North America Community Meeting 2023

PCI Security Standards Council

PCI Security Standards Council

Migration to AES Protected Payments:

Current Support and Ongoing Work to Aid Adoption

Presenters

Richard Kisley,
Chief Engineer, HSM
IBM Corporation

Dr. Susan Langford,
Senior Cryptographer,
Utimaco Inc

Steven Bowles,
Regional Security Officer,
NAR, Ingenico, Inc.

PCI Security Standards Council

Advanced Encryption Standard (AES)

- Symmetric-key block cipher algorithm designed to supersede the Data Encryption Standard (DES)
- Submitted as Rijndael to NIST AES competition in 1997 by Joan Daemen & Vincent Rijmen; chosen in 2000
- Adopted as ‘the AES’ by NIST in 2001 (FIPS 197) & ISO in 2005 (ISO.IEC 18033-3)
- AES fixes the Rijndael block length to 128 bits and fixes key sizes to 128, 192, and 256 bits
- Trusted globally now for symmetric key encryption

Agenda

The current state of AES support in Payments

- What are the requirements & mandates?
- What progress has been made?

Ongoing AES work in standards

- What tools can you use today and what is missing?
- What do the new standards mean to your system?

Planning your AES migration

- What should you start doing today?
- What is decisions need to be made?

PCI Security Standards Council

PCI Security Standards Council

Current State

Requirements & Implementation Progress

PCI Mention of AES

Moves by Standards & Requirements Bodies

PCI PTS

- HSM v3 (2016) – HSM v4 12/2021
  - AES required for online PIN translation
- POI v3 (2016) – POI v6.2 1/2023
  - (B11) AES PIN encryption with DUKPT or M/S must be supported

Note: Support of AES operational keys requires AES device MK/MFKs, AES Key Encrypting Keys, etc.

PCI PIN

- PIN v3.0 8/2018
  - AES sunrise: 1/1/2023
  - TDES fixed key sunset 1/1/2023
- PIN v3.1 3/2021
  - AES sunrise ‘must have support’ dates suspended
  - TDEA fixed key sunset 1/1/2023

Note: not compliant(!)

- Encryption of AES keys with TDES keys
- Encryption of AES-192/AES-256-bit keys with RSA-2048
- Just don’t do this

PCI Security Standards Council

Other Organizations

Specific View of Moves by Standards & Requirements Bodies

EMVCo

- ~Complete with 3/2023 update for contact/contactless for AES, ECC

Payment brands (public info)

- No public requirement for AES
- No public sunset of TDES

NIST dates

- 2 key TDEA encryption disallowed after 12/31/2015 (SP800-131Ar1)
- 3 key TDEA encryption disallowed after 12/31/2023 (SP800-131Ar2)

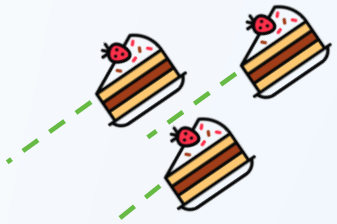
AusPayNet

- ATMs are critical infrastructure
- Sunrise AES 2026
- Sunset TDES ~2030

Why Move?

Other Takes

Cryptography



- TDES
  - 3key: 168 → 112 bits: birthday attack
    - Web search ‘sweet32’
  - 2key: 80 bits: chosen-plaintext, known plaintext attacks
  - 1key: broken in July 1997
  - Small block size: 220 64-bit blocks limit per key
- AES
  - Faster, more secure

Legal

- Sep 1998: German court
  - Called DES for EC bank cards “out of date and not safe enough”,
  - Ordered a bank to repay a customer’s stolen funds

Takeaway: consider 7/1997 - 9/1998

- When the crypto is broken, the speed of liability may be faster than you expect

Implementation Progress

An Informal Poll

- **Device cycle only**
- + Industry association
- + Government
- + Project well underway

PCI Security Standards Council

Implementation Progress

An Informal Poll: Part 1

Availability?

- **CA:** AES hardware is available, pay schemes must drive
- **FR:** Switching has migrated, POI started
- **DE:** ATM auth uses AES, other parts →2031
- **AU:** Pay schemes driving key block, APN driving host/POI move
- **CN:** SM4 widely used, AES available, TDES in legacy with no sunset
- **BE/LU/NL:** C-TAP upgrading now to AES

Regulatory?

