ETSI The Standards People

IQC Institute for Quantum Computing

ETSI/IQC Quantum Safe Cryptography Conference 2026

X9.146 QTLS Extensions with Chimera Certificates for Post-Quantum Migration

Presented by:

wolfSSL

X9.146 QTLS Extensions with Chimera Certificates for Post-Quantum Migration

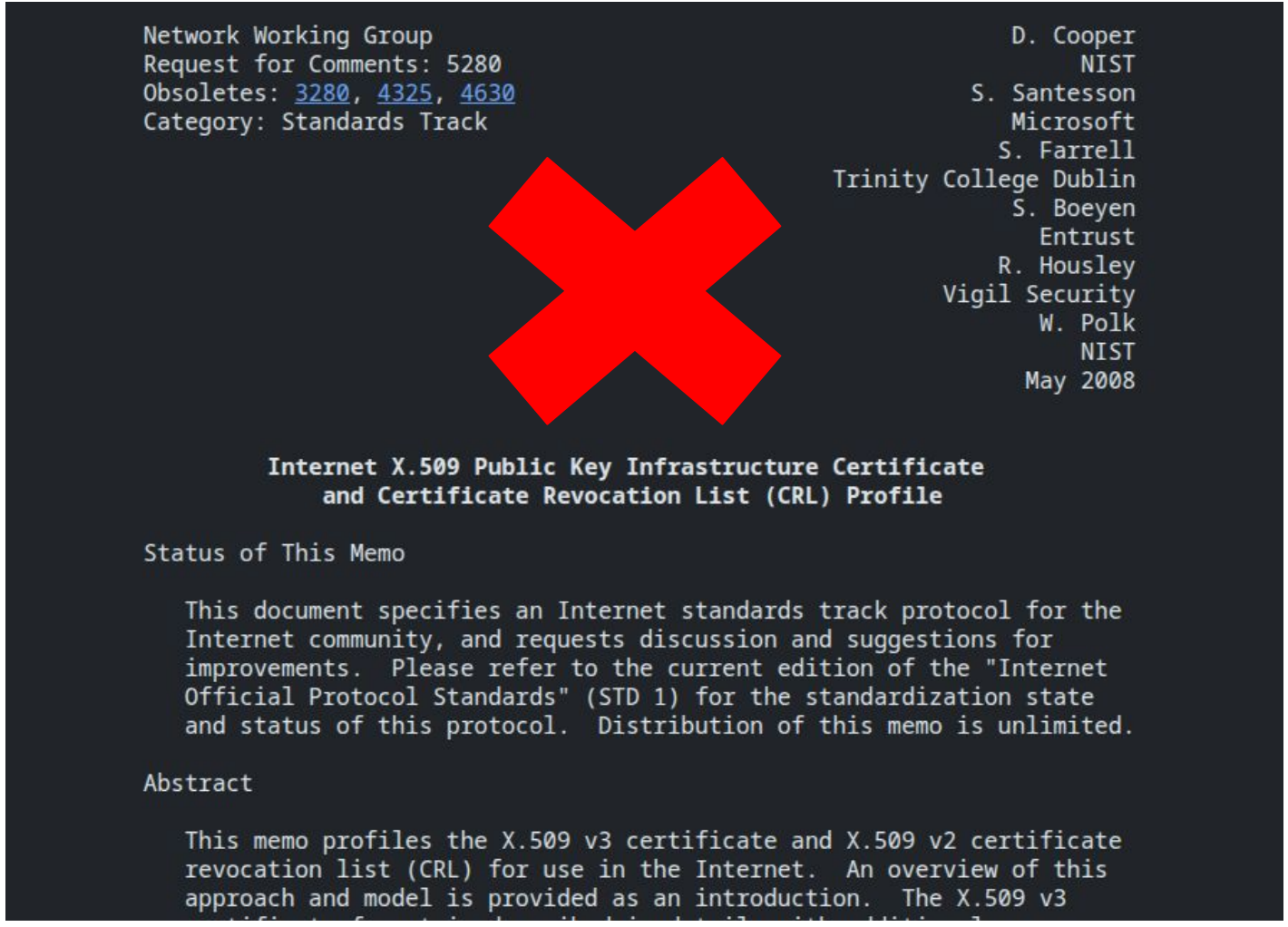
Anthony Hu
ETSI-PQC-Ottawa

Agenda

- Standards
- X.509 Certificates and the Alternative Extensions
- TLS 1.3 Handshake Messages and X9.146 Extensions
- Post-Quantum Algorithms in wolfSSL

