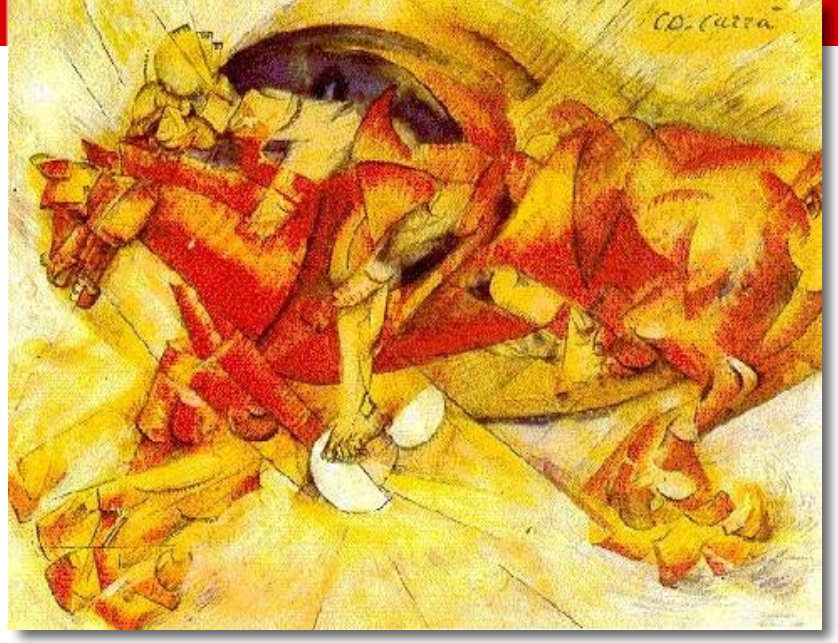
the information security provider



FIPS 201-2 Product Approval Expectations:

Draft FIPS 201-2 Workshop 2011-04-08

Auston Holt, CISSP
atsec information security,
GSA FIPS 201 Evaluation Program Approved Laboratory

Programs

Government Agencies Involved

- ➔ PIV
  1. GSA FIPS 201 Evaluation Program
  2. NIST PIV Validation Program (NPIVP)

- ➔ Cryptographic Module
  3. Cryptographic Module Validation Program (CMVP)
  4. Cryptographic Algorithm Validation Program (CAVP)

■ ■ ■

Programs

Government Agencies Involved (cont.)

- ➔ Biometrics and Path Discovery and Validation (PD-VAL)

5. FBI‘s Integrated Automated Fingerprint Identification System (IAFIS)
6. NIST Minutiae Interoperability Exchange Test Program (MINEX)
7. Federal Public Key Infrastructure (FPKI) Policy Authority- (certificate validator products)

End Game

What Draft FIPS 201-2 changes affect final approval

- ➔ GSA FIPS 201 Evaluation Program (EP)
  - New product approval procedures possible
    - Biometric comparison (on-card)
    - Iris Capture Station
    - PIV interoperability profile ISO/IEC 2427 in [SP 800-73]

- ➔ NIST PIV Validation Program (NPIVP)
  - Updated testing tool and derived testing requirements
    - New PIV card application data objects
    - New PIV middleware API features

End Game (cont.)

What FIPS 201-2 changes affect final approval

- ➔ Cryptographic Module Validation Program (CMVP)
  - Increased scope of cryptographic module validation testing
- ➔ Cryptographic Algorithm Validation Program (CAVP)
  - No foreseen change

End Game (cont.)

What FIPS 201-2 changes affect final approval

- ➔ FBI‘s IAFIS certification and MINEX
  - Unclear

- ➔ Iris Exchange (IREX)
  - Possible introduction of IREX testing requirements for new iris GSA FIPS 201 EP product categories (similar to MINEX)

Thank You, Resources

Resources

- ➔ Auston Holt,
  Deputy GSA FIPS 201 EP Laboratory Manager
  - holt@atsec.com, +1-512-615-7392

- ➔ NPIVP and GSA FIPS 201 **EP**
  Testing and consulting
  - FAQ, RFI, …http://www.atsec.com/us/gsa-fips-201-resources.html
  - Vendor test data report; http://www.atsec.com/us/vendor-test-report.html

Thank You, Resources

Resources (cont.)

- ➔ **FIPS 140-2 Testing and Consulting**
  - FAQ, RFI, ... http://www.atsec.com/us/fips-140-2-resources.html
  - FIPS 140-2 Training Presentation for Project Managers and Developers http://www.atsec.com/us/presentations/fips140-2.html

- ➔ **Cryptographic Algorithm Testing**
  - FAQ, CST contact, ... http://www.atsec.com/us/cryptographic-algorithm-testing-lab-resources.html

Thank You, Resources

Resources (cont.)

- GSA FIPS 201 EP
  http://fips201ep.cio.gov
- NPIVP
  http://csrc.nist.gov/groups/SNS/piv/npivp/index.html
- CMVP
  http://csrc.nist.gov/groups/STM/cmvp/index.html
- CAVP
  http://csrc.nist.gov/groups/STM/cavp/index.html
- FBI (IAFIS certification)
  http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_cert
- MINEX
  http://www.nist.gov/itl/iad/ig/minex.cfm
- IREX
  http://www.nist.gov/itl/iad/ig/irex.cfm
- FPKI Policy Authority
  http://www.idmanagement.gov/fpkima/