



COMPUTER NETWORKS



PHYSICAL FACILITIES



APPLICATIONS



MANUFACTURING AUTOMATION SYSTEMS

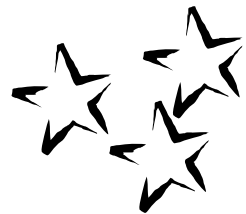


TIME & ATTENDANCE SYSTEMS

IDENTITY ASSURANCE MANAGEMENT™

Remote Authentication & Biometrics

C. Tilton



Agenda

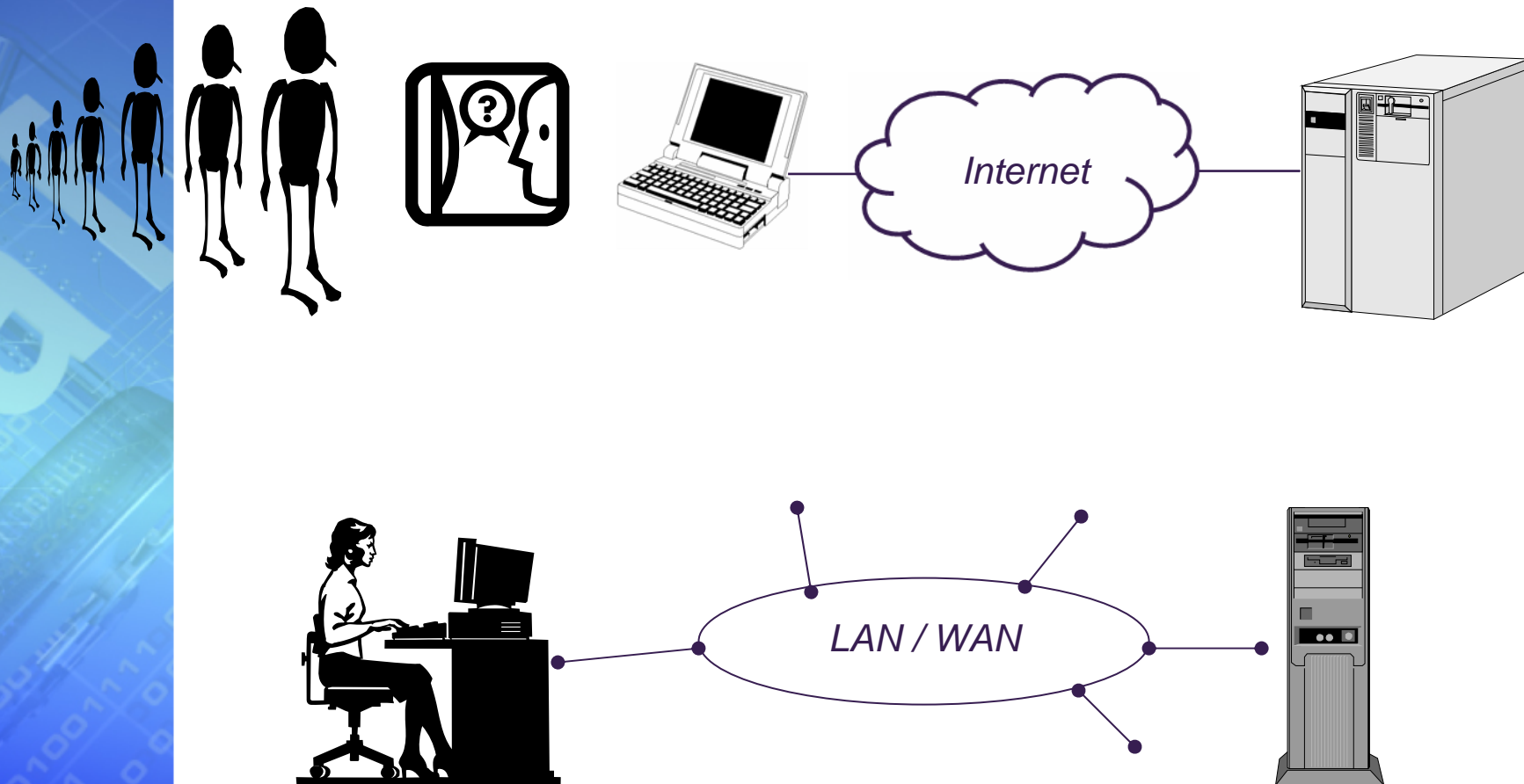
- The remote authentication problem
- OMB M-04-04 & SP 800-63 overview
- Issues to be addressed
- Architectures & possible solution space
- AHGBEA & progress to date

