the Payment People

Identity: Technology and Policy Issues of Trust Contact Smart Cards

John Sheets
Director, Product Security, VeriFone
Chair, ANSI X9F6, Cardholder Authentication & ICCs
US Expert, ISO TC68/SC6/WG6

Agenda

- **Smart Card Payment Security**
- **Smart Card Security Standards Status**
- **Influencing Security Standards**

Agenda

- **Smart Card Payment Security**
- *Smart Card Security Standards Status*
- *Influencing Security Standards*

Smart Card Payment Security

- **Contact Smart Cards Issues**
  - PIN Protection at POS
    - Avoiding compromise of PIN during (lengthy) period of mag/smart hybrid cards
    - Use trusted PED
  - PIN Protection for Open Network Transactions
    - Trusted PED not economically feasible
    - Threat is remote, not local
    - Focus on card data protection rather than PIN

Smart Card PIN Protection – POS

- **PIN at Risk**
  - EMV allows for cleartext PINs (lower cost cards)
  - PIN for smart card same as PIN for magstripe on back of card
  - Compromise of PIN in smart card reader could lead to losses in magstripe ATMs
  - Smart card PEDs must be authenticateable by transaction acquirer
    - Authentication must fail if PED is tampered with

Smart Card PIN Protection – Open Network Transactions

- **Assumption: use model is smart card enabled (non-secure) PC, PDA, or mobile phone**
  - Untrusted
  - Computing environment subject to attack/virus/worms
  - PIN not (adequately) protectable
- **Paradigm shift**
  - Protect card data, not PIN
  - Smart card only; no magstripe cards
  - Smart card never emits sufficient data to create useable magstripe card

Agenda

- *Smart Card Payment Security*
- **Smart Card Security Standards Status**
- *Influencing Security Standards*

Security Standards Status

Standard	Status
ISO 9564-1-2002 *Online PIN handling*	**Approved June 2002 (not yet published)**
ISO DIS 9564-2 *PIN encryption algorithms*	**Draft to add 3DES & RSA (offline) – target release 2003**
ISO FDIS 9564-3 *Offline (ICC) PIN handling*	**In final draft – target release 2003**
ISO DTR 9564-4 *PIN handing in Open Networks*	**In draft form – target release late 2003**

Security Standards Status

Standard	Status
ISO 9564-1-2002 *Online PIN handling*	Approved June 2002 (not yet published)
ISO DIS 9564-2 *PIN encryption algorithms*	**Draft to add 3DES & RSA (offline) – target release 2003**
ISO FDIS 9564-3 *Offline (ICC) PIN handling*	In final draft – target release 2003
ISO DTR 9564-4 *PIN handing in Open Networks*	In draft form – target release late 2003

Security Standards Status

Standard	Status
ISO 9564-1-2002 *Online PIN handling*	Approved June 2002 (not yet published)
ISO DIS 9564-2 *PIN encryption algorithms*	Draft to add 3DES & RSA (offline) – target release 2003
ISO FDIS 9564-3 *Offline (ICC) PIN handling*	**In final draft – target release 2003**
ISO DTR 9564-4 *PIN handing in Open Networks*	In draft form – target release late 2003

Security Standards Status

Standard	Status
ISO 9564-1-2002 *Online PIN handling*	Approved June 2002 (not yet published)
ISO DIS 9564-2 *PIN encryption algorithms*	Draft to add 3DES & RSA (offline) – target release 2003
ISO FDIS 9564-3 *Offline (ICC) PIN handling*	In final draft – target release 2003
ISO DTR 9564-4 *PIN handing in Open Networks*	**In draft form – target release late 2003**

Agenda

- *Smart Card Payment Security*
- *Smart Card Security Standards Status*
- Influencing Security Standards

Join ANSI X9!

- **We take direction from our Members!**
- **Become a member, and tell us what is important to you**
- **http://www.x9.org/members.html**
- **Next X9F6 Working Group meeting:**
  - When: March 4-7
  - Where: Foster City, CA
  - Contact: john_s@verifone.com