TECHNOLOGY OVERVIEW

TLSH

Hybrid Post-Quantum TLS 1.3



Architecture, cryptography, performance and compatibility

QSA_TLSH

OPT_TLSH

TLS 1.3 CORE

OVERVIEW

TLSH at a glance

Three complementary goals, one coherent chain of trust.

SECURE

Establish session secrets using both classical and post-quantum mechanisms.

OPTIMIZE

Manage the additional overhead of key exchanges and certificates.

DEPLOY

Integrate with TLS 1.3 infrastructure and support a gradual transition.

AGENDA

Presentation roadmap

Six chapters, from the challenge to validation.

01 Why hybrid TLS?

02 TLSH technology portfolio

03 Key exchange and signatures

04 How TLS 1.3 works

05 OPT_TLSH network optimization

06 Interoperability, testing and roadmap

CHAPTER 01

Pourquoi un TLS hybride ?

Understanding quantum risk and the cryptographic transition.

The challenge ahead

The “harvest now, decrypt later” threat is driving migration.

TODAY

TLS protects communications through public-key algorithms and symmetric encryption.

TOMORROW

Sufficiently capable quantum computers could weaken classical public-key mechanisms.

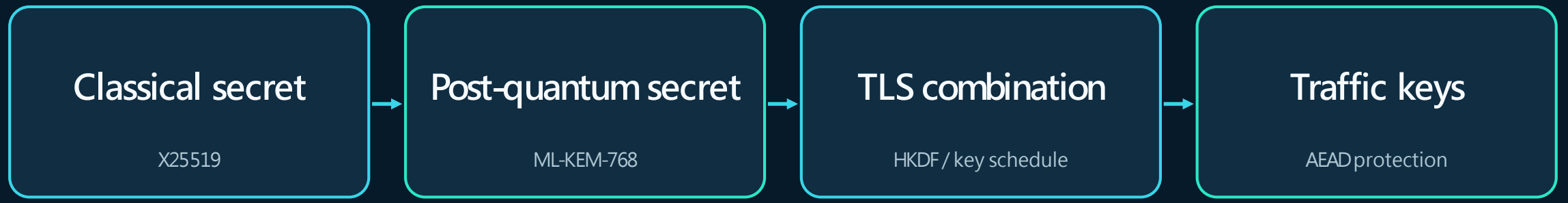
START NOW

The goal is to prepare communications before existing mechanisms are compromised.

CONCEPT

Classical + post-quantum = hybrid

Two independent contributions to the session secret.



The combiner's security depends on its construction and cryptographic assumptions.

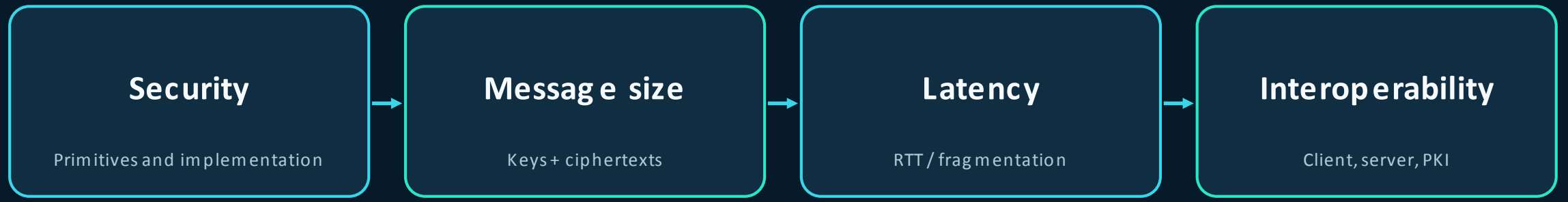
OBJECTIVES

What TLSH is designed to deliver

- Parameter negotiation within TLS 1.3.
- Hybrid key establishment combining classical and post-quantum mechanisms.
- A progressive evolution of certificates and authentication.
- Operational compatibility demonstrated through testing.

Migration involves trade-offs

There is more to it than algorithm strength.



CHAPTER 02

Three components. One solution.

The technology portfolio described in the source document.

COMPONENTS

Architecture at a glance

Two specialized technologies and a protocol-compliant core.

QSA_TLSH

Cryptographic core for hybrid exchanges and digital signatures.