- **CA:** No reg/gov drivers
- **FR:** CB driving.
- **DE:** BSI only recommends AES now
- **AU:** APN backed by gov
- **CN:** OSCCA (National Crypto. Admin.) driving
- **BE/LU/NL:** No reg/gov drivers, some industry pressure

Implementation Progress

An Informal Poll: Part 2

Timeline?

- **CA:** Depends on pay schemes
- **FR & NL:** Local is ~following initial PCI dates
- **DE:** Have started, 2031 completion
- **AU:** 2024-2031
- **CN:** N/A
- **BE/LU/NL:** No overall timeline without pay scheme mandates

Best practices?

- Advise everyone starting a new project to use AES!
- PCI guidance documents on AES PIN Blocks

Blockers/Standards?

- **CA:** Cost of devices and time to swap
- **FR:** Lack of global requirement; standards can cause confusion with incompatibility
- **DE:** Need host-host UKPT for AES communication keys in 11568
- **AU:** Need AES PIN verification
- **CN:** None
- **BE/LU/NL:** Would like good AES session key document

PCI Security Standards Council

Implementation Progress

It's a Big Job, but You Started

Secure devices

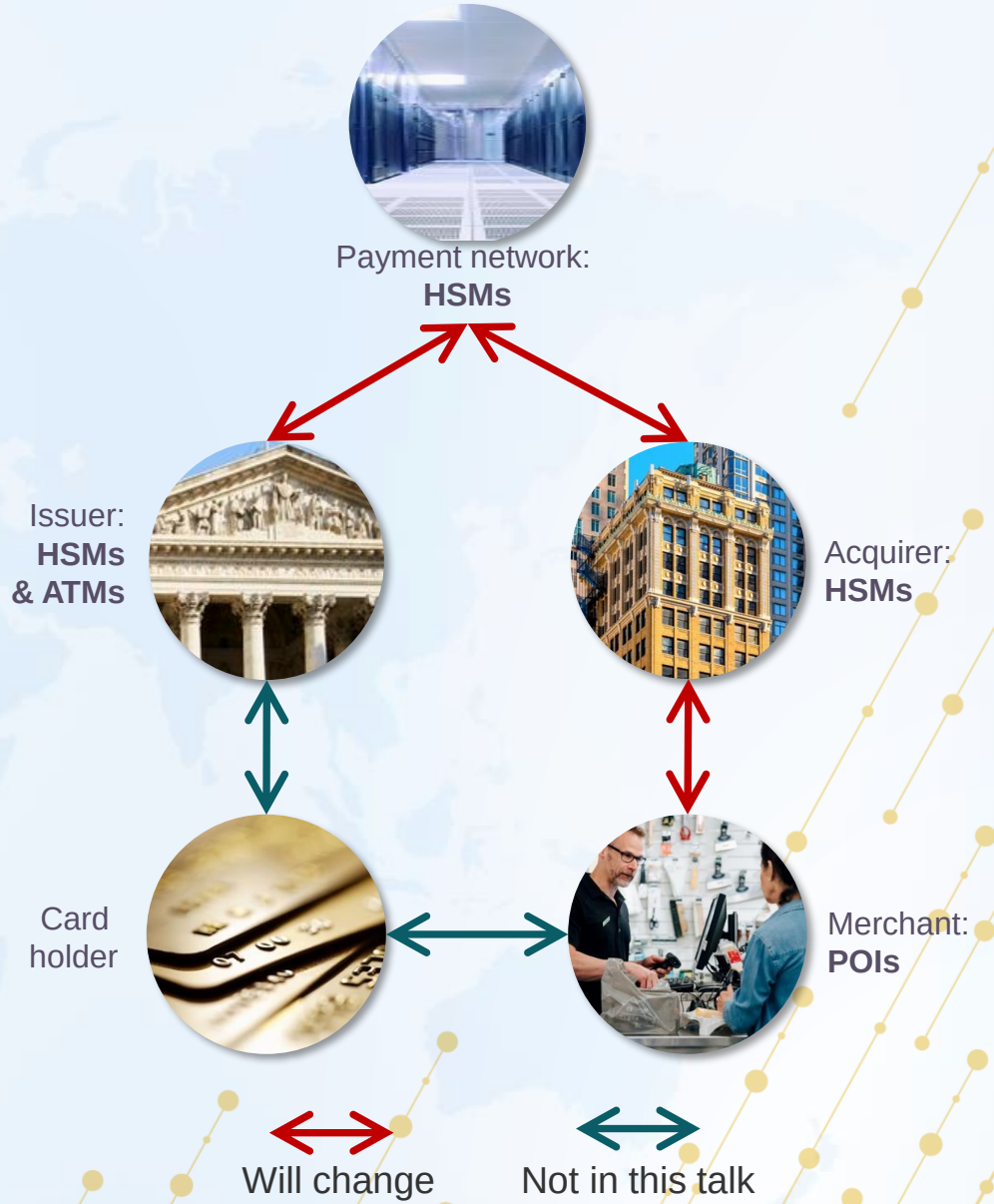
- **POIs**
  - There are many of these, but they're cheaper
  - Roll started but will take a long time
- **ATMs**
  - Fewer, but more expensive
- **HSMs**
  - Major manufacturers have AES PIN & MFK/MK support

