal violations
  - Personal safety

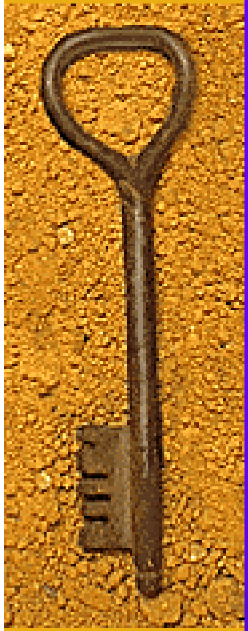


Assurance Levels

- Level 1 – Minimal Assurance
- Level 2 – Low Assurance
- Level 3 – Substantial Assurance
- Level 4 – High Assurance

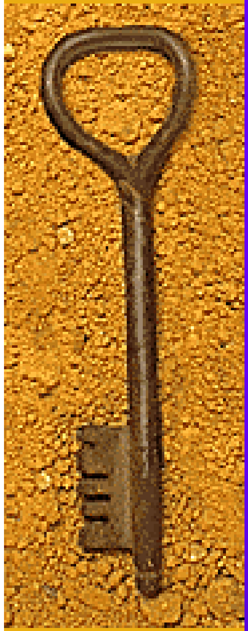
Technical Guidance Constraints

- Technology neutral
  - Required (if practical) by e-Sign, Paperwork Elimination and other laws
  - Difficult: many technologies, apples and oranges comparisons
- Practical with COTS technology
  - To serve public must take advantage of existing password based solutions and relationships
- Only for remote network authentication
- Only about identity authentication
  - not about attributes or authorization or access control



E-auth Guidance Outline

- Authentication Technical Model
- Registration and Identity Proofing
- Authentication Protocols
- Agency Process Requirements



E-Auth Guidance Scope

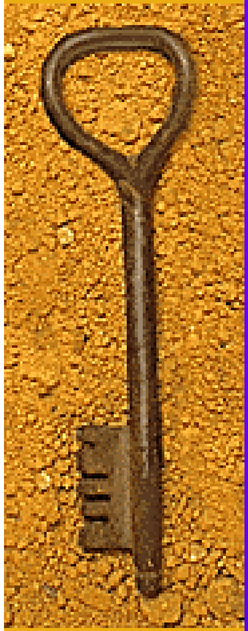
- ♦ Remote Authentication over open networks
  - – Does not address in-person authentication
    - Consequence is that biometrics are not useful except in identity proofing process
      - – Protocols for remote network authentication are based on secret tokens (typically passwords or keys)
      - – Biometrics make lousy secrets

Authentication Model Terms

- *Claimant*:
  - wants to prove his or her identity
- *Electronic credentials*
  - Bind an identity or attribute to a token or something associated with a claimant
- *Credentials Service Provider (CSP)*
  - Claimant is a subscriber of a CSP
  - Issues electronic credentials and registers or issues tokens
- *Registration Authority (RA)*
  - Identity proofs the subscriber

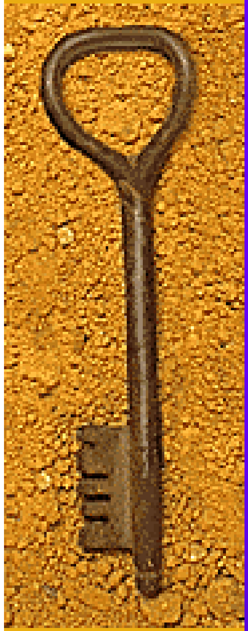
Authentication Model Terms

- *Token*
  - Secret used in an authentication protocol
- *Relying party*
  - Relies on credentials to grant access – typically an agency web application
- *Verifier*
  - Uses an authentication protocol that verifies the claimant’s identity by making the claimant prove possession of a token



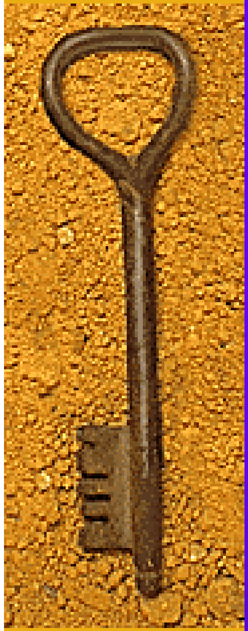
Tokens

- Hard token
  - Hardware device with cryptographic key
  - FIPS 140 level 2, with level 3 physical security
  - Key is unlocked by password or biometrics
- Soft token
  - Cryptographic key encrypted under password
  - FIPS 140 Level 1 or higher crypto module
- Password
  - Strong password or PIN
- Personal knowledge



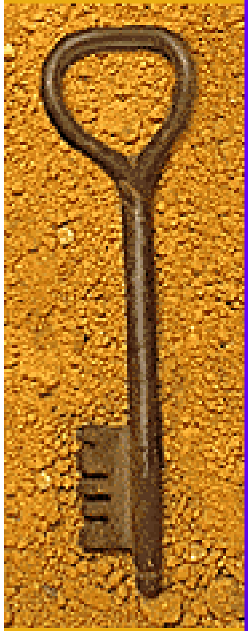
Electronic Credentials

- ♦ Bind an identity to
  - – A token, or
  - – A network address
  - – Must be authenticated
- ♦ Typical credentials
  - – X.509 public key certificate
  - – SAML assertion
  - – Trusted directory entries