OPT_TLSH

Optimization of network exchanges and operational overhead.

TLS 1.3 CORE

Protocol integration, message handling, negotiation and interoperability.

DATA FLOW

A layered architecture

Separating primitives, negotiation and transport.



OPT_TLSH: cross-layer exchange optimization

COMPONENT A

QSA_TLSH: cryptographic core

Designed around composable and auditable primitives.



Constant-time and side-channel resistance goals require measurement and audit.

SECURITY

QSA design principles

Requirements to prove, not properties to assume.

EXECUTION

Aim for secret-independent execution wherever required by a primitive.

RESILIENCE

Reduce side-channel leakage and key-management risks.

COMPLIANCE

Rely on recognized standards without confusing specification and certification.

COMPONENT B

OPT_TLSH: network efficiency

Post-quantum cryptography increases the size of some messages.



Every optimization must preserve TLS 1.3 formats, limits and cryptographic invariants.

COMPONENT C

The TLS 1.3 core

The protocol is not reinvented: TLS 1.3 compatibility is essential.

HANDSHAKE

Negotiation, key establishment, authentication and transcript verification.

RECORD

Protection of application data using authenticated encryption.

ALERTS

Error handling and connection termination.

CHAPTER 03

Hybrid cryptography



X25519, ML-KEM, signatures and hash functions.

The default hybrid group

Combining classical and post-quantum algorithms.



Another configuration mentioned in the source: SecP256r1MLKEM768.

PARAMETERS

ML-KEM: three parameter sets

FIPS 203 specifies ML-KEM-512, ML-KEM-768 and ML-KEM-1024.

ML-KEM-512

Security level 1

ML-KEM-768

Security level 3 — TLSH default

ML-KEM-1024

Security level 5 — larger option

CRYPTO FLOW

How a session secret is established

Conceptual view of a hybrid exchange.



The byte encoding and combination order follow the negotiated hybrid group specification.

AUTHENTICATION

Authenticating the TLS peer

A post-quantum key exchange does not automatically provide post-quantum authentication.

CERTIFICATES

The X.509 chain and trusted authorities remain part of authentication.

SIGNATURES

ML-DSA is standardized in FIPS 204; its use in TLS must be negotiated and interoperable.

TRANSITION

Coexistence with RSA / ECDSA depends on PKI, clients, servers and policy.

SIGNATURES

ML-DSA and FN-DSA: two paths

Two signature mechanisms planned for QSA_TLSH.

ML-DSA-44

Post-quantum signature standardized by FIPS 204. A target option for the project.

FN-DSA-512

Falcon: a candidate component, subject to verification of FIPS 206 status and applicable profiles.

SHA-3 and SHAKE within the primitives

FIPS 202 defines Keccak-based functions.

SHA-3

Cryptographic hash functions, including SHA3-256 and SHA3-384.

SHAKE

Extendable-output functions (XOFs) used in many post-quantum constructions.

Three essential distinctions

- A standardized algorithm is not necessarily a certified product.
- Theoretically secure cryptography does not guarantee a side-channel-resistant implementation.
- A capability in the crypto engine may not be available in every TLS stack.
- The available profiles depend on the library, PKI and software versions.

CHAPTER 04

Inside TLS 1.3 messages

The modern handshake and protected data processing.

Simplified TLS 1.3 sequence

Example of hybrid negotiation with server authentication.

CLIENT	ClientHello + hybrid key_share
SERVER	ServerHello + hybrid key_share
SERVER	EncryptedExtensions + Certificate + CertificateVerify + Finished
CLIENT	Finished
EXCHANGE	Application Data — encrypted

CLIENT HELLO

The client advertises its capabilities

The hybrid group is advertised through TLS extensions.



