



PROTECTING YOUR ENTERPRISE THROUGH SECURE AUTHENTICATION™



## Breakout Session 2

# Elements of Secure Biometric-Based Authentication Systems



**National Institute of Standards  
and Technology**

Technology Administration  
U.S. Department of Commerce

*Workshop on Biometrics and Remote E-Authentication Over Open Networks*

## Objective

- Determine: How should biometrics play a role at each of the 4 'identity authentication assurance levels'

Level	Confidence in Asserted Identity's Validity
1	Little or none
2	Some
3	High
4	Very High

## Currently Specified

- Biometric methods are widely used to authenticate individuals who are physically present at the authentication point, for example for entry into buildings.
- **Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document.**
- In the local authentication case, where the claimant is observed and uses a capture device controlled by the verifier, authentication does not require that biometrics be kept secret.
- The use of biometrics to “unlock” conventional authentication tokens and to prevent repudiation of registration is identified in this document.

## Questions to be answered

- What architectures are appropriate?
- What properties of the biometric components are required?
- What issues need to be addressed?
- How can cryptographic and other security mechanisms be used in conjunction with biometrics to provide a robust authentication solution?
- What architectures provide the features needed for use at each level?
- What criteria should be used to rate these architectures?

## Questions (cont'd)

- How does the fact that biometrics are not secrets affect the way they are used?
- What role do certifications play?
- What differences exist between access by employees and the citizenry?
- Can/should FAR requirements be identified for each level?

## Architectures

- Basic considerations
  - Where is the biometric enrollment data stored?
  - Where is the matching performed?
  - How is the data protected during storage & transmission?
  - What protections exist on the system as a whole & on the individual components?
  - What protections are assumed for a physical token and do these same protections apply to a biometric device?
  - What are the threats and risks, really? What can we assume about an attacker at each level?
  - Is local/token matching always better than server based matching? Why?

## Biometrics as an authentication token

- 800-63 precludes this (even at Level 1)
  - Tokens are always secrets
  - Biometrics are not secrets
  - ergo, biometrics cannot be used as tokens
  
- Analogy between biometrics & the public key?

*Device  
security  
level*

*Signed/  
encrypted*

*Header  
contains  
type/DTG/etc*

Live sample

Secure  
channel

SSL/TLS

Enrolled  
template

*Signed/  
encrypted*

*Secure  
Storage*

*Type=enroll*

# Authentication Tokens

**Table 2. Token Types Allowed at Each Assurance Level**

<i>Token type</i>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

## Potential issues to be addressed

- Secrecy
- Randomness
- Revocation
- Spoofing and other attacks
- Non-repudiation
- Public review
- Privacy considerations
  
- What issues are unique to biometrics?
  
- How does the introduction of biometrics alter or place additional requirements on the underlying security infrastructure?

## More Questions

- How can biometric data be compromised?
  - What would it take to do this?
  
- What could it be used for if obtained?
  - What **existing** security mechanisms are in place to protect against this?
  - What **new** mechanisms are needed?

800-63 does a good job of identifying potential attacks, but does not look at attacks against a biometric specifically.

## Comparison of technologies

	Strengths	Weaknesses
Passwords One-time passwords Random passwords		
Soft crypto token Symmetric Asymmetric		
Hard token		
Physical token		
Biometric		
...		

Time permitting & if deemed worthwhile

## Problem to be solved

- Remember:
  - “security and privacy of sensitive **unclassified** information”
- Example scenarios from OMB M-04-04:
  - Level 1:
    - an individual applies to a Federal agency for an annual park visitor's permit
  - Level 2:
    - A beneficiary changes her address of record through the Social Security web site.
  - Level 3:
    - A patent attorney electronically submits confidential patent information to the US Patent and Trademark Office.
  - Level 4:
    - A law enforcement official accesses a law enforcement database containing criminal records.

## Discussions

- Impossible to avoid discussion of threats and countermeasures, but will attempt to not delve too deeply into this
  - Subject of separate breakout session
- However, it is difficult to discuss a security architecture in isolation from the threats against it.

