Contactless Biometrics for PACS

PAIIWG Viewpoints by an Industry Expert
September 21, 2005
Where are we now?

• FIPS 201 does not define contactless biometrics for PACS
• To use biometrics, FIPS 201 requires
  – Insert card in contact based reader
  – Enter PIN for access
  – Reader accesses biometric information
  – Bearer presents livescan biometric for comparison
• What brought this methodology into being?
• What may we need to work on to improve it?
Issues with Biometrics

• Lab vs. Real-world
  – Three effective standards available (image, minutiae, pattern)
  – Why would you pick one over the other?

• When and where is a biometric appropriate vs. PIN?
  – Which one offers a better solution?
  – Which one is better understood in daily use?

• Which mode to use?
  – Match on card (MOC)
  – Match to card at reader (M2C)
  – Match to system by index (M2S)
Core Issues

• Discussion at token level vs. system level
  – Token only will lead us nowhere

• Security can collapse to single point of failure
  – If all security factors are all correlated to the card (MOC and PIN verification), the system will rely on the integrity of the card (and only that) to make sure everything is fine

• Biometrics must be used to confirm bearer matches transaction requirements at a system level
  – Enforced by readers, crypto protocols, back-end systems
  – Not just the card (avoid the YES card please!)
Core Issues, contd.

• Entry of a PIN and the capture of a livescan biometric present the same problems to the system
  – Where is the source image?
  – How is it protected?
  – Think of PIN standards for POS in Financials
  – Think of typical attacks on Windows based systems
Core Issues, contd.

• Privacy Act of 1974 says I can not do this
  – Issue is more inertia than anything else
  – Properly managed Privacy Impact Assessment and publication on the Federal Register is the enabler
  – Are you (the agency Privacy Officer) willing to do it?
  – Should it be across the board for all FIPS 201 compliant agencies?

• Cardholder participation
  – Do not want to be in the news that you can read a biometric from a distance
  – Contact requires you to insert to participate
Summary

• Top items for PAIIWG future work
• Systemic use for physical access needs to be addressed
  – Which standard (image, minutiae, pattern)?
  – Where is verification done (MOC, M2C, M2S)?
  – What are the performance requirements?
• Privacy issues must be addressed
  – Model PIAs and Federal Register notices
  – Cardholder participation solution required
Contact Information

Stephen P. Howard
Partner
ID Technology Partners, Inc.
316-B Cross Green Street
Gaithersburg, MD 20878
703.319.3171 (Direct Phone)
703.319.3172 (Direct Fax)
SteveHoward@idtp.com
WEB: www.idtp.com