TECHNOLOGY OVERVIEW

TLSH

Hybrid Post-Quantum TLS 1.3



Architecture, cryptographie, performances et compatibilité

QSA_TLSH

OPT_TLSH

TLS 1.3 CORE

SYNTHÈSE

La proposition TLSH en un regard

Trois ambitions complémentaires, une chaîne de confiance cohérente.

SÉCURISER

Établir des secrets de session à partir de mécanismes classiques et post-quantiques.

OPTIMISER

Prendre en compte les volumes supplémentaires des échanges et des certificats.

DÉPLOYER

S’ intégrer aux infrastructures TLS 1.3 et anticiper une transition progressive.

PLAN

Le parcours de la présentation

Six chapitres, du besoin à la qualification.

01 Pourquoi le TLS hybride ?

02 Portefeuille technologique TLSH

03 Échange de clés et signatures

04 Fonctionnement de TLS 1.3

05 Optimisation réseau OPT_TLSH

06 Interopérabilité, essais et feuille de route

CHAPITRE 01

Pourquoi un TLS hybride ?

Comprendre le risque quantique et la transition cryptographique.

ENJEU

Le défi à résoudre

Le risque « récolter aujourd’ hui, déchiffrer demain » motive la migration.

AUJOURD’ HUI

TLS protège les communications grâce à des algorithmes de clé publique et au chiffrement symétrique.

DEMAIN

Des capacités quantiques suffisamment avancées pourraient fragiliser des mécanismes classiques de clé publique.

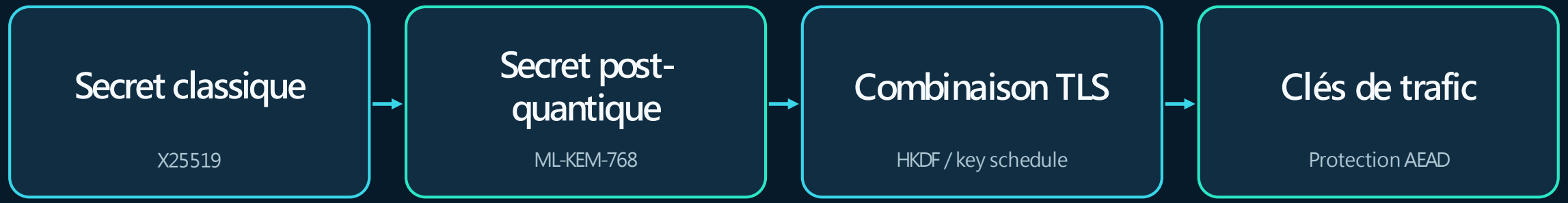
DÈS MAINTENANT

L’ objectif est de préparer les échanges, sans attendre la rupture des mécanismes actuels.

CONCEPT

Classique + post-quantique = hybride

Deux contributions indépendantes au secret de session.



La sécurité du combinateur dépend de sa construction et de ses hypothèses cryptographiques.

OBJECTIFS

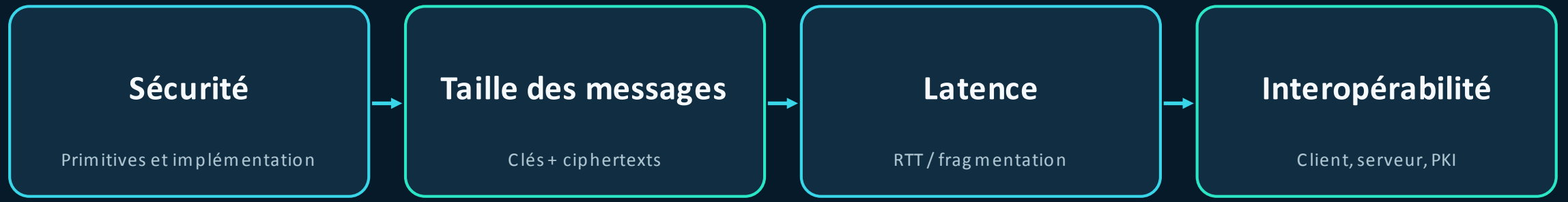
Ce que le TLSH vise à garantir

- Une négociation des paramètres au sein de TLS 1.3.
- Un établissement hybride de clés avec un mécanisme classique et un mécanisme post-quantique.
- Une évolution progressive des certificats et de l’ authentification.
- Une compatibilité opérationnelle vérifiable par essais.