The problem - defined

- Electronic authentication (e-authentication):
 - the process of establishing confidence in user identities electronically presented to an information system

- Remote e-authentication
 - Establishing identity over an open network that you do not control from a node that is outside of your supervision

Open & Closed Networks



Background

- Security in remote authentication in general, and user authentication in particular, has been an issue since the internet has existed
- The government addressed this for e-authentication last year with OMB M-04-04 and NIST's SP800-63
- A number of possible authentication methods exist
- Question is –
 - What is the role of biometrics at the various security levels and what architectures and surrounding security mechanisms are appropriate for use in this environment?
- NIST held a workshop Mar 30-31 this year

What do these documents say?

- 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 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

- “This guidance addresses only traditional, widely widely implemented methods for remote authentication **based on secrets.**”
- NIST is continuing to study both the topics of knowledge based authentication and biometrics biometrics and may issue additional guidance on on their uses for remote authentication of individuals across a network.
- This technical guidance covers remote electronic 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 this document.” [5.2]

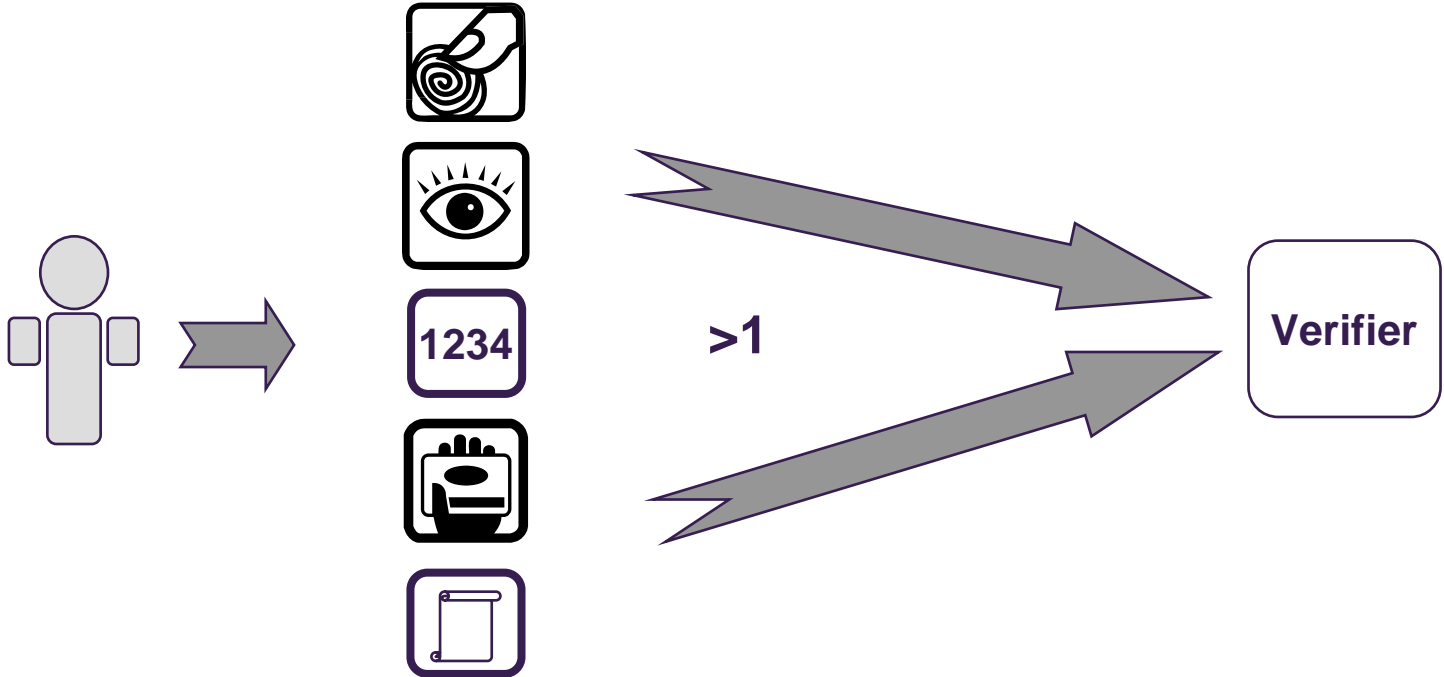
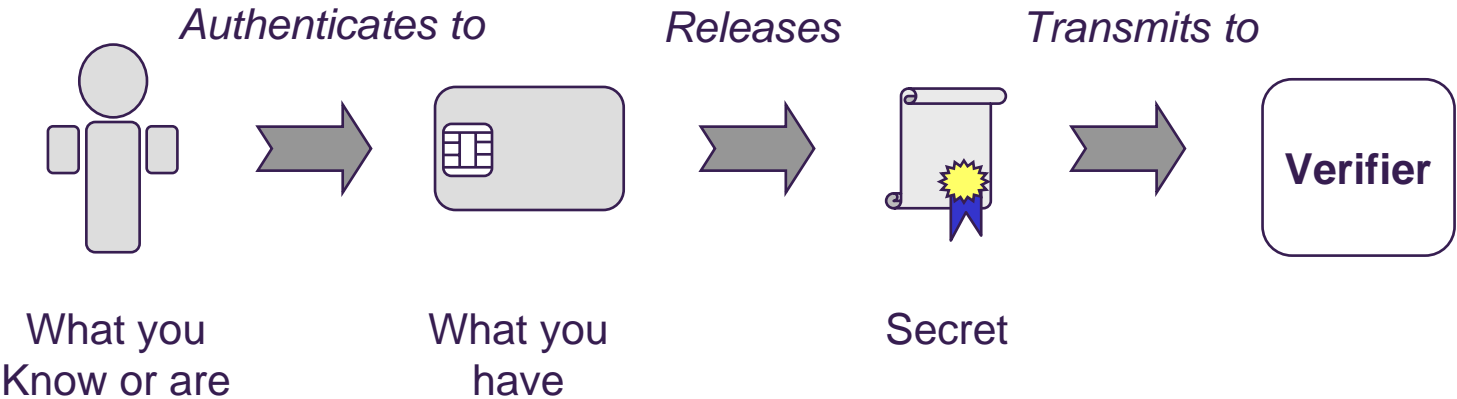
Authentication Tokens

Table 2. Token Types Allowed at Each Assurance Level

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

- Level 1 and 2 require only one factor authentication
- Levels 3 and 4 require two factor authentication

Multi-factor



Some of the questions to be answered

- Are biometrics secrets or not, and if not, how does this limit their use?
- How are the underlying assumptions for secret-secret-based authentication different from biometric based authentication?
- How important is entropy in a non-secrets-based based authentication and what does it equate to to in biometrics?
- Is integrity really the key issue with biometric authentication (rather than secrecy)?
- How can cryptographic and other security mechanisms be used in conjunction with biometrics to provide a robust authentication solution?
- What differences exist between access by employees and the citizenry?

Some more questions

- What architectures provide the features needed for use at each level?
- What properties of the biometric components are required?
 - Trust level required for biometric device (at what level)
 - What role do certifications play?
- Are the system security mechanisms required for physical token/cryptographic credential sufficient for biometric authentication also?
- Are we trying to force-fit biometrics into an existing paradigm?
- Are we looking at everything as a level 4 problem?

