NIST E-Authentication Guidance SP 800-63

Federal PKI TWG
Feb. 18, 2004

Bill Burr
william.burr@nist.gov

NIST E-Authentication Tech Guidance

- OMB Guidance to agencies on E-Authentication
  - OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, Dec. 16, 2003
    - http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
  - About identity authentication, not authorization or access control
- NIST SP800-63: *Recommendation for Electronic Authentication*
  - Companion to OMB e-Authentication guidance
  - Draft for comment at: http://csrc.nist.gov/eauth
  - Comment period ends: March 15
  - Covers conventional token based remote authentication
    - Does not cover Knowledge Based Authentication

Assurance Levels

- OMB guidance defines 4 assurance levels
  - Level 1 little or no confidence in asserted identity’s validity
  - Level 2: Some confidence in asserted identity’s validity
  - Level 3: High confidence in asserted identity's validity
  - Level 4: Very high confidence in asserted identity’s validity
- Needed assurance level determined *for each type of transaction* by the risks and consequences of authentication error with respect to:
  - Inconvenience, distress & damage to reputation
  - Financial loss
  - Harm to agency programs or reputation
  - Civil or criminal violations
  - Personal safety

E-Auth Guidance Process

- Risk assessment
  - Potential impacts
  - likelihood
- Map risks to assurance level
  - profile
- Select technology
  - NIST Technical E-Authentication Guidance, SP800-63
- Validate implemented system
- Periodically reassess

Max. Potential Impacts Profiles

Potential Impact Categories for Authentication Errors	*Assurance Level Impact Profiles*			
	1	2	3	4
Inconvenience, distress, reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency prog. or pub. interests	N/A	Low	Mod	High
Unauth. release of sensitive info	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

NIST
National Institute of
Standards and Technology

Technical Guidance Constraints

- Technology neutral (if possible)
  - Required (if practical) by e-Sign, Paperwork Elimination and other laws
  - Premature to take sides in web services wars
  - Difficult: many technologies, apples and oranges comparisons
- Practical with COTS technology
  - To serve public must take advantage of existing solutions and relationships
- Only for remote network authentication
  - Not in person, therefore not about biometrics
- Only about identity authentication
  - Not about attributes, authorization, or access control
    - This is inherited from OMB guidance
  - Agency owns application & makes access control decisions

Personal Authentication Factors

- Something you know
  - A password
- Something you have: a token
  - for remote authentication typically a key
    - Soft token: a copy on a disk drive
    - Hard token: in a special hardware cryptographic device
- Something you are
  - A biometric
    - But biometrics don’t work well in remote authentication protocols, because you can’t keep a biometric secret

Remote Authentication Protocols

- Conventional, secure, remote authentication protocols all depend on proving possession of some secret "token"
  - May result in a shared cryptographic session key, even when token is a only password
- Remote authentication protocols assume that you can keep a secret
  - Private key
  - Symmetric key
  - Password
- Can be "secure" against defined attacks if you keep the secret
  - Amount of work required in attack is known
    - Make the amount of work impractical
  - Hard for people to remember passwords that are "strong" enough to make the attack impractical

Multifactor Remote Authentication

- The more factors, the stronger the authentication
- Multifactor remote authentication typically relies on a cryptographic key
  - Key is protected by a password or a biometric
  - To activate the key or complete the authentication, you need to know the password, or poses the biometric
  - Works best when the key is held in a hardware device (a “hard token”)
    - Ideally a biometric reader is built into the token, or a password is entered directly into token

E-Authentication Model

- A *claimant* proves his/her identity to a *verifier* by proving possession of a *token*, often in conjunction with *electronic credentials* that bind the identity and the token. The verifier may then inform a relying party of the claimant’s identity with an *assertion*. The claimant got his/her token and credentials from a *Credentials Service Provider (CSP)*, after proving his identity to a *Registration Authority (RA)*. The roles of the verifier, relying party, CSP and RA may be variously combined in one or more entities.
  - ***Claimant:*** Wants to prove his or her identity
  - ***Electronic credentials****:* Bind an identity or attribute to a token or something associated with a claimant
  - ***Token:*** Secret used in an authentication protocol
  - ***Verifier:*** verifies the claimant’s identity by proof of possession of a token
  - ***Relying party:*** Relies on an identity
  - ***Assertion:*** *Passes information about a claimant from a verifier to a relying party*
  - ***Credentials Service Provider (CSP):*** Issues electronic credentials and registers or issues tokens
  - ***Registration Authority (RA):*** Identity proofs the subscriber