CONTRAINTES

La migration exige des arbitrages

Au-delà de la solidité des algorithmes.



CHAPITRE 02

Trois composants. Une solution.

Le portefeuille technologique décrit dans le document source.

COMPOSANTS

Vue d ensemble de l architecture

Deux briques technologiques spécialisées et un cœur conforme au protocole.

QSA_TLSH

Noyau cryptographique pour les échanges hybrides et les fonctions de signature.

OPT_TLSH

Optimisation des échanges réseau et de leur coût opérationnel.

TLS 1.3 CORE

Intégration du protocole, des messages, de la négociation et de l’ interopérabilité.

Une architecture en couches

Séparer primitives, négociation et transport.



OPT_TLSH : optimisation transversale des échanges

COMPOSANT A

QSA_TLSH : noyau cryptographique

La conception vise des primitives composables et auditables.



Les objectifs constant-time et résistance aux canaux auxiliaires nécessitent des mesures et audits.

Les engagements de conception du QSA

Des exigences à démontrer, pas des propriétés présumées.

EXÉCUTION

Viser une exécution indépendante des secrets lorsqu'une primitive l'exige.

ROBUSTESSE

Réduire les risques de fuites par les canaux auxiliaires et de mauvaise gestion des clés.

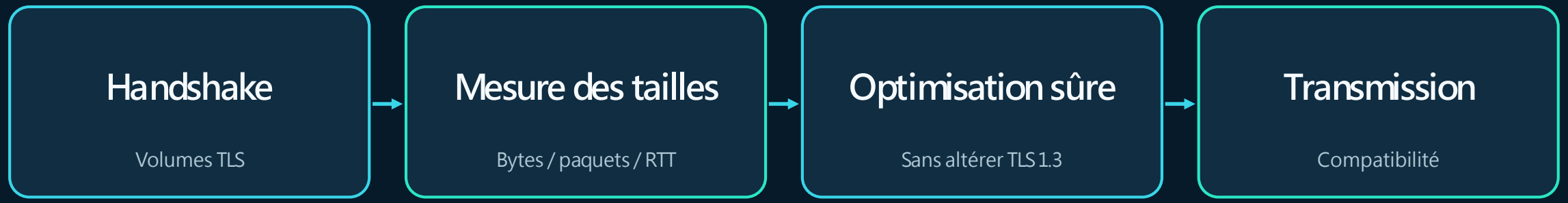
CONFORMITÉ

S'appuyer sur des standards reconnus sans confondre spécification et certification.

COMPOSANT B

OPT_TLSH : l'efficacité réseau

La cryptographie post-quantique augmente la taille de certains messages.



Toute optimisation doit respecter les formats, limites et invariants cryptographiques de TLS 1.3.

COMPOSANT C

Le cœur TLS 1.3

Le protocole n’ est pas réinventé : la compatibilité TLS 1.3 est centrale.

HANDSHAKE

Négociation, établissement des clés, authentification et vérification du transcript.

RECORD

Protection des données applicatives par chiffrement authentifié.

ALERTES

Gestion des erreurs et des interruptions de connexion.

CHAPITRE 03

Cryptographie hybride



X25519, ML-KEM, signatures et fonctions de hachage.

Le groupe hybride par défaut

Association du classique et du post-quantique.



Une autre configuration mentionnée dans la source : SecP256r1MLKEM768.

PARAMÈTRES

ML-KEM : trois niveaux de paramètres

FIPS 203 définit ML-KEM-512, ML-KEM-768 et ML-KEM-1024.

ML-KEM-512

Niveau de sécurité 1

ML-KEM-768

Niveau de sécurité 3 — choix TLSH par défaut

ML-KEM-1024

Niveau de sécurité 5 — option plus volumineuse

Comment naît un secret de session

Schéma conceptuel d’ un échange hybride.



