Protocole TLS Hybride Post-Quantique **PTH**



By **Lockheed** LLC

Novembre 2026

Auteur : Guillaume Oneill

INTÉGRATION DANS L'ÉCOSYSTÈME LINUX

Protocole TLS Hybride Post-Quantique Adaptatif pour l'IoT





Positionnement sur le serveur Linux

Le protocole est conçu comme une **brique ouverte** qui s'appuie sur le TLS existant (via des extensions) et ne réécrit pas la couche transport. Sur un serveur Linux classique, il se grefferait donc principalement :

- sur la pile TLS (OpenSSL, BoringSSL, ou équivalent avec support post-quantique),
- en complément du **module QSA** déjà développé,
- sous forme d'une extension ou d'un module configurable.

Le serveur reste un serveur TLS standard (Nginx, HAProxy, un serveur applicatif Java/Python/Go, etc.), mais enrichi de la logique adaptative et de la validation ZKP.

Positionnement sur le serveur Linux

PROTOCOLE OUVERT : BRIQUE OUVERT BASÉE SUR TLS (VIA EXTENSIONS)

S'appuie sur TLS existant via extensions • Ne réécrit pas la couche transport



BRIQUE PROTOCOLE OUVERT
EXTENSION OU MODULE CONFIGURABLE

MODULE QSA
ZÉRO-CONNAISSANCE & ADAPTATIF

PILE TLS (EXTENSIONS)
OpenSSL, BoringSSL ou équivalent avec post-quantique

RÉSEAU & TRANSPORT
TCP / IP

- GREFFE SUR LA PILE TLS
- EN COMPLÉMENT DU MODULE QSA
- SOUS FORME D'EXTENSION OU MODULE CONFIGURABLE

SERVEUR LINUX CLASSIQUE

Le serveur reste un serveur TLS standard, enrichi de logique adaptative et de validation ZKP



SERVEUR LINUX

Nginx · HAProxy · Java · Python / Go

SERVEURS & APPLICATIONS STANDARDS

ENRICHI PAR

- LOGIQUE ADAPTATIVE
- VALIDATION ZKP

TLS STANDARD RENFORCÉ

SÉCURITÉ POST-QUANTIQUE • VALIDATION ZKP • EXTENSIBLE • INTÉGRÉ À L'ÉCOSYSTÈME TLS EXISTANT

Fonctionnement du handshake adaptatif côté serveur

1. **Réception des signaux du client IoT**

   Pendant le handshake, le client envoie (via une extension TLS) trois informations :

   - niveau de batterie,
   - exigence de sécurité (Top Secret / Secret / Confidentiel),
   - qualité du réseau perçu.

2. **Application de la politique serveur**

   Le serveur dispose d'une **politique configurable** (fichier de configuration, base de règles, ou module dédié). Il croise :

   - les 3 signaux du client,
   - sa propre politique de sécurité,
   - les ressources disponibles.

3. **Sélection de la combinaison hybride**

   Il choisit dynamiquement :

   - les algorithmes (classiques + post-quantiques),
   - les paramètres adaptés (taille de clés, mode allégé ou maximal, etc.).

   Exemples :

   - Batterie faible + criticité modérée → mode allégé (moins de charge crypto et radio).
   - Transaction critique + ressources OK → protection post-quantique maximale.

4. **Interface multi-algorithmes**

   L'interface permet de brancher plusieurs primitives post-quantiques. Priorité au module QSA existant. L'architecture facilite les tests ACVP (NIST) réalisés par des laboratoires accrédités.

3. Sélection de la combinaison hybride & 4. Interface multi-algorithmes

SÉLECTION DYNAMIQUE
DE LA COMBINAISON HYBRIDE

ALGORITHMES HYBRIDES + CLASSIQUE (ex. ECC, RSA) → POST-QUANTIQUE (ex. Kyber, Dilithium)

PARAMÈTRES ADAPTÉS
TAILLE DE CLÉ & MODE OPÉRATOIRE

TAILLE DE CLÉ
LÉGÈRE OU MAXIMALE

MODE
LÉGER OU MAXIMAL

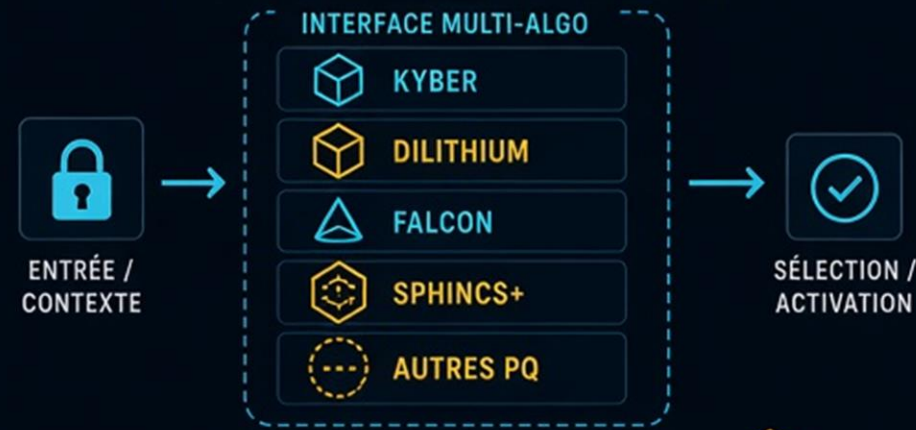
FAIBLE BATTERIE
+ CRITICITÉ MODÉRÉE
→ **MODE LÉGER**
Moins de charge crypto et radio

TRANSACTION CRITIQUE
+ RESSOURCES OK
→ **MODE MAXIMAL**
Protection post-quantique maximale

Sélection intelligente : sécurité optimale, performance adaptée.

INTERFACE MULTI-ALGORITHMES

BRANCHEMENT DE PLUSIEURS PRIMITIVES PQ



PRIORITÉ AU MODULE QSA EXISTANT
Intégration native et réutilisation des services QSA

QSA
QUANTUM SAFE ALGORITHM MODULE

ARCHITECTURE CONÇUE POUR FACILITER LES TESTS ACVP (NIST)
Prête pour les laboratoires accrédités

ACVP (NIST)
Tests par laboratoires accrédités

Sécurisation du 0-RTT par ZKP

- Un ticket de session est accompagné d'une **preuve à divulgation nulle de connaissance (ZKP)** ultra-rapide.
- Côté serveur Linux, la vérification de cette preuve est quasi instantanée.
- Résultat : le 0-RTT devient utilisable même pour des transactions critiques, sans aller-retour supplémentaire, tout en garantissant l'authenticité et en empêchant les rejeux (y compris en contexte post-quantique).

Sécurisation du 0-RTT par ZKP



RÉSULTAT :
0-RTT UTILISABLE

MÊME POUR TRANSACTIONS CRITIQUES
SANS ALLER-RETOUR SUPPLÉMENTAIRE

AUTHENTICITÉ GARANTIE
REPLAYS BLOQUÉS

RÉSISTANCE POST-QUANTIQUE
SÉCURITÉ DURABLE, MÊME FACE AUX ORDINATEURS QUANTIQUES

AUTHENTICITÉ
GARANTIE

ANTI-REPLAY
PRÉVENTION EFFICACE

POST-QUANTIQUE
PRÊT POUR L'AVENIR

Intégration typique sur Linux

Élément	Rôle sur le serveur Linux
Extension de signalisation	Reçoit et parse les 3 signaux du client
Moteur de politique	Décide du niveau hybride selon règles + état client
Interface QSA / multi-algo	Sélectionne et active les primitives (classiques + PQ)
Validateur ZKP	Vérifie le ticket de session pour le 0-RTT
Configuration	Fichiers de politique, niveaux de sécurité, seuils batterie/réseau

Le protocole ne remplace pas Nginx/OpenSSL : il s'y intègre comme couche d'adaptation et de sélection. Il reste complémentaire des produits de sécurité déjà en place.

Intégration typique sur Linux

1. Extension de signalisation
Reçoit et parse les 3 signaux client

2. Moteur de politique
Décide du niveau hybride selon règles + état client

3. Interface QSA / multi-algo
Sélectionne et active les primitives (classiques + PQ)

4. Validateur ZKP
Vérifie le ticket de session pour le 0-RTT

5. Configuration
Fichiers de politique, niveaux de sécurité, seuils batterie/réseau



SUR SERVEUR LINUX

N'REMPLACE PAS NGINX / OPENSS

IL S'INTÈGRE COMME UNE COUCHE D'ADAPTATION ET DE SÉLECTION

Rest complementary aux produits de sécurité existants.

NGINX

OPENSSL

SOLUTIONS DE SÉCURITÉ EXISTANTES

Complémentaire • Sécurisé • Performant • Post-quantique

En résumé

Sur un serveur Linux, l'outil agit comme un **orchestrateur intelligent du handshake TLS** :

- il écoute l'état réel du capteur IoT,
- il applique une politique de sécurité adaptative,
- il active le bon niveau de protection hybride post-quantique,
- et il sécurise le 0-RTT grâce aux ZKP.

Cela permet de protéger durablement les infrastructures critiques tout en respectant les contraintes énergétiques des équipements de terrain.

En résumé



SERVEUR LINUX
ORCHESTRATEUR INTELLIGENT

1. ÉCOUTE

État réel du capteur IoT

2. POLITIQUE ADAPTATIVE

Applique la politique de sécurité optimale

3.

Active le niveau de protection hybride post-quantique adapté

4. 0-RTT SÉCURISÉ

Grâce à **ZKP** (Preuve à Connaissance Nulle)

PROTÉGER LES INFRASTRUCTURES CRITIQUES, DURABLEMENT

ET RESPECTER LES CONTRAINTES ÉNERGÉTIQUES DES ÉQUIPEMENTS DE TERRAIN.