To move the needle

- Standards: covered later
- Payment scheme requirements
- Government involvement

Without more action

- 2031 is *the good case*



PCI Security Standards Council

A Sample Program: AusPayNet (Australian Payments Network)

Transition points

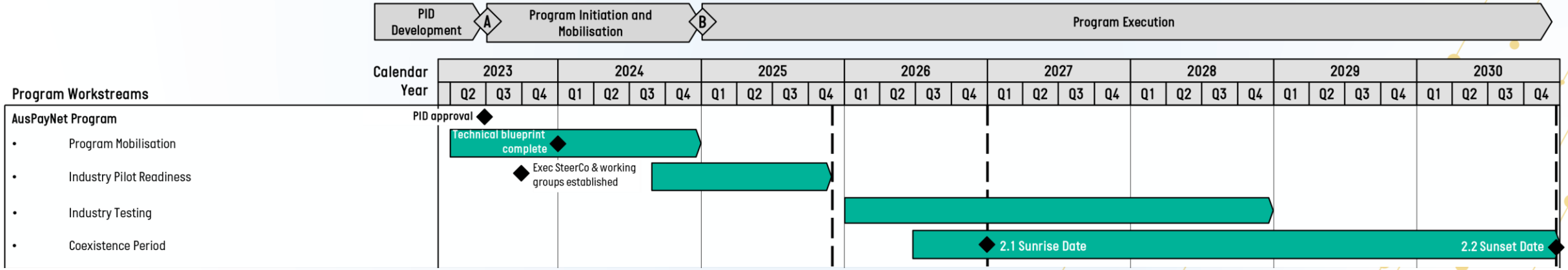
- Switching to key blocks?
- Switch to AES
- Updating ATM protocols?
- Use X9 TR-34 with AES keys

Critical infrastructure

- Payment and ATM networks are critical to national security

Industry group with government backing

- 3 years planning
- 7 years project



PCI Security Standards Council

PCI Security Standards Council

Standards

Functional enablement of the transition

Status

What Standards Are Already in Place for You to Use?

Standards Type	Status
Building Blocks (modes, KDFs, etc.)	
Data Protection	
Key Management	 No key block using ECC, No Host-host UKPT
PIN	 No PIN verify
Payments (CVV/CVC/CSC, EMV)	 No CVV/CVC/CSC, PIN scripting
Transitioning Older Devices	

 Standards ready to use

 You can start, but some standards are missing

 Major blocker exists

PCI Security Standards Council

What Needs to STOP

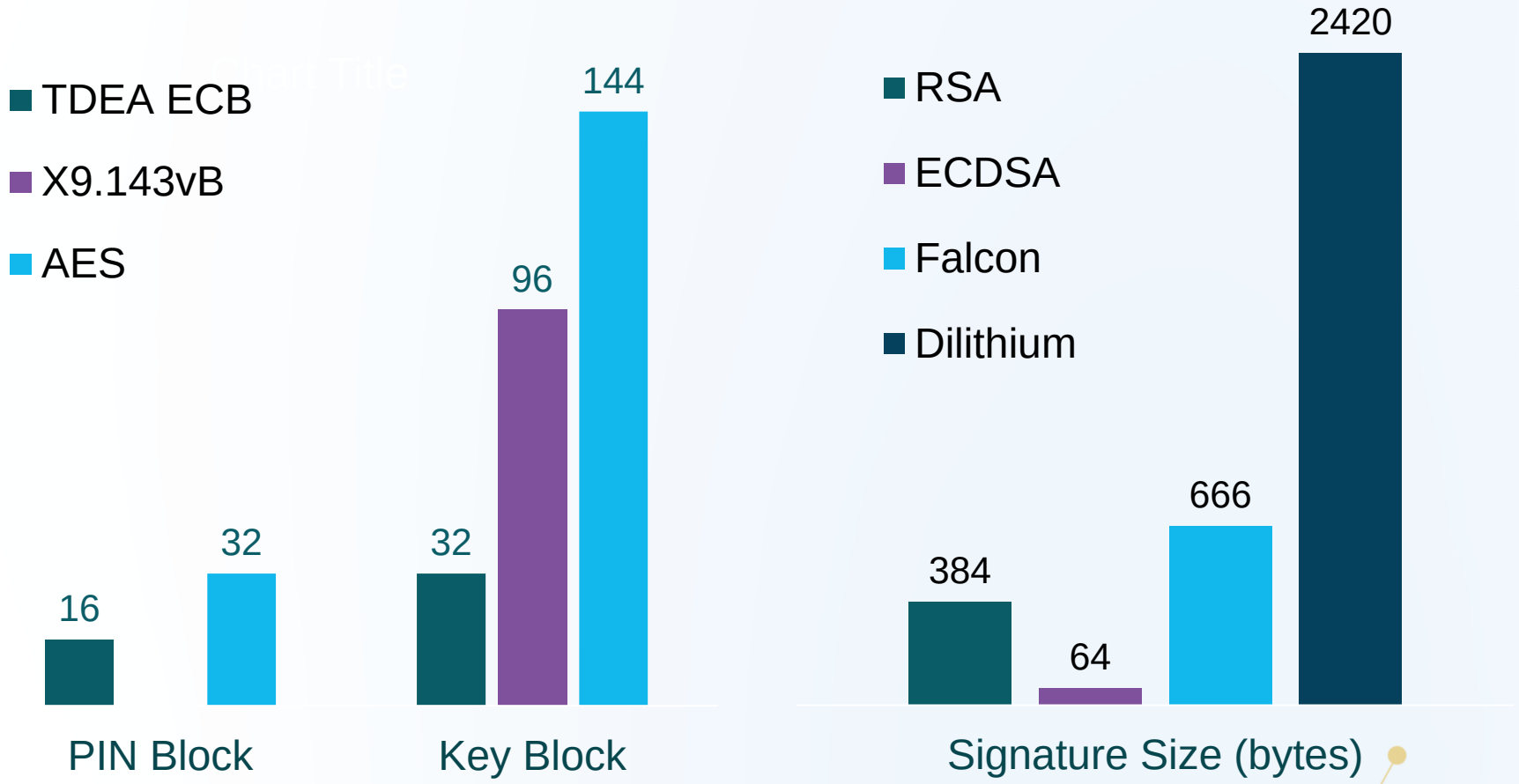
Older Technique that **Should Not** Be Used with AES

- CBC-MAC
- Variants for Key Management
- Encrypting keys with ECB or CBC (no key block)
- PIN Verification via the 3624 Offset Method
- PIN block without a PAN or PAN-linked token.
  - ISO didn’t define one – DON’T ADD IT
    - PIN block without a PAN is a security issue at the host
    - PIN block with a PAN is a debatable security issue at uncontrolled client

PCI Security Standards Council

What Do These Changes Mean to You?

The Biggest Impact, Sizes Change



Also, watch out for key usage enforcement.

PCI Security Standards Council

PCI Security Standards Council

Migration Planning

The Road Goes Ever On

Planning the Move

Start Now!

