Post-Quantum

Cryptography Conference

PKI and PQC Strategy for Payment Card Industry

Jeremy King

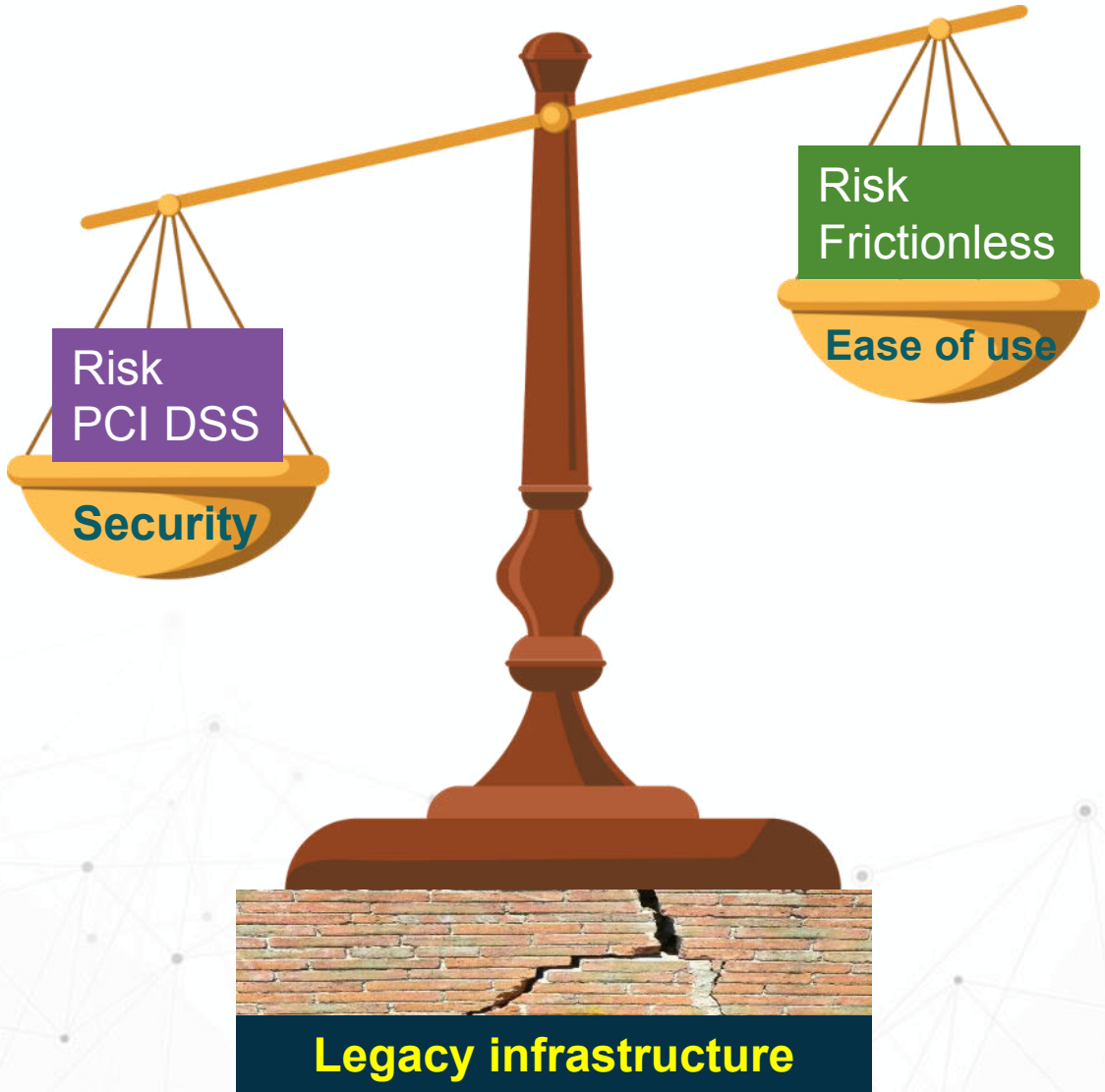
Regional VP, EMEA at PCI Security Standards Council