- FAIBLE EMPREINTE ÉNERGÉTIQUE
- RÉSILIENTE POST-QUANTIQUE
- SÉCURITÉ RENFORCÉE SANS COMPROMIS

• ORCHESTRATION • INTELLIGENCE • SOBRIÉTÉ • SÉCURITÉ DURABLE •

Fonctionnement de Principe attendu

Simulation du fonctionnement attendu –
Handshake adaptatif + Reprise 0-RTT sécurisée par ZKP

CLIENT IoT (CAPTEUR)

SERVEUR / GATEWAY

MODULE QSA (PRIMITIVES PQ)

MOTEUR ZKP

1 PHASE 1 – HANDSHAKE INITIAL ADAPTATIF

1. ClientHello + Extension signalisation
   - BATTERIE MOYENNE
   - SÉCURITÉ SECRET
   - RÉSEAU STABLE
   - <DÉRPPL
2. MOTEUR DE DÉCISION ADAPTATIVE
   POLITIQUE
   → MODE HYBRIDE ALLÉGÉ
   ex. Kyber-512 + AES-GCM
3. PARAMÈTRES ET CLÉS PUBLIQUES
4. ServerHello + Décision hybride
5. GÉNÉRATION / ENCAPSULATION CLÉS VIA INTERFACE MULTI-ALGO
6. GÉNÉRATION TICKET DE SESSION + PREUVE ZKP
7. SESSION CHIFFRÉE ÉTABLIE (MODE HYBRIDE ALLÉGÉ)

2 PHASE 2 – REPRISE 0-RTT

1. EARLY DATA + TICKET + PREUVE ZKP
2. VÉRIFICATION ZKP (<1 ms)
   <1 ms
3. PREUVE VALIDE
4. CONTRÔLE NIVEAU SÉCURITÉ
   (AUTORISE CAR SECRET + PREUVE OK)
5. ACCEPTATION 0-RTT
   (DONNÉES TRAITÉES IMMÉDIATEMENT)
6. SESSION REPRISE SANS ROUND-TRIP
   RÉSISTANCE QUANTIQUE + ANTI-REJEU ASSURÉES

- CHIFFREMENT HYBRIDE POST-QUANTIQUE
- ZKP = PREUVE SANS RÉVÉLER LES SECRETS
- 0-RTT RAPIDE ET SÉCURISÉE
- SÉCURITÉ ADAPTATIVE CONTEXTUELLE

Lecture du diagramme

1. **Handshake initial**
   Le client signale son état (batterie moyenne, exigence Secret, réseau stable).
   Le serveur décide d'un mode hybride allégé, interroge le module QSA pour les primitives adaptées, puis établit les clés.
   Un ticket de session accompagné d'une preuve ZKP est généré et transmis au client.
2. **Reprise 0-RTT**
   Lors d'une transmission ultérieure, le client envoie directement ses données (Early Data) avec le ticket et la preuve ZKP.
   Le serveur vérifie la preuve en moins d'1 ms. Si elle est valide et compatible avec le niveau de sécurité, les données sont acceptées immédiatement, sans aller-retour supplémentaire.
   La preuve ZKP garantit l'authenticité et empêche les rejeux, même dans un contexte post-quantique.

Ce flux illustre le fonctionnement cible : adaptation énergétique dès le premier handshake et 0-RTT sûr pour les échanges suivants, sans compromettre la résistance quantique.

Phase 1 – Handshake initial adaptatif

1 Client IoT envoie ClientHello + Extension signalisation
(Batterie: Moyenne | Sécurité: Secret | Réseau: Stable)



2 Serveur / Moteur de décision adaptative applique la politique → sélectionne Mode hybride allégé (ex. Kyber-512 + AES-GCM)

MODE HYBRIDE ALLÉGÉ
Kyber-512 + AES-GCM

3 Demande et réception des paramètres et clés publiques via Module QSA



4 ServerHello + Décision hybride + Paramètres choisis renvoyés au client

5 Génération et encapsulation des clés via l'interface multi-algorithmes

Kyber-512 | AES-GCM | ...

6 ClientKeyExchange / Finished

7 Génération du ticket de session + preuve ZKP par le Moteur ZKP

TICKET DE SESSION
ZKP PROOF

8 Session chiffrée établie en mode hybride allégé

Client IoT | Serveur/Gateway | QSA — Module Quantum-Safe Adaptatif | Moteur ZKP — Preuve à Connaissance Nulle

Phase 2 – Reprise 0-RTT sécurisée par ZKP

CLIENT IoT



Appareil connecté

① ENVOI 0-RTT

Early Data + Ticket + Preuve ZKP

SERVEUR / GATEWAY



Sécurise & autorise

② VÉRIFICATION ULTRA-RAPIDE

< 1 ms

MOTEUR ZKP



Vérification de preuve

① Client IoT envoie Early Data (0-RTT) + Ticket de session + Preuve ZKP



② Serveur / Moteur ZKP effectue la Vérification de la preuve ZKP



ULTRA-RAPIDE

③ Preuve valide.



PREUVE VÉRIFIÉE ET VALIDE

④ Contrôle du niveau de sécurité (autorise le 0-RTT car Sécurité: Secret + preuve OK)



NIVEAU DE SÉCURITÉ ACCEPTÉ

⑤ Acceptation 0-RTT – données traitées immédiatement



TRAITEMENT IMMÉDIAT SANS ATTENTE

⑥ Session reprise sans round-trip supplémentaire, Résistance quantique + anti-rejeu assurées



SANS ROUND-TRIP SUPPLÉMENTAIRE

RÉSISTANCE QUANTIQUE + + ANTI-REJEU

AUCUN ROUND-TRIP SUPPLÉMENTAIRE | ULTRA-RAPIDE • SÉCURISÉ • POST-QUANTIQUE

POSITIONNEMENT SUR LE MARCHÉ

Protocole TLS Hybride Post-Quantique Adaptatif pour l'IoT



Positionnement du produit sur le marché

Niveau de performance
(Fonctionnalités, qualité, innovation)

Élevé

Faible

PREMIUM
Haute performance
Forte valeur perçue



Notre produit
Performance supérieure et expérience premium

ÉCONOMIQUE
Performance modérée
Valeur perçue accessible

- Concurrent A
- Concurrent B
- Concurrent C

BASIQUE
Performance limitée
Valeur perçue faible

- Concurrent D
- Concurrent E

ME TOO
Performance moyenne
Valeur perçue moyenne

- Concurrent F
- Concurrent G

Faible — **Perceived Value** — Élevé

(Prix perçu, image de marque, expérience client)

Croissance du marché
+8,7%
par an

Taille du marché
42,6 Md€
en 2024

Parts de marché estimées

Premium	28%
Économique	32%
Basique	18%
Me Too	22%

Contexte du marché

Le marché de la cybersécurité des infrastructures critiques et de l'IoT industriel entre dans une phase de transformation contrainte. D'une part, la menace quantique impose, à moyen terme, le remplacement ou l'hybridation des algorithmes asymétriques classiques utilisés dans TLS. D'autre part, les équipements déployés sur le terrain (capteurs de réseaux électriques, systèmes de supervision, chaînes du froid, contrôle du trafic) restent fortement limités en autonomie, puissance de calcul et bande passante radio. Les solutions post-quantiques « lourdes » existantes ou en cours de standardisation ne sont pas adaptées à ces contraintes énergétiques et opérationnelles.

Dans ce contexte, le **Protocole TLS Hybride Post-Quantique Adaptatif pour l'IoT à Basse Consommation** se positionne comme une couche réseau spécialisée, conçue pour répondre simultanément à ces deux exigences.

Contexte du marché

CYBERSECURITY MARKET FOR CRITICAL INFRASTRUCTURES & INDUSTRIAL IoT

1. MENACE QUANTIQUE

Menace quantique impose le remplacement ou l'hybridation à moyen terme des algorithmes asymétriques classiques utilisés dans TLS.

IMPACT À MOYEN TERME → REMPLACEMENT OU HYBRIDATION

PHASE DE TRANSFORMATION CONTRAINTE

2. ÉQUIPEMENTS DE TERRAIN CONTRAINTS

Équipements de terrain fortement limités en autonomie, puissance de calcul et bande passante radio.



AUTONOMIE LIMITÉE | PUISSANCE DE CALCUL LIMITÉE | BANDE PASSANTE RADIO LIMITÉE | CONTRAINTES OPÉRATIONNELLES FORTES

SOLUTIONS PQ EXISTANTES OU EN NORMALISATION : TROP LOURDES, TROP ÉNERGIVORE, NON ADAPTÉES À CES CONTRAINTES.

PROTOCOLE HYBRIDE POST-QUANTIQUE ADAPTATIF TLS

POUR IoT À FAIBLE CONSOMMATION



SÉCURITÉ POST-QUANTIQUE dès aujourd'hui et demain

FAIBLE EMPREINTE consommation, calcul et bande passante minimisés.

ADAPTÉ AUX INFRASTRUCTURES CRITIQUES & IoT INDUSTRIEL contraintes terrain

UNE COUCHE RÉSEAU SPÉCIALISÉE QUI RÉPOND SIMULTANÉMENT À CES DEUX EXIGENCES.

Problématiques adressées

Le produit cible trois faiblesses récurrentes du marché actuel :

- L'obsolescence programmée des mécanismes TLS classiques face aux ordinateurs quantiques.
- L'incompatibilité des approches post-quantiques génériques avec les équipements IoT contraints (autonomie et trafic).
- L'absence de mécanismes permettant d'adapter dynamiquement le niveau de protection selon le contexte réel du terminal (batterie, criticité, qualité réseau) et selon la politique de l'opérateur.