## Approach

- Begin with review of how biometrics are characterized and utilized within the current 800-63 document
  - Perhaps challenging some underlying assumptions & paradigms
- Brainstorm & suggest ways that biometrics can be used effectively
- Identify limitations, constraints, and requirements to how they should be used
- Determine what requirements on the system as a whole are needed to allow biometrics to be integrated appropriately

## End Goal

- Prepare a recommendation on use of biometrics at each of the 4 levels, providing:
  - A general description of the mechanism
  - Identification of requirements for use
  - An example use case scenario
  - Identification of components
  
- Recommend contents for a Biometric Appendix (?)

## Ancillary Goals

- Identify areas for additional research
- Provide recommendations for:
  - Standards – existing/new
  - Testing & certification
- Provide recommendations for improvements to industry:
  - Biometric component vendors
  - System integrators / solution providers

## Keep in Mind

- Perfection is neither achievable nor required
- Our job is to figure out how good is has to be  
  
and
- How to make it so.

# The Beginning

Catherine J. Tilton  
SAFLINK Corp.  
1875 Campus Commons Dr, Suite 301  
Reston, VA 20191

[ctilton@saflink.com](mailto:ctilton@saflink.com)  
703-547-0404  
Cell 703-472-5546  
Fax 703-547-0399



PROTECTING YOUR ENTERPRISE THROUGH SECURE AUTHENTICATION™

A central graphic featuring a transparent blue cube with the "saf" logo inside. The background is a blue grid with binary code (0s and 1s) scattered throughout. Below the cube is a horizontal bar with five icons and their corresponding labels.

COMPUTER NETWORKS

PHYSICAL FACILITIES

APPLICATIONS

MANUFACTURING AUTOMATION SYSTEMS

TIME & ATTENDANCE SYSTEMS

IDENTITY ASSURANCE MANAGEMENT™

## Breakout Session #2

## What do the documents say today?

- OMB M-04-04
  - Does not mention biometrics
    - Does not identify which technologies should be implemented
  - Scope is e-Government
    - Includes individual user, business, or government entities
  - Credential: an object that is verified when presented to the verifier in an authentication transaction.
  - Credential Service Providers (CSPs) – issue electronic credentials.
  - Privacy Impact Assessments
  - Cost/Benefit Analysis

## OMB M-04-04

- Each step of the authentication process influences the assurance level chosen. From identity proofing, to issuing credentials, to using the credential in a well-managed secure application, to record keeping and auditing—the step providing the lowest assurance level may compromise the others.

Level	Confidence in Asserted Identity's Validity
1	Little or none
2	Some
3	High
4	Very High

## Who Goes There?

- “Individual Authentication”
  - The process of establishing an understood level of confidence that an identifier refers to a specific individual.
- “Biometric authentication is fundamentally different from the other two classes because it does not rely on secrets.”
- “The scoring aspect of biometrics is a major departure from other classes of individual authentication technologies, which provide a simple, binary determination of whether an authentication attempt was successful.”

## Who Goes There?

- “Biometric values that are captured for authentication and transmitted to a remote location for verification must be protected in transit.”
  - Protection from interception & replay
- + protection of templates stored on servers
- “... compromise of an authentication server could have a very significant impact owing to the special characteristics of biometrics: namely, that they are not secret and cannot be easily modified.”
- “in practice, most biometric authentication systems require the use of a password or PIN to improve security ...”

## Who Goes There?

- Recommendation 5.2:
  - “Biometric technologies should not be used to authenticate users via remote authentication servers because of the potential for large-scale privacy and security compromises in the event of a successful attack (either internal or external) against such servers. The use of biometrics for local authentication – for example, to control access to a private key on a smart card – is a more appropriate type of use for biometrics.”

