Biometrics Security

*And Biometrics*

Alice Sturgeon

Presentation to Biometrics Consortium Conference

September 24, 2003
Biometrics v Biometric security

- Biometrics
  - Identification and verification based on physical characteristics

- Biometrics security
  - System assurance and data protection
  - Authentication based on biometric identification and verification
Relative Nature of Authentication

Software-based
No pswd/PIN or policy control

Certified software-based
Policy control

Smart token
No PIN or policy control

Certified smart token
PIN control
No policy control

CC evaluated
Certified smart token
Policy control

LOW
Biometrics with no crypto token or No biometric

MEDIUM

HIGH
Encrypted biometric template

Authentication Continuum

© Copyright 1998-2003 SPYRUS Inc.
Security Risk Management

ISO/IEC WD 13335-2, Figure 2
Classical Approach to Security

Risk Management

Personnel

Audit

Information & Property

Physical

Contract

External Environmental Pressures

Corporate Culture
Biometric Security Standardization

- ISO/IEC JTC 1/SC 27 – IT Security techniques
- NP 19792 Framework for security evaluation and testing of biometric technology:
  - Biometric evaluation methodology (BEM): Framework for security evaluation and testing of biometrics technologies
- NP Biometric template protection

- ISO/IEC JTC 1/SC 37 – Biometrics

- ISO TC 68/SC 2 – Financial Systems Security:
  - NP 19092 – Biometric information management & security
Case Study: U.S. DoD CAC-Biometric Trials

- Proof of concept for adding biometrics to existing smart card capabilities for logical and physical access
- Three projects to date (CAC-A, CAC-B, CAC-C)
- CAC-C brought in X.509 PKI Attribute Certificates for carrying X9.84 encoded biometric templates
Alice Sturgeon

Manager of Standards, SPYRUS, Inc.

and

Chair, Canadian Advisory Committee to ISO/IEC SC 27 – IT Security Techniques

International Liaison Officer SC 27 to SC 37

Phone: (613) 232-2350
asturgeon@spyrus.com
www.spyrus.com