SERVER HELLO

The server selects a shared group

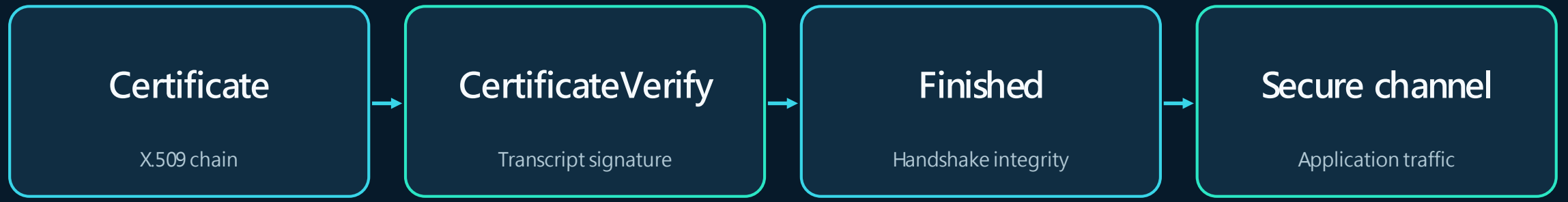
The selection must match the client’ s offer.



CERTIFICATE

Authentication and verification

Trust requires more than the key exchange alone.



TLS RECORD

Three layers of channel protection

TLS 1.3 uses AEAD cipher suites to protect application records.

CONFIDENTIALITY

Application data is encrypted using keys derived from the handshake.

INTEGRITY

Authenticated encryption detects unauthorized modifications.

AUTHENTICATION

Certificates and cryptographic checks bind the session to the intended peer.

The application data path

The Record protocol packages data into protected TLS records.



Legacy TLS compression is not a negotiated feature of TLS 1.3.

Do not mix up TLS 1.2 and TLS 1.3

The source document also describes legacy handshake messages.

Legacy TLS 1.2 messages

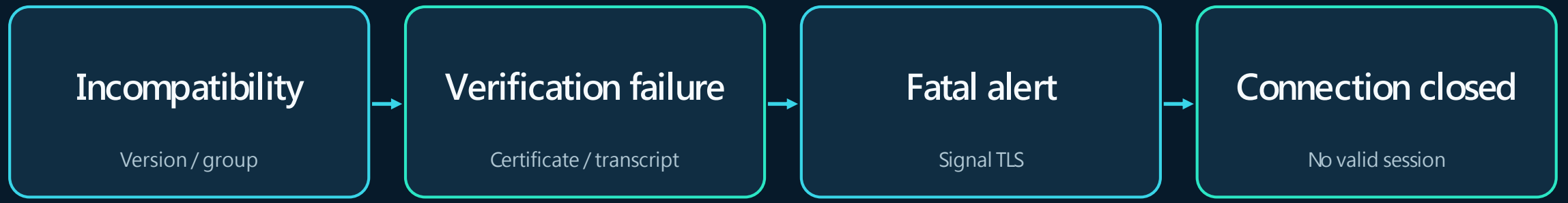
ServerKeyExchange, ServerHelloDone and ClientKeyExchange belong to the TLS 1.2 handshake.

Handshake TLS 1.3

ClientHello / ServerHello extensions, encrypted messages and the key schedule define the modern flow.

Connection failures and termination

A security mechanism must fail explicitly.



ChangeCipherSpec is not the key transition mechanism in TLS 1.3.

CHAPTER 05

Optimize without weakening security

OPT_TLSH: measure, adapt and preserve TLS invariants.

PERFORMANCE

Why message size matters

Hybrid group selection affects transmission overhead.

PACKETS

Post-quantum public keys and ciphertexts increase the volume of exchanged data.

NETWORK

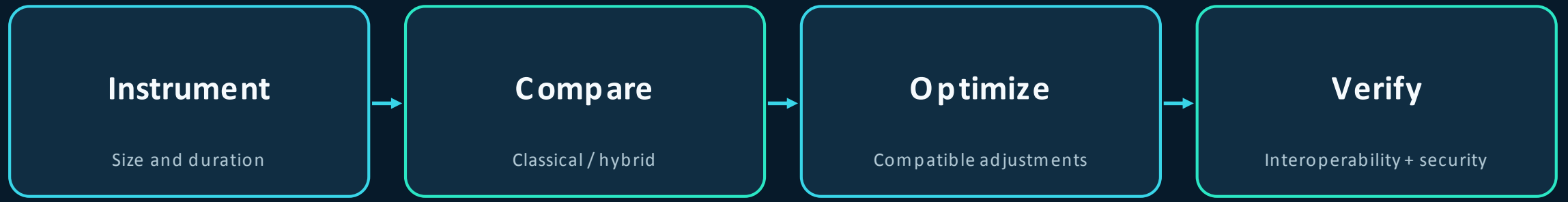
MTU, IP fragmentation and TCP segmentation may affect transmission.