Issues

- The following issues have been identified, which which are either unique to the use of biometrics biometrics in an e-authentication environment, or or which have unique aspects to them as a result result of the use of biometrics.
- Revocation.
- Sensor Spoofing/Liveness Detection.
- Characterization of Entropy/Strength-of-Function. Function.
- Integrity -vs- secrecy.
- Privacy considerations.

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!

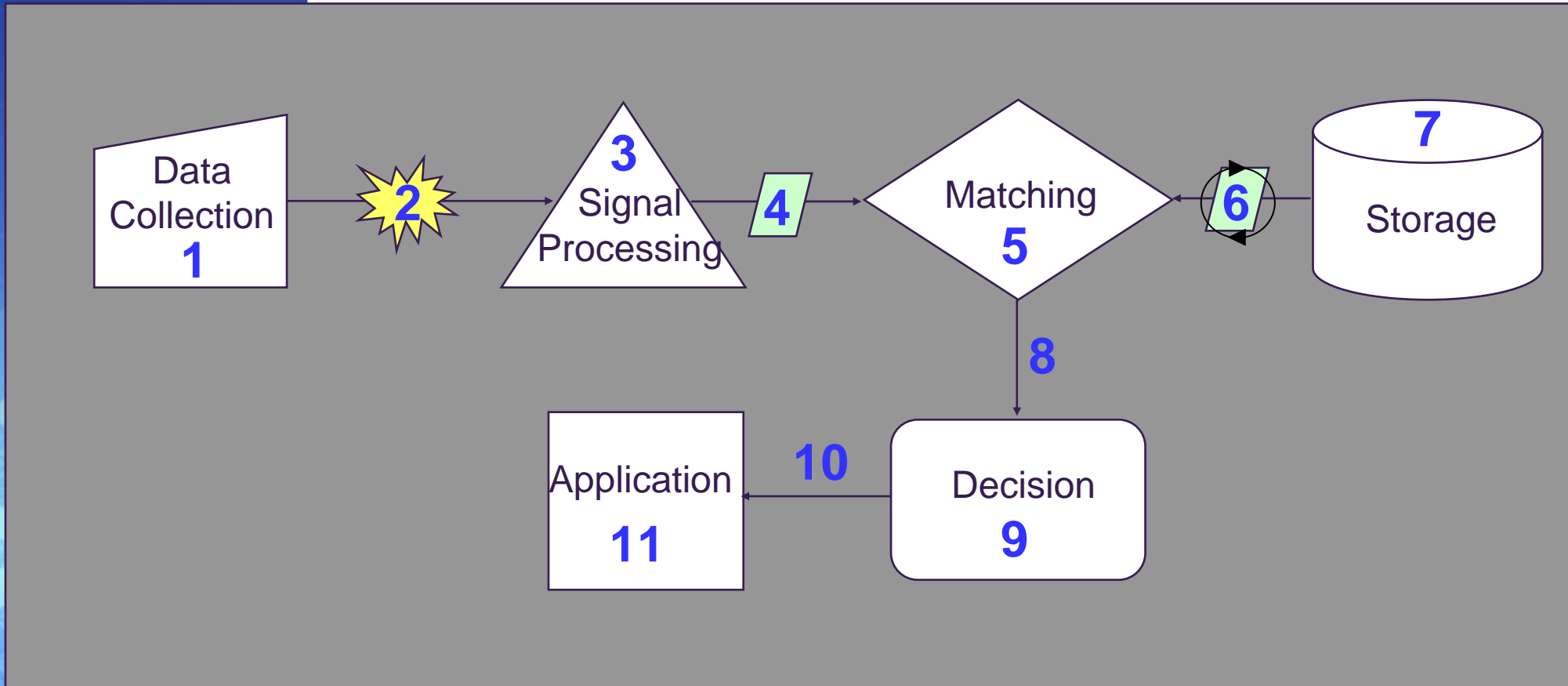
More Questions

- 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.