Les octets et l’ ordre de combinaison suivent la spécification du groupe hybride négocié.

Authentifier le pair TLS

L'échange de clés post-quantique ne rend pas automatiquement l'authentification post-quantique.

CERTIFICATS

La chaîne X.509 et les autorités de confiance restent une composante de l'authentification.

SIGNATURES

ML-DSA est standardisé dans FIPS 204 ; son emploi en TLS doit être négocié et interopérable.

TRANSITION

Coexistence avec RSA / ECDSA selon la PKI, les clients, les serveurs et les politiques.

SIGNATURES

ML-DSA et FN-DSA : deux trajectoires

Deux fonctions prévues par QSA_TLSH.

ML-DSA-44

Signature post-quantique normalisée par FIPS 204.
Option ciblée pour le projet.

FN-DSA-512

Falcon : composant envisagé sous réserve de vérification de l’ avancement de FIPS 206 et des profils applicables.

SHA-3 et SHAKE dans les primitives

FIPS 202 définit les fonctions fondées sur Keccak.

SHA-3

Fonctions de hachage cryptographique, notamment SHA3-256 et SHA3-384.

SHAKE

Fonctions à sortie extensible (XOF), utilisées dans de nombreuses constructions post-quantiques.

Séparer trois notions cruciales

- Un algorithme standardisé n’est pas nécessairement un produit certifié.
- Une cryptographie théoriquement sûre n’implique pas automatiquement une implémentation résistante aux canaux auxiliaires.
- Une capacité du moteur crypto n’implique pas sa disponibilité dans chaque pile TLS.
- Les profils exacts dépendent de la bibliothèque, de la PKI et des versions.

CHAPITRE 04

Dans les messages TLS 1.3

Le handshake moderne et le traitement des données protégées.

Séquence simplifiée TLS 1.3

Exemple de négociation hybride avec authentification du serveur.

CLIENT	ClientHello + key_share hybride
SERVEUR	ServerHello + key_share hybride
SERVEUR	EncryptedExtensions + Certificate + CertificateVerify + Finished
CLIENT	Finished
ÉCHANGE	Application Data — protégées

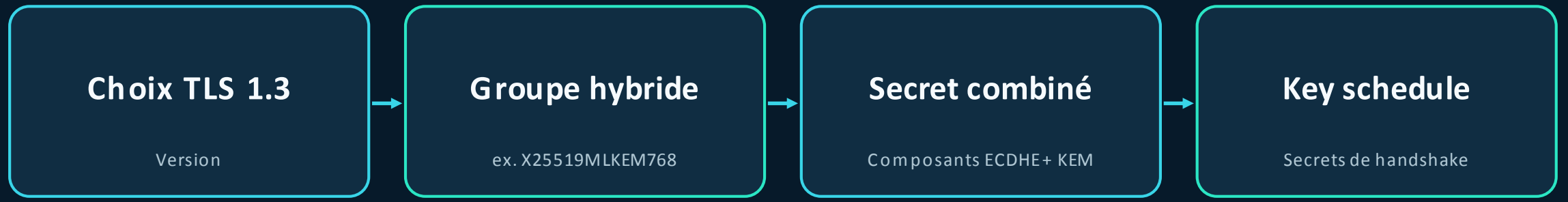
Le client annonce ses capacités

Le groupe hybride est transporté au sein des extensions TLS.



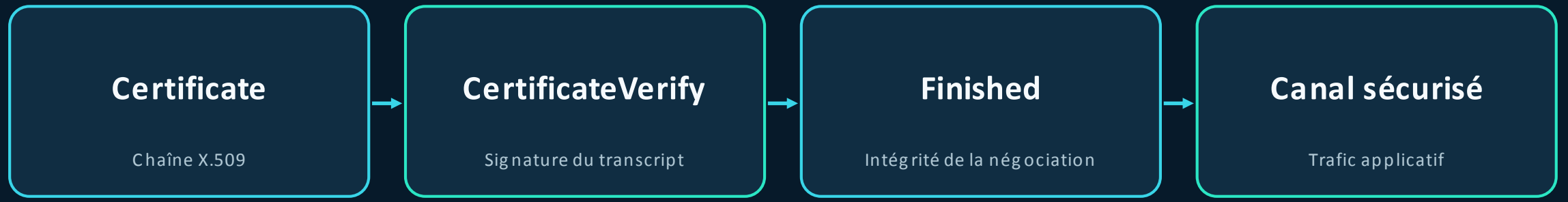
Le serveur choisit un groupe commun

La négociation doit respecter l'offre du client.



