Post-Quantum

Cryptography Conference

X9.146 Quantum TLS

The draft standard X9.146 Quantum TLS is nicknamed for enhancing the Transport Layer Security (TLS) protocol to support the NIST PQC algorithms. Security protocols such as TLS, developed and managed by the Internet Engineering Task Force (IETF) various workgroups, are heavily relied upon the financial services industry. However, the financial services industry wants to transition to PQC algorithms sooner rather than later, including banks, merchants, and third party financial service providers. This session introduces the draft X9.146 standard under development by the X9F5 Financial PKI workgroup, and the software engineering for enhancing and successfully testing this standard amongst collaborating industry vendors.

Jeff Stapleton

Executive Director Cybersecurity Researcher at Wells Fargo

David Hook

VP Software Enginering at Keyfactor

Mike Ounsworth

Software Security Architect at Entrust

SSL.com

PQ SHIELD

HID

KEYFACTOR

ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium

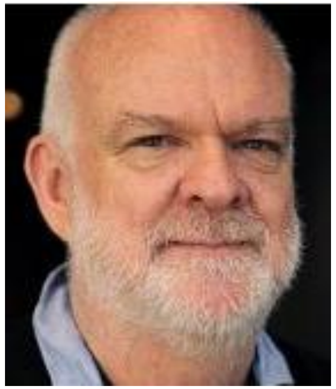
Accredited Standards Committee X9 Inc.
Financial Industry Standards

X9.146 Quantum TLS

PQC Readiness and Crypto-Agility for Financial Services

X9F5 Financial PKI

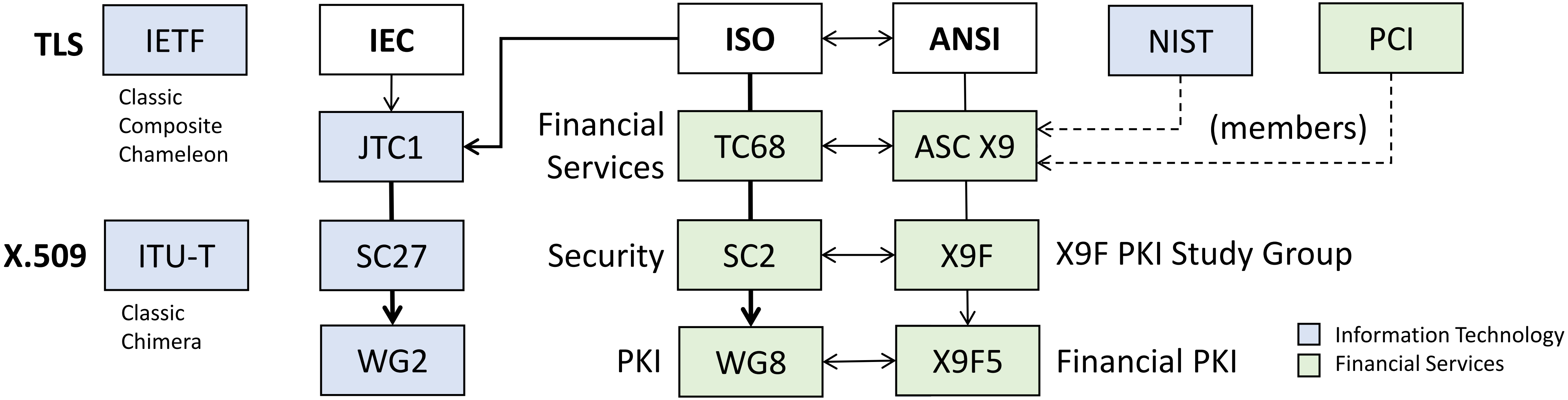
Jeff Stapleton
Wells Fargo



David Hook
Keyfactor

Mike Ounsworth
Entrust

Industry Standards Organizations



TLS IETF

Classic
Composite
Chameleon

X.509 ITU-T

Classic
Chimera

IEC

JTC1

SC27

WG2

ISO

ANSI

NIST

PCI

(members)

Financial Services TC68

ASC X9

Security SC2

X9F

X9F PKI Study Group

PKI WG8

X9F5

Financial PKI

🟦 Information Technology
🟩 Financial Services

- **X.509** Information technology – Public-key and attribute certificate frameworks
- **RFC 5280** Internet X.509 PKI Certificate and CRL Profile
- **ISO 21188** PKI Policy and Practices Framework (USA submission **X9.79**)
    - **ISO/IEC 27099** PKI Policy and Practices Framework
- **RFC 8446** The Transport Layer Security (TLS) Protocol Version 1.3

X9.146 Certificates

Certificate Format	Native	Extensions
Classic	Legacy public key Legacy signature	N/A
Classic	PQC public key PQC signature	N/A
Chimera	Legacy public key Legacy signature	PQC public key PQC signature
Composite	Legacy public key PQC public key	N/A
	Legacy signature PQC signature	N/A
Chameleon	Legacy public key Legacy signature	DTD Certificate
DTD Certificate	PQC public key PQC signature	N/A

X9.146 CKS extension (Certificate Key Selection)

CKS Codes	Fields	Extensions	Description
Default (0)	Native	N/A	Classic: Native only – Alternate not present
Native (1)	Native	Alternate	Chimera: Native default – ignore Alternate
Alternate (2)	Native	Alternate	Chimera: Alternate only – ignore Native
Both (3)	Native	Alternate	Chimera: Native and Alternate
Composite (4)	Native	N/A	Composite:
Chameleon (5)	Native	Delta	Chameleon:
Classic (6)	Native	N/A	Classic: certificate pair
Reserved (7)	N/A	N/A	Reserved for future use
… …	…	…	Reserved for future use
Reserved (254)	N/A	N/A	Reserved for future use
External (255)	N/A	N/A	Codes are external to TLS protocol

X9.146 CKS beta testing

- Coordinating ASC X9 and IETF work
  - Mike Ounsworth (Entrust) assisting X9.146 standard development
  - Tim Hollebeek (DigiCert) chair X9F5 workgroup (and co-chair LAMPS)
- Status X9.146 proof of technology using TLS extension
  - Anthony Hu (wolfSSL) provided beta wolfCrypt
  - David Hook (Keyfactor) provided beta Bouncy Castle
  - Max Pala (Wells Fargo) working composite certificates and OpenSSL

Beta	wolfSSL	Bouncy Castle	OpenSSL
✓ wolfSSL	working	TBD	TBD
✓ Bouncy Castle	working	working	TBD
OpenSSL	TBD	TBD	TBD

CNSA 2.0 Algorithms

Security Component	Algorithm	Quantum Threat
Authentication Level 5	ML-DSA 87 (Dilithium)	Shor’s Algorithm
Key Establishment Level 5	ML-KEM 1024 (Kyber)	Shor’s Algorithm
Symmetric Cipher	AES-256	Grover’s Algorithm
Hash Algorithm	SHA-384*	Grover’s Algorithm

* FIPS 204 ML-DSA and FIPS 203 ML-KEM refer to FIPS 203 SHA3