Tokens

- Hard token
  - Cryptographic key in a hardware device
  - 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
- One-time password device (1TPD)
  - Symmetric key in a hardware device with display - FIPS 140 level 1
  - Generates password from key plus time or counter
  - User typically inputs password through browser
- Zero Knowledge Password
  - Strong password used with special “zero knowledge” protocol
- Password
  - Password or PIN with conventional protocol

Token Type by Level

	Assurance Level			
Allowed Token Types	1	2	3	4
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
Zero knowledge password	√	√	√	
One-time Password Device	√	√	√	
Strong password	√	√		
PIN	√			

Protections by Level

	Assurance Level				
	1	2	3		4
Protection Against			Soft/ZKP	1TPD	
Eavesdropper		√	√	√	√
Replay	√	√	√	√	√
On-line guessing	√	√	√	√	√
Verifier Impersonation			√	√	√
Man-in-the-middle			√	*	√
Session Hijacking			√		√

*** Protection for shared secret only**

Auth. Protocol Type by Level

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

ID Proofing

- Level 1
  - Self assertion, minimal records
- Level 2
  - On-line, more or less instant gratification may be possible
    - Close the loop by mail, phone or (possibly) e-mail
- Level 3
  - in-person registration not required
    - Close the loop by mail or phone
- Level 4
  - In person proofing
    - Record a biometric
      - Can later prove who got the token
  - Consistent with FICC Common Certificate Policy

Passwords

- Password is a secret character string you commit to memory.
  - — Secret and memory are the key words here
    - As a practical matter we often do write our passwords down
- A password is really a (weak) key
  - — People can’t remember good keys
- We all live in Password Hell – too many passwords
  - — And they try to make us change them all the time
- In E-auth we’re only concerned with on-line authentication
  - — Assume that the verifier is secure and can impose rules to detect or limit attacks
- What is the “strength” of a password?

Attacks on Passwords

- In-band
  - Attacker repeatedly tries passwords until he is successful
    - guessing, dictionary, or brute force exhaustion
  - Can’t entirely prevent these attacks
    - can ensure they don’t succeed very often
- Out of band – everything else
  - Eavesdropper
  - Man-in-the-middle
  - Shoulder surfing
  - Social engineering

Password Strength

- Over the life of the password the probability of an attacker with no *a priori* knowledge of the password finding a given user's password by an in-band attack shall not exceed
  - one in 2^{16} (1/65,563) for Level 2
  - one in 2^{11} (1/2048) for Level 1
- Strength is function of both password entropy, the system and how it limits or throttles in-band guessing attacks
- Many ways to limit password guessing attack
  - 3-strikes and reset password, hang up on bad login attempt…
  - Limited password life, but…
  - Note that there is not necessarily a time limit
  - Many things are trade-offs with help desk costs

Password Entropy

- Entropy of a password is roughly speaking, the uncertainty an attacker has in his knowledge of the password, that is how hard it is to guess it.

$$H(X) := -\sum_{x} P(X = x) \log_2 P(X = x)$$

- Easy to compute entropy of random passwords
- We typically state entropy in bits. A random 32-bit number has 2^{32} values and 32-bits of entropy
- A password of length l selected at random from the keyboard set of 94 printable (nonblank) characters has 94^{l} values and about $6.55 \times l$ bits of entropy.

Password Entropy

- Entropy is measure of randomness in a password
  - Stated in bits: a password with 24 bits of entropy is as hard to guess as a 24 bit random number
  - The more entropy required in the password, the more trials the system can allow
- It’s easy to calculate the entropy of a system generated random password
  - But users can’t remember these
- Much harder to estimate the entropy of user chosen passwords
  - Composition rules and dictionary rules may increase entropy
  - NIST estimates of password entropy

Shannon's Estimate of Entropy

- Shannon used 26 English letters plus space
  - —Left to their own devices user will choose only lower case letters.
- Shannon's method involves knowing the *i*-1 first letters of a string of English text; how well can we guess the *i*th letter?
- Entropy per character decreases for longer strings
  - —1 character 4.7 bits/character
  - —≤ 8 characters 2.3 bits per character
  - —order of 1 bit/char for very long strings