Standards

X.509 RFC 5280



Network Working Group
Request for Comments: 5280
Obsoletes: 3280, 4325, 4630
Category: Standards Track

D. Cooper
NIST
S. Santesson
Microsoft
S. Farrell
Trinity College Dublin
S. Boeyen
Entrust
R. Housley
Vigil Security
W. Polk
NIST
May 2008

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This memo profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet. An overview of this approach and model is provided as an introduction. The X.509 v3

https://www.ietf.org/archive/id/draft-truskovsky-lamps-pq-hybrid-x509-02.txt

LAMPS
Internet-Draft
Intended status: Standards Track
Expires: 25 February 2024

A. Truskovsky
D. Van Geest
ISARA Corporation
S. Fluhrer
P. Kampanakis
Cisco Systems
M. Ounsworth
S. Mister
Entrust Datacard, Ltd

24 August 2023

Multiple Public-Key Algorithm X.509 Certificates
draft-truskovsky-lamps-pq-hybrid-x509-02

Abstract

Tombstone notice:

This draft is no longer being pursued at the IETF. A variant of this proposal was adopted in [itu-t-x509-2019], which allows two keys to

ITU-T X.509

https://www.itu.int/rec/T-REC-X.509-201910-I/en

9.8 Alternative cryptographic algorithms and digital signature extensions

9.8.1 Introduction

There is a need to provide capabilities for easy migration within a PKI from one set of cryptographic algorithms to another more suitable set of cryptographic algorithms. The following cryptographic algorithm and digital signature extensions are defined for that purpose:

a) subject alternative public key information extension;

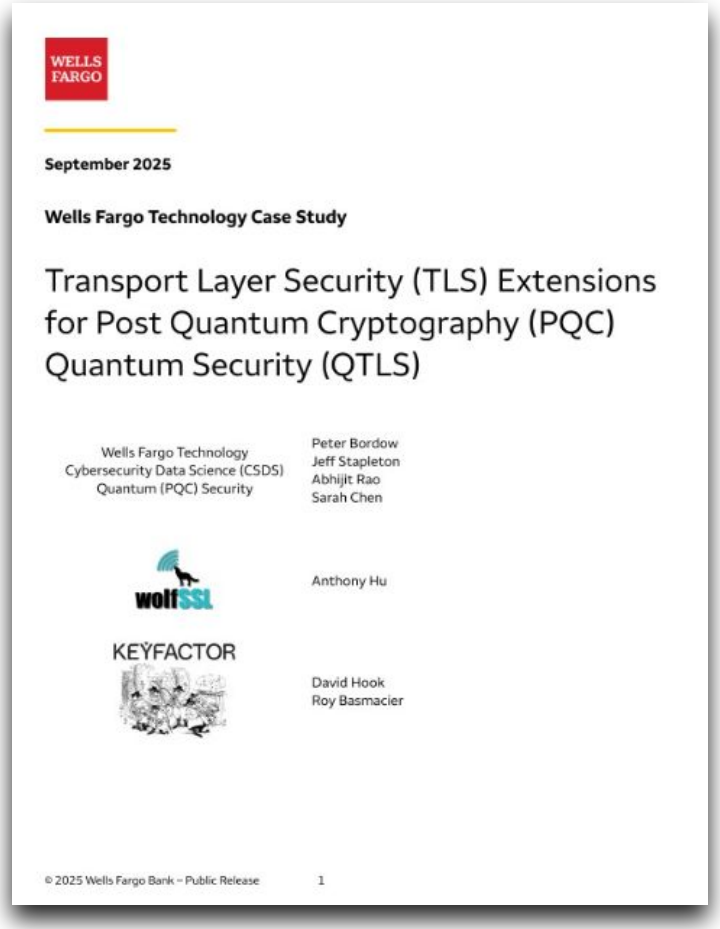
b) alternative digital signature algorithm extension; and

c) alternative signature value extension.

These extensions may be included in both CA certificates and end-entity public-key certificates. Alternative digital signature algorithm extension and alternative signature value extension may also be used as CRL and AVL extensions.