ENTRUST HID PKI Consortium

PKI and PQC Strategy for Payment Card Industry

Jeremy King
VP EMEA
PCI Security Standards Council

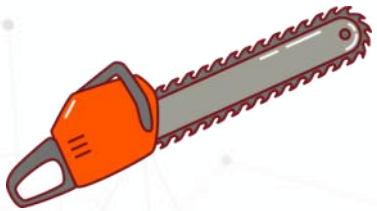
Balancing Security vs Ease of Use



Who Lives In A House Like This?

PCI Security Standards Council

But What If The Wolf Had Choices?



PCI Security Standards Council

What Do You Have That the Criminals Want?

Intellectual Property

- New design ideas
- Research data
- Next seasons fashion
- Promotion ideas and dates

Customer Personal Data

- Names
- Addresses
- Passwords
- Social security numbers
- Passport numbers

Payment Data

- PAN
- Sensitive Data
- Other payment data

Money

- CEO fraud
- Ransoms
- Redirected payments

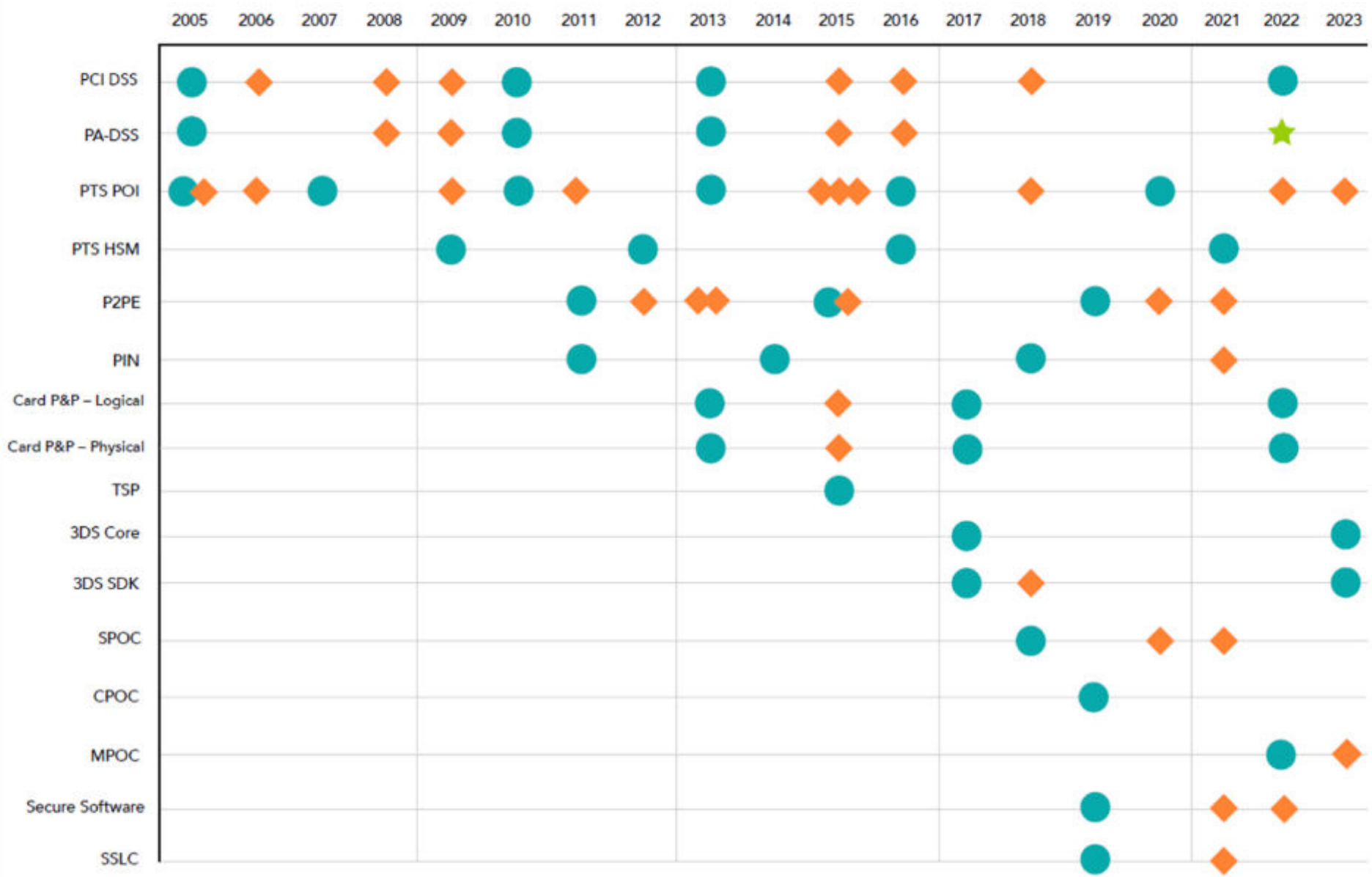
And Technology Just Keeps on Changing

PCI Security Standards Council

PCI Security Standards Council

Standards Revision History

- Major Revision
- Minor or Other Revision
- Retirement



We Are In A Never-Ending Race

PCI Security Standards Council

Cryptography Not Immune

Secure Socket Layer

- SSL version 3.0. was released in 1996, produced by Paul Kocher
- In 2014, SSL 3.0 was found to be vulnerable to the POODLE attack that affects all block ciphers in SSL.
- SSL 3.0 was deprecated in June 2015
- April 2015 PCI SSC release PCI DSS V3.1 including requirement to migrate from SSL to TLS by June 2016
- December 2015 PCI SSC responding to market feedback push the migration date back to June 2018
- June 2018 PCI SSC release PCI DSS V3.2.1 removing use of SSL

PCI Security Standards Council

Triple Data Encryption Algorithm (TDEA or 3DES)

- 1978: a triple encryption method using DES with two 56-bit keys was proposed by Walter Tuchman
- 1981: Merkle and Hellman proposed a more secure triple key version of 3DES with 112 bits of security.
- 1998: TDEA Rolled out into common use in the Financial Industry
- 2023 Dec: TDEA will be officially deprecated and prohibited from use.

Does TDEA meet the requirements of “strong cryptography” as defined in PCI DSS?

FAQ: 1570

At the end of 2023, NIST disallows the use of three-key TDEA for use in protecting security sensitive data within US Federal information systems. However, as per NIST SP800-57 part 1, TDEA using three keys can still provide an effective strength of 112 bits when applied using appropriate key management and modes of operation.