Authentification et vérification

La confiance ne dépend pas du seul échange de clés.



Les trois protections du canal

TLS 1.3 utilise des suites AEAD pour les enregistrements applicatifs.

CONFIDENTIALITÉ

Les données applicatives sont chiffrées avec des clés dérivées de la négociation.

INTÉGRITÉ

Le chiffrement authentifié détecte les modifications non autorisées.

AUTHENTIFICATION

Certificats et vérifications cryptographiques lient la session au pair attendu.

Le chemin des données applicatives

Le protocole Record transforme les octets en enregistrements protégés.



La compression TLS historique n’ est pas une fonction négociée de TLS 1.3.

DIFFÉRENCES

Ne pas mélanger TLS 1.2 et TLS 1.3

Le document source évoque des messages hérités des anciennes versions.

Messages historiques TLS 1.2

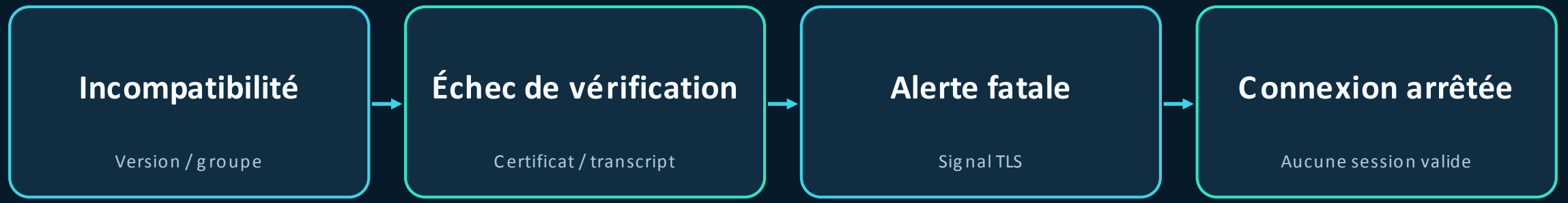
ServerKeyExchange, ServerHelloDone et ClientKeyExchange appartiennent au modèle de handshake TLS 1.2.

Handshake TLS 1.3

Les extensions de ClientHello / ServerHello, les messages chiffrés et le key schedule constituent le flux moderne.

Échecs et interruptions de connexion

Un mécanisme de sécurité doit échouer de manière explicite.



ChangeCipherSpec n’ est pas le mécanisme de bascule des clés dans TLS 1.3.

CHAPITRE 05

Optimiser sans affaiblir

OPT_TLSH : mesurer, adapter et préserver les invariants TLS.

Pourquoi la taille des messages compte

Les choix de groupes impactent les coûts de transmission.

PAQUETS

Les clés publiques et ciphertexts post-quantiques augmentent les volumes échangés.

RÉSEAU

MTU, fragmentation IP ou segmentation TCP peuvent peser sur la transmission.

LATENCE

Le temps d' établissement dépend aussi des RTT et du traitement cryptographique.

La boucle de mesure OPT_TLSH

Mesurer avant d'affirmer un gain de performance.



MÉTRIQUES

Un tableau de bord de qualification

Indicateurs à produire pour chaque scénario.

Bytes handshake	Volume total émis / reçu
Durée handshake	Médiane et percentiles
Nombre de records	Empaquetage et segmentation
CPU / mémoire	Coût client et serveur
Taux de succès	Erreurs et négociations invalides

GARDE-FOUS

Ce que l'optimisation ne doit pas faire

Le cadre de sécurité TLS 1.3 prime sur les économies d'octets.