Threat Model - sample



- For each processing, storage, & transmission point, define:
 - Threat
 - Countermeasures

Unique threats

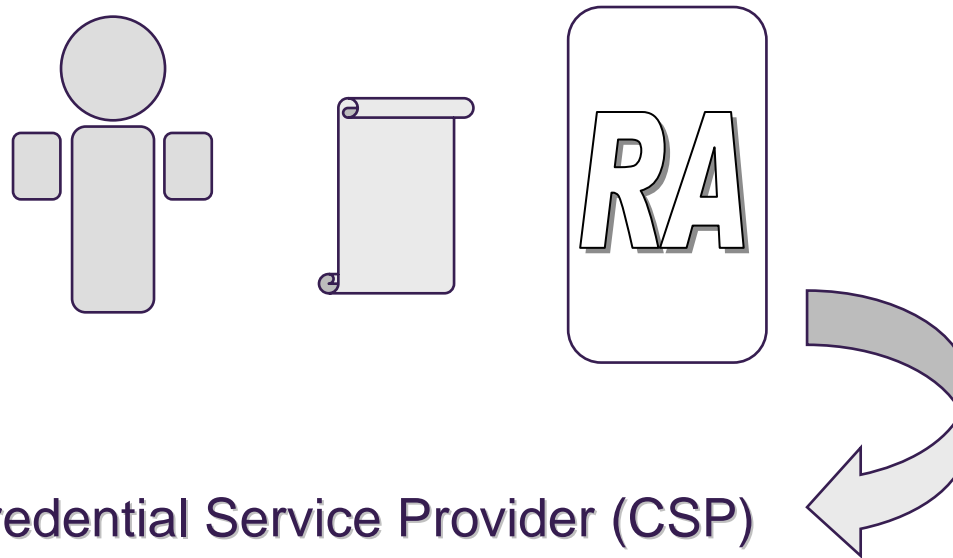
- Sensor attacks
 - Spoofing
- Verifier attacks
 - Modify results of match
 - Modify threshold
 - Hillclimbing attack
- Revocation (?)

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)