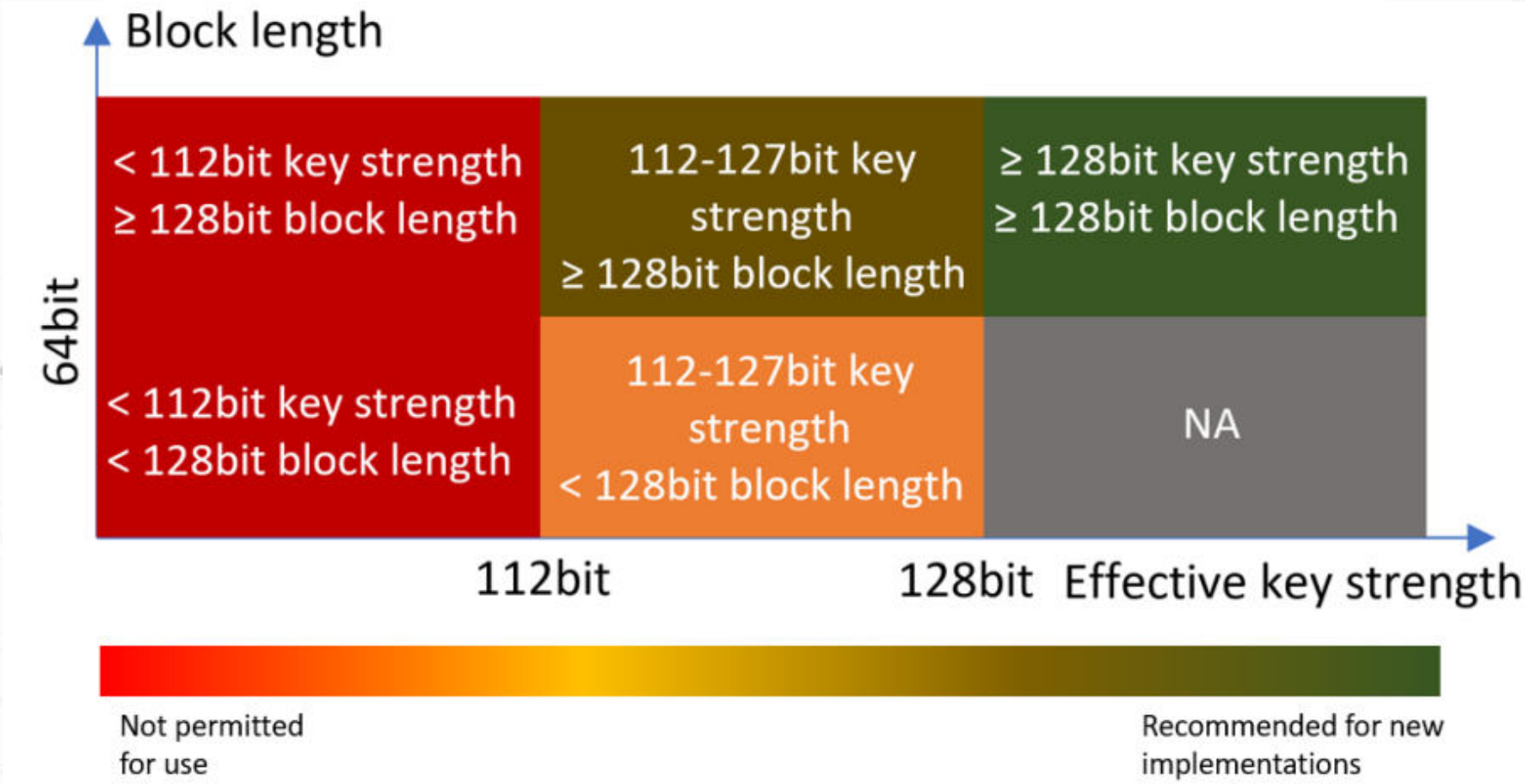
The definition of 'strong cryptography' was updated in PCI DSS v4.0 to reference the effective key size of the algorithm/key combination rather than any specific algorithms - specifically the effective key strength is a minimum of 112 bits, with a recommendation to use systems that provide 128 bits of effective strength. Additionally, ‘strong cryptography’ requires the use of industry-tested and accepted algorithms and proper key-management practices.

For other PCI SSC standards, refer to the subject standard for whether and how use of three-key TDEA is allowed.

PCI Security Standards Council

Removing TDEA from the Payments Environment

Block Sizes, Modes of Operation and Padding



PCI Security Standards Council

And just every now and then something comes along that changes the whole paradigm

PCI Security Standards Council

Only this time like London busses two came along at the same time

Quantum Computing

Today

Tomorrow

PCI Security Standards Council

Which Cryptographic Techniques are Susceptible to Quantum Computing

- RSA
- Finite Field Cryptography (FFC)
- Elliptic Curve Cryptography

Why does this matter?