LATENCY

Connection establishment time also depends on RTTs and cryptographic processing.

The OPT_TLSH measurement loop

Measure before claiming performance gains.



METRICS

A validation dashboard

Metrics to capture for each test scenario.

Handshake bytes	Total bytes sent / received
Handshake duration	Median and percentiles
Number of records	Packetization and segmentation
CPU / memory	Client and server overhead
Success rate	Errors and failed negotiations

SAFEGUARDS

What optimization must never do

TLS 1.3 security requirements take priority over saving bytes.

01 Do not alter standardized messages arbitrarily.

02 Do not compress secrets or reintroduce TLS compression.

03 Do not weaken the key schedule or authentication.

04 Do not conceal negotiation failures.

CHAPTER 06

From design to evidence

Compatibility, cryptographic qualification and field validation.

An essential compatibility matrix

Distinguish explicit classical fallback from silent downgrades.

CLIENT	SERVER	EXPECTED RESULT
Hybrid	Hybrid	Hybrid group if mutually supported
Hybrid	Classical TLS 1.3	Classical if allowed by policy
Classical TLS 1.3	Hybrid	Classical if permitted
TLS 1.2	TLSH hybrid TLS 1.3	No TLS 1.3 hybrid group

The validation campaign

Evidence and reporting matter as much as the architecture.

CRYPTOGRAPHY

Test vectors, controlled failures, combiner checks and key properties.

PROTOCOL

Diverse clients and servers, packet captures, failure cases and negotiation policies.

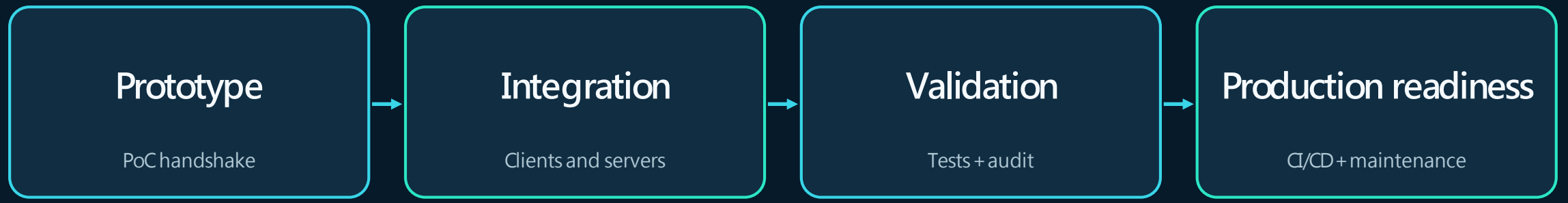
PERFORMANCE

Size, RTT, CPU, memory and stability measurements under degraded networks.

VALIDATION

A four-phase progression

From technical demonstration to operational confidence.



Standards guiding the project

Distinguish finalized standards, deployment profiles and certification status.

FIPS 202	SHA-3 / SHAKE
FIPS 203	ML-KEM
FIPS 204	ML-DSA
FIPS 206	FN-DSA: finalization status to be checked
TLS 1.3	RFC 8446 and hybrid group specifications

RISKS

Key areas requiring attention

A transparent view of dependencies and limitations.

PKI

Actual support for PQ certificates and signatures

Libraries

Versions, providers and key management

Performance

Network and compute costs under load

Certification

Gap between standardization and official validation

OVERVIEW

Secure the transition. Manage the complexity.

TLSH combines a hybrid cryptographic architecture, network optimization goals and an interoperable TLS 1.3 foundation.

Five takeaways for decision-makers

01 TLSH targets TLS 1.3, not an incompatible proprietary variant.

02 X25519+ ML-KEM-768 is the reference hybrid configuration.

03 ML-DSA addresses authentication; FN-DSA depends on its standardization status.

04 OPT_TLSH must demonstrate measurable gains without compromising TLS.

05 Qualification requires testing, interoperability and audits.

TLSH

Hybrid Post-Quantum TLS 1.3



Architecture • Hybrid exchange • Signatures • Performance • Interoperability

Technology presentation