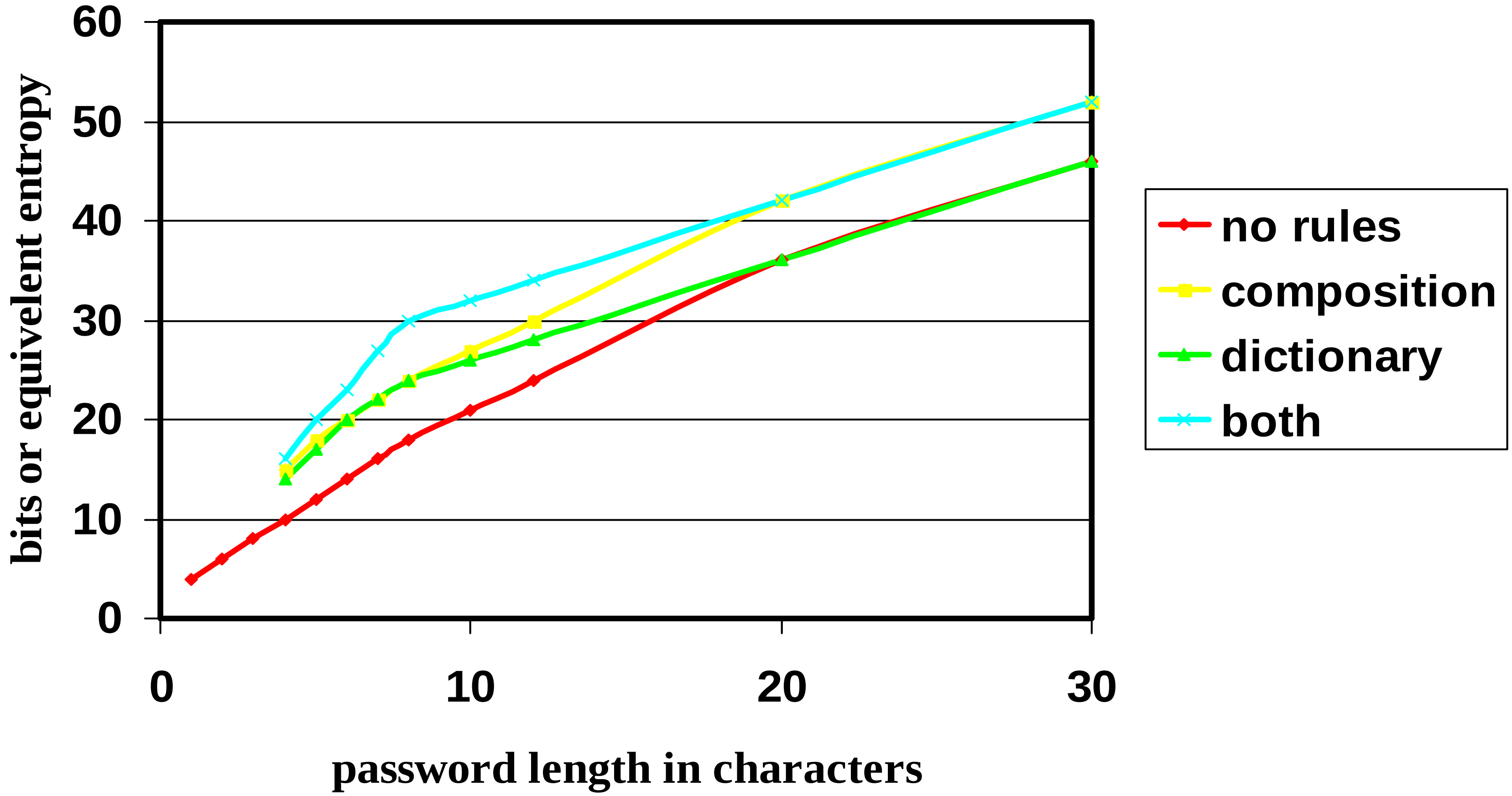
NIST
National Institute of
Standards and Technology

Use Shannon as Estimate

- Shannonn gives us an estimate of the number of bits needed to represent ordinary English text
  - — Seems intuitive that if it takes n bits to represent a text string, that is related to how hard it is to guess the string
- It should be as hard to guess or compress passwords as ordinary English text
  - — Users are supposed to pick passwords that don't look like ordinary English, to make them harder to guess
    - But, of course, users want to remember passwords
  - — Attacker won't have a perfect dictionary or learn much by each unsuccessful trial
  - — Surely, the only long passwords that are easy to remember are based on phrases of text that make sense to the person selecting the password
- Give "bonuses" for composition rules and dictionary

