PCI Security Standards Council®

Migrating to AES (Advanced Encryption Standard)

Learnings and Perspectives from Australia and France

Riaz Hussain

Head of Security Standards & Transformation
Australian Payments Network

Guillaume Dabosville

Security Expert
Cartes Bancaires CB

PCI Security Standards Council

AES Migration – The Case for Change

- Migration to AES is considered **necessary** and **inevitable**
  - The primary risk we are addressing is transaction integrity for the card payments system
  - TDES is deprecated but used everywhere in card present payments
  - Advances in classical and quantum computing increases the risk of compromise for TDES
  - Migration to AES will take time, dependencies on multiple specifications, manufacturers, vendors, financial and return on investment challenges
  - The ‘store now, decrypt later’ risk increases the risk window, requiring earlier action
- Alternative paths **extend** the risk profile
  - Implementing Key Blocks without AES causes inevitable re-work and delays
  - Timing of TDES being compromised is uncertain, waiting for AES mandates escalates the risk of a costly and unplanned migration later
  - IBM Quantum quoting research suggesting a 50% chance of compromise by 2031

PCI Security Standards Council®

AES Migration – Target State and Solution

- Establish a target state
  - Migrate to AES wherever TDES is used
  - Layered defense ensures completeness and coverage without over-reach into areas already addressed elsewhere (e.g. PCI DSS, EMV)
  - Secure key management practices
  - Transport layer encryption, including message and PIN Block encryption in the transaction path
  - Prepare for the quantum computing era
- Define the solution
  - Leverage international standards **and** provide additional guidance to address gaps

PCI Security Standards Council®

AES Migration – AusPayNet Case Study

- The domestic context
  - Federal Government and regulatory support (Treasury, Reserve Bank, Australian Signals Directorate, Home Affairs)
  - Industry alignment, 94% of Members supportive, 6% of Members are neutral
- Progress to date
  - Industry program led by AusPayNet
  - Phase 1 (Initiation & Mobilisation) almost complete, Phase 2 (Execution Phase) to begin from 2025
  - AES Technical blueprint completed, Migration and Industry Testing strategies completed
  - Focus on pre-pilot and pilot activities in 2025

PCI Security Standards Council®

AES Migration – AusPayNet Case Study

- Issues and challenges
  - Pace and timing, ‘sunrise’ and ‘sunset’ dates for AES required
  - ATMs and the decline of cash
  - National standards requiring development, gaps in international standards (PCI standards)
  - Only 22% of Members considered current mandates sufficient
- Lessons learnt
  - Focus on the technical blueprint early, provides confidence and direction to manufacturers and vendors
  - Align migrations with natural asset replacement schedules reduces risk and cost
  - Upgrade transport layer early, a quick win
  - Testing and certification essential