Il répond également au besoin des intégrateurs de disposer d'une brique ouverte et complémentaire, capable de s'appuyer sur des modules de sécurité déjà développés (notamment le module QSA) plutôt que de remplacer l'ensemble de la pile.

PROBLÉMATIQUES ADRESSÉES

1



OBSOLESCENCE PROGRAMMÉE DES MÉCANISMES TLS CLASSIQUES

face aux ordinateurs **quantiques**

2



INCOMPATIBILITÉ DES APPROCHES POST-QUANTIQUES GÉNÉRIQUES

avec les équipements **IoT contraints** (autonomie et trafic)

3



ABSENCE DE MÉCANISMES D'ADAPTATION DYNAMIQUE

du niveau de **protection** selon le contexte réel du terminal et de la politique opérateur



BRIQUE OUVERTE ET COMPLÉMENTAIRE

Répond au besoin des intégrateurs : **s'appuyer sur** les modules de sécurité existants (notamment **QSA**) plutôt que de remplacer toute la stack.



ADAPTER. PROTÉGER. PRÉSERVER. | SÉCURITÉ POST-QUANTIQUE CONÇUE POUR LA **RÉALITÉ IoT.**

Positionnement différenciant

Le protocole se positionne comme une **brique ouverte d'adaptation et de sécurisation du handshake TLS**, et non comme un remplacement complet de la couche transport ou comme une solution post-quantique monolithique.

Ses éléments différenciants sont :

- **Adaptativité réelle** : négociation dynamique fondée sur l'état du client IoT (batterie, exigence de sécurité, qualité réseau) et sur la politique du serveur.
- **Hybridation contrôlée** : combinaison d'algorithmes classiques et post-quantiques, avec modes allégés ou maximaux selon le contexte.
- **0-RTT sécurisé par ZKP** : reprise de session sans aller-retour, rendue compatible avec les exigences post-quantiques grâce à des preuves à divulgation nulle de connaissance ultra-rapides.
- **Complémentarité** : s'appuie sur le TLS existant via des extensions et s'intègre aux produits et modules déjà en place (priorité au module QSA, interface multi-algorithmes facilitant les tests ACVP).
- **Respect des contraintes énergétiques** : réduction explicite de la charge computationnelle et radio côté client lorsque cela reste compatible avec le niveau de sécurité requis.

Positionnement différenciant



BRIQUE D'ADAPTATION ET DE SÉCURISATION
DU TLS HANDSHAKE

Extension du handshake TLS – Pas une couche de transport alternative

Pas une solution post-quantique monolithe

ADAPTATIVITÉ RÉELLE

Négociation dynamique selon l'état du client IoT et la politique du serveur.

HYBRIDATION CONTRÔLÉE

Combinaison classique + PQ selon modes léger ou maximal.

0-RTT SÉCURISÉ PAR ZKP

Reprise de session sans aller-retour, preuves ultra-rapides.

COMPLÉMENTARITÉ

S'appuie sur TLS via extensions, intègre les modules existants (priorité QSA), interface multi-algo pour ACVP.

RESPECT DES CONTRAINTES ÉNERGÉTIQUES

Réduction explicite de la charge calcul et radio du client quand compatible avec le niveau de sécurité requis.

Segments de marché et clients cibles

Le produit s'adresse prioritairement à :

- **Opérateurs d'infrastructures critiques** (énergie, eau, chaîne du froid, contrôle du trafic aérien et terrestre) qui doivent garantir une protection durable contre les menaces quantiques sans dégrader l'autonomie et la disponibilité de leurs capteurs.
- **Intégrateurs et éditeurs de solutions de sécurité** qui recherchent une brique ouverte, multi-algorithmes et extensible, capable de compléter leurs offres existantes plutôt que de les concurrencer frontalement.
- **Laboratoires et organismes de certification** grâce à l'interface conçue pour faciliter les tests ACVP (NIST) et la validation des primitives post-quantiques.

Segments de marché et clients cibles

OPÉRATEURS D'INFRASTRUCTURES CRITIQUES

ÉNERGIE | EAU | CHAÎNE DU FROID | CONTRÔLE AÉRIEN ET TERRESTRE

BESOIN : protection quantique durable sans dégrader l'autonomie ni la disponibilité des capteurs.

INTÉGRATEURS ET ÉDITEURS DE SOLUTIONS DE SÉCURITÉ

RECHERCHENT : un composant ouvert, multi-algorithmes et extensible pour compléter leur offre existante, et non concurrencer frontalement.

LABORATOIRES ET ORGANISMES DE CERTIFICATION

GRÂCE À : une interface pensée pour faciliter les tests ACVP (NIST) et la validation de primitives post-quantiques.

SÉCURITÉ POST-QUANTIQUE DÈS AUJOURD'HUI

BRIQUE AGILE ET EXTENSIBLE

CONÇU POUR LA CONFIANCE LA CERTIFICATION ET L'AVENIR

Position par rapport aux solutions existantes

Contrairement aux approches qui consistent soit à appliquer systématiquement des algorithmes post-quantiques lourds, soit à conserver le TLS classique en attendant, le protocole propose une voie intermédiaire et pragmatique. Il ne cherche pas à réécrire TLS ni à imposer une architecture unique et rigide. Il se concentre sur les mécanismes d'adaptation, de sélection d'algorithmes et de sécurisation du 0-RTT, tout en restant compatible avec l'écosystème existant.

Cette position lui permet d'adresser un spectre large de cas d'usage (mode hybride allégé pour les capteurs de réseau électrique, mode économie maximale pour les frigos connectés, mode hybride maximal avec ZKP pour le contrôle de trafic, reprises 0-RTT sécurisées) avec une architecture unique.

INTRODUCTION AU TLS HYBRIDE

Protocole TLS Hybride Post-Quantique Adaptatif pour l'IoT



INTRODUCTION

- Pourquoi ce projet ?
- Ce que propose le projet
- Les piliers techniques
- Bénéfices attendus et positionnement

Pourquoi ce projet ?

Les infrastructures critiques — centrales électriques, réseaux d'eau, chaîne du froid, contrôle du trafic aérien et terrestre — sont de plus en plus pilotées par des objets connectés. Ces capteurs et actionneurs apportent des gains d'efficacité majeurs, mais ils introduisent aussi une surface d'attaque croissante. Les incidents récents (frigos connectés compromis, centrales ciblées) montrent que les protocoles de sécurité classiques ne sont plus adaptés à ce contexte.

Deux défis se superposent. D'une part, la menace quantique rendra obsolètes, à moyen terme, les algorithmes asymétriques utilisés aujourd'hui dans TLS. D'autre part, les équipements IoT industriels sont fortement contraints : autonomie limitée, faible puissance de calcul, liens radio économes. Appliquer de manière systématique des algorithmes post-quantiques lourds dégraderait leur durée de vie et leur disponibilité opérationnelle. Il manque donc une couche réseau capable de concilier une sécurité post-quantique crédible et les réalités énergétiques du terrain.

INFRASTRUCTURES CRITIQUES



CENTRALE NUCLÉAIRE

TEMPÉRATURE



TRAITEMENT DE L'EAU

PRESSION



CAMION RÉFRIGÉRÉ
(COLD CHAIN)

DÉBIT



DÉTECTION



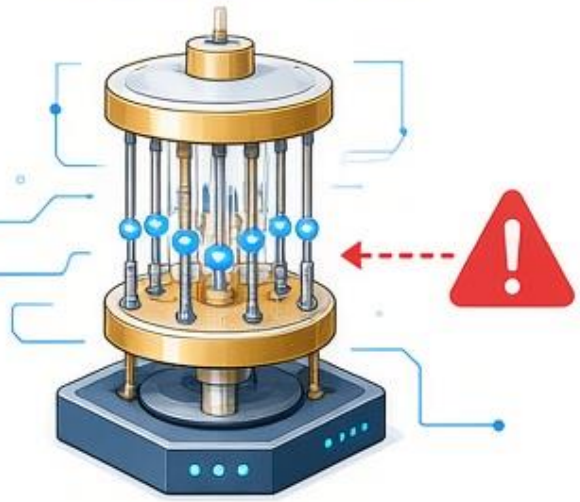
TLS Hybride Post-Quantique Adaptatif

Sécurité renforcée • Résilience quantique • Efficacité énergétique
Adaptation dynamique selon le contexte et les contraintes

HAUTE SÉCURITÉ
(Résistance quantique)

FAIBLE CONSOMMATION
(Efficience énergétique)

RISQUE QUANTIQUE



ORDINATEUR QUANTIQUE
(MENACE POUR LES ALGORITHMES CLASSIQUES)