PCI SSC PIN Security Standard Acceptable Cryptographic Techniques

	Algorithm				
Bits of Security	**DEA**	**IFC** (RSA)	**ECC** (ECDSA, ECDH, ECMQV)	**FFC** (DSA, DH, MQV)	**AES**
80	112	1024	160	1024/160	–
112	168	2048	224	2048/224	–
128	–	3072	256	3072/256	128
192	–	7680	384	7680/384	192
256	–	15360	512	15360/512	256

Development Roadmap

Executed by IBM
On target

IBM **Quantum**

	2019	2020	2021	2022	2023	2024	2025	2026+
	Run quantum circuits on the IBM cloud	Demonstrate and prototype quantum algorithms and applications	Run quantum programs 100x faster with Qiskit Runtime	Bring dynamic circuits to Qiskit Runtime to unlock more computations	Enhancing applications with elastic computing and parallelization of Qiskit Runtime	Improve accuracy of Qiskit Runtime with scalable error mitigation	Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime	Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Model Developers					Prototype quantum software applications → Quantum software applications		Machine learning | Natural science | Optimization	
Algorithm Developers		Quantum algorithm and application modules			Quantum Serverless			
		Machine learning | Natural science | Optimization				Intelligent orchestration	Circuit Knitting Toolbox	Circuit libraries
Kernel Developers	Circuits		Qiskit Runtime					
				Dynamic circuits	Threaded primitives	Error suppression and mitigation		Error correction
System Modularity	Falcon 27 qubits	Hummingbird 65 qubits	Eagle 127 qubits	Osprey 433 qubits	Condor 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	Scaling to 10K-100K qubits with classical and quantum communication
					Heron 133 qubits x p	Crossbill 408 qubits		

Do we need to be worried?

The figures vary and the caveats are many but…

A 2048 bit RSA would require around 10,000 qubits to brute force attack it.

Which according to IBM's roadmap should be sometime after 2026

But even then, it is not as simple as that

A Very Old-World Problem Exists to a New World Issue

- 250 million point of interaction devices in service globally
- 3.2 million ATM’s in use globally
- Potentially simar number of HSM’s