01 Ne pas modifier arbitrairement les messages normalisés.

02 Ne pas compresser des secrets ou réintroduire la compression TLS.

03 Ne pas réduire la robustesse du key schedule ou de l'authentification.

04 Ne pas masquer les échecs de négociation.

CHAPITRE 06

De la conception à la preuve

Compatibilité, qualification cryptographique et validation terrain.

Une matrice de compatibilité indispensable

Ne pas confondre repli classique explicite et downgrade silencieux.

CLIENT	SERVEUR	RÉSULTAT ATTENDU
Hybride	Hybride	Groupe hybride si partagé
Hybride	Classique TLS 1.3	Classique si autorisé par la politique
Classique TLS 1.3	Hybride	Classique si permis
TLS 1.2	TLSH hybride TLS 1.3	Pas de groupe hybride TLS 1.3

La campagne de qualification

Les preuves et les rapports comptent autant que l'architecture.

CRYPTOGRAPHIE

Vecteurs de tests, erreurs contrôlées, validation des combinateurs et propriétés des clés.

PROTOCOLE

Clients et serveurs différents, captures d'échanges, cas d'échec et politiques de négociation.

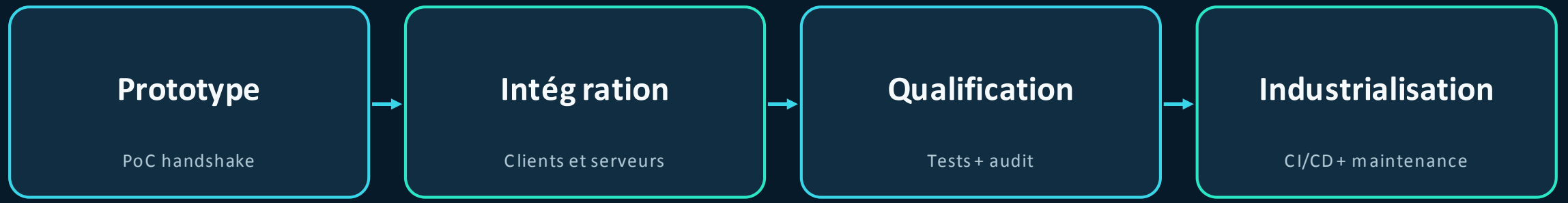
PERFORMANCE

Mesures de taille, RTT, CPU, mémoire et stabilité en réseau dégradé.

VALIDATION

Une progression en quatre phases

De la démonstration technique au niveau de confiance opérationnel.



Standards : les repères du projet

Distinguer standards finalisés, profils d’emploi et statut de certification.

FIPS 202	SHA-3 / SHAKE
FIPS 203	ML-KEM
FIPS 204	ML-DSA
FIPS 206	FN-DSA : état de finalisation à vérifier
TLS 1.3	RFC 8446 et spécifications des groupes hybrides

RISQUES

Les principaux points d'attention

Une approche transparente des dépendances et des limites.

PKI

Support réel des certificats et signatures PQ

Bibliothèques

Versions, fournisseurs et gestion des clés

Performance

Coûts réseau et calcul sous charge

Certification

Écart entre standard et validation officielle

SYNTHÈSE

Sécuriser la transition. Maîtriser la complexité.

TLSH réunit une architecture cryptographique hybride, une ambition d'optimisation réseau et un socle TLS 1.3 interopérable.

Cinq messages pour décider

01 TLSH cible TLS 1.3, pas une variante propriétaire incompatible.

02 X25519 + ML-KEM-768 forme le cas d'usage hybride de référence.

03 ML-DSA relève de l'authentification ; FN-DSA reste à suivre selon son statut.

04 OPT_TLSH doit démontrer des gains mesurables sans compromettre TLS.

05 La qualification repose sur tests, interopérabilité et audits.

TLSH

Hybrid Post-Quantum TLS 1.3



Architecture • Échange hybride • Signatures • Performance • Interopérabilité

Document de présentation technologique