## Question

- Biometrics are not secrets, so ...
  - Compromise of templates on a server should be LESS of an issue, not more of one.
  - Theoretically, knowledge of the biometric characteristic could be used in a spoofing attack in EITHER a server-based or local matching scenario.
  - Template compromise is more of a privacy issue than a security issue.
    - But we've already agreed they are not secrets in the first place.
  - Technologies exist (i.e., strong encryption, DB access controls) to address this.
- Mechanisms exist to ensure enrollment templates cannot be used as verification samples

- “This guidance addresses only traditional, widely implemented methods for remote authentication based on secrets.”
- NIST is continuing to study both the topics of knowledge based authentication and biometrics and may issue additional guidance on their uses for remote authentication of individuals across a network.
- This technical guidance covers remote electronic authentication of human users to Federal agency IT systems over a network.

## 800-63 Intro

- Biometric methods are widely used to authenticate individuals who are physically present at the authentication point, for example for entry into buildings.
- **Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols addressed in this document.**
- In the local authentication case, where the claimant is observed and uses a capture device controlled by the verifier, authentication does not require that biometrics be kept secret.
- The use of biometrics to “unlock” conventional authentication tokens and to prevent repudiation of registration is identified in this document.

## Remote authentication

- Remote authentication mechanisms
  - Combination of credentials, tokens, and authentication protocols
  
- Credentials
  - Bind the (authentication) token to the identity
- Token
  - Something a claimant possesses & controls
  - e.g., a key or a password
  - a secret
- “Biometrics are not used directly as tokens in this document.” [5.2]

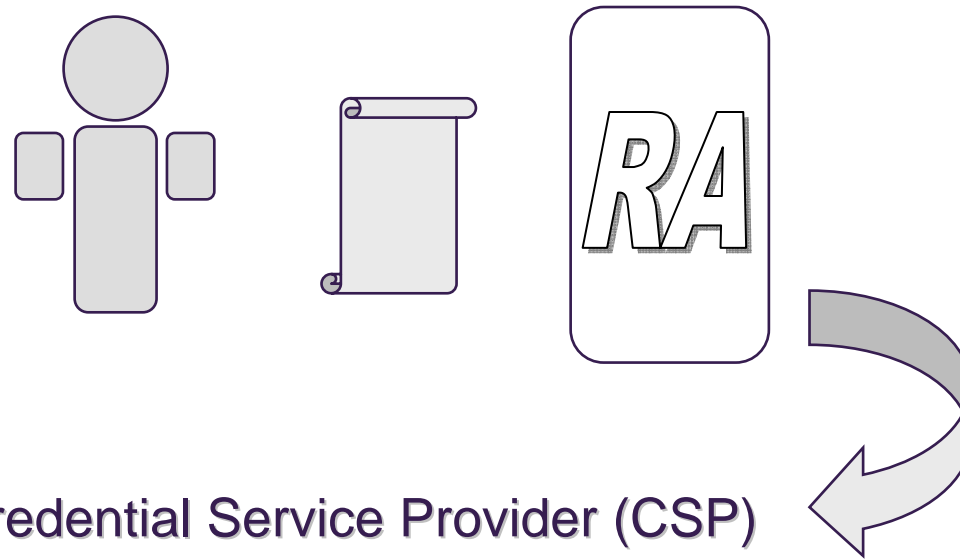
## What are the concerns?