CONTRAINTES ÉNERGÉTIQUES



BATTERIE
LIMITÉE



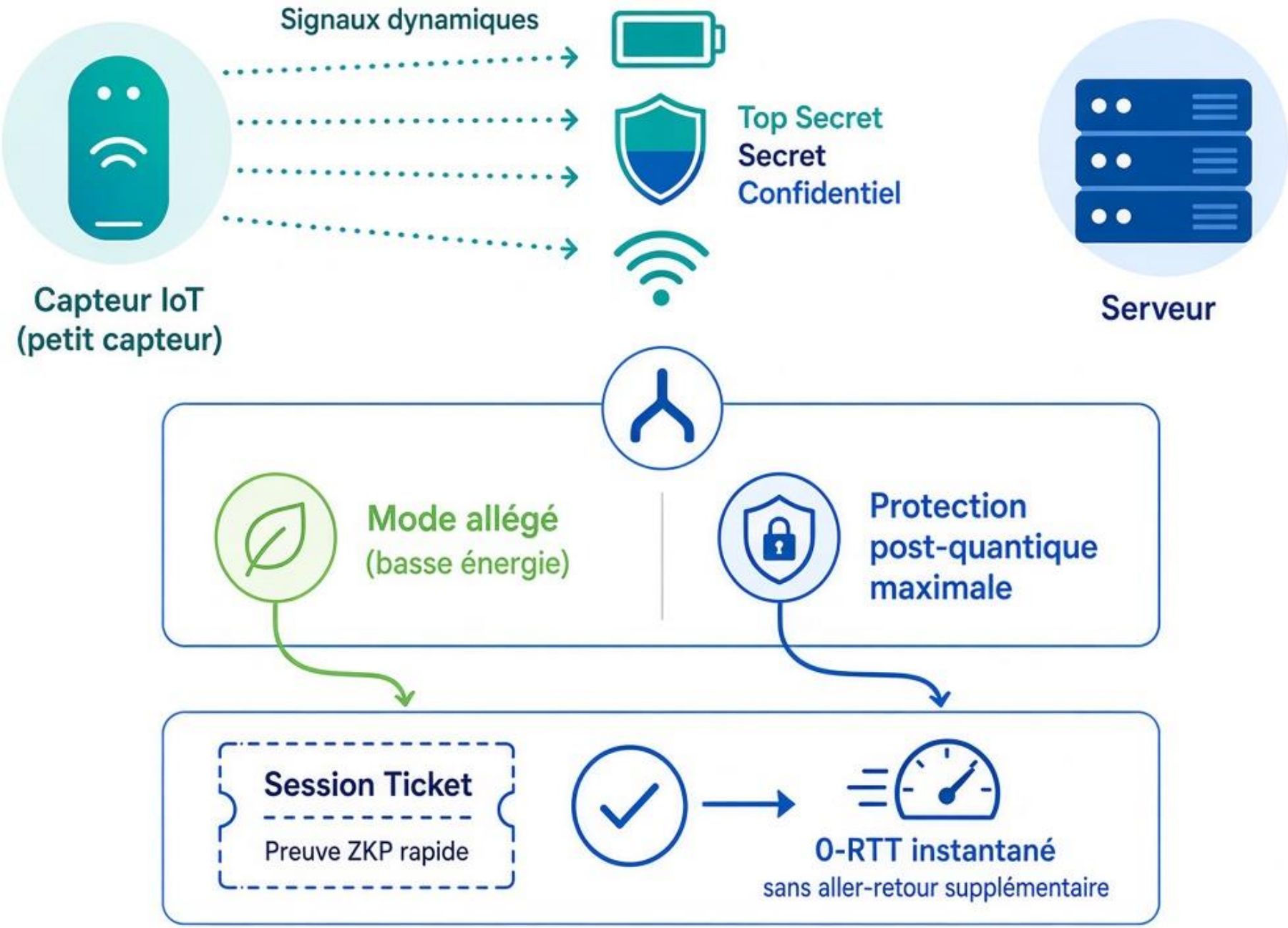
CONSOMMATION
ÉNERGÉTIQUE

Ce que propose le projet

Le projet consiste à concevoir un protocole TLS hybride post-quantique dont le handshake est hyper-adaptatif. Il s'agit d'une brique ouverte qui complète les produits existants, en particulier le module QSA déjà développé.

Le principe est simple : le client IoT signale dynamiquement trois informations essentielles — son niveau de batterie, son exigence de sécurité (Top Secret, Secret ou Confidentiel) et la qualité du réseau perçu. Le serveur utilise ces données, ainsi que sa propre politique, pour choisir le niveau de chiffrement hybride le plus approprié. Lorsque la batterie est faible et que la criticité est modérée, un mode allégé est retenu ; lorsque la transaction est critique et que les ressources le permettent, le niveau de protection post-quantique maximal est appliqué. L'objectif est d'économiser l'énergie et le trafic tout en restant résistant quantique.

Un second pilier concerne le 0-RTT. Dans TLS classique, la reprise de session sans aller-retour est pratique mais fragile face aux attaques de rejeu et peu compatible avec les exigences post-quantiques. Le projet propose de valider les tickets de session au moyen de preuves à divulgation nulle de connaissance (ZKP) ultra-rapides. La vérification étant quasi instantanée, le 0-RTT peut être utilisé même pour des transactions critiques, sans round-trip supplémentaire et avec une garantie de sécurité quantique.


Signaux dynamiques
Top Secret
Secret
Confidentiel
Capteur IoT
(petit capteur)
Serveur
Mode allégé
(basse énergie)
Protection
post-quantique
maximale
Session Ticket
Preuve ZKP rapide
0-RTT instantané
sans aller-retour supplémentaire

Les piliers techniques

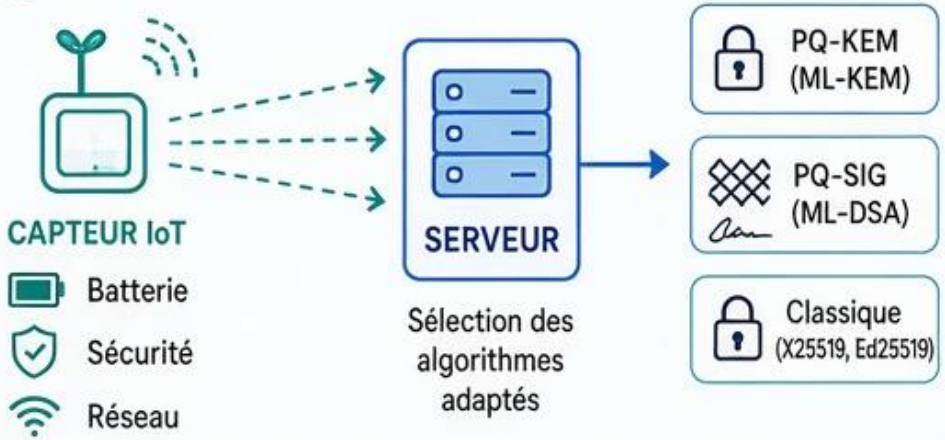
L'architecture repose sur quatre éléments principaux :

1. **Handshake adaptatif** — Une extension de signalisation permet au client de transmettre son état. Le serveur applique une politique configurable pour sélectionner la combinaison d'algorithmes (classiques + post-quantiques) et les paramètres adaptés.
2. **Interface multi-algorithmes** — Plusieurs primitives post-quantiques peuvent être branchées. L'interface est conçue pour faciliter les tests ACVP réalisés par des laboratoires accrédités et s'appuie en priorité sur le module QSA.
3. **Validation de tickets par ZKP** — Une preuve à divulgation nulle de connaissance accompagne le ticket de session. Sa vérification rapide garantit l'authenticité et empêche les rejeux, rendant le 0-RTT sûr à 100 % dans un contexte post-quantique.
4. **Gestion des contraintes énergétiques** — L'adaptation réduit explicitement la charge computationnelle et radio côté client lorsque cela est compatible avec le niveau de sécurité requis.

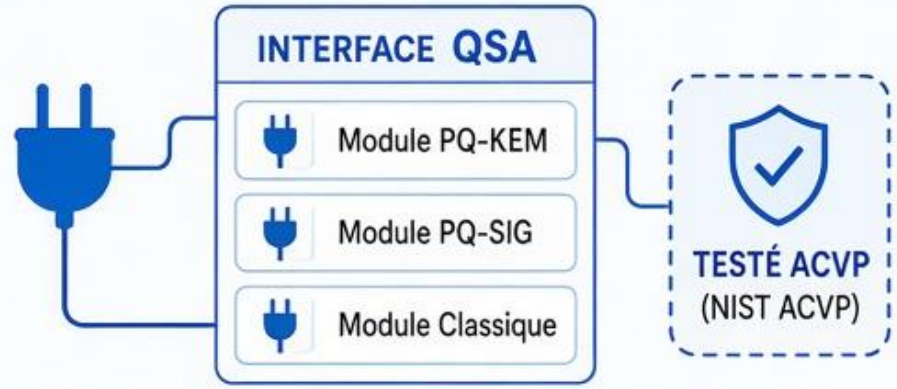
Le protocole s'appuie sur TLS existant (via des extensions) et ne réécrit pas la couche transport. Il se concentre sur les mécanismes d'adaptation, de sélection d'algorithmes et de sécurisation du 0-RTT.

Piliers techniques – TLS Hybride Post-Quantique Adaptatif

1 Handshake adaptatif



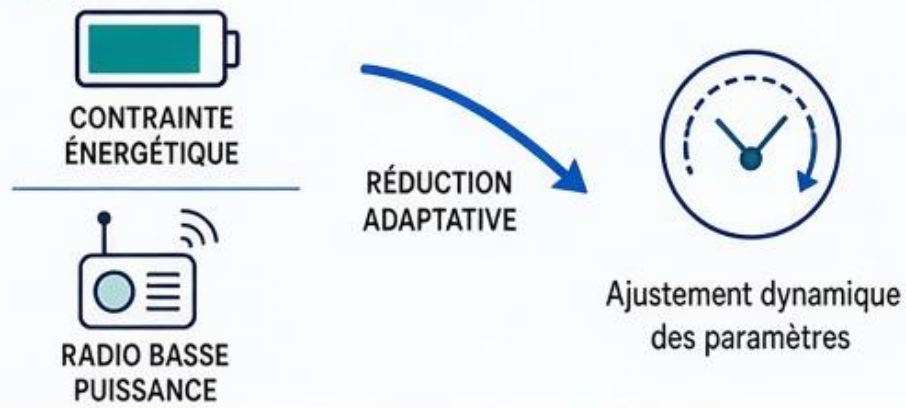
2 Interface multi-algorithmes



3 Validation de tickets par ZKP



4 Gestion des contraintes énergétiques



S'appuie sur TLS existant via extensions

Bénéfices attendus et positionnement

Pour les opérateurs d'infrastructures critiques, le protocole offre une protection durable contre les menaces quantiques sans sacrifier l'autonomie des capteurs. Il répond concrètement aux faiblesses observées sur les équipements de la chaîne du froid ou les systèmes de supervision électrique. Pour les intégrateurs, il constitue une brique ouverte et extensible, complémentaire des modules de sécurité déjà en place.

