PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING

Compliance Evolution Enabling Technology Innovation for Faster and More Secure Device Deployments

2025 NORTH AMERICA COMMUNITY MEETING

PCI Security Standards Council

Jason Way

VP of Payment Cryptography Services

Futurex

FUTUREX

PCI Security Standards Council

A Historical Perspective

2005

Original publication of ANSI X9.TR-31 for Key Blocking double length keys.

2006-2011

TG-3/ TR-39/ VISA PIN were primary audit guidelines

2010

Mandated migration from Singe DES to Triple DES

2011

PCI SSC adopts best practices of TG-3/TR-39/VISA PIN for “PCI PIN”

2012

ANSI X9.TR-34 Published for Asymmetric Distribution of Symmetric Keys

2017

Last FIPS 140-2 Level 3 supports double length TDES (X9.24 DUKPT)

PCI Security Standards Council

How did we get here?

- Strategic enablement vs enforcement
- Gradual, baby-step adoption
- Millions of endpoints → staged rollout

TDES & Key Block Evolution

TR-31 is a key wrapping standard developed by the ASC X9 financial industry working group. It improves the security of keys by binding them to their usage and fosters interoperability between different parties in the payments ecosystem. The standard was ratified in 2005 and implementation is ongoing to this day.

2005
Initial publication in ASC X9.24-1:2004
v2 published 2010

→

2009-2012
Early adoption of TR-31 in HSMs

→

2015
PCI PIN v2.0 encourages key block adoption

→

2017
PCI PIN v3.0 mandates key block usage

Phase 1 (June 2019)
For acquirers, internal connections must use key blocks

⇢

Phase 2 ~~(June 2021)~~
External connections between entities must use key blocks

⇢

Phase 3 ~~(June 2023)~~
All stored keys must be in key block format

2020
TR-31 key block deadlines extended

→

- ✔ **Phase 1:** June, 2019
- ✔ **Phase 2:** Jan, 2023
- ✔ **Phase 3:** Jan, 2025

PCI Security Standards Council

Algorithm & FIPS Influence

3DES to AES, mandated by NIST SP 800-131A Rev 2 (2020)

	DES	3DES	AES
Year mandated	Legacy (pre-2010)	**2010** (double-length DES)	**2017** (FIPS 140-2 L3 requirement)
Effective strength	56 bits	112 bits	128 / 192 / 256 bits
FIPS 140-2 L3 status	Deprecated for new L3 certs	Banned for Level 3 if enabled (post-2017)	Required for Level 3 compliance

Secure Key Distribution Options

HSM
(tamper-responsive module)

Pro: Highest protection

Con: Higher cost & operational complexity

Key Wrap
(encrypt under stronger key)

Pro: Simplifies distribution

Con: Requires secure bootstrap key management

Split Parts
(split-knowledge ceremonies)

Pro: No single point of compromise

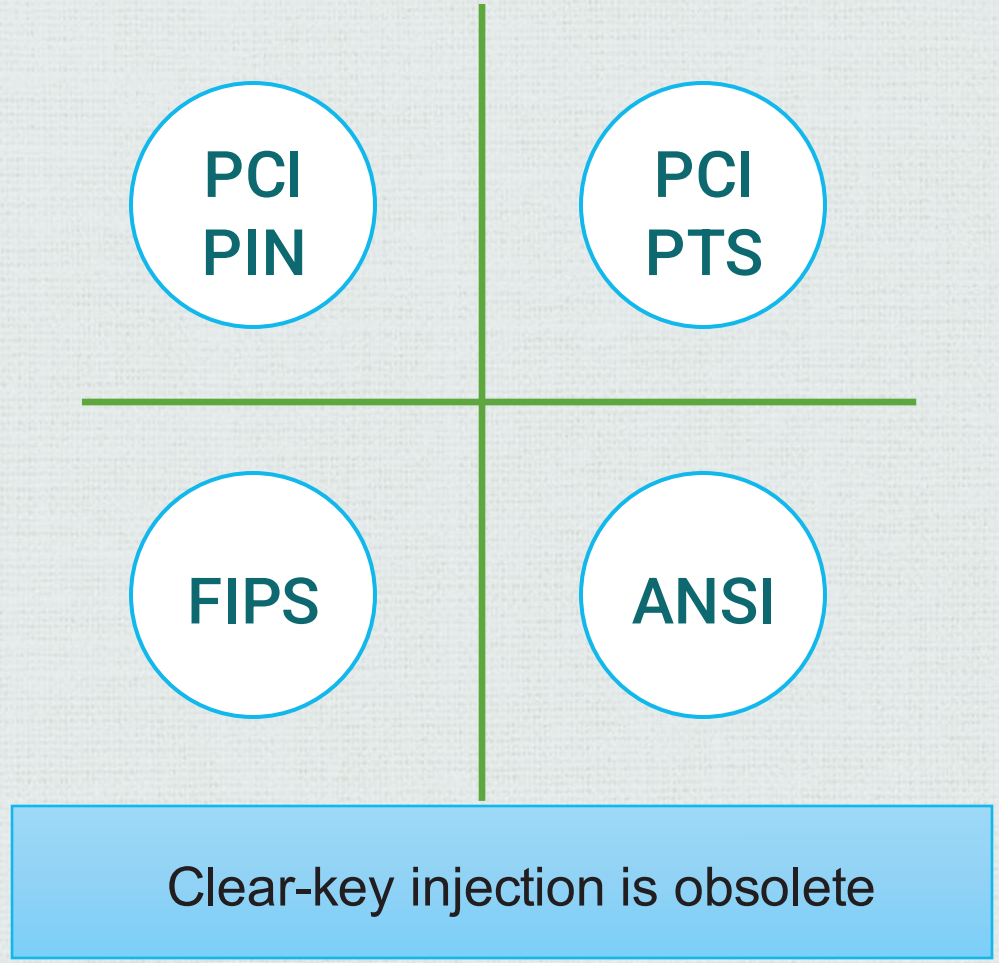
Con: Time-intensive and labor-heavy

TR-34 & Asymmetric Exchange

- TR-34 published 2012; updated 2018; ANSI X9.139 in 2025
- Interoperable secure key exchange
- Eliminates multi-party ceremonies

Enforcement Through Standards

- **PCI PIN 18-3:** Signed asymmetric keys
- **PCI PIN 32-9:** Encrypted loading mandate
- **PCI PTS V5+:** Clear-key deprecated



Bringing It All Together

- Staged mandates enabled secure automation
- Compliance harmonized across standards
- Manual injection now obsolete

PCI Security Standards Council

Summary

- Compliance has enabled scalable innovation
- Automation enhances both speed and security
- Support the standardization of TR-34 (X9.139)

PCI Security Standards Council

Thank You!

info@futurex.com

www.future.com

PCI Security Standards Council