
Communications-Electronics Security Group

FIPS 140 Evaluations for UK Government

David Simpson - CESG

CMVP Conference - March 2002

CESG

What is CESG?

- The Communications-Electronics Security Group (CESG) is the Infosec arm of the Government Communications Headquarters (GCHQ)
- UK's national technical authority for information security/assurance
- Provides policy and guidance; solutions and services
- Has strong partnerships with industry

CESG

Infosec Cryptography Group

- Sets cryptographic policy
- Designs and evaluates algorithms
- Evaluates cryptographic products
- Three grades:
  - Baseline (RESTRICTED)
  - Enhanced (CONFIDENTIAL)
  - High (SECRET/TOP SECRET)

CESG

E-Government

- Office of the e-Envoy (www.e-envoy.gov.uk)
  - aim is to make all UK government services available electronically by 2005
  - services to business (G2B) and citizen (G2C)
  - Security Framework (refers to FIPS 140)
- New marking - UNCLASSIFIED PRIVATE
  - will replace much of RESTRICTED
  - …. but data needs protection (hackers, legal duties)
- Baseline standard is not appropriate

CCSG

Use of FIPS 140

- Well-established standard - no others
- Well-documented and managed
- Use as a basis for evaluations for UNCLASSIFIED PRIVATE
- Define levels
- Define extra lab work
- No CESG involvement in evaluations
- Have policy approved in June 2002?

CESG

The Future

- Logica has applied for lab accreditation
- Evaluations by North American labs will, of course, be accepted
- Set up new CESG scheme
  - low cost
  - fast
  - advertised on www.cesg.gov.uk
- Extend FIPS 140 into Europe

CESG


Communications-Electronics Security Group