How to Achieve "Rapid Electronic Authentication"

Kevin Kozlowski
Vice President, Government Initiatives
XTec Incorporated

Technical Ramifications of 800-116

- XTec has been a leader in Smart Card Physical Access Control for over 15 years,
- We understand the technology as well as the challenges surrounding the technology.
- We also understand that interoperability is not a new concept nor is it a reach in our current environment. Interoperability was achieved a long time ago through the GSC-IS standards.
- What you will see here is The Interagency Interoperability Task Force's Demonstration on Smart Card Interoperability for Physical Access Control which took place back in 2003.
- See Video

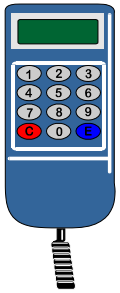
Technical Ramifications of 800-116

- As you can see, The question is not whether or not interoperability can be achieved.
- The Question is….

How do we make interoperability secure with “rapid authentication”?

- In the Physical Access World we all know that if transaction time is longer than 2 seconds people will find the reason to not use authentication thus making for a less secure system.

Authentication Factors



- Authentication is accomplished by verifying one or more factors:
  - Objects that can be presented: tokens , cards etc.
  - Secret items that are known: passwords, PINs etc.
  - Personal characteristics: biometrics, portrait, etc
- Simply establishing that an ID Number or Credential is valid is not authentication, especially in the case of published data such as PKI certificates.

Technical Ramifications of 800-116

- Lets take a look at another production environment. Which shows true interoperability with “rapid authentication”.

- GSA Region 1 has set up the Physical Security Infrastructure so as to allow the use of PIV II cards to be used for access to the building.

Technical Ramifications of 800-116

- The GSA identification cards issued nationwide starting in 2004 and the GSA Region 1 Access Control System, supported high assurance profile utilizing symmetric keys and has been in use since the summer of 2006.

Technical Ramifications of 800-116

- For the user to gain access to a control point (turnstile, door, elevator floor, etc) the card must have the proper authentication key (in the 9E container as specified in FIPS 201) as well as an active permission for that reader on the PACS system.

- If the card cannot be authenticated the user will get an authentication failed or access denied indication.

- Presently GSA Region 1 has tenants with PIV cards issued by the Department of State, Department of Labor, and the Peace Corps that meet the criteria.

PIV Authentication Factors

Independent Authentication Factors

X.509 Certificate for PIV Card Authentication 5FC101 – Optional	Key 9E PKI	Key 9E Symmetric
PIV Authentication Certificate X.509 Certificate for PIV Authentication 5FC105 - Mandatory	Key 9A PKI	
X.509 Certificate for Digital Signature 5FC10A – Optional	Key 9C PKI	
X.509 Certificate for Key Management Escrow ? - 5FC10B – Optional	Key 9D PKI	