PCI Security Standards Council

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

For General Encryption

- the CRYSTALS-Kyber algorithm

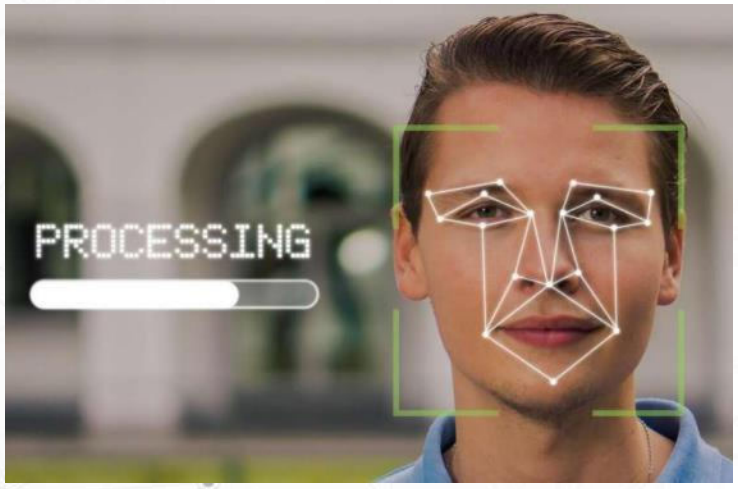
For digital signatures

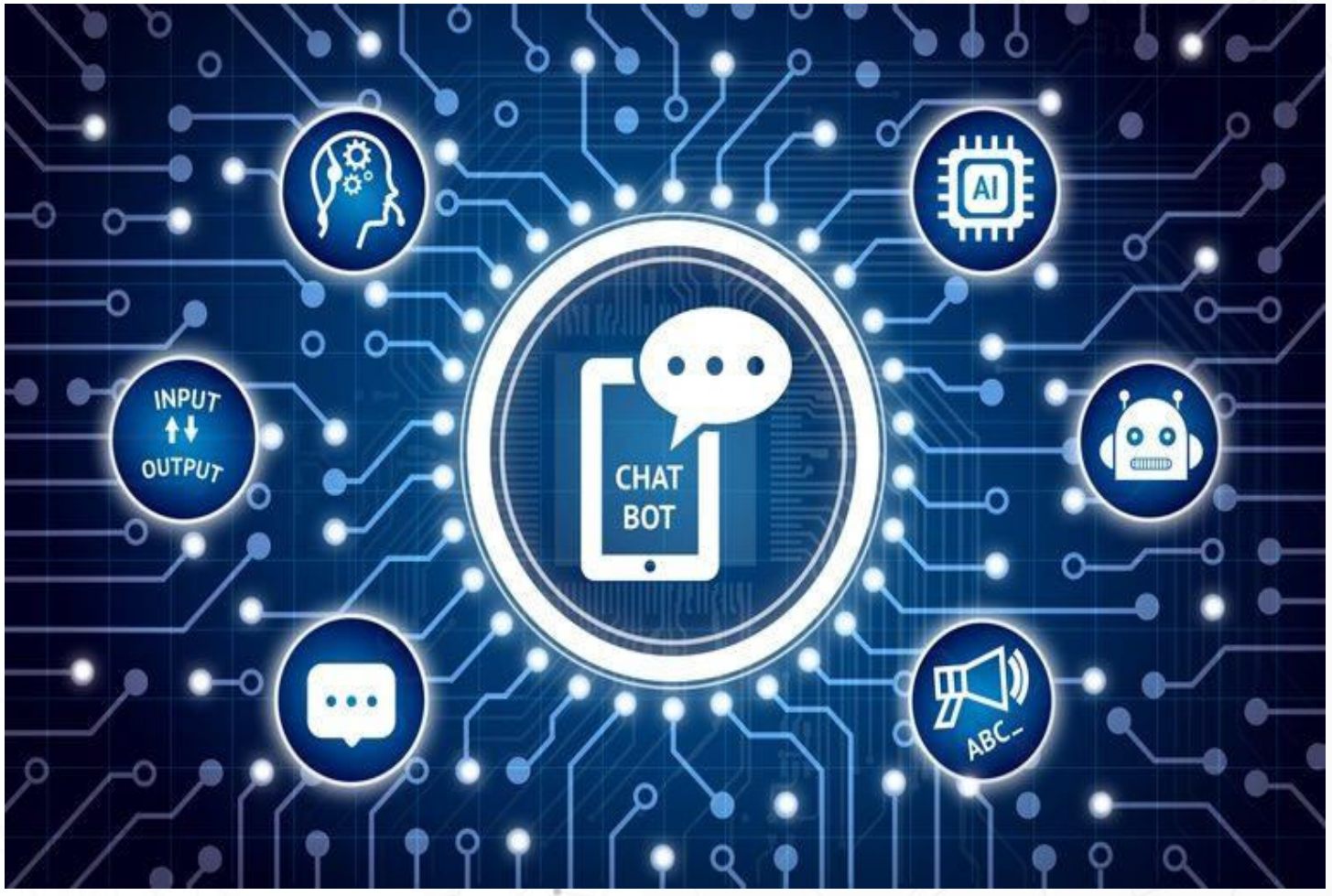
- CRYSTALS-Dilithium algorithm
- FALCON algorithm
- SPHINCS+ algorithm

PCI Security Standards Council

So, what does all this mean for the PCI SSC?

Artificial Intelligence – Authentication?