## What is the solution space?

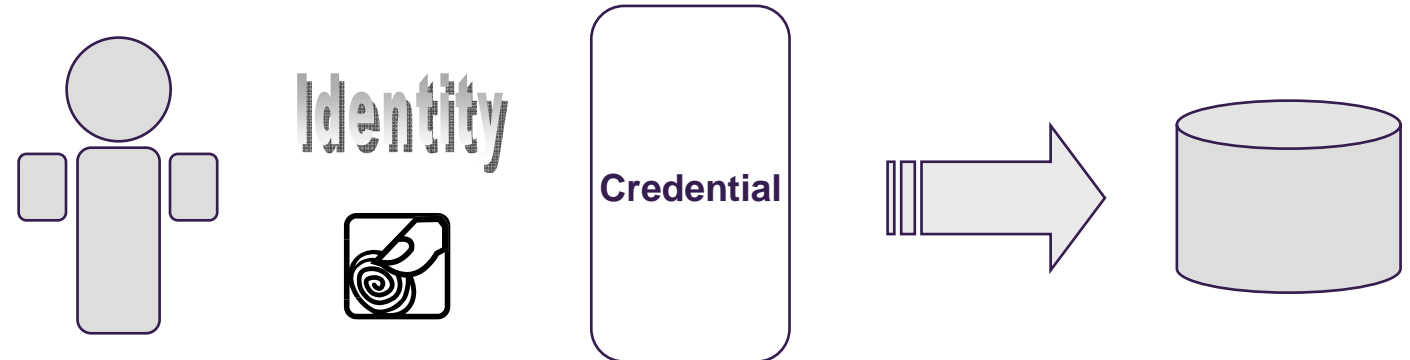
- The role of:
  - Encryption
  - Signing
  - Nonce's
  - Timestamps
  - Attribute certs
  - Mutual authentication
  - Trusted path / secure messaging
  - Certified devices
  - MOC
  - Challenge/response
  - Protocols

# Registration

## Identity Proofing



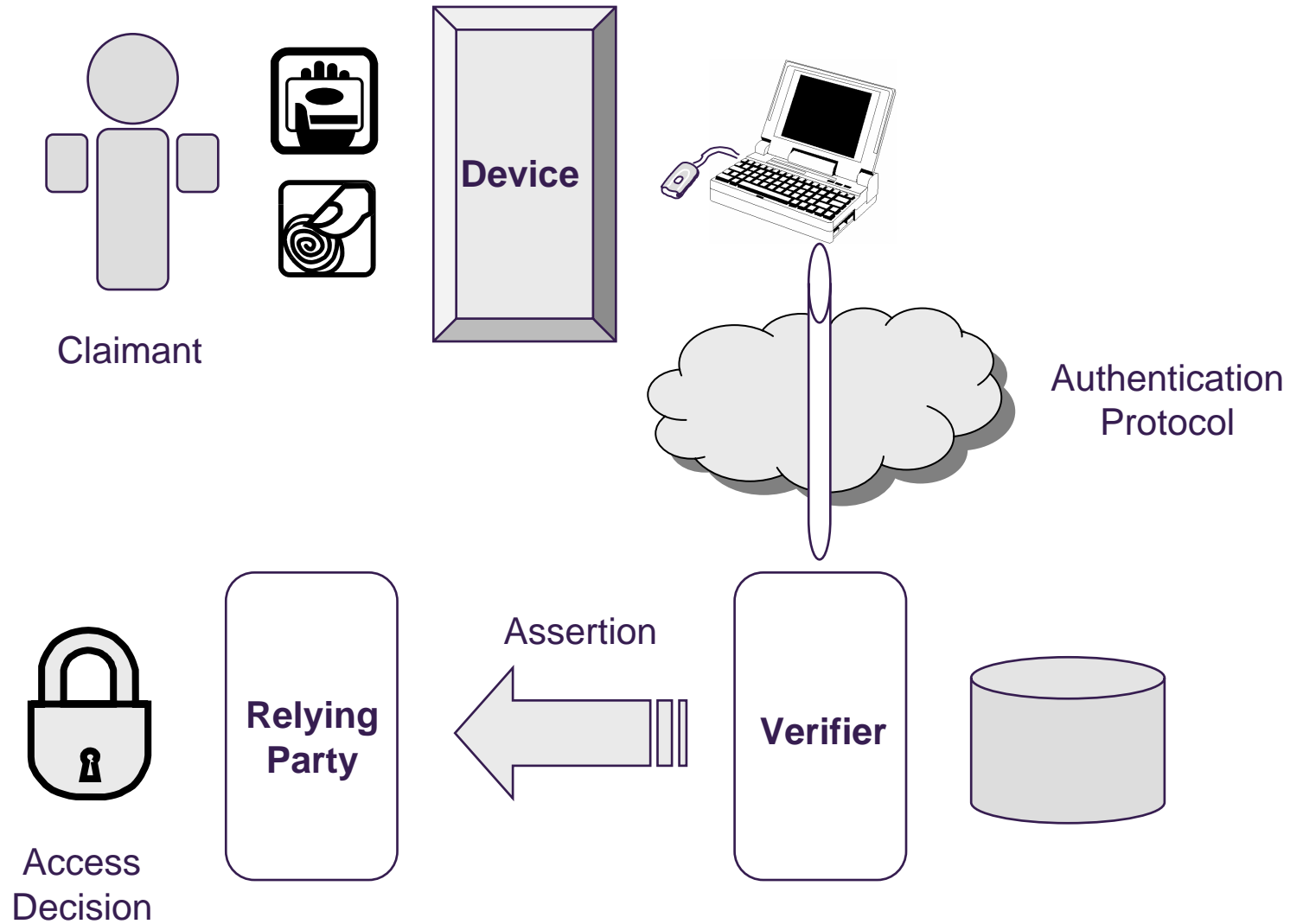
## Credential Service Provider (CSP)