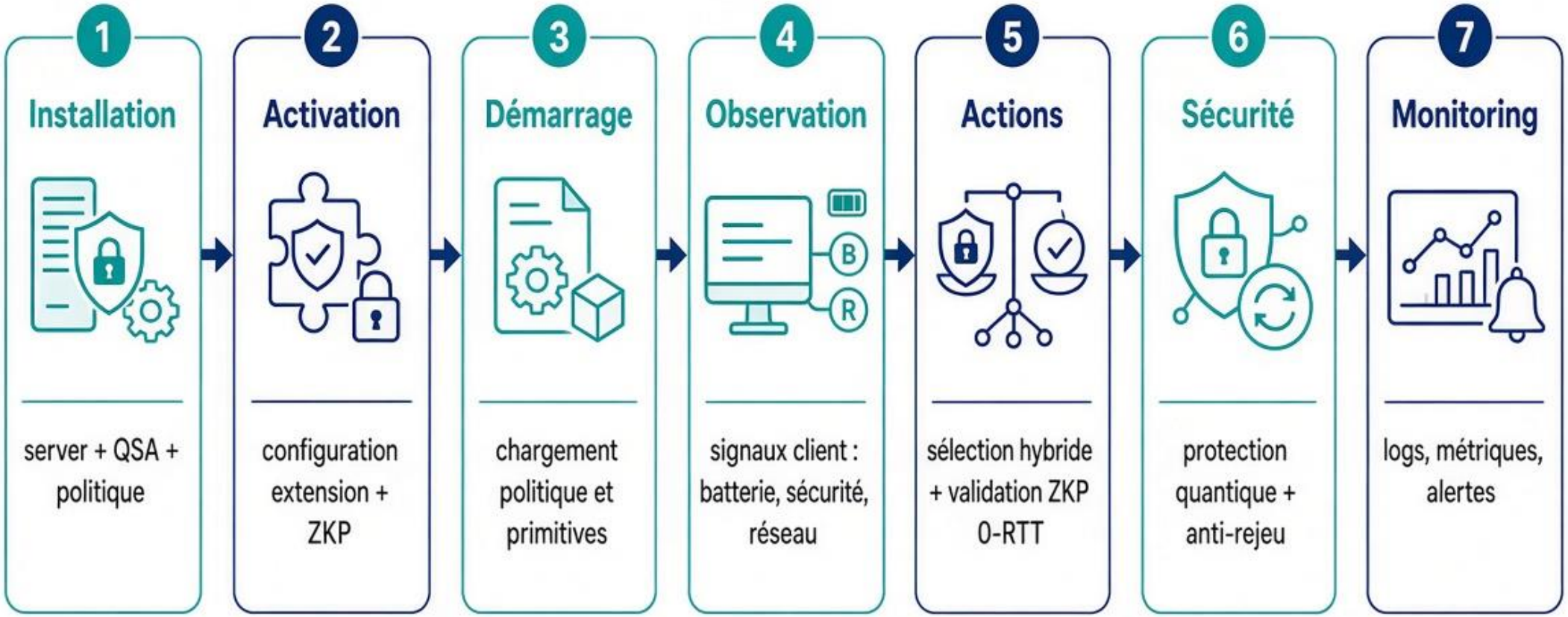
Les cas d'usage couvrent un spectre large : capteurs de réseau électrique en mode hybride allégé, frigos connectés en mode économie maximale, systèmes de contrôle de trafic en mode hybride maximal avec ZKP obligatoire, et reprises de session 0-RTT sécurisées. Cette flexibilité permet d'adresser des secteurs aux contraintes très différentes tout en conservant une architecture unique.

Fonctionnement du Protocole TLS Hybride Post-Quantique Adaptatif

Protocole TLS Hybride Post-Quantique Adaptatif pour l'IoT



Fonctionnement du Protocole TLS Hybride Post-Quantique Adaptatif



1. Installation

Sur un serveur Linux (Nginx, HAProxy, serveur applicatif, etc.) :

- Intégration de la brique sous forme de module / extension TLS (complémentaire au module QSA existant).
- Installation des bibliothèques post-quantiques et de l'interface multi-algorithmes (support ACVP).
- Déploiement des fichiers de politique (règles de sélection d'algorithmes selon batterie, criticité et réseau).
- Aucune réécriture de la couche transport : le protocole s'appuie sur le TLS existant via des extensions.

2. Activation

- Activation de l'extension de signalisation et du moteur de politique dans la configuration du serveur.
- Définition des seuils et des niveaux de sécurité (Top Secret / Secret / Confidentiel).
- Activation de la validation des tickets de session par ZKP pour le 0-RTT.
- Le serveur reste un serveur TLS classique ; la brique adaptative est simplement activée.

3. Démarrage

- Au démarrage du service, le serveur charge :
  - la politique de sélection,
  - les primitives disponibles (classiques + post-quantiques via QSA),
  - le validateur ZKP.
- Le service écoute les handshakes TLS entrants et attend les signaux dynamiques des clients IoT.

4. Observation des résultats

Pendant chaque handshake, le serveur observe :

- Niveau de batterie du client
- Exigence de sécurité demandée
- Qualité du réseau perçue
- Politique locale applicable

Il en déduit le mode retenu (allégé ou maximal) et les algorithmes sélectionnés.

5. Actions

- Sélection dynamique de la combinaison hybride (classique + post-quantique).
- Application du mode adapté (réduction de charge computationnelle et radio si compatible avec la sécurité).
- Validation quasi instantanée du ticket de session via ZKP → autorisation ou refus du 0-RTT.
- Établissement de la session sécurisée.

6. Sécurité

- Résistance quantique grâce à l'hybridation et aux primitives post-quantiques.
- Protection contre les rejeux grâce à la validation ZKP des tickets.
- Adaptation contrôlée : le niveau de sécurité minimum exigé n'est jamais dégradé.
- Compatibilité avec les exigences de certification (interface facilitant les tests ACVP).

7. Monitoring

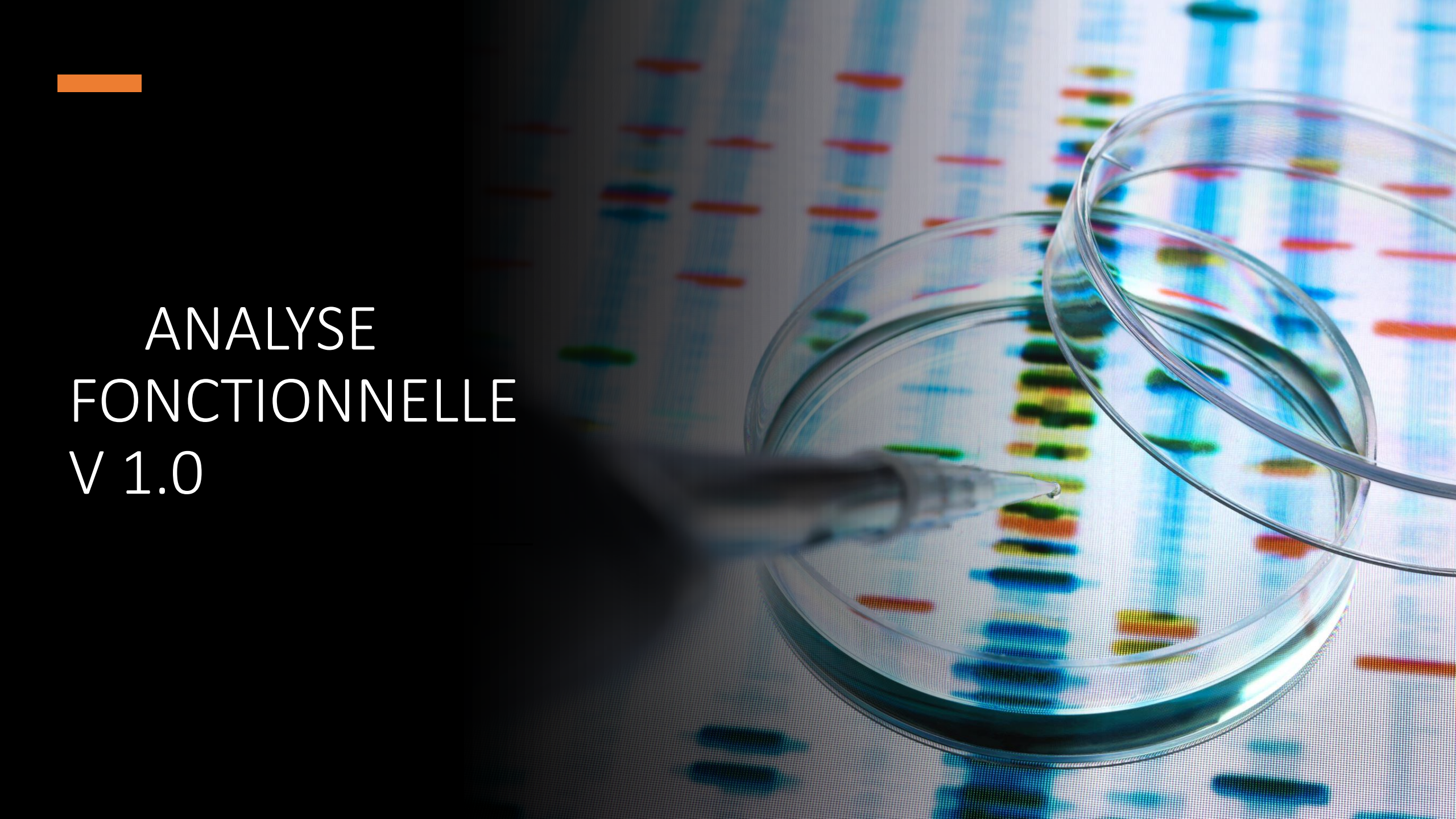
- Journalisation des décisions d'adaptation (signaux reçus, mode choisi, algorithmes retenus).
- Métriques : taux de sessions en mode allégé vs maximal, utilisation du 0-RTT, charge crypto, échecs de validation ZKP.
- Alertes en cas de déviation par rapport à la politique ou de comportement anormal.
- Tableaux de bord pour les opérateurs (autonomie préservée, niveau de protection effectif).

