

WIC EBT SECURITY CONCERNS

RISKS TO COMMON KEYS

RISKS TO WIC EBT

POSSIBLE CHANGES TO WIC EBT - SMARTCARDS

Mike Neal

Booz Allen Hamilton

RISKS TO COMMON KEYS – WHAT DO THEY MEAN?

Risk Name	What it is	Example
Decipherment	Discovering private key by using millions of values to derive public key	Attacker has public key, makes assumption on hash algorithm and length to create the same public key.
Bypass	Tricking equipment so it does not use correct keys or does not use PKI function	Yes Card attack – counterfeit card says yes to cryptogram sent by terminal
Capture	Reveals PIN in the clear	Fake terminal does not encrypt result of PIN entry

RISKS TO COMMON KEYS – WHAT DO THEY MEAN?

Risk Name	What it is	Example
Certificate Authority (CA) Breach	Attackers get private keys from CA	Feb 2 2012 attack on VeriSign Mar 18 2011 attack on RSA
Counterfeits	Card with copied certificate and programmed to convince terminal it is legitimate	Yes Card Attack (Entire transaction must take place off-line)
On-going cycle of innovations in attacks and defense	An attack on a card prompts development of a defense by issuers. The new defenses becomes the platform for new attacks.	Chip and PIN needed to evolve from SDA to DDA to CDA because attackers determined new methods for new defenses

WIC EBT AND WIC STATE AGENCIES *LESS VULNERABLE TO ATTACK*

- **Current Practices Evolved from Existing Secure Retail Payment Systems**
- **Risk vs. Reward – Much bigger targets out there**
- **Limited Number of Private Keys**

Greatest Risk – Complacency Leading to Poor Key Management

POSSIBLE CHANGES TO WIC EBT DUE TO EMV

If Decision is made to use PKI and other EMV solutions then:

- Make a list of the Key Holders, Key Location and the Revocation Dates
- Build Requirements to Create (Generate) Keys
- Build Requirements to Cancel (Revoke) Keys
- Build Requirements for the Certificate Authority
- Build Requirements for Transition
- Test the Process Before Implementation
- Build Consensus with Stakeholders

POSSIBLE CHANGES TO WIC EBT DUE TO EMV

- Software Upgrades to Clinic/Retailer Terminals
- Possible Hardware Changes Depending on Solution and Existing Hardware
- Monitoring Function for Private and Public Keys
- Possible New Certification Testing Scenarios – Such as Key Generation and Distribution Process Testing
- Knowledge to Generate, Distribute, and Revoke Keys