## Potential mechanisms

- How bound?
  - Cryptographically
  
- How protected?
  - Type & DTG in header
  - Digitally signed
  - Encrypted
  - Stored in cert
  
- Differences
  - Subject provides token (not “issued” by CSP)
  - Verifier may

# Authentication



## Potential mechanisms

- Device
  - Tamper resistant
  - Anti-spoofing countermeasures
  - Signs & encrypts verification sample
  - Binds sample to other data (nonce, card data)
  - Mutual authentication to verifier
- Or remote computer
  - Performs binding, mutual authentication
- Differences
  - BACKWARDS!
  - Original registration is for template
  - Authentication token is live sample

## Question

Can cryptographic methods be effectively employed to address concerns?

## Threats

- Token
  - Compromise of token
    - Disclosed, stolen, duplicated/replicated, sniffed, guessed
    - Malicious code, intrusion
- Authentication Protocols
  - Eavesdropping
  - Imposters
    - Claimants/subscribers, verifiers, relying parties
  - Hijacking sessions
  - Replay attacks
  - Man-in-the-middle

Countermeasures exist for all of these!

## Unique threats

- Sensor attacks
  - Spoofing
- Verifier attacks
  - Modify results of match
  - Modify threshold
  - Hillclimbing attack
- Revocation (?)

## Architectures

### ➤ Storage Location

- Server
- Client
- Device
- Token

### ➤ Matching Location

- Server
- Client
- Device
- Token

16 Permutations

## Which are appropriate? At what level(s)?

Store \ Match	Server	Client	Device	Token
Server				
Client				
Device				
Token				

## Recommendations

- Level 1
- Level 2
- Level 3
- Level 4

## Additional Recommendations

- Appendix outline
- Areas for further research
- Recommendations to industry

## Actions

- Follow on process to assemble & vet recommendations regarding use of biometrics at each level
- Wrap template in secure package



PROTECTING YOUR ENTERPRISE THROUGH SECURE AUTHENTICATION™

A banner for Saf link Identity Assurance Management. The background is a blue grid with a large, 3D, transparent glass cube in the center containing the "saf" logo and binary code. Below the grid is a dark blue horizontal bar with five icons and their corresponding labels: a laptop for "COMPUTER NETWORKS", a keyhole for "PHYSICAL FACILITIES", the "saf" logo for "APPLICATIONS", a factory for "MANUFACTURING AUTOMATION SYSTEMS", and a group of people for "TIME & ATTENDANCE SYSTEMS". At the bottom of the banner, the text "IDENTITY ASSURANCE MANAGEMENT™" is written in white capital letters.