PCI SSC Strategic Framework

Mission

To enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

Strategic Pillars

Increase Industry Participation and Knowledge

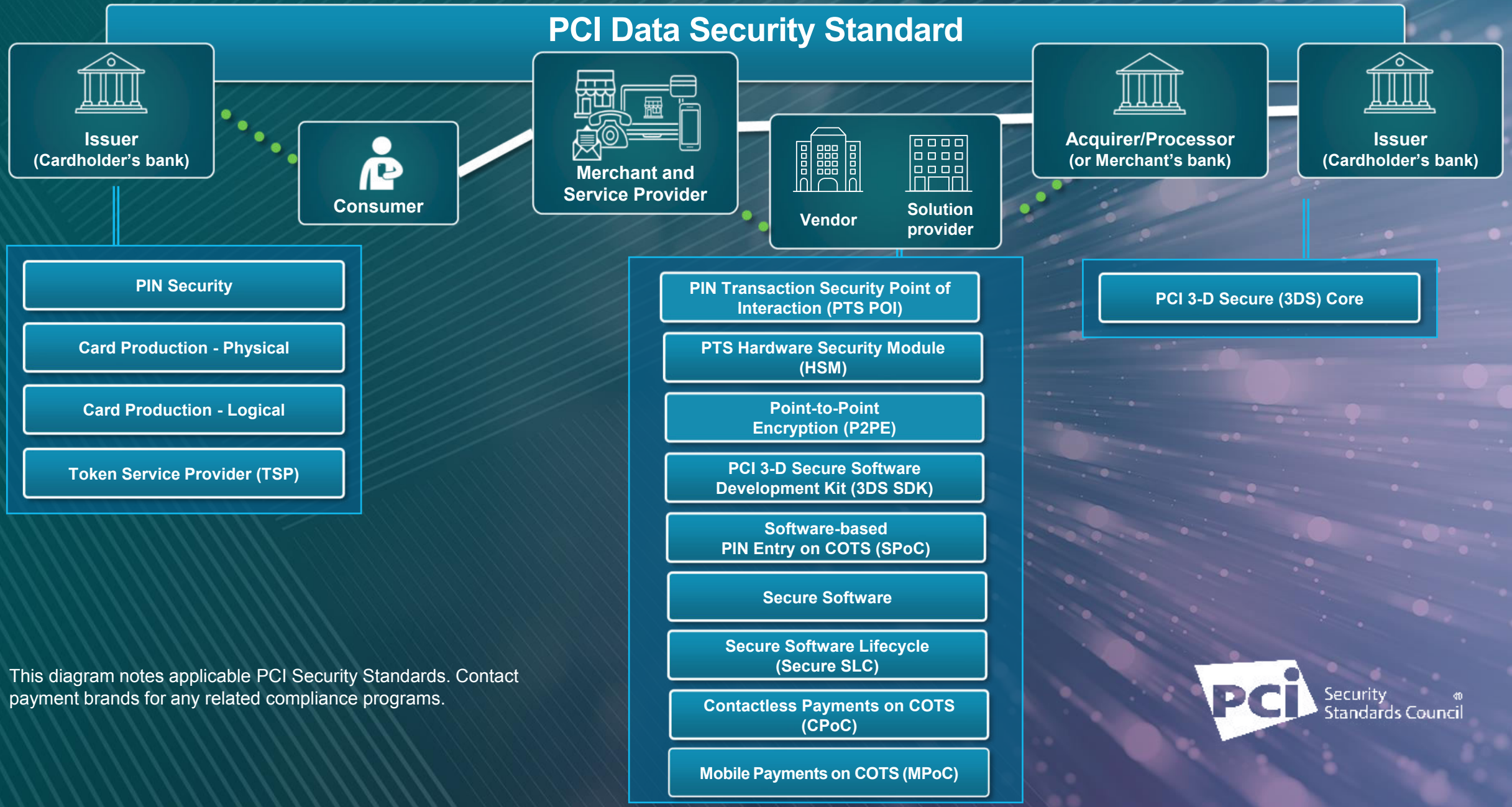
Evolve Security Standards and Validation

Secure Emerging Payment Channels

Increase Standards Alignment and Consistency

PCI Security Standards Council

15 PCI Security Standards



This diagram notes applicable PCI Security Standards. Contact payment brands for any related compliance programs.