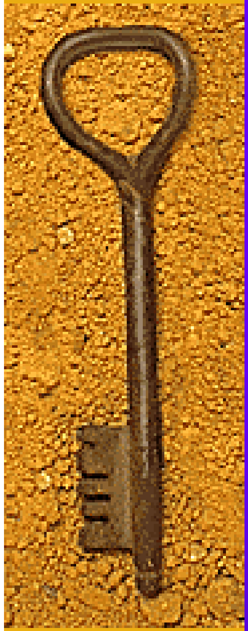
ID Proofing

- ♦ Level 1
  - – Self assertion, minimal records
- ♦ Level 2
  - – Assurance for low risk, routine transactions
  - – More or less instant gratification
  - – Organizational RA
    - Relies on existing significant customer or employee relationship
    - Confirmation of postal or electronic address in token issuance



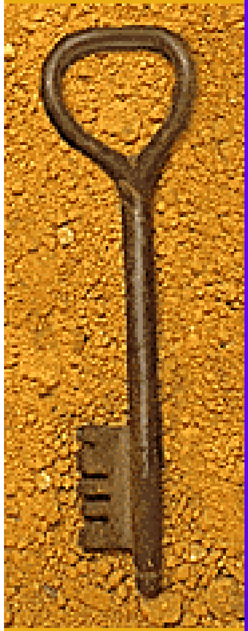
ID Proofing

- ♦ Level 2
  - – Public RA
    - Remote registration
      - – Some currently verifiable ID (e.g. credit card)
      - – Database/credit record confirmation
      - – Close loop: confirmation of postal, phone or e-mail
    - In-person
      - – Current gov. photo-ID
      - – Close loop: confirmation of postal, phone or e-mail address on Gov. ID



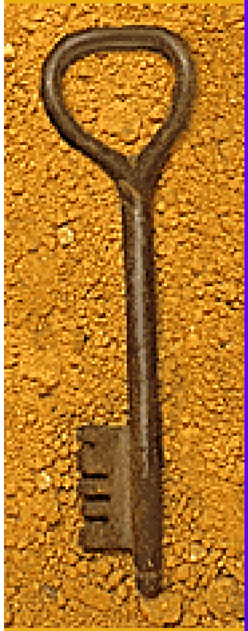
ID Proofing

- Level 3 – Substantial Assurance
  - Organizational RA
    - “significant” relationship, eg.
      - employment, banking, substantial credit, insurance, payment of taxes, matriculation at degree granting institution…
      - At least a one year duration
      - Issue token/credentials in manner that confirms either postal address or wire-line phone number of record



ID Proofing

- ♦ Level 3 – Substantial Assurance (cont.)
  - – Public RA
    - Remote registration.
      - – Database identity verification (how many?)
      - – Verify some currently valid ID (e.g. credit or bank card)
      - – Issue token/credentials in manner that confirms either postal address or wire-line phone number of record
    - In-person
      - – Current gov. issued primary photo-ID verified by live records check, or
      - – Current gov. issued primary photo-ID plus other ID verified by live records check (e.g. credit card, student ID…)
      - – Issue token/credentials in manner that confirms either postal address or wire-line phone number of record

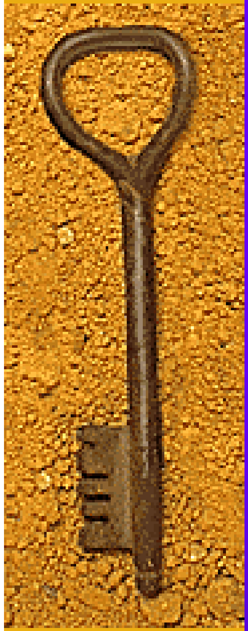


ID Proofing

- Level 4 – High Assurance
  - Gov. Employees
    - In-person proofing
    - Current agency photo-ID or two IDs including one government photo ID
      - Verify through current database check
    - Take a biometric (e.g. photo or fingerprint during registration)
  - Government Affiliates
    - similar to Gov. employees
  - Corporate or Organizational Employees
    - Similar to Gov. employees
  - Customers and Organizational Affiliates ???
  - Public RA ???

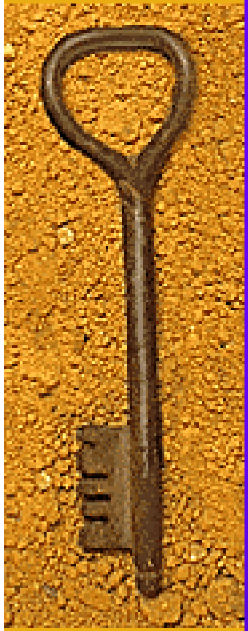
Token Type by Level

Allowed Token Types	1	2	3	4
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
Zero knowledge password	√	√	√	
Strong password	√	√		
PIN	√			



Required Protections by Level

Protection Against	1	2	3	4
Eavesdropper		√	√	√
Replay	√	√	√	√
On-line guessing	√	√	√	√
Verifier Impersonation			√	√
Man-in-the-middle			√	√
Session Hijacking			√	√



Auth. Protocol Type by Level

Allowed Protocol Types	1	2	3	4
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
Zero knowledge password	√	√	√	
Tunneled password	√	√		
Challenge-reply password	√			

Required Protocol Properties by Level

Required properties	1	2	3	4
Shared secrets not revealed to 3rd parties		√	√	√
Session Data transfer authenticated			√	√