ANALYSE FONCTIONNELLE

Protocole TLS Hybride Post-Quantique Adaptatif pour l'IoT



ANALYSE FONCTIONNELLE V 1.0



AGENDA

- Chapitre 1 – Introduction et Contexte
- Chapitre 2 – Objectifs du Projet
- Chapitre 3 – Périmètre et Acteurs
- Chapitre 4 – Exigences Fonctionnelles
- Chapitre 5 – Architecture Fonctionnelle
- Chapitre 6 – Description des Fonctions Principales
- Chapitre 7 – Contraintes Techniques et Non-Fonctionnelles
- Chapitre 8 – Cas d’Usage Principaux
- Chapitre 9 – Impacts et Bénéfices
- Chapitre 10 – Prochaines Étapes Recommandées

Chapitre 1 – Introduction et Contexte

Les infrastructures critiques (énergie, eau, centrales, chaîne du froid, contrôle du trafic aérien et terrestre) sont de plus en plus connectées via l'Internet des Objets. Les incidents récents (frigos connectés compromis, centrales piratées) montrent les limites des protocoles classiques face aux menaces quantiques et aux contraintes énergétiques des capteurs.

Le projet propose une couche réseau chiffrée du futur : un protocole TLS hybride post-quantique dont le handshake est hyper-adaptatif. Il concilie :

- la sécurité post-quantique (via le module QSA existant),
- les contraintes matérielles IoT (autonomie, faible trafic, compression),
- la réduction des allers-retours réseau grâce à un 0-RTT rendu sûr par preuves à divulgation nulle de connaissance (ZKP).

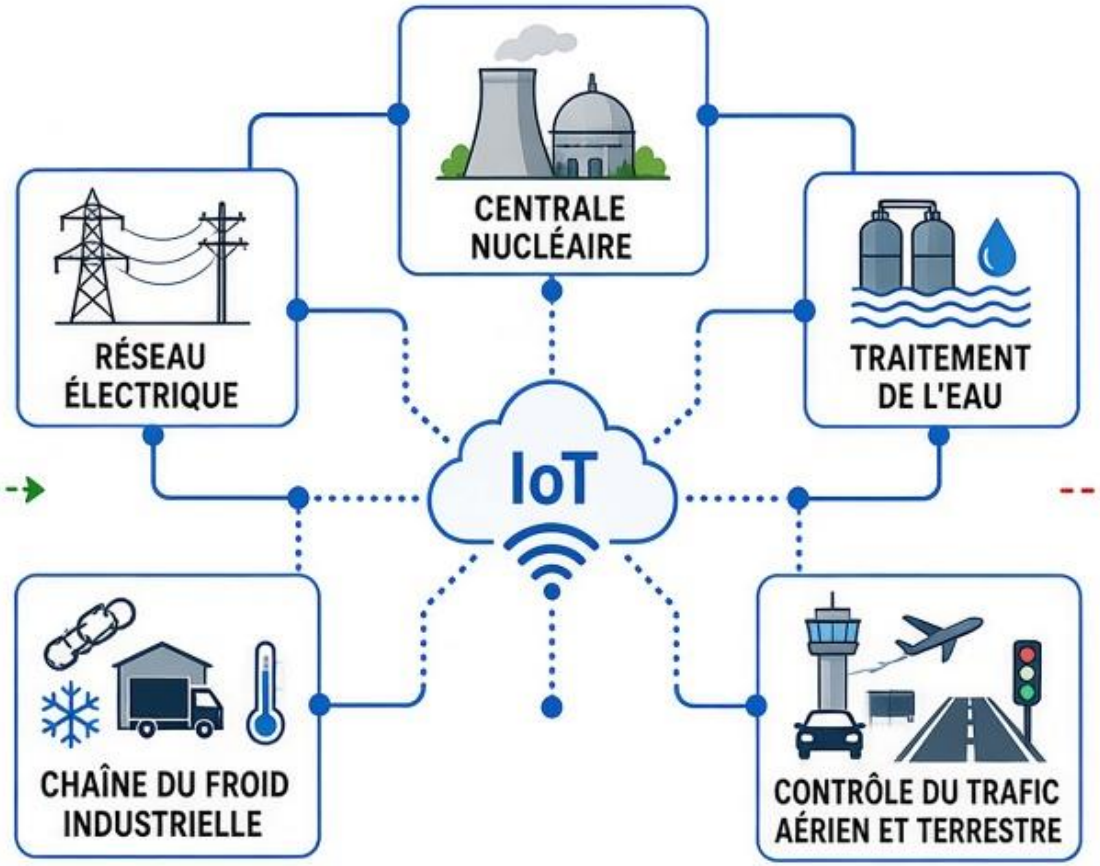
L'outil est conçu comme une brique ouverte, multi-algorithmes (NIST/ACVP) et complémentaire des produits existants.

INFRASTRUCTURES CRITIQUES ET CONNECTIVITÉ IoT

Systèmes interconnectés • Supervision, commande et maintenance

GAINS D'EFFICACITÉ

- Optimisation énergétique
- Maintenance prédictive
- Pilotage en temps réel



RISQUES DE CYBERSÉCURITÉ

- Accès non autorisé
- Malware
- Interception de données
- Impact sur la sûreté

CONTRAINTES MATÉRIELLES DES ÉQUIPEMENTS IoT

- Faible puissance de calcul
- Autonomie limitée
- Débit radio restreint
- Conditions environnementales difficiles

Chapitre 2 – Objectifs du Projet

Objectifs principaux

1. Fournir une négociation TLS hybride post-quantique adaptative pour l'IoT basse consommation.
2. Permettre au client de signaler dynamiquement son niveau de batterie, ses exigences de sécurité (Top Secret / Secret / Confidentiel) et la qualité du réseau.
3. Autoriser le serveur à adapter le niveau de chiffrement hybride (classique + post-quantique) pour économiser l'énergie tout en restant résistant quantique.
4. Rendre le 0-RTT sûr à 100 % pour les transactions critiques grâce à une validation de tickets de session par ZKP ultra-rapide (sans round-trip supplémentaire).
5. Offrir une interface multi-algorithmes post-quantiques validés NIST (ACVP par laboratoires accrédités), en s'appuyant sur le module QSA.

Objectifs secondaires

- Réduction du trafic réseau inutile.
- Compatibilité avec les exigences industrielles des secteurs vitaux.
- Outil ouvert et extensible.

Chapitre 2 – Objectifs du Projet

Objectifs principaux



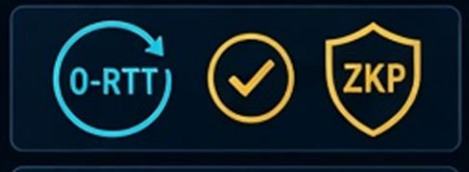
1. Négociation **TLS hybride post-quantique** adaptative pour IoT basse consommation.



2. Signalement dynamique du client (batterie, niveau de sécurité **Top Secret/Secret/Confidentiel**, qualité réseau)



3. Adaptation serveur du chiffrement hybride (classique + post-quantique) pour **économiser l'énergie** tout en restant **résistant quantique**.



4. **0-RTT sûr à 100%** via validation de tickets de session par **ZKP ultra-rapide**.



5. Interface multi-algorithmes post-quantiques **validés NIST (ACVP)** via **module QSA**.

Objectifs secondaires



Réduction du trafic réseau inutile.



Compatibilité avec exigences industrielles des secteurs vitaux.



Outil ouvert et extensible.

Chapitre 3 – Périmètre et Acteurs

Inclus dans le périmètre

- Handshake hybride adaptatif (signalisation client + décision serveur).
- Sélection dynamique des algorithmes post-quantiques (plusieurs algorithmes).
- Protocole de validation des tickets de session par ZKP.
- Interface d'intégration avec le module QSA.
- Gestion des niveaux de sécurité et des contraintes énergétiques.

Hors périmètre (à ce stade)

- Implémentation complète de la couche transport (s'appuie sur TLS existant).
- Certification ACVP finale (préparée mais réalisée par laboratoires accrédités).
- Déploiement matériel spécifique.

Acteurs

- Client IoT (capteur, actionneur, équipement critique).
- Serveur / Gateway réseau.
- Module QSA (fournisseur des primitives post-quantiques).
- Opérateur d'infrastructure critique.
- Laboratoire d'évaluation (ACVP).