NIST
National Institute of Standards and Technology

Very Rough Password Entropy Estimate



PKI & E-Auth

- PKI solutions widely available
  - Can use TLS with client certs. for levels 3 & 4
- May be the predominant solution for levels 3 & 4 in gov.
  - Federal Identity Credentialing Committee
  - Common Credential and Federal Identity Card
    - Common certificate policy and shared service providers
    - Gov. Smart Card Interoperability Standard (GSC-IS)
- Fed. Bridge CA and Fed. Policy Authority are PKI vehicle
- Non-PKI level 3 & 4 solutions
  - One-time password devices in common use – can meet level 3
    - Cell phones could be a good 1TPD platform
  - Zero knowledge passwords for level 3 – not widely implemented
  - Level 4 could be done with symmetric key tokens

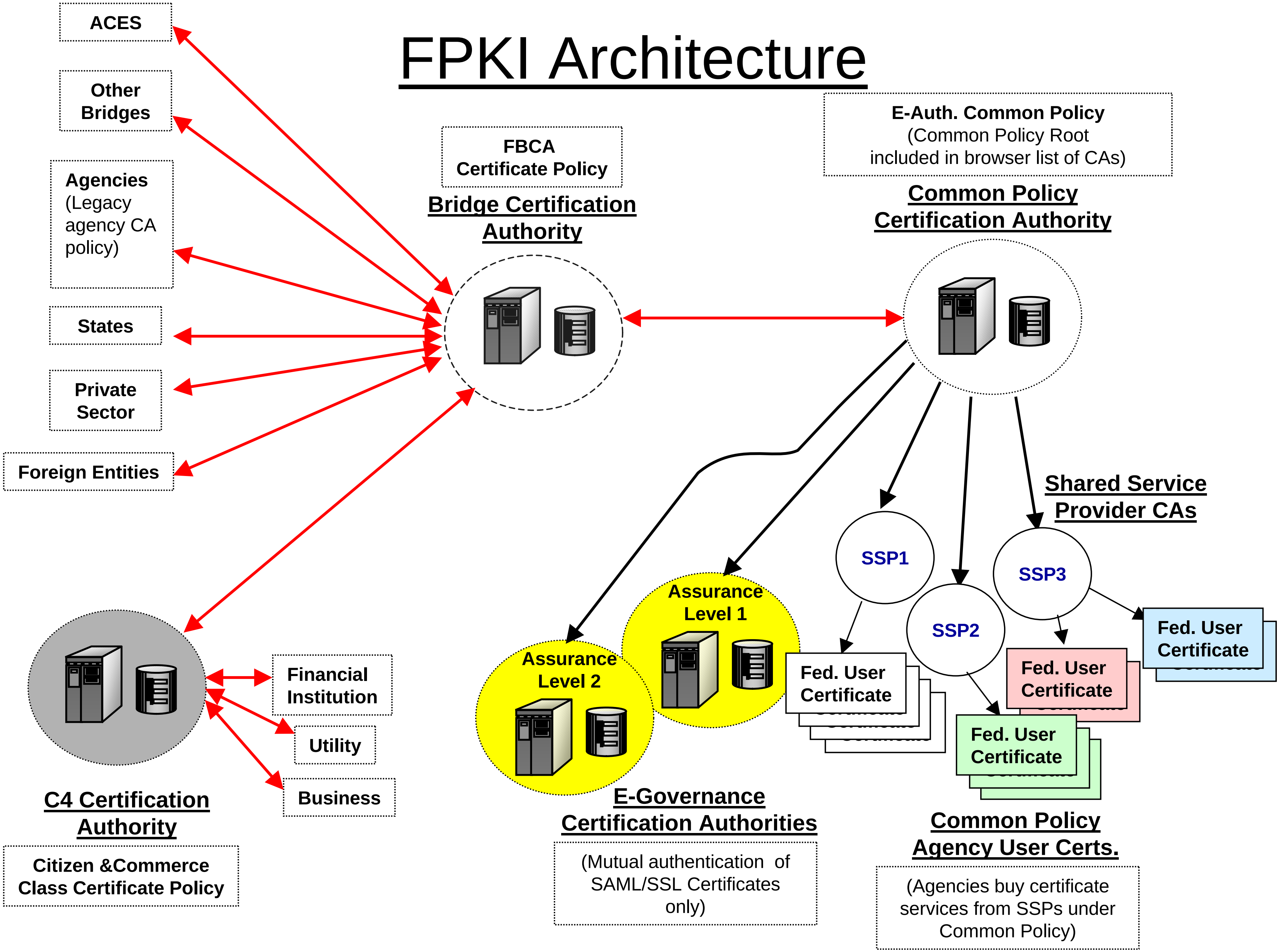
PKI & E-Auth

- PKI solutions widely available
  - Can use TLS with client certs. for levels 3 & 4
- May be the predominant solution for levels 3 & 4 in gov.
  - Federal Identity Credentialing Committee
  - Common Credential and Federal Identity Card
    - Common certificate policy and shared service providers
    - Gov. Smart Card Interoperability Standard (GSC-IS)
- Fed. Bridge CA and Fed. Policy Authority are PKI vehicle
- Non-PKI level 3 & 4 solutions
  - One-time password devices in common use – can meet level 3
    - Cell phones could be a good 1TPD platform
  - Zero knowledge passwords for level 3 – not widely implemented
  - Level 4 could be done with symmetric key tokens

Federal Employee Credentials

- Employees & affiliates
- Primarily levels 3 & 4
  - Most will eventually be hard token (CAC card)
  - Near term a lot will be soft token
- PKI based
  - New agency PKIs will be use shared service provider CAs
    - Common certificate policy framework
  - Legacy agency operated PKIs will be around for a while
  - Bridge CA will remain for policy mapping
    - Legacy agency operated PKIs
    - States & local government, business, foreign, etc.
    - Commerce & citizen class

FPKI Architecture



ACES

Other Bridges

Agencies (Legacy agency CA policy)

States

Private Sector

Foreign Entities

FBCA Certificate Policy

Bridge Certification Authority

E-Auth. Common Policy (Common Policy Root included in browser list of CAs)

Common Policy Certification Authority

Shared Service Provider CAs

SSP1

SSP2

SSP3

Fed. User Certificate

Fed. User Certificate

Fed. User Certificate

Fed. User Certificate

Assurance Level 1

Assurance Level 2

E-Governance Certification Authorities

(Mutual authentication of SAML/SSL Certificates only)

Common Policy Agency User Certs.

(Agencies buy certificate services from SSPs under Common Policy)

