

M1/05-0408

Issues and Questions list for 2nd AHGBEA meeting

**September 21st, 2005
Hyatt Regency Crystal City
Arlington, VA U.S.A.**

Issues:

The following issues have been identified, which are either unique to the use of biometrics in an e-authentication environment, or which have unique aspects to them as a result of the use of biometrics.

- 1) Revocation.
- 2) Sensor Spoofing/Liveness Detection.
- 3) Characterization of Entropy/Strength-of-Function.
- 4) Integrity -vs- secrecy.
- 5) Privacy considerations.

Related Issues (by category):

IT Security

- Define requirements at each assurance level defined in OMB-04-04:
 - **Level 1:** Little or none
 - **Level 2:** Some
 - **Level 3:** High
 - **Level 4:** Very High
- Binding the biometric and other identifying information to the user of the system
- Maintaining integrity of the data
- Maintaining privacy of the data
- Multiple routing and routed protocols at OSI Layers 3 and 4
- Implementing solutions in wireless architectures, both WLAN and Cellular
- Existing information security policies in place by individual organizations
- Protocol Attacks
 - Eavesdropping
 - Replay
 - Man in the Middle
- System Compromise
 - Database compromise
- Brute Force
 - Dictionary attacks
- Out of Band
 - Social engineering
 - Phishing

Cryptographic

- Correlate assurance levels with applicable tokens in NIST SP800-63:

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	√	√		

- Maintaining integrity of the data
- Maintaining confidentiality of the data
- Integrating with PKI
- Key management

Biometric

- Biometrics cannot be changed (as passwords can) when compromised
- Biometrics are not considered secrets
- Do biometrics possess an adequate degree of randomness?
- Biometric algorithms are not public or available for public review (as encryption algorithms are)
- Perception that if a biometric is stolen, an identity is stolen and can be used for identity theft
- Spoofing attacks
- Proper authentication and authorization of enroller
- Revoking credentials and tokens
- Binding the biometric and other identifying information to the user of the system
- Verifier attacks (threshold/result modification, hill climbing attacks)
- Storage location, verifier, and comparison matching mechanism need to have mutual trust
- Sharing of biometric data/mechanism across domains (i.e., use in a federated identity management environment)
- Static -vs- dynamic biometrics

Questions:

IT Security

- What architectures are appropriate?
- How can biometric data integrity be maintained?
- How can biometric data privacy be maintained?
- What differences exist between access by employees and the citizenry?
- 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?
- What is the relationship between authentication and authorization once the user successfully enters the system?
- What role can VPN and SSL technologies play in solutions?

Cryptographic

- How can cryptographic and other security mechanisms be used in conjunction with biometrics to provide a robust authentication solution?
- What role do certifications play?
- Is local/token matching always better than server based matching?
- How is the data protected during storage & transmission?
- How can crypto maintain biometric integrity?
- How can crypto maintain biometric privacy?
- What is the role of PKI, shared, named and symmetric keys?

Biometric

- What properties of the biometric components are required?
- How does the fact that biometrics are not secrets affect the way they are used?
- Can/should FAR requirements be identified for each level?
- Where is the biometric enrollment data stored?
- Where is matching performed?
- What other credentials are suitable for use in verification systems?
- What security techniques currently exist for use with biometrics authentication and how do they fit in the architecture?
- How can the device be spoofed?
- How can credentials and tokens be revoked?
- How does the introduction of biometrics alter or place additional requirements on the underlying security infrastructure?
- If a biometric is compromised, how can it be used to attack a system and what countermeasures (existing/new) can be applied?
- Is local/token based matching always better than server-based matching and why?