Chapitre 3 – Périmètre et Acteurs

INCLUS DANS LE PÉRIMÈTRE

- Handshake hybride adaptatif
- Sélection dynamique algorithmes post-quantiques
- Validation tickets ZKP
- Interface module QSA
- Gestion niveaux sécurité et contraintes énergétiques

HORS PÉRIMÈTRE

- Couche transport complète (TLS existant)
- Certification ACVP finale
- Déploiement matériel spécifique

ACTEURS

- Client IoT (capteur/actionneur)
- Serveur/Gateway
- Module QSA
- Opérateur infrastructure critique
- Laboratoire évaluation ACVP

Chapitre 4 – Exigences Fonctionnelles

ID	Exigence	Priorité	Description
EF-01	Signalisation adaptative client	Haute	Le client transmet dans le ClientHello (ou extension dédiée) : niveau batterie, exigence sécurité, qualité réseau estimée.
EF-02	Décision d'adaptation serveur	Haute	Le serveur choisit dynamiquement la combinaison hybride (algorithmes classiques + PQ) et les paramètres (taille de clé, nombre de rounds, etc.) selon les signaux reçus et la politique de sécurité.
EF-03	Multi-algorithmes post-quantiques	Haute	Support d'au moins plusieurs algorithmes KEM et signatures PQ validés NIST, avec interface interchangeable.
EF-04	Intégration QSA	Haute	Le module QSA fournit les primitives ; le protocole les appelle via une interface standardisée.
EF-05	Validation de tickets par ZKP	Haute	Les tickets de session sont validés par preuve ZKP ultra-rapide, garantissant l'authenticité et la résistance quantique du 0-RTT sans round-trip supplémentaire.
EF-06	0-RTT sûr pour transactions critiques	Haute	Le 0-RTT n'est autorisé que si la preuve ZKP est valide et que le niveau de sécurité demandé le permet.
EF-07	Gestion des niveaux de sécurité	Moyenne	Mapping clair : Top Secret → hybride maximal, Secret → hybride allégé, Confidentiel → hybride minimal ou classique renforcé.
EF-08	Optimisation énergétique	Haute	L'adaptation doit réduire significativement la consommation CPU/radio du client IoT.

EF-09	Ouverture et extensibilité	Moyenne	Architecture permettant l'ajout d'algorithmes sans modification du cœur du handshake.
EF-10	Compatibilité TLS	Haute	S'appuie sur TLS 1.3 (extensions) pour rester interopérable.

Chapitre 4 – Exigences Fonctionnelles

HAUTE PRIORITÉ

EF-01
Signalisation adaptive client



HAUTE

EF-02
Décision d'adaptation serveur



HAUTE

EF-03
Multi-algorithmes post-quantiques



HAUTE

EF-04
Intégration QSA



HAUTE

EF-05
Validation tickets par ZKP



HAUTE

EF-06
0-RTT sûr



HAUTE

MOYENNE PRIORITÉ

EF-07
Gestion niveaux de sécurité



MOYENNE

EF-08
Optimisation énergétique



MOYENNE

EF-09
Ouverture et extensibilité



MOYENNE

EF-10
Compatibilité TLS 1.3



MOYENNE

Conception sécurisée. Performance. Interopérabilité. **Préparation quantique.**

Chapitre 5 – Architecture Fonctionnelle

text

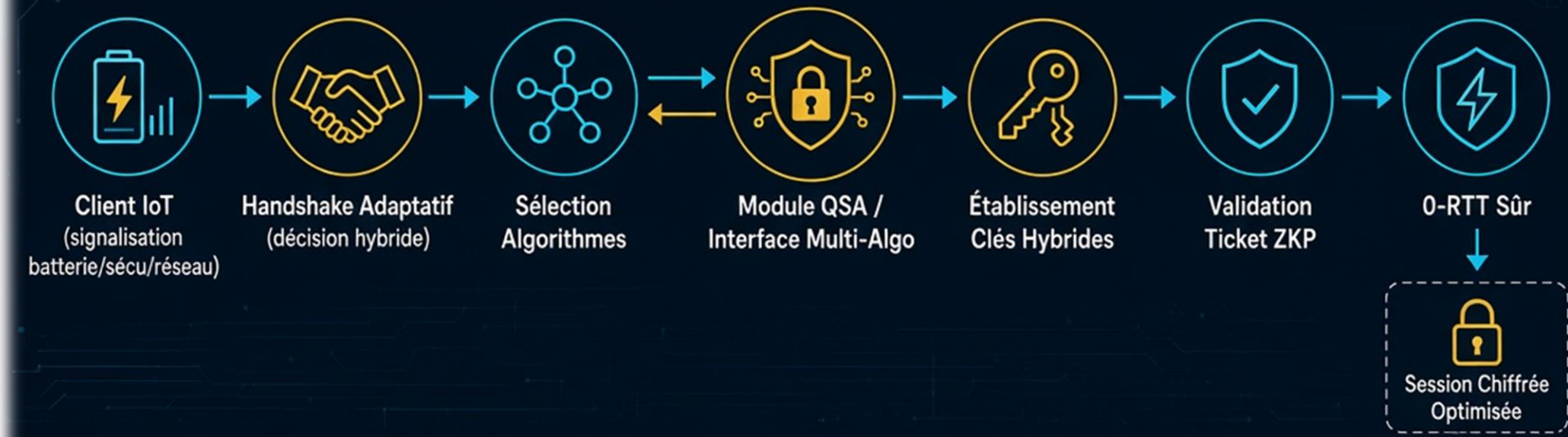
Copier

```
[Client IoT]
    |  Signalisation (batterie, sécu, réseau)
    ▼
[Handshake Adaptatif]
    |  Décision hybride
    ▼
[Sélection Algorithmes] ↔ [Module QSA / Interface Multi-Algo]
    |
    ▼
[Établissement Clés Hybrides]
    |
    ▼
[Validation Ticket ZKP] ⟶ [0-RTT Sûr]
    |
    ▼
[Session Chiffrée Optimisée]
```

Blocs fonctionnels principaux

1. Module de signalisation client.
2. Moteur de décision adaptative (serveur).
3. Couche d'abstraction multi-algorithmes PQ.
4. Moteur ZKP de validation de tickets.
5. Gestionnaire de politique de sécurité et d'énergie.

Chapitre 5 – Architecture Fonctionnelle



1. Module de signalisation client
2. Moteur de décision adaptative (serveur)
3. Couche d'abstraction multi-algorithmes PQ
4. Moteur ZKP de validation de tickets
5. Gestionnaire de politique de sécurité et d'énergie

Chapitre 6 – Description des Fonctions Principales

6.1 Handshake Hybride Adaptatif

- Le client envoie une extension contenant :
  - Niveau batterie (pourcentage ou état discret : critique / bas / normal).
  - Exigence de sécurité (Top Secret / Secret / Confidentiel).
  - Qualité réseau (latence estimée, bande passante, perte de paquets).
- Le serveur applique une politique (configurable) pour choisir la combinaison d'algorithmes et les paramètres (ex. : Kyber-512 + AES-GCM si batterie faible et Secret ; Kyber-1024 + Dilithium + AES-GCM si Top Secret et batterie correcte).

6.2 Interface Multi-Algorithmes Post-Quantiques

- Abstraction permettant de brancher plusieurs KEM et signatures.
- Validation ACVP prévue via interface standard.
- Le module QSA est la première implémentation ; d'autres peuvent être ajoutées.

6.3 Protocole de Validation de Tickets par ZKP

- Lors de la création du ticket de session, une preuve ZKP est générée (prouvant la possession de la clé de session et l'intégrité sans la révéler).
- Au 0-RTT, le client présente le ticket + preuve.
- Le serveur vérifie la preuve en temps constant et très faible (objectif : quelques microsecondes).
- Si valide → 0-RTT accepté même pour transactions critiques, avec garantie de résistance quantique.
- Aucun round-trip supplémentaire n'est introduit.

6.4 Optimisation Énergétique et Trafic

- Réduction de la taille des messages de handshake selon le niveau choisi.
- Compression optionnelle des données applicatives.
- Limitation des calculs lourds côté client lorsque la batterie est faible.

Chapitre 6 – Description des Fonctions Principales

6.1 HANDSHAKE HYBRIDE ADAPTATIF

CLIENT

Envoie l'extension

NIVEAU BATTERIE

EXIGENCE DE SÉCURITÉ
Top Secret / Secret / Confidentiel

QUALITÉ RÉSEAU

Le serveur applique la politique
et choisit les algorithmes hybrides et paramètres optimaux

SERVEUR

EXEMPLE DE SÉLECTION HYBRIDE

KYBER
(KEM)

+

AES-256-GCM
(Chiffrement)

INTERFACE MULTI-ALGORITHMES POST-QUANTIQUES

COUCHE D'ABSTRACTION
Interface unifiée pour
KEM et signatures

MODULES POST-QUANTIQUES

QSA
(Premier module)

+

EXTENSIBLE
Ajout de nouveaux algorithmes

ACVP READY
Tests et validation automatisés

• ABSTRACTION = INTEROPÉRABILITÉ • PERFORMANCE • ÉVOLUTIVITÉ

6.3 PROTOCOLE DE VALIDATION DE TICKETS PAR ZKP

1. CRÉATION DU TICKET

Ticket créé avec preuve ZKP

Preuve de possession (ZKP)

ZKP

2. PRÉSENTATION 0-RTT

Présente le ticket + preuve

0-RTT : sans aller-retour préalable

0-RTT

3. VÉRIFICATION SERVEUR

Vérification en temps constant

O(1) ~ microsecondes

µs

4. ACCEPTATION

Accès autorisé pour transactions critiques

Résistance quantique

QUANTUM RESISTANT

AUCUN ALLER-RETOUR SUPPLÉMENTAIRE • LATENCE MINIMALE • SÉCURITÉ MAXIMALE

Chapitre 7 – Contraintes Techniques et Non-Fonctionnelles

- **Performance réseau** : latence du handshake adaptatif ≤ handshake TLS 1.3 classique + overhead minimal ; vérification ZKP < 1 ms.
- **Énergie** : réduction mesurable de la consommation CPU et radio par rapport à un handshake PQ non adaptatif.
- **Sécurité** : résistance aux attaques quantiques (au moins niveau NIST 1 ou supérieur selon politique) ; forward secrecy conservée ; 0-RTT résistant aux attaques de rejeu grâce au ZKP.
- **Interopérabilité** : extensions TLS standards ou clairement documentées.
- **Maintenabilité** : code ouvert, interfaces stables, tests ACVP automatisables.
- **Robustesse** : comportement dégradé contrôlé si signalisation absente ou malformée.

