Bankcard Compliance Group

PIN Security & Key Management

TR-39 / PCI PIN

2015

peter@bankcardcompliance.com 518-792-7320

BANKCARD
COMPLIANCE GROUP

What is the TR-39?

- ANSI Technical Release – 39
  - Originally developed in late 1990's, fka TG-3
- Secure administration and distribution of cryptographic keys used for PIN debit
- Secure PIN Transmission and Processing
- Method of Validation of compliance
  - Industry Standard
  - Biennial Review

BANKCARD
COMPLIANCE GROUP

What is the TR-39?

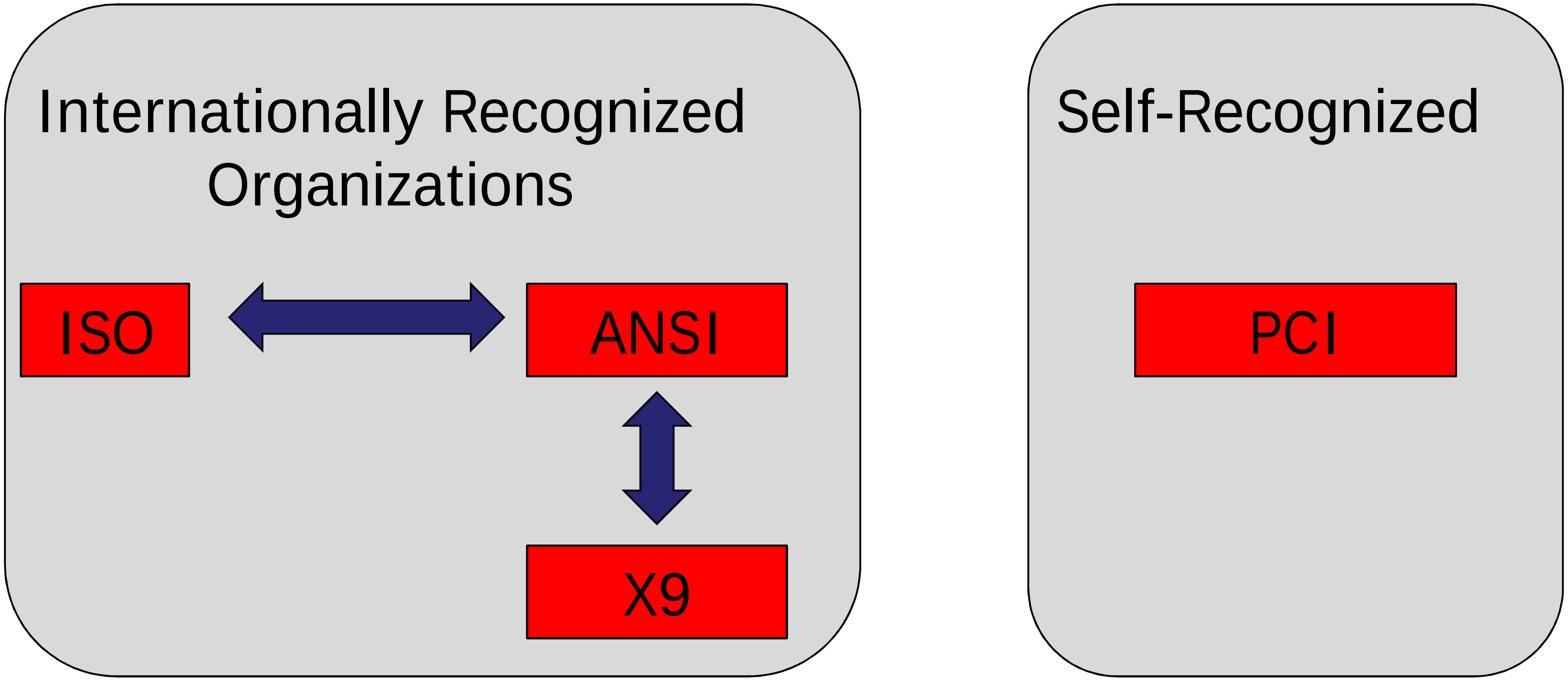
- Policies and practices dealing with keys, keying material, hardware, and software
  - 40 Control Requirements Sec. IV
  - 50 Control Requirements Sec. V
- Developed by X9 Stds Committee
  - Closely related to ISO 9564, 11568, and 13491, Global Standards

BANKCARD
COMPLIANCE GROUP

What is the PCI PIN?

- PCI PIN Version 1.0 created 09/2011
- Originally developed internally by VISA
- PCI PIN Version 2.0 released 12/2014
  - 33 Control Requirements

Control Organizations


Internationally Recognized Organizations

ISO

ANSI

X9

Self-Recognized

PCI

What do they address?

- Policies and practices dealing with keys, keying material, hardware, and software
  - Physical
  - Administrative
  - Technical

BANKCARD COMPLIANCE GROUP

What are we protecting?

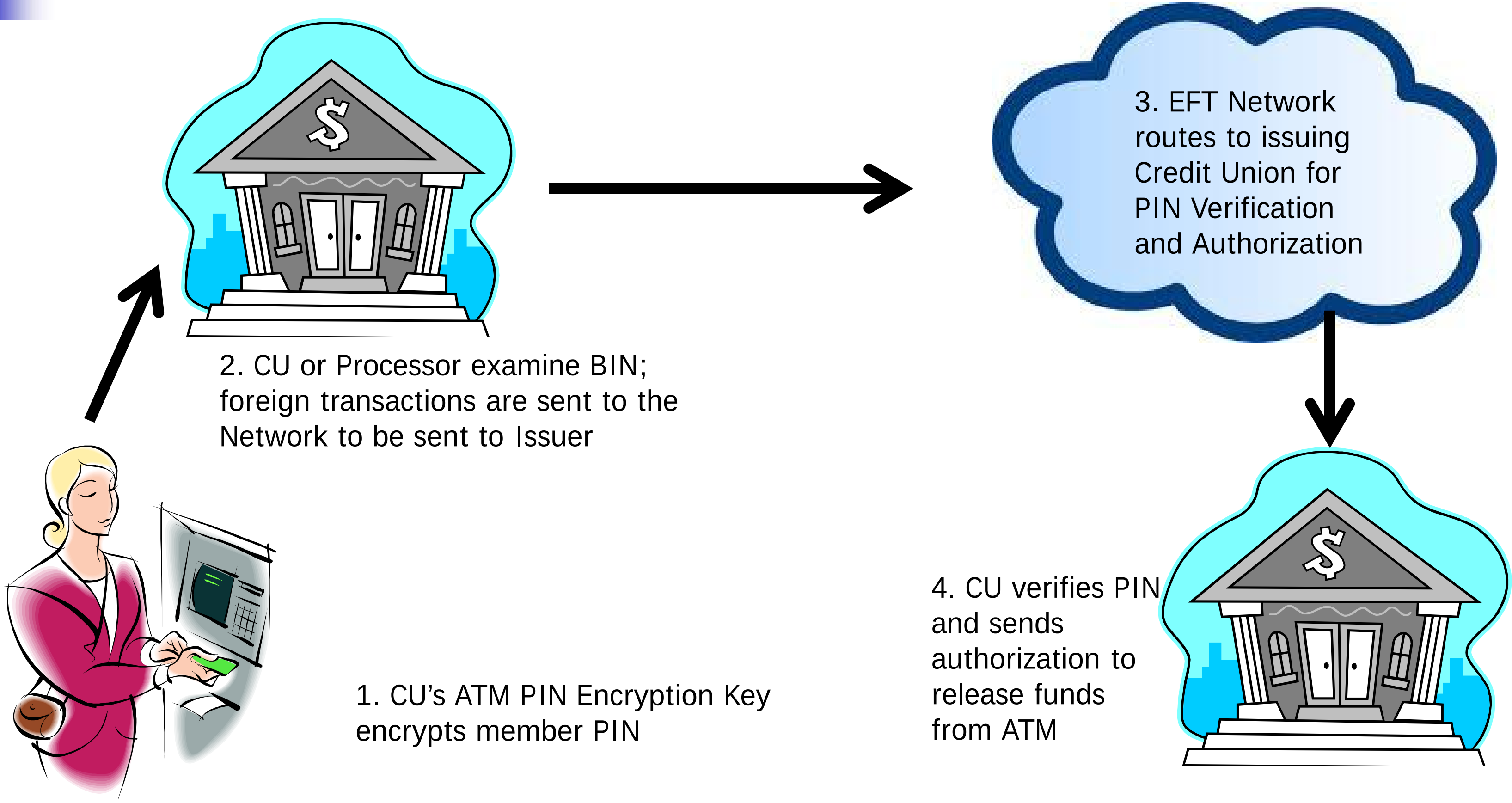
- PIN Encryption Keys
  - A052 BFD8 155E 0AA9 19AC 6DBF EABA 0CD1
- 32 Hexadecimal Characters
- Protects PIN from entry to issuing FI authorization

What are we protecting?

Key Component #1
32 Hexadecimal

Key Component #2
32 Hexadecimal

How does the ATM work?



1. CU's ATM PIN Encryption Key encrypts member PIN

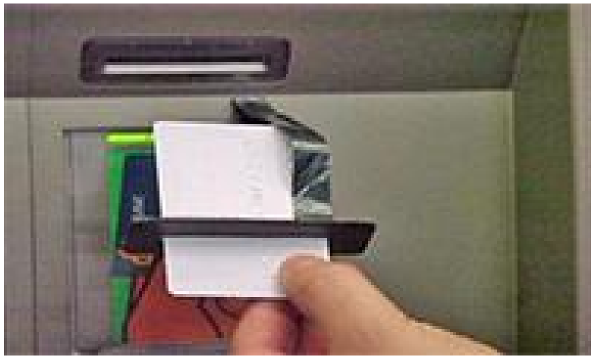
2. CU or Processor examine BIN; foreign transactions are sent to the Network to be sent to Issuer

3. EFT Network routes to issuing Credit Union for PIN Verification and Authorization

4. CU verifies PIN and sends authorization to release funds from ATM

What are the attacks?

- Card and Currency
  - Skimming
  - Card Trapping
  - Currency Trapping
  - Dummy ATM’s
  - Shoulder Surfing
  - Malware



What are the attacks?

- Logical/Data
  - Key compromise
  - Network
  - OS
  - IVR PIN resets
- Physical
  - Smash and Grab

What are the controls?

- Physical
  - Focus on Equipment
    - ATM
    - Encrypting PIN Pad (EPP)
    - Host Processing System (HSM)
    - Safes for Clear Text Key Components

BANKCARD
COMPLIANCE GROUP

What are the controls?

- Administrative
  - Focus on Documentation and Personnel
    - Policy
    - Procedures
    - Activity Logging
    - Personnel Training

What are the controls?

- Technical
  - Focus on Key Life Cycle
    - Key Generation
    - Key Storage
    - Key Transport
    - Key Loading
    - Key Destruction

Who must complete?

- Depends:
  - NCUA CFR 748- obligation to protect the security and confidentiality of the PIN – requires documented and implemented procedures to protect
  - Your PIN Debit Network requirements – see charts
    - Most processing acquirers must submit biennial report to networks
    - Most Non processing acquirers must complete biennial report
      - Must meet required controls
      - Be able to demonstrate compliance
- Credit Unions which acquire and/or process PIN's should complete a PIN Security Review

Who must complete?

Network	PIN Transactions Performed	Submit TR-39 to Network	Complete TR-39, keep on file	Complete PCI PIN V 2.0, keep on file
STAR NYCE PULSE	Acquire and Process PINS	🟥		
STAR NYCE PULSE	Acquire PINS		🟥	
CO-OP	Acquire and Process PINS	🟥		
ACCEL	Acquire OR Process PINS		🟥	
VISA MasterCard	Acquire OR Process PINS			🟥

Note about PCI PIN

- VISA updated its requirements
- All Acquirers must be able to demonstrate compliance
- Enforcement Plan Announced in 2015
- VISA now taking all cybersecurity very seriously

BANKCARD
COMPLIANCE GROUP

Benefits?

- Comply with NCUA CFR 748
- Comply with your network contract
- Reduce risk of debit compromise
  - Financial loss to member
  - Financial loss to Credit Union
  - Reputational loss to Credit Union
  - Liability to 3rd party network members

Benefits?

- TR-39 Specific to PIN encryption but provides a “gut check” for other critical functions
  - Thoroughness of Procedures
  - Information Security Stance
  - Segregation of Duties
  - Activity Logging/Tracking
- Exposure to Best Practices

Who performs review?

- Qualified Internal or External Auditors
- Most networks require processing entities to use a certified TR-39 auditor
- Non-processing entities must attest that the person completing the review is:
  - Independent from operations being reviewed
  - Knowledgeable of encryption controls
  - Knowledgeable of audit techniques

Who performs review?

- Due to complexity of subject matter, the leading EFT networks created certification for auditors - CTGA
- Aim to avoid the “check the box” routine

How are they done?

- Onsite Field Audit:
  - Device Inventory/Inspection
  - Policy & Procedure Review and Update (as necessary)
  - PIN Flow Diagram
  - Key Methodologies
  - Key Lengths
  - PIN Block Formats
  - Third Parties
  - Working Paper Forms
  - Preliminary Findings / Action Plan

BANKCARD
COMPLIANCE GROUP

How are they done?

- Offsite TR-39 Report Completion
- Review of Deliverable w/ Management
- Sign off by Officer
- Auditor Attestation and 3rd party Submission of TR-39 (if required)
    - Network
    - Approved 3rd party requesters (clients)

How long does it take?

- Usually 1 Day Site visit -
  - Locations
  - Cryptographic keys and key components maintained
  - Key life cycle functions
  - Hardware
  - Software
  - Policy/Procedures

Common Findings

- Lack of documented procedures
- Insecure storage of comvelopes/keys
- Allowing ATM tech to load both key parts
- Failure to log key life cycle events
- “Check the Box” prior TR-39 with erroneous responses

Best Practices

- Frequent ATM inspection
- Collect TR-39 from all affiliates
- Strengthen your IVR PIN reset
- Document Procedures, log events
- Recognize the impact of compromise and train staff to reduce risk
  - Risk = Probability X Impact

ATM Compliance Issues

- March 2012 – ADA Compliance
- April 2014 – new or moved requires a PCI V. 3.0 EPP
- April 2014 – Migration from XP to Win 7
- October 2016 – Liability shift for Mastercard
- October 2017 – Liability shift for VISA

A Note about EMV

- US ATM’s will continue to use online PIN Verification
- With or without chip card, PIN will be entered via EPP
    - Skimming risk continues

BANKCARD
COMPLIANCE GROUP

Thank you!

For more information:

Peter@BankcardCompliance.com