X9.146 (Peter Bordow and Jeff Stapleton)

https://www.linkedin.com/feed/update/urn:li:activity:7379627562072936448/



WELLS FARGO

September 2025

Wells Fargo Technology Case Study

Transport Layer Security (TLS) Extensions for Post Quantum Cryptography (PQC) Quantum Security (QTLS)

Wells Fargo Technology
Cybersecurity Data Science (CSDS)
Quantum (PQC) Security

Peter Bordow
Jeff Stapleton
Abhijit Rao
Sarah Chen

wolfSSL

Anthony Hu

KEYFACTOR

David Hook
Roy Basmacier

X9.146 (Peter Bordow and Jeff Stapleton)

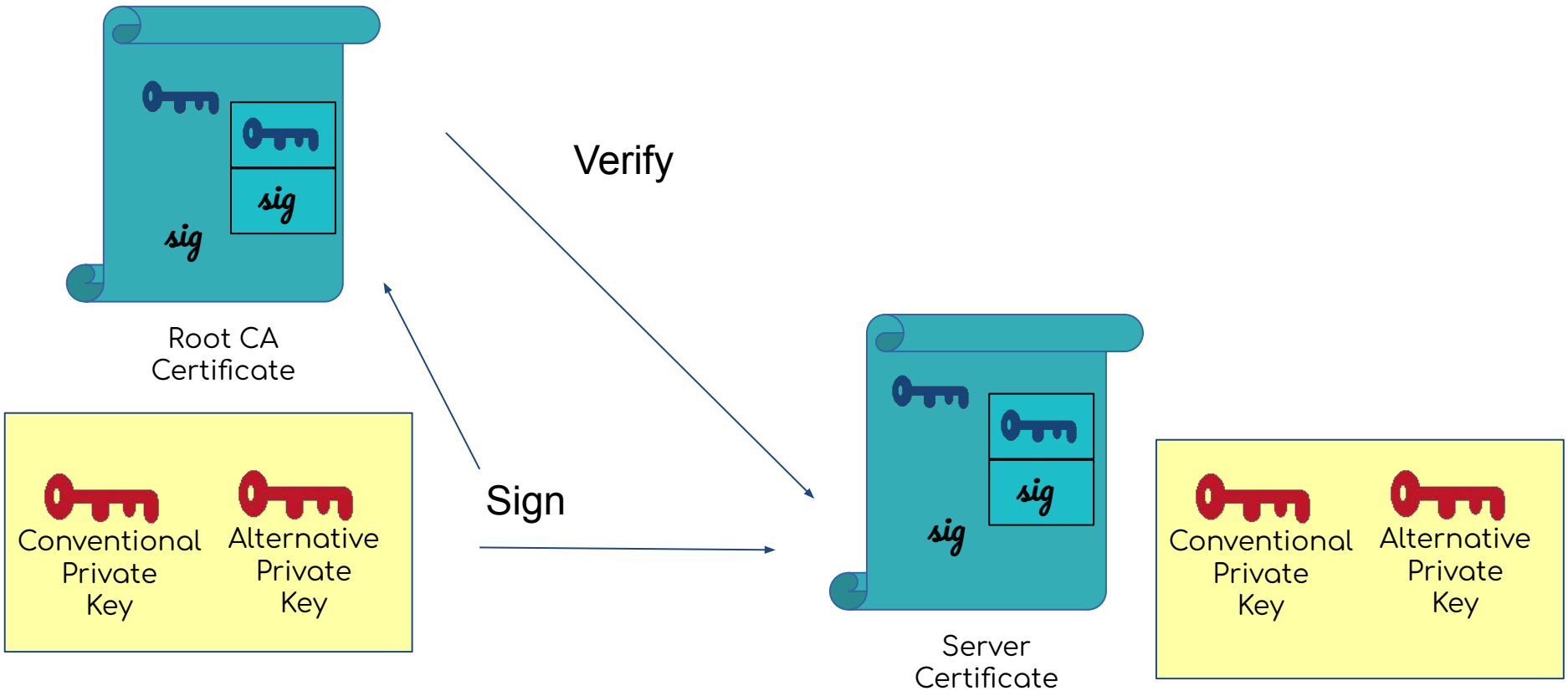
https://www.linkedin.com/feed/update/urn:li:activity:7379627562072936448/

"The X9F5 Financial PKI Workgroup will continue developing the X9.146 standard."