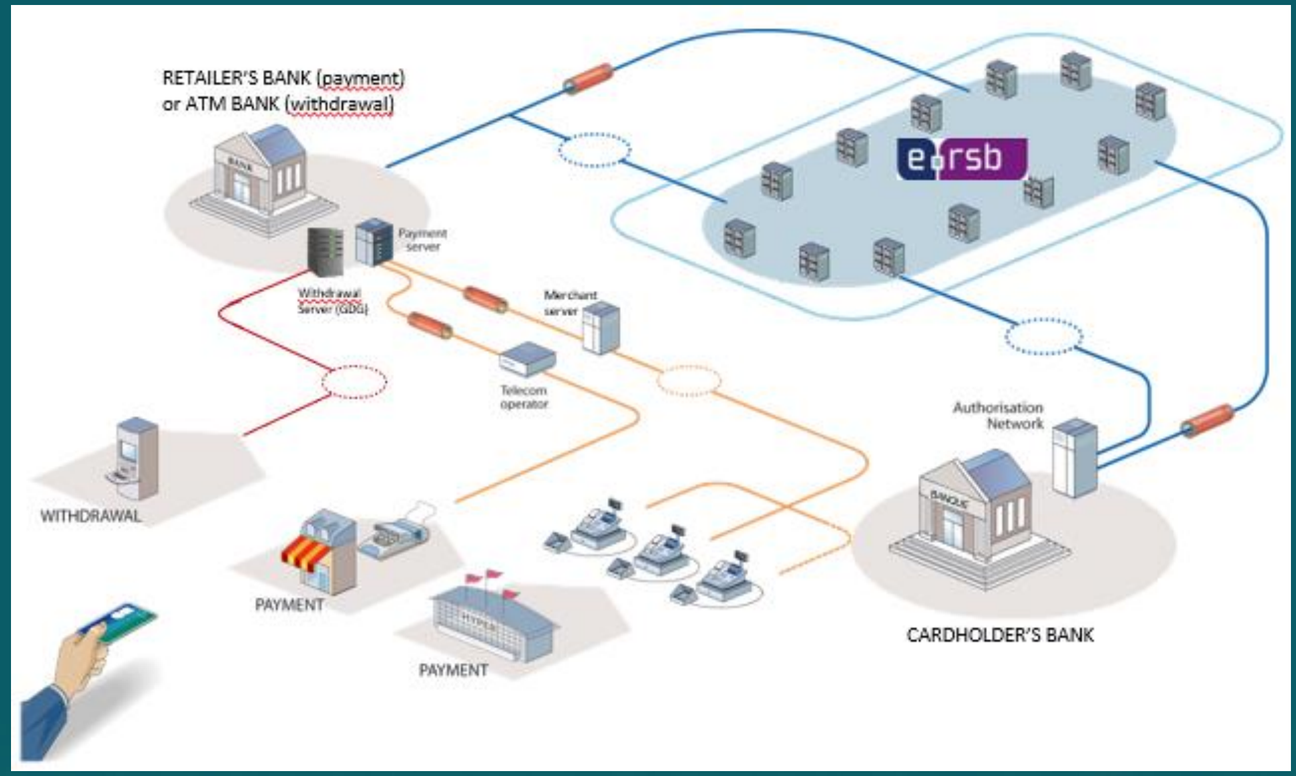
AES Migration – CB Case Study

- Domestic context
  - ANSSI (French cybersecurity agency)
  - Banque de France
  - French Banks

  Even more regulation at the EU level

- Progress / achievements
  - Interbank Network migration to AES completed (as well as TR-31 Key Block) since 1st May 2024
    - More than 310 servers
  - Attended terminals are (mostly) AES-ready
    - 80% standalone
    - 90% distributed
  - Issuer servers are decrypting AES-PIN Blocks

  => The path taken by PIN is either AES-ready or AES



AES Migration – CB Case Study

- Issues / challenges found
  - Regulatory obligations are missing
  - Some manufacturers are using this to delay AES to their 2030 ROADMAP
  - 7 to 10 years to update the entire POI estate
- Lessons learnt
  - Regulation is key
    - PCI PIN 3.0 (August 2018) had clear milestones
    - And helped us obtain budget and engagement
  - Combine AES and Key Block migrations (same devices and protocols are concerned)
  - Migrate end-to-end functions of the system (Online PIN verification in our case)

PCI Security Standards Council®

AES Migration - Conclusion

Lessons learnt from history

- Long-standing history in cryptography and cryptanalysis
  - Punctuated by alternating breakthroughs by cryptographers and cryptanalysts
- Cryptography has been particularly stable over 40 years
  - Providing stable and long-term security to the payment industry
- We are lucky to be able to anticipate (quantum) cryptanalysts' win in coming years
- We are also lucky to have AES to help us to partially pass this Y2Q
- So, let's move to AES and more globally, let's move to a minimum 128-bit security strength
  - Quick win is TLS1.3 (with quantum safe ciphersuite for hybridization)

PCI Security Standards Council®

Security Standards Council®