Something I Have which is capable of being authenticated by itself

Dependent Authentication Factors

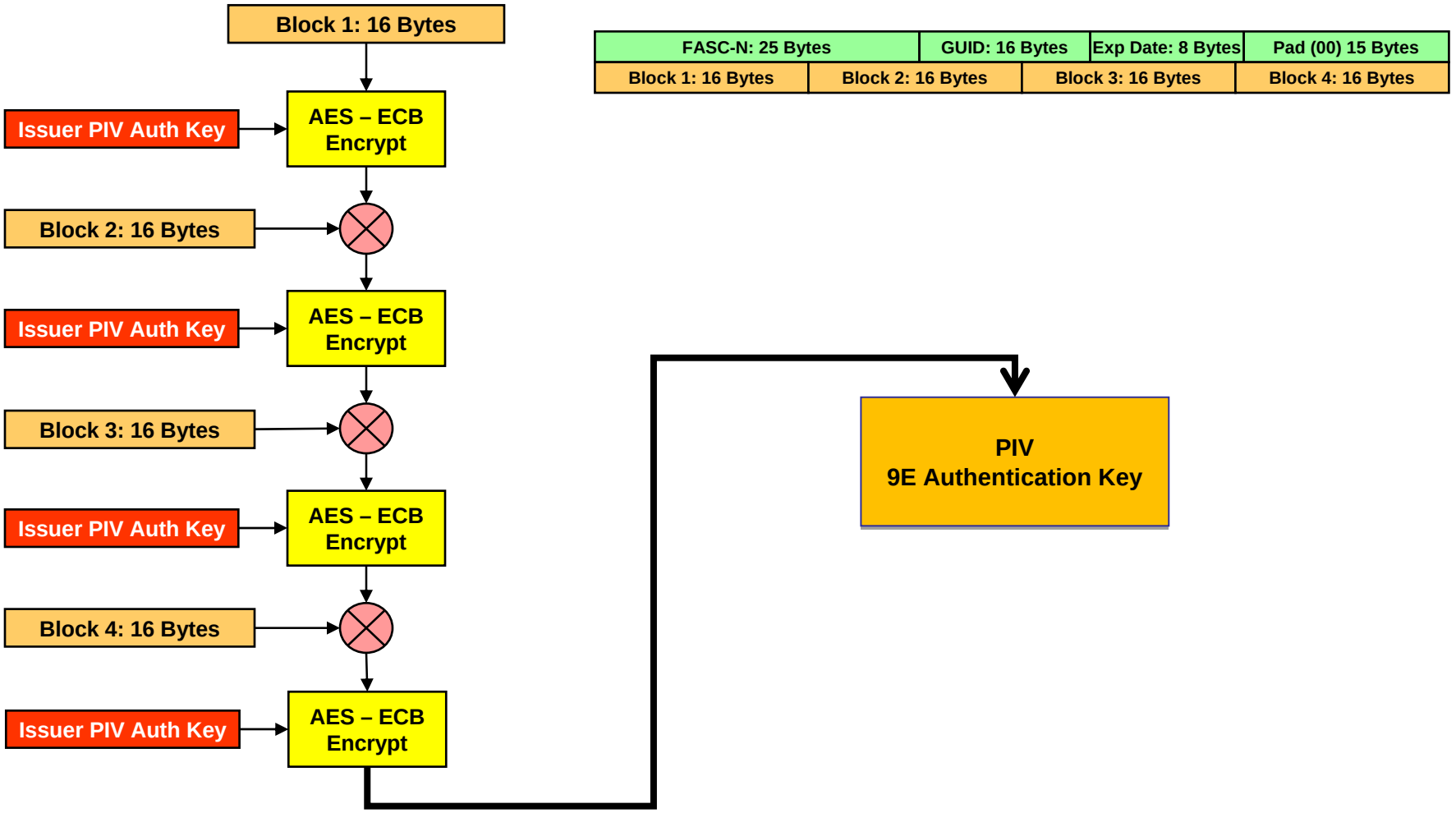
- User PIN
  PIN
  Special Command
- Card Holder Fingerprints
  CBEFF + Signed Data Object
  5FC103 - Mandatory
- Card Holder Facial Image (Portrait)
  CBEFF + Signed Data Object
  5FC108 – Optional

Something I Know or Something I am which is reliant on another factor

- Using a PKI cert and asymmetric key for the card authentication 9E key is redundant since that function can already be accomplished better with the mandatory PIV Authentication Certificate, and asymmetric 9A key.

- In August 2004 HSPD-12 called for:
  - 3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; **(b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically**; and (d) is issued only by providers whose reliability has been established by an official accreditation process.
- Excerpt from HSPD-12 by George W. Bush August 27, 2004

PIV Authentication Key Generation



Conclusion

- XTec proposes that the 9E key be symmetric and mandatory in following the PAIIWG TIG 2.3 guidelines which allow for card and data authentication in a single transaction.

- This proposal is a proven method to allow the standards to meet the "rapidly authenticated electronically" aspect of the presidential directive

XTec Incorporated

Corporate Offices

5775 Blue Lagoon Drive, Suite 280

Miami, Florida 33126

Tel: (305) 265-1565 Fax: (305) 265-1569

Government Division

11400 Commerce Park Drive, Suite 210

Reston, Virginia 20191

Tel: (703) 547-3524 Fax: (703) 547-3533

www.xtec.com

E-Mail info@xtec.com

Kevin Kozlowski

Vice President Government Initiatives

703-547-3524

Kkozlowski@xtec.com

Tom Murphy

Director of Sales

703-547-3528

Tmurphy@xtec.com