PCI Security Standards Council

New Participation Program

Levels

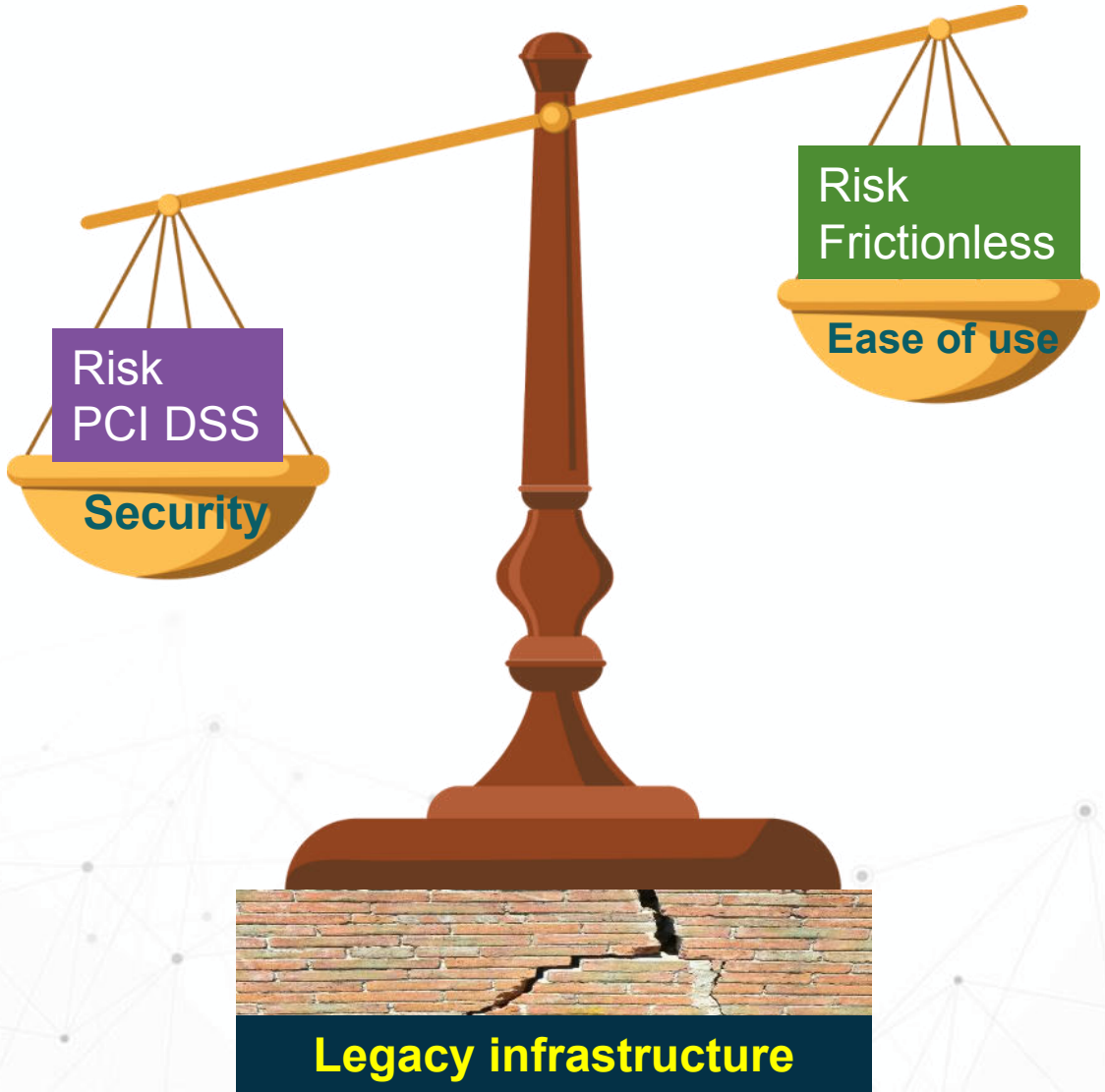
Expanding

Influence

Anyone Can Be A Member

Summary

Balancing Security vs Ease of Use



Get Involved Today!

participation@pcisecuritystandards.org

Thank you

Any questions or topics you would like to discuss further?

PCI Security Standards Council

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia