

Public Key Technology FDIC Case Study

Russ Davis

December 13, 2000

What's the Assurance?

- Planning a GAO sanctioning effort.
- Coordinating closely with our Office of Inspector General.
- Negotiating an Inter Agency Agreement with the National Institute of Standards & Technology (NIST).
- Knowledgeable support contractors:
 - CygnaCom Solutions/Entrust
 - IMSI
- We are open to peer review.

FDIC PKI Overview

- The FDIC Core PKI uses a dual certificate implementation.
 - Electronic Travel Voucher (ETV).
- For the Extranet, a single certificate PKI is used.
 - Outlook Web Access.
 - Secure Web Connection.

Current Core PKI

- Software Moderate Assurance based COTS.
- Select users have smart cards combined with their picture ID.
- All travelers must use the ETV work flow application.
 - No paper.
 - Payments within 48 hours.
- Over 7,000 users.

Key Recovery

- The Core PKI includes an encryption key recovery capability.
- If a user forgets his or her password, the encryption key is recovered.
- In contrast, a password reset necessitates the generation of a new signature key pair.

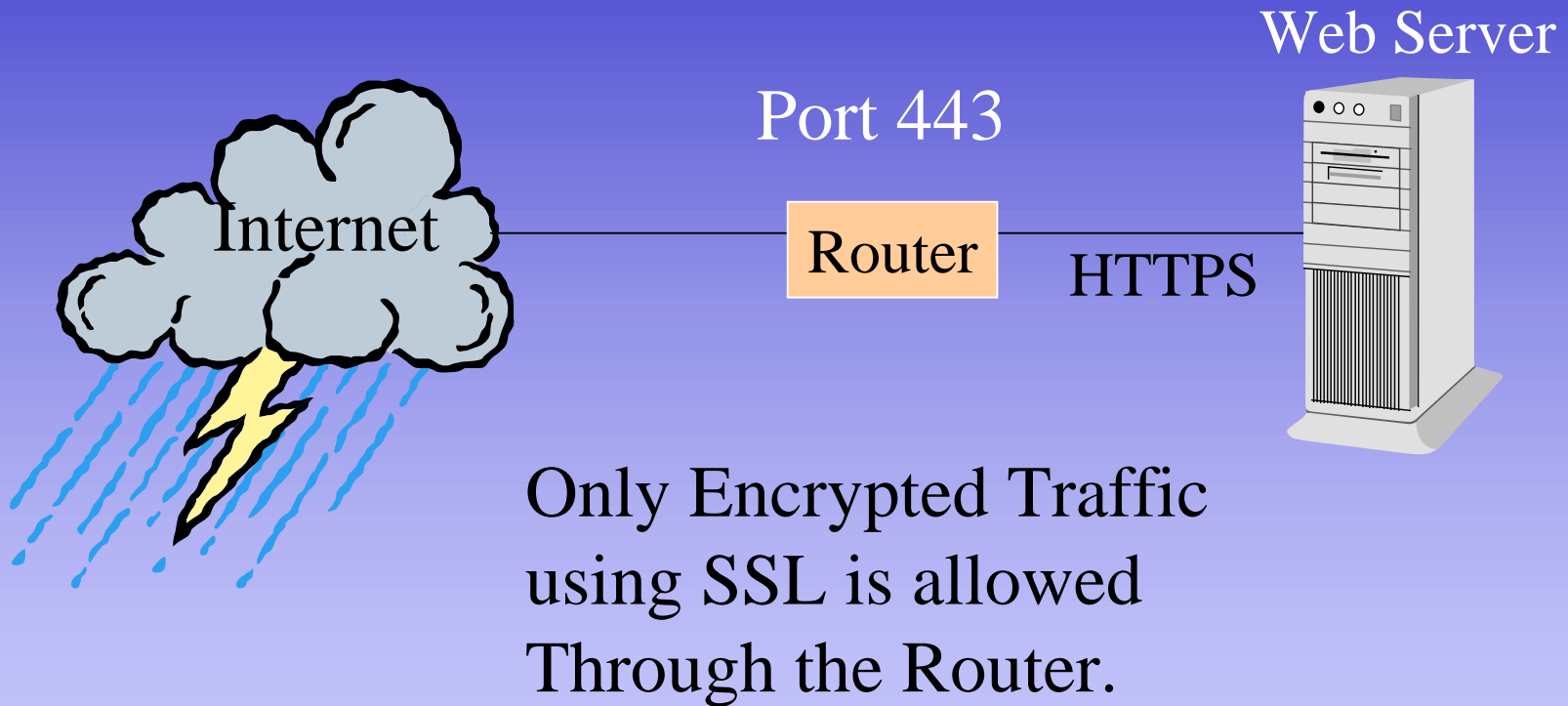
Target Core PKI

- Hardware based cryptography
 - CA (Level 4)
 - RA (Level 2 - 4)
 - User (Level 2)
- Secure email (S/MIME)

Current Extranet PKI

- External users issued certificates.
- Two way authenticated SSL.
 - User to the server.
 - Server to the user.
- All Web centric.
- Approximately 2,000 users (600 are actively using the PKI).
- An additional 460 are using Outlook Web Access

Using Layered Security



Target Extranet PKI

- Ease in certificate issuance.
- Secure email uses.
- IP Security Virtual Private Networks.
- Cross-Certification with Core PKI.
- Bridge CA Interface.

Smart Card Technology

- Signature Key generated on the card.
- Private key never leaves the card.
- Signatures possible only using the smart card.
- After 10 successive failed log on attempts, the smart card locks and new signature keys must be generated.
- Can be combined with photo ID.
- Coordinated with physical security office.
- Interfaces to Windows 2000.

CA Hardware Crypto Device

- Support for n of m control (dual control and split knowledge).
- Provides tamper protection.
- Includes an ability to backup keys.
- Standards based.
- Validated Crypto module.

Secure Mail

- Provides ability to sign email.
- Uses a push approach.
- Works through existing firewalls.
- Provides ability to encrypt email and attachments.
- Standards based.
- Client based security.

Common Crypto Interface

- High Level Interface.
- Removes developers from algorithm specifics.
- Will be examined by the NIST.
- Core to the GAO sanctioning effort.
- May promulgate a NIST standard.

<http://csrc.nist.gov/pki/pkiapi/welcome.htm>

Help Desk

- Personnel were trained on the PKI.
- During ETV roll-out, additional resources were needed.
- Personnel not exclusive to PKI support.

Training

- Training aids and instructions were developed and distributed.
- A train the trainer session was given to the Information Security Officers.
- A road show used to train on-site personnel.
- Internal Web page provides additional information.

Summary

- Several topics have been quickly discussed. If you'd like to contact me, please call me at (703) 516-5107 or email at RDavis@FDIC.Gov.
- Questions?