PKI and PQC Strategy for Payment Card Industry

Jeremy King
VP EMEA
PCI Security Standards Council
Balancing Security vs Ease of Use

- Security
- Risk
- PCI DSS

- Ease of use
- Risk
- Frictionless

Legacy infrastructure
Who Lives In A House Like This?
But What If The Wolf Had Choices?
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

**Ethical group**

**State Sponsored Hacker**

**OCG**
And Technology Just Keeps on Changing
We Are In A Never-Ending Race
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
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.
Removing TDEA from the Payments Environment
Block Sizes, Modes of Operation and Padding

- **< 112bit key strength**
  - **< 128bit block length**: Not permitted for use
  - **≥ 128bit block length**: Recommended for new implementations

- **112-127bit key strength**
  - **≥ 128bit block length**: Not permitted for use
  - **< 128bit block length**: Recommended for new implementations

- **≥ 128bit key strength**
  - **≥ 128bit block length**: Not permitted for use
  - **< 128bit block length**: Recommended for new implementations

- **128bit Effective key strength**: NA
And just every now and then something comes along that changes the whole paradigm

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

Today

Tomorrow
Which Cryptographic Techniques are Susceptible to Quantum Computing

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

Why does this matter?

<table>
<thead>
<tr>
<th>Bits of Security</th>
<th>DEA</th>
<th>IFC (RSA)</th>
<th>ECC (ECDSA, ECDH, ECMQV)</th>
<th>FFC (DSA, DH, MQV)</th>
<th>AES</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>112</td>
<td>1024</td>
<td>160</td>
<td>1024/160</td>
<td>–</td>
</tr>
<tr>
<td>112</td>
<td>168</td>
<td>2048</td>
<td>224</td>
<td>2048/224</td>
<td>–</td>
</tr>
<tr>
<td>128</td>
<td>–</td>
<td>3072</td>
<td>256</td>
<td>3072/256</td>
<td>128</td>
</tr>
<tr>
<td>192</td>
<td>–</td>
<td>7680</td>
<td>384</td>
<td>7680/384</td>
<td>192</td>
</tr>
<tr>
<td>256</td>
<td>–</td>
<td>15360</td>
<td>512</td>
<td>15360/512</td>
<td>256</td>
</tr>
</tbody>
</table>
## Development Roadmap

**IBM Quantum**

<table>
<thead>
<tr>
<th>Year</th>
<th>Milestones</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019</td>
<td>Run quantum circuits on the IBM cloud</td>
</tr>
<tr>
<td>2020</td>
<td>Demonstrate and prototype quantum algorithms and applications</td>
</tr>
<tr>
<td>2021</td>
<td>Run quantum programs 100x faster with Qiskit Runtime</td>
</tr>
<tr>
<td>2022</td>
<td>Bring dynamic circuits to Qiskit Runtime to unlock more computations</td>
</tr>
<tr>
<td>2023</td>
<td>Enhancing applications with elastic computing and parallelization of Qiskit Runtime</td>
</tr>
<tr>
<td>2024</td>
<td>Improve accuracy of Qiskit Runtime with scalable error mitigation</td>
</tr>
<tr>
<td>2025</td>
<td>Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime</td>
</tr>
<tr>
<td>2026+</td>
<td>Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime</td>
</tr>
</tbody>
</table>

### Model Developers
- Quantum algorithm and application modules
- Machine learning | Natural science | Optimization

### Algorithm Developers
- Quantum Serverless
- Intelligent orchestration |
- Circuit Knitting Toolbox |
- Circuit libraries

### Kernel Developers
- **Circuits**
  - **Falcon** 27 qubits
  - **Hummingbird** 65 qubits
  - **Eagle** 127 qubits
  - **Osprey** 433 qubits
  - **Condor** 1,121 qubits
  - **Flamingo** 1,386+ qubits
  - **Kookaburra** 4,158+ qubits

- **Qiskit Runtime**
  - Dynamic circuits
  - Threaded primitives
  - Error suppression and mitigation
  - Error correction

- **Scaling to 10K-100K qubits with classical and quantum communication**
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 similar number of HSM’s
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
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
This diagram notes applicable PCI Security Standards. Contact payment brands for any related compliance programs.
New Participation Program

Levels

Principal

Associate

Individual

Expanding

Influence

Anyone Can Be A Member
Summary
Balancing Security vs Ease of Use

- Security
- PCI DSS
- Legacy infrastructure

- Risk
- Ease of use
- Frictionless
Get Involved Today!

participation@pcisecuritystandards.org

Thank you

Any questions or topics you would like to discuss further?