Financial Institution

Utility

Business

C4 Certification Authority

Citizen &Commerce Class Certificate Policy

Common Policy Framework

- Applies to Federal Employees, Affiliates (e.g., guest researchers), & Devices (e.g., servers)
- Three policies
  - Two user policies
    - FIPS 140 Level 2 Hardware Cryptomodule
      - Meets e_Auth assurance level 4
    - FIPS 140 Level 1 Software Cryptomodule
      - Meets e-Auth assurance level 3
  - One device policy (Level 1 Cryptomodule)
- Assurance comparable to FBCA Medium
  - More detailed Identity Proofing requirements
  - Transition strategy to 2048 bit RSA, SHA-256

Identity Proofing of Fed. Applicants

- A priori request from management required
- Employees' employment verified through use of "official agency records"
- In-person identity proofing
  - Credentials verified for legitimacy
  - Biometric recorded for nonrepudiation
- Trusted Agent may perform proofing
  - RA still verifies credentials

Cryptographic Transition Strategy

- Certs and CRLs expiring after 12/31/2008 must be signed using 2048 bit RSA keys
- User Certs generated after 12/31/2008 must contain 2048 bit RSA keys
- Certs and CRLs generated after 12/31/2008 must be signed using SHA-256

FPKI Certificate Policies

- Federal Certificate Policy
  - Rudimentary, Basic, Medium and High
  - Federal Policy Authority “maps” agency policy
  - currently x-certified
    - Medium: Treasury, DoD, Agriculture (NFC), NASA, DST ACES, Illinois
    - High: State Dept & Treasury
- Common Certificate Policy
  - Shared Service providers
- Citizen and Commerce Class
  - Streamlined process based on memo of agreement rather than detailed review of CP & CPS
    - Does anybody want this?

Knowledge Based Authentication (KBA)

- Not covered in 800-63
  - Symposium on 9-10 Feb. at NIST
- Can we just ask questions to authenticate users?
  - People do it now
  - “Walk-in” customers, real business need
    - It’s the age of instant gratification
- Similar to ID proofing process, but without closing the loop
- Could view KBA as similar to passwords
  - Only these passwords are not very secret
  - Valid claimant might not know them all
- How can we quantify KBA, what are the standards?

KBA: some questions

- What is a reasonable model for KBA?
  - What are the functions and features of each component?
  - What are the security implications of the components?
- For Users:
  - How much confidence do you need? Can KBA get there?
- What are the information sources and how do we evaluate them?
  - How accurate are the sources?
- What are the Mechanisms and Metrics?
- How do we score responses and what does a score mean?
- What can we standardize?

Questions