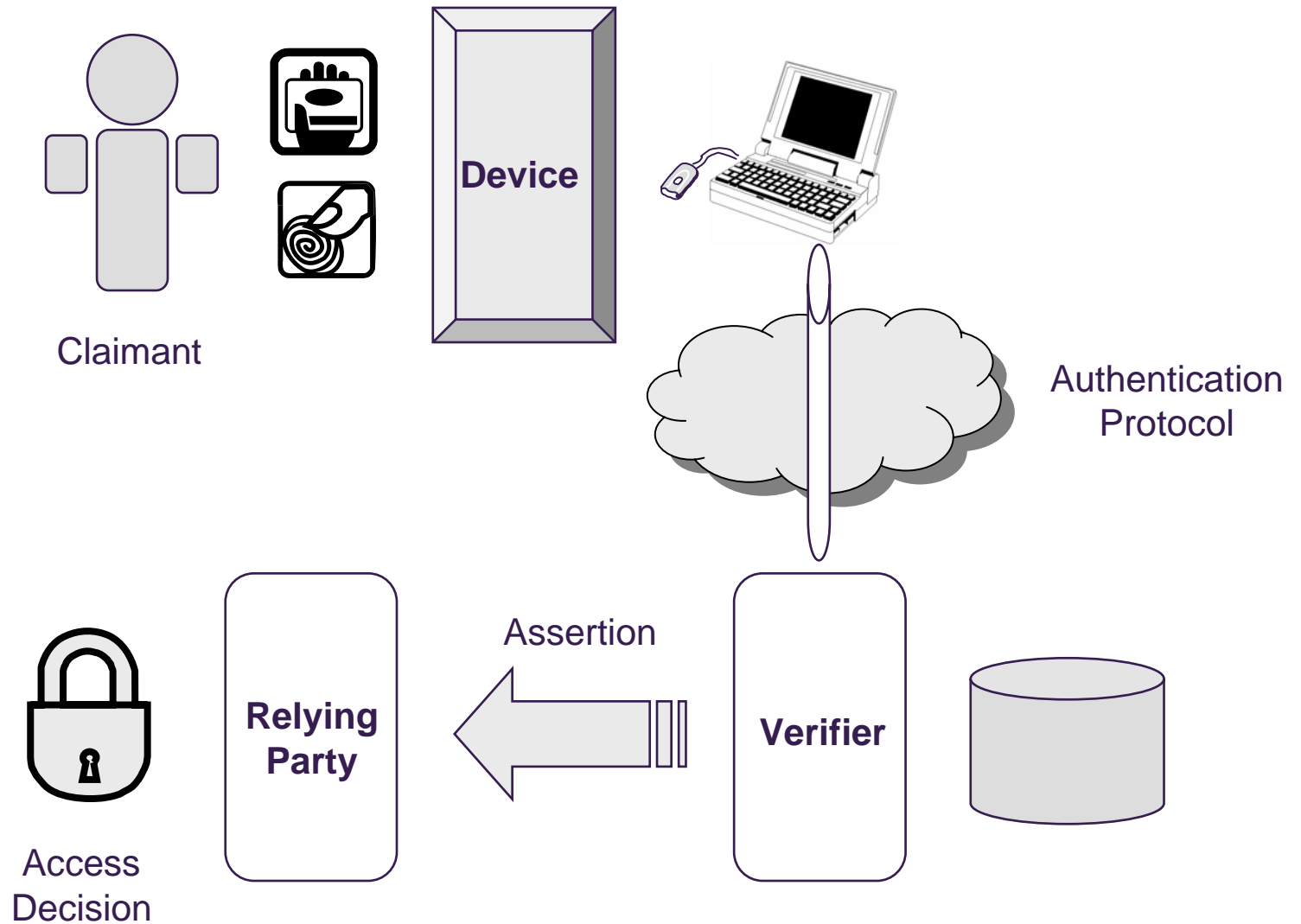
Potential mechanisms

- How bound?
 - Cryptographically

- How protected?
 - Type & DTG in header
 - Digitally signed
 - Encrypted
 - Stored in cert

- Differences
 - Subject provides token (not “issued” by CSP)

Authentication



Potential mechanisms

- Device
 - Tamper resistant
 - Anti-spoofing countermeasures
 - Sign & encrypt verification sample
 - Bind 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

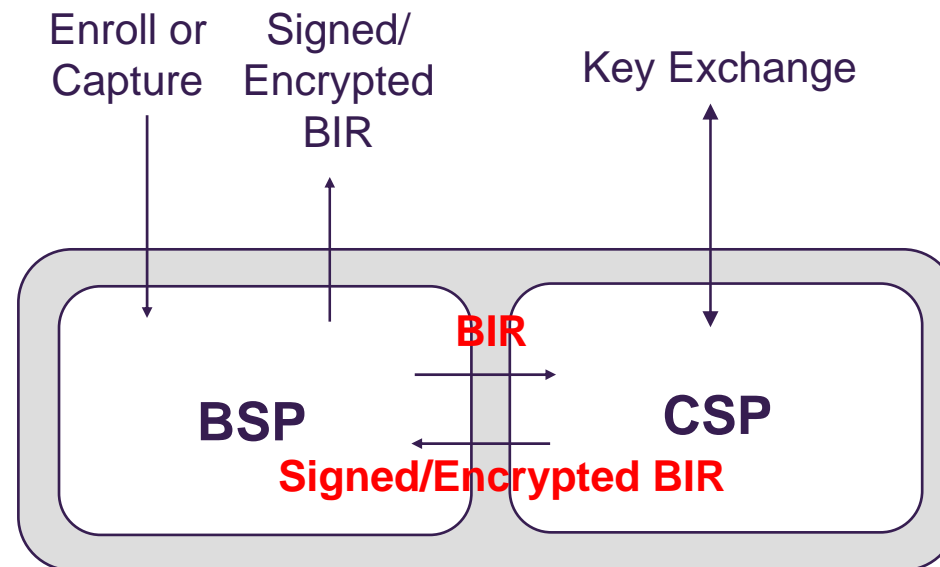
Other mechanisms

- Revocation
 - Wrap template in secure, revocable package
 - Distortion schemes
- Multi-factor
- Liveness detection

- Consider role of a “Biometric CSP” for non-token token based biometric implementations within a a remote e-Auth architecture.

Option

- Combined BSP/CSP
 - Biometric functions accessed via BioAPI
 - Cryptographic functions accessed via crypto API
 - e.g., key exchange
 - Ability for BSP to sign/encrypt BIRs



System level architecture

- How does the introduction of biometrics alter or place additional requirements on the underlying security infrastructure?

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 whole & on the individual components?
- What protections are assumed for a physical token and do these same protections apply to a a biometric device?
- What are the threats and risks, really? What can we assume about an attacker at each level? level?
- Is local/token matching always better than server server based matching? Why?

Architectures

➤ Storage Location

- Server
- Client
- Device
- Token

➤ Matching Location

- Server
- Client
- Device
- Token

16 Permutations

Architecture Analysis Matrix

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

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 of a successful attack (either internal or external) against such servers. The use of biometrics for local authentication – for example, example, to control access to a private key on a a smart card – is a more appropriate type of use use for biometrics.”

“Who Goes There? - Authentication Through the Lens of Privacy”, Dr. Stephen T. Kent and Ms. Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council

But ...

- If biometrics are not secrets, then ...
 - 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

M1 AHGBEA

- In response to the workshop and the work left to to be done, INCITS M1 formed an group to study study these issues:
 - Ad Hoc Group on Biometrics in E-Authentication Authentication
- Objective
 - Recommendations on how biometrics should be be used in remote authentication
- Kick-off meeting held 7 June 05
- Next meeting: 21 Sep 05, 1-6 PM
 - Regency Ballroom B

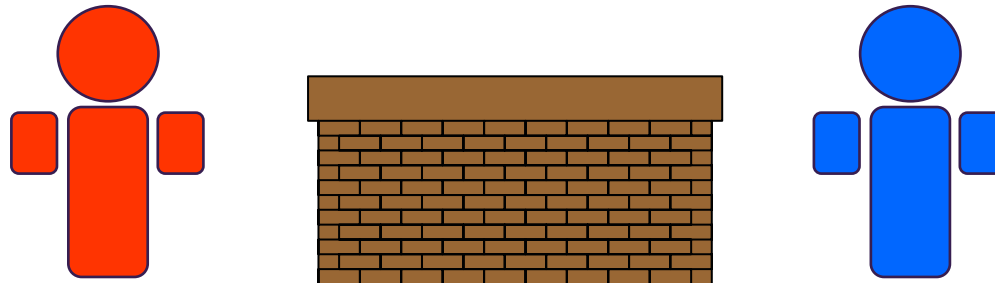
AHGBEA participation

- Participation in any M1 meeting is open to any directly or materially affected parties.
- Participation by those with expertise in the areas areas of biometrics architectures and interfaces, interfaces, authentication, information security, security, cybersecurity, and the application of security mechanisms, particularly cryptographic cryptographic mechanisms, is solicited.

Can you contribute?

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 domain



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.

Thanks!

Catherine J. Tilton
Chair, BioAPI Consortium
International Rep, INCITS M1
VP, Standards & Technology
SAFLINK Corporation
1875 Campus Commons Drive, Suite 301
Reston, VA 20191
703-547-0404
Fax: 703-547-0399
ctilton@saflink.com
www.saflink.com