



Panel: Biometrics in Identity Management and Credentialing

presented to:

Smart Card Alliance Government Conference

30 October 2014

Agenda

Overview

Introduction of Panelists

Round-table Discussion

Overview: Biometrics in Identity Management and Credentialing

One of many applications of biometrics

- Cross-over area between biometrics and smart cards
- Several use cases for civil ID, credentialing, criminal ID, background checks, physical and IT access control

Practical concerns for implementation

- Privacy, security, regulations
- Standards and frameworks for interoperability

Global trends

- Mobile Commerce
- Healthcare IT

Panelists

Geoff Slagle

- Director of Identity Management, American Association of Motor Vehicle Administrators (AAMVA)

David Coleman

- Senior Director, Novetta

Walter Hamilton

- Senior Consultant, Identification Technology Partners (IDTP)

Jim Loudermilk

- Senior Level Technologist, Science and Technology Branch, Federal Bureau of Investigation (FBI)

Discussion Topic 1

Biometric Technology Characteristics

- What are some key benefits of biometrics over other authentication mechanisms (e.g., tokens, passwords, PINs)?
- What are some disadvantages and risks?

Discussion Topic 2

Large Scale Implementation

- What are some examples of large scale implementations of biometrics in a citizen registry or national ID scheme?
- What benefits do biometrics bring to these systems?
- How is the U.S. Government utilizing biometrics in large scale implementations?

Discussion Topic 3

Global Deployments

- Why do biometrics seem to be more widespread and accepted in developing countries in comparison to developed countries like the U.S. and in Europe?
- Do regulations and/or technical understanding play a role?
- Are there any examples of biometric deployments that cross national borders?

Discussion Topic 4

Privacy, Ethical and Cultural Implications

- What are some key privacy concerns related to biometrics and how should they be addressed by the industry?
- What are some best practices for privacy to keep in mind when deploying biometric solutions?
- What are some of the ethical and cultural concerns to keep in mind when deploying biometric solutions?

Discussion Topic 5

Data Security

- We hear stories about the fingerprint sensor in consumer devices like the iPhone being hacked within days of its announcement. Generally, how secure are biometric systems from hacker attack, and what steps should implementers consider in designing and deploying biometric systems to make them as secure as possible?
- What steps should users take to keep their data safe and secure?

Discussion Topic 6

System Implementation

- What are some of the standards, interfaces and regulations of which implementers of biometric systems need to be cognizant?
- What is the NIEM Biometrics domain?
- What is the relationship between the National Strategy for Trusted Identities in Cyberspace (NSTIC) and biometrics?

Discussion Topic 7

Identity Proofing and Enrollment

- What role can biometric technology play to enhance the integrity of the identity proofing and enrollment process?

Discussion Topic 8

Technology Trends: Mobile Commerce

- How does biometric technology fit in with the trend to mobile commerce (e.g., financial transactions performed from smart phones)?
- How does biometric technology enable or limit the adoption of mobile commerce?
- Can existing mobile biometric devices be leveraged for mobile commerce?

Discussion Topic 9

Technology Trends: Healthcare IT

- How does biometric technology fit in with the trend to migrate to electronic healthcare records (EHR) and the use of electronic health information exchanges (HIE)?
- What are the risks, if any, of utilizing biometric authentication with single sign-on access to patient data?

Discussion of Audience Questions

Questions from the audience

Wrap-up

Key Issues relating to Biometrics in Identity Management and Credentialing

Moderator: Brian Wong

- bwong@novetta.com
- Visit Booth 602