1. Understand what you are using now.
2. Target your moves – what are most vulnerable and what are easiest to move.
   - Get rid of Single-DES. 😊
3. TEST, TEST, TEST!
4. Keep an eye on Post-Quantum.
   - Algorithm agility sounds good and is a good goal, but budget constraints mean that 2 changes in a short time may not be feasible.

The Challenge of Upgrading Keys

The Scary Part of This Talk

Two basic methods for upgrading keys

- Local Key Injection
- Remote Key Injection

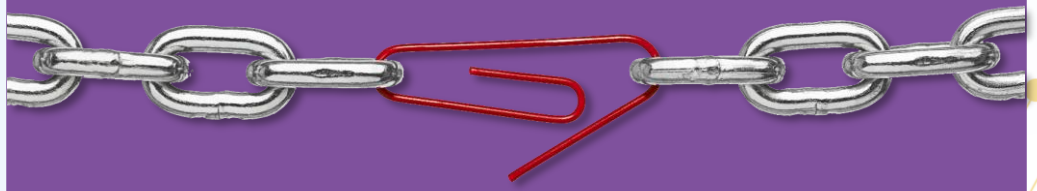
Remote Key Upgrades are not currently possible!*

- You'll need to physically visit your remote devices to upgrade the keys; or
- Deployed Devices will need to be returned to the factory of re-keying

… pending TR-56 approval

The cryptographic strength of a key SHALL be considered the minimum of the strength of that key and the strength of any cryptographic key that has ever been used to encrypt it.

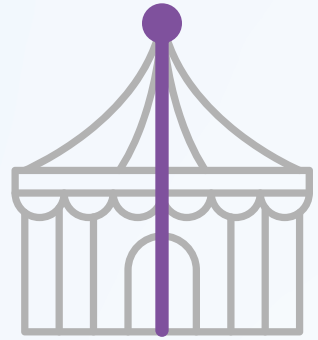
ANSI X9.24-1-2017



PCI Security Standards Council

Device Readiness

Start Your Project With the Longest Pole



POIs

- Existing estate will have to be returned to factory for re-keying before AES can be used… unless we can get TR-56 approved.
  - PCI includes an allowance for RKI of AES-128 keys using RSA-2048, but key strength is reduced.
- Accelerate the implementation of AES-256 KBPKs or ECC TMKs in new or repaired devices… even if you aren't ready to make use of AES for PIN or PAN encryption.

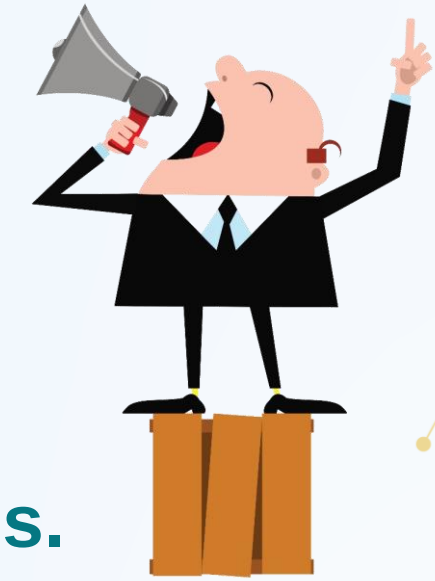
HSMs

- Make sure your HSM support AES and the newer standards.
- Consider an immediate move to AES for key Storage.

PCI Security Standards Council

Timelines

IMHO



Mandates will be needed for this to become a reality.

Such mandates will either need to exclude the existing estate or they will need to allow for **migration strategies.**

For example:

- Mandate day 0: all new devices and repaired devices must use AES Keys
- Mandate +1 year: 25% of the estate must use AES Keys
- Mandate +2 years: 50% of the estate must use AES Keys
- Mandate +3 year: 75% of the estate must use AES Keys
- Mandate +4 years: 100% of the estate must use AES Keys

Take Aways

The Transition Will Not Be Quick

- The AES transition has begun.
- Mandates are needed to drive coordinated change.
- The basic tools are in place to start, but not everything is finished.
- Know your system and get started:
  - New hardware must support AES.
  - Get a key transport key with 256-bits of strength in place within your POIs ASAP, even if you aren't ready to use AES yet for transactions.
  - Start using AES where you don't have to worry about interoperability: MFK, internal systems, new deployments.

Thank You.