# Breakout Session #2

## Wrap Up

## The good news and the bad news

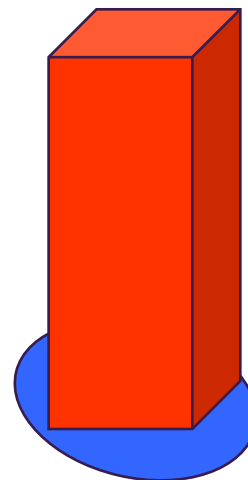
- The Good News
  - Lots of lively, intelligent discussion
  
- The Bad News
  - Very little agreement or consensus

## Primary areas of discussion

- What does 800-63 really say/mean?
- Are biometrics secrets or not, and if not, how does this limit their use?
- How are the underlying assumptions for secret-based authentication different from biometric based authentication?
- Are the system security mechanisms required for physical token/cryptologic credential sufficient for biometric authentication also?
- Spoofing and revocation remain issues with unique application to biometrics.
- Is integrity really the key issue with biometric authentication (rather than secrecy)?

## Primary areas of discussion

- How important is entropy in a non-secrets-based authentication and what does it equate to in biometrics?
- Trust level required for biometric device (at what level).
- Are we trying to force-fit biometrics into an existing paradigm?
- Are we looking at everything as a level 4 problem?



## A few points

- No corresponding ability to selecting different passwords for different applications.
- Biometric modalities and implementations are not created equal and demonstrate different characteristics – e.g., behavioral biometrics have different secrecy, spoofability, and challenge/response characteristics from physical biometrics.
- Specific security criteria (not tied to secrets) for each level would be useful for assessing suitability of possible biometric architectures/ implementations.
- Consider role of a “Biometric CSP” for non-token based biometric implementations within a remote e-Auth architecture.

## A hope dashed - ?

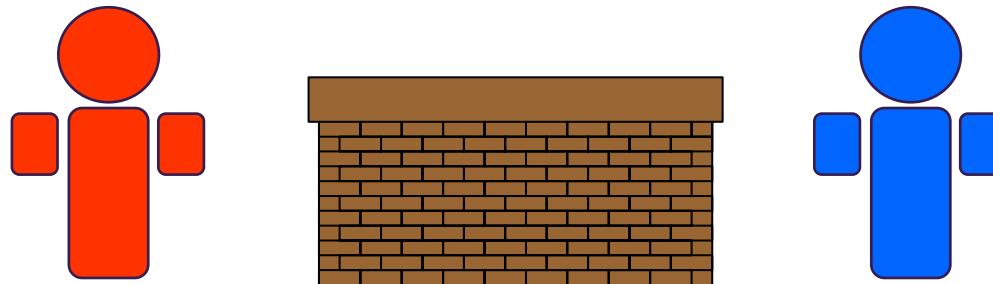
Store Match	Server	Client	Device	Token
Server				
Client		Level Requirements Constraints		
Device				
Token				

## Areas for further work

- Request INCITS M1 to begin a project for documenting within an application profile the use of biometrics for remote e-Authentication
  
- Perhaps initiate a study project to draft a technical report describing biometric architectures & security requirements
  - assuming biometrics would be allowed for each of the authentication levels

## Areas for further work

- Need more collaborative work between cryptographic and biometric experts
  - Cross-fertilization
  - Cross the culture/language chasm
  - Apply crypto techniques to the biometrics domain



## Suggestion

- Create proposed biometric requirements for 800-63 in same form/content:
  - Threats
  - Resistance to threats
  - Mechanism requirements
    - Level X
      - Credential lifetime, status, and revocation
      - Assertions
      - Protection of long term shared secrets
      - Password strength
      - Example implementations

## Recommendations

- Arrange a follow on to this workshop to develop recommendations for the use of biometrics at each of the 4 levels (M1).
  - Call for contributions
  - Compile
  - Vet
- Recommend biometrics industry accelerate work in the area of anti-spoofing/liveness detection.
- Perhaps arrange a separate workshop/study on the topic of biometric revocation alone.
  - Group generally agreed that wrapping the biometric data in a revocable package is an idea worth investigating/refining.
  - Similar group for entropy/SOF