Peter Bordow

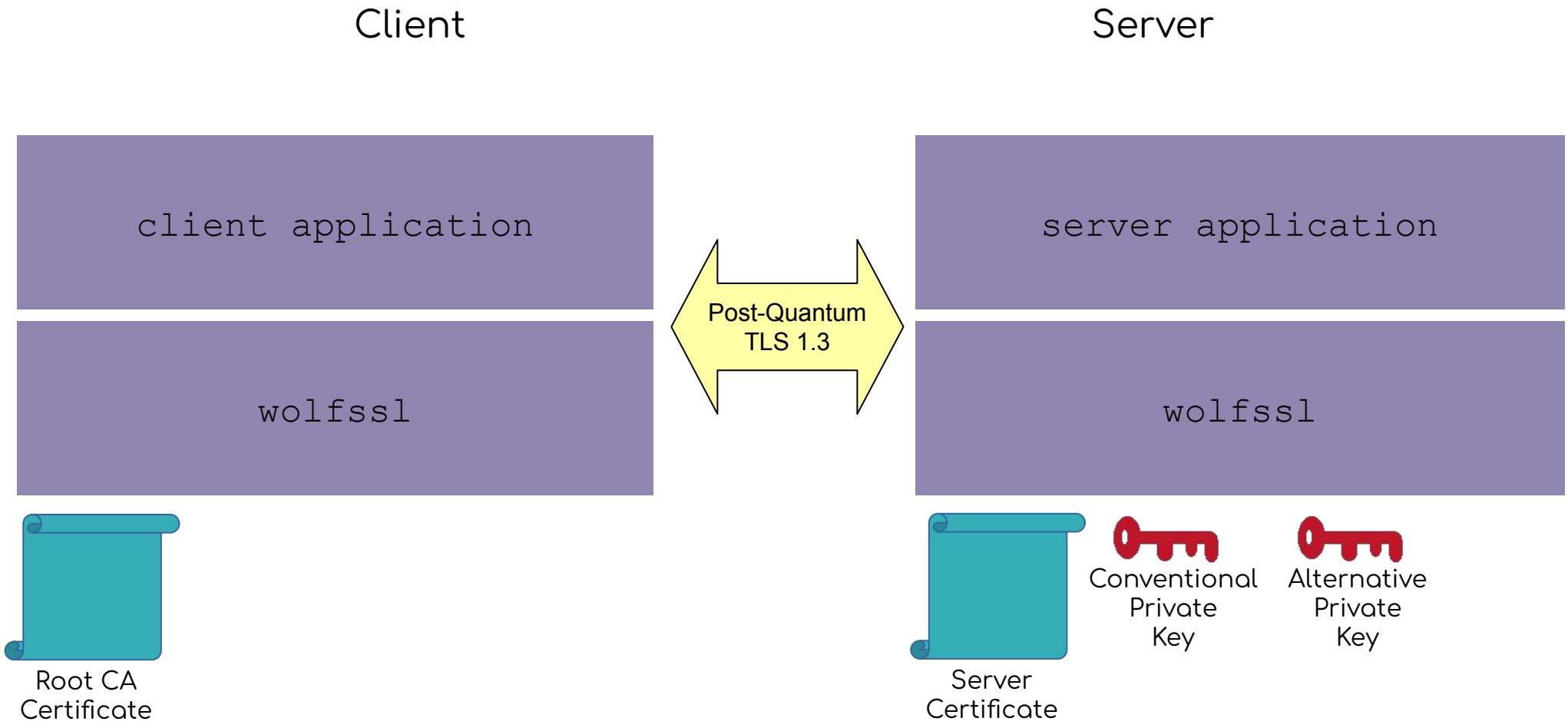
X.509 Certificates and the Alternative Extensions

Chimera Certificate Chains



TLS 1.3 Handshake Messages and X9.146 Extensions

A TLS 1.3 Connection



Hybrid Scheme List (HSL) Extension (ClientHello & ServerHello)

Field Name	Extension Type	Payload Length	CKS Signature Specification
Content	0xFFFF	0x0002	0x0001

0xFF designates Personal Use

0xFF Placeholder; TBD

Possible Values

Meaning	Value
NONE	0x0000
CHIMERA	0x0001
COMPOSITE	0x0002
DUAL CERT	0x0100
CERT + PSK	0x0200
RESERVED	0xFFFF

Certificate Key Selection (CKS) Extension (CertificateVerify)

Field Name	Extension Type	Payload Length	CKS Signature Specification
Content	0xFF92	0x0001	0x02

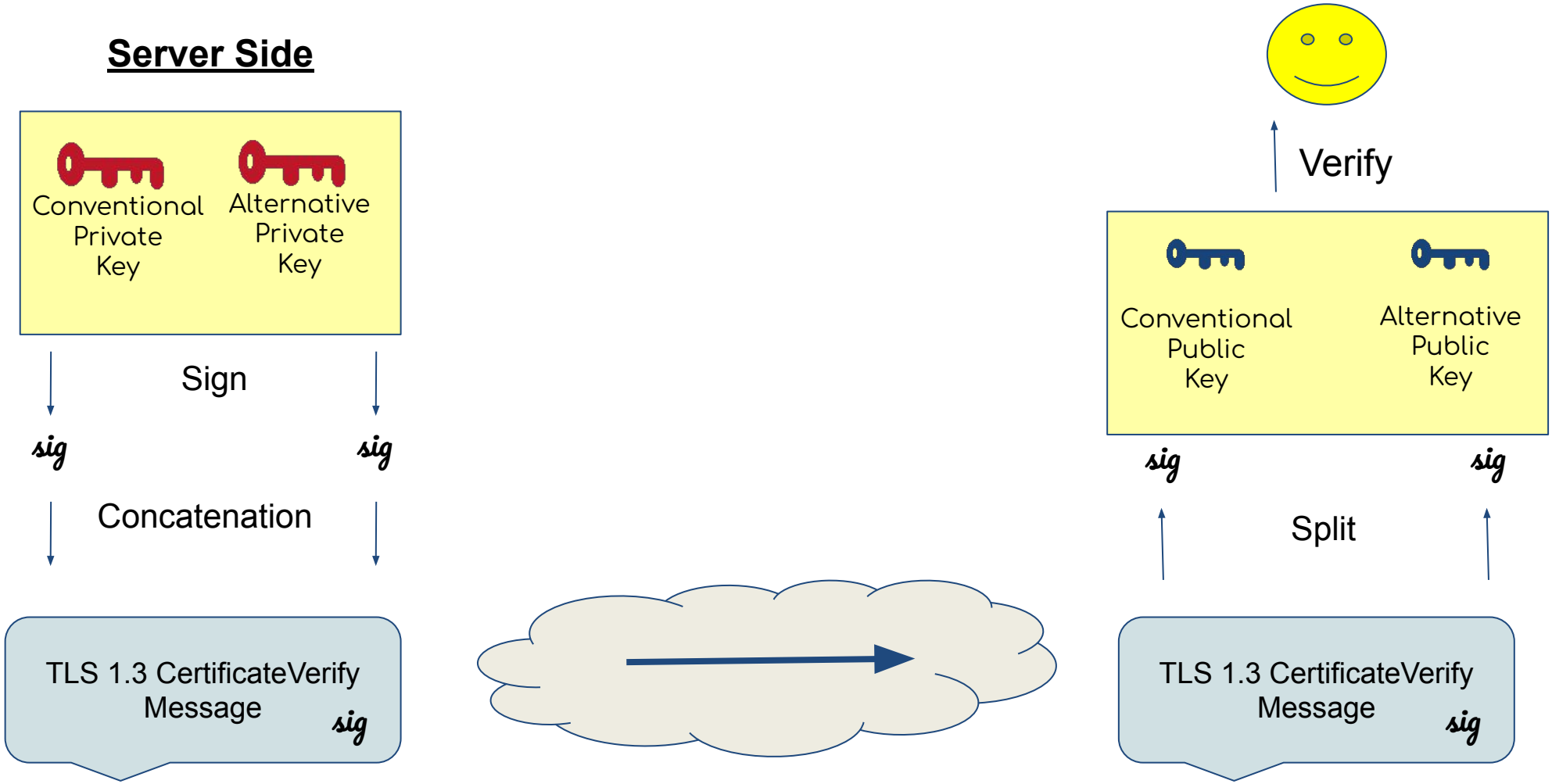
0xff designates Personal Use

0x92 is hexadecimal for 146

Possible Values

Meaning	Value
CLASSICAL (default)	0x00
CHIMERA Native	0x01
CHIMERA Alt	0x02
CHIMERA Hybrid	0x03
Composite Hybrid	0x04
DUAL CERT Hybrid	0x05
RESERVED	0xFE
EXTERNAL	0xFF

Handshake Authentication



Post-Quantum Algorithms in wolfSSL

Implemented Post-Quantum Algorithms and Variants

Signature Schemes

- ML-DSA 44
- ML-DSA 65
- ML-DSA 87
- LMS/HSS (not appropriate for TLS)
- XMSS/XMSS^MT (not appropriate for TLS)
- SLH-DSA (Many variants)

KEM Groups

- ML-KEM 512
- ML-KEM 768
- ML-KEM 1024

Hybrid Groups

- SecP256r1MLKEM512
- SecP384r1MLKEM768
- SecP521r1MLKEM1024
- SecP256r1MLKEM768
- SecP521r1MLKEM1024
- SecP384r1MLKEM1024
- X25519MLKEM512
- X25519MLKEM768
- X448MLKEM768

Hybrid Signatures

- P-256 and ML-DSA44
- P-384 and ML-DSA65
- P-521 and ML-DSA87
- RSA-3072 and ML-DSA44

Questions?

Email: facts@wolfssl.com