



CESG

The UK Government Biometrics Working Group

Update on Activities

Philip Statham, CESG

Aim - Enabling Biometric Authentication for Information Age Government

- Improving government awareness
 - Education
- Provide biometrics guidance on:
 - Standards, security, testing
 - Policy, legislation, privacy issues
 - Applications, implementation

Biometrics Working Group

- CESG
- Office of the e-Envoy
- UK Government departments
- UK National Physical Laboratory
- San Jose State University biometric test Center
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

Other Contributors

- British Telecommunications
- Germany –TeleTrusT
- USA – NSA, NIST, BMO/BFC
- Italy – CNR
- Japan – biometrics working group
- Netherlands – Home Office
- Canada – CSE, EWA
- IBIA, AfB

Deliverables

- Advice document – awareness of issues
- Testing best practices
- Protection profile
- Biometric evaluation methodology
- Biometric vulnerabilities
- Test programme report
- www.cesg.gov.uk/technology/biometrics

UK Govt. Biometric Projects

- Applications
 - Prison service: staff, contractor, visitor access
 - Asylum seekers: identity card & fingerprint system
 - Probation: offender monitoring
 - Newham: face recognition assisted CCTV surveillance
- Trials
 - Heathrow
- Under consideration
 - Entitlement cards
 - Biometrics on passports

Best Practice Testing – Why?

- Need for repeatable & objective methodology
 - Consistent results
 - Free from bias
- Results to be meaningful for
 - Current systems
 - Current applications
- Small(est) uncertainty for effort expended
- Limits of applicability understood

Best Practice Testing

- Input from leading testing organisations
- Version 1, 2000 (13 pages)
 - International review
 - Used in FVC2000, FRVT2000
- Referenced in X9.84
- Version 2.01, 2002 (32 pages)
 - Restructured
 - More advice
 - More on test size, uncertainties

Protection Profile 1

- Reference set of functional and assurance requirements for CC Evaluation
 - To meet customer requirements (e.g. govt.)
 - Provide a common target for developers
- History of Biometric PP
 - UK BWG draft - 2001
 - BMO developed PP from UK draft to meet US DoD requirements - 2002
 - Harmonisation activity now under way

Protection Profile - Harmonisation 1

- Why harmonise?
 - Remove confusion of similar but different requirements - benefit to customers and developers
 - Multinational, multi-government applications (e.g. NATO)
 - Mutual Recognition of Evaluation Certificates

Protection Profile - Harmonisation 2

- Principal difference between UK and US draft profiles
 - UK PP aimed at low-medium assurance
 - EAL 1 to EAL 4 - existing COTS products
 - BMO PP aimed at “medium robustness” environment
 - EAL 4+ - future COTS products?

Protection Profile - Harmonisation 3

- Detail differences
 - Additional function requirements in US PP
 - Template Encryption - FIPS 140-2 level 3 accreditation
 - Many additional cryptographic support functions
 - e.g. key generation, maintenance, destruction, cryptographic self-tests
 - Separation of Administrator functions
 - security administrator, enrolment administrator, audit administrator
 - Proprietary SFRs (i.e. not from CC library)
 - biometric authentication, enrolment, revocation, template life-span

Protection Profile - Harmonisation 4

- (Personal Views)
- UK will continue to monitor and input to BMO/DoD PP
- UK will recognise US DoD PP for higher assurance uses
- UK will seek to develop lower assurance evaluation standards for unclassified uses i.e. privacy sensitive applications
 - e.g. government services for the citizen

Biometric Evaluation Methodology

- To support Common Criteria Evaluations
- To promote mutual recognition
- Supplement to Common Evaluation Methodology (not a replacement)
- Addresses biometric specific aspects:
 - Interpretation of CC assurance components
 - Performance testing
 - Vulnerabilities
 - Strength of Function

BEM Working Group

- **International**
 - (Canada, Finland, Germany, Italy, Netherlands, UK, US)
- **Multi-community**
 - Government
 - Industry
 - Academe
 - Test organisations

BEM Timetable

- Inaugurate BEM WG – September 2001
- Draw together inventory of existing documents – Nov 2001
- Framework - February 2002
- Internal working drafts – April - July 2002
- First published draft – August 2002

Vulnerabilities

- Assessment methodology
 - In development
- Programme of investigation
 - Possibility of spoofing devices
- Impact on policy of use
 - Procedures to secure vulnerable devices
- Metrics for risk assessment models
 - Attacker potential - expertise, opportunity, time, etc.
 - Countermeasures - supervision, etc

BIOVISION: Mapping the Future of European Biometrics

- EU sponsored project
- Partners
 - Within BWG:
 - CESG, NPL, BT, CNR, TeleTrust & subcontractors
 - Additionally:
 - Daon, CWI, University Giessen Friedberg, Nationwide Building Society
- 1 year duration June 2002-May 2003

Key Objectives

- Roadmap for biometrics in Europe 2002-2010
- Specific studies:
 - User acceptability and perceptions
 - Security, application and personal viewpoint
 - Medical and safety issues
 - Legal and regulatory framework
- European Biometric Forum
 - Provide a European focus for industry, governments, users
 - Improve European contribution to world arena
- Outputs to be available for critical industry review

BIOVISION

- Roadmap for biometrics in Europe 2002-2010
 - Identify key application areas, current & future
 - Deal with geographic and sector fragmentation of biometrics work across Europe
 - Identify gaps in R&D and priorities for next EU research framework
 - European focus

European Biometric Forum

- To link biometric organisations, customers, end- users, industry, media, universities, ...
- To share knowledge and remove the fragmentation of effort that exists at present
- To maintain the European biometrics roadmap
- Centre of information on:
 - technologies
 - applications
 - user concerns
 - legal framework

BWG – the Future

- Centre of excellence for UK Government
- Broaden area of work
 - Requirements & procurement
 - Privacy & legislation
 - Education & Communication
 - Continue to address security issues
- Work more closely with industry bodies
- Maintain and expand international cooperation



Questions?

- www.cesg.gov.uk/technology/biometrics
- Philip.statham@cesg.gsi.gov.uk