Chapitre 7 – Contraintes Techniques et Non-Fonctionnelles

1 PERFORMANCE RÉSEAU



- Latence ≤ TLS 1.3 classique + overhead minimal
- Vérification ZKP < 1 ms

2 ÉNERGIE



Réduction mesurable de la consommation CPU et radio

vs handshake PQ non-adaptatif

3 SÉCURITÉ



- Résistance quantique NIST niveau 1+
- Forward secrecy
- 0-RTT replay resistant via ZKP

4 INTEROPÉRABILITÉ



- Extensions TLS standards ou documentées

5 MAINTENABILITÉ



- Code ouvert
- Interfaces stables
- Tests ACVP automatisés

6 ROBUSTESSE



- Comportement dégradé contrôlé si signaling absent ou malformé,

Chapitre 8 – Cas d'Usage Principaux

1. **Capteur de centrale / réseau électrique**
   Batterie moyenne, exigence Secret, réseau stable → hybride allégé.
2. **Frigo connecté (chaîne du froid)**
   Batterie faible, exigence Confidentiel → adaptation maximale pour préserver l'autonomie.
3. **Contrôle de trafic aérien / terrestre**
   Exigence Top Secret, batterie correcte → hybride maximal + ZKP obligatoire pour tout 0-RTT critique.
4. **Reprise de session 0-RTT**
   Ticket + preuve ZKP validée → session ouverte immédiatement, sans round-trip, même en environnement quantique.

Chapitre 8 – Cas d'Usage Principaux

1 Capteur de centrale / réseau électrique



BATTERIE MOYENNE | EXIGENCE SECRET | RÉSEAU STABLE → HYBRIDE ALLÉGÉ

2 Frigo connecté (chaîne du froid)



BATTERIE FAIBLE | EXIGENCE CONFIDENTIEL → ADAPTATION MAXIMALE pour préserver l'autonomie

3 Contrôle de trafic aérien / terrestre



EXIGENCE TOP SECRET | BATTERIE CORRECTE → HYBRIDE MAXIMAL + ZKP OBLIGATOIRE pour tout 0-RTT critique

4 Reprise de session 0-RTT



TICKET + PREUVE ZKP VALIDÉE → SESSION OUVERTE IMMÉDIATEMENT, sans round-trip, même en environnement quantique

SÉCURITÉ • PERFORMANCE • AUTONOMIE

Chapitre 9 – Impacts et Bénéfices

- **Sécurité** : protection post-quantique des infrastructures critiques tout en conservant des performances IoT.
- **Énergie et réseau** : prolongation de l'autonomie des capteurs et réduction du trafic inutile.
- **Souveraineté et ouverture** : outil ouvert multi-algorithmes, compatible avec les validations NIST/ACVP.
- **Complémentarité** : s'intègre aux produits existants via le module QSA et l'interface adaptable.
- **Impact mondial** : réponse concrète aux menaces observées sur les secteurs vitaux (énergie, eau, froid, transport).

Chapitre 9 – Impacts et Bénéfices

1 SÉCURITÉ



Protection post-quantique des infrastructures critiques

tout en conservant des performances IoT

- QUANTUM SHIELD
- PERFORMANCE IoT

2 ÉNERGIE ET RÉSEAU



Prolongation de l'autonomie des capteurs

et réduction du trafic inutile

- AUTONOMIE ÉTENDUE
- TRAFIC RÉDUIT

3 SOUVERAINETÉ ET OUVERTURE



Outil ouvert multi-algorithmes

compatible NIST/ACVP

- OPEN SOURCE
- NIST & ACVP

4 COMPLÉMENTARITÉ



S'intègre aux produits existants

via module QSA et interface adaptable

- INTÉGRATION
- INTERFACE ADAPTABLE

5 IMPACT MONDIAL



ÉNERGIE EAU FROID TRANSPORT

Réponse concrète aux menaces

sur secteurs vitaux

Chapitre 10 – Prochaines Étapes Recommandées

1. Spécification détaillée de l'extension de signalisation et de la politique d'adaptation.
2. Prototypage du moteur de décision + interface multi-algorithmes (en s'appuyant sur QSA).
3. Conception et implémentation du protocole ZKP de validation de tickets (choix de la primitive ZKP ultra-rapide).
4. Tests de performance (énergie, latence, taille des messages).
5. Préparation des vecteurs ACVP et interface d'évaluation.
6. Validation sur cas d'usage industriels (frigo, centrale, trafic).

Résultats attendus et indicateurs de succès

Protocole TLS Hybride Post-Quantique Adaptatif pour l'IoT



1. Résultats fonctionnels attendus

Le projet doit livrer un ensemble de fonctions opérationnelles et vérifiables :

- Un handshake TLS hybride post-quantique adaptatif pleinement fonctionnel, capable de recevoir la signalisation client (batterie, exigence de sécurité, qualité réseau) et d'appliquer une décision d'adaptation côté serveur.
- Un mécanisme de 0-RTT sécurisé par preuve ZKP, autorisant la reprise de session sans round-trip supplémentaire uniquement lorsque la preuve est valide et que le niveau de sécurité le permet.
- Une interface multi-algorithmes post-quantiques opérationnelle, permettant d'appeler plusieurs KEM et signatures de manière interchangeable, avec le module QSA comme première implémentation.
- Une gestion cohérente des niveaux de sécurité (Top Secret / Secret / Confidentiel) et des politiques d'adaptation configurables.

Ces résultats fonctionnels constituent le socle minimal du protocole. Leur atteinte se mesure par la capacité à exécuter de bout en bout les flux décrits dans l'architecture et les cas d'usage, sans régression sur les propriétés de base de TLS 1.3.

1. Résultats fonctionnels attendus

1.
Handshake TLS hybride post-quantique adaptatif pleinement fonctionnel



✓ Reçoit signalisation client et décide l'adaptation côté serveur

2.
Mécanisme 0-RTT sécurisé par preuve ZKP



✓ Reprise de session sans round-trip uniquement si preuve valide et niveau de sécurité le permet

3.
Interface multi-algorithmes post-quantiques opérationnelle



✓ Plusieurs KEM et signatures interchangeables, module QSA comme première implémentation

4.
Gestion cohérente des niveaux de sécurité et politiques d'adaptation configurables



✓ Niveaux Top Secret / Secret / Confidentiel et politiques d'adaptation configurables

BASE MINIMALE DU PROTOCOLE

Mesurée par la capacité à exécuter de bout en bout les flux décrits sans régression sur les propriétés de base de **TLS 1.3.**

SÉCURITÉ. PERFORMANCE. ADAPTATIVITÉ. VÉRIFIABLE.

2. Résultats de performance attendus

Des objectifs chiffrés doivent être atteints et mesurés :

- **Latence** : le handshake adaptatif doit rester inférieur ou égal à un handshake TLS 1.3 classique, avec un overhead limité (cible indicative : < 20 % d'augmentation).
- **Vérification ZKP** : temps de vérification de la preuve inférieur à 1 ms afin de préserver l'intérêt du 0-RTT.
- **Énergie** : réduction mesurable de la consommation CPU et radio côté client IoT par rapport à un handshake post-quantique non adaptatif (objectif cible : −30 % à −60 % selon le mode et le scénario).
- **Taille des messages** : réduction du volume de données échangées lors du handshake et des reprises de session grâce à l'adaptation et à l'optimisation des paramètres.

Ces indicateurs doivent être validés par des campagnes de mesures sur des plateformes représentatives des équipements IoT industriels, dans des conditions réseau variées.

2. Résultats de performance attendus

LATENCE

Handshake adaptatif ≤ handshake TLS 1.3 classique, overhead limité, cible **< 20%** d'augmentation



VÉRIFICATION ZKP

Temps de vérification de la preuve **< 1 ms** pour préserver l'intérêt du 0-RTT



ÉNERGIE

Réduction mesurable CPU et radio côté client IoT vs handshake PQ non adaptatif, objectif **–30% à –60%** selon mode et scénario



TAILLE DES MESSAGES

Réduction du volume de données échangées lors du handshake et des reprises grâce à l'adaptation et l'optimisation



INDICATEURS VALIDÉS PAR CAMPAGNES DE MESURES

Sur plateformes représentatives de l'IoT industriel, dans des conditions réseaux variées

ÉQUIPEMENTS IoT INDUSTRIELS

RÉSEAUX VARIÉS

RÉSULTATS MESURÉS

3. Résultats de sécurité attendus

Le protocole doit garantir les propriétés de sécurité suivantes :

- Résistance aux attaques quantiques d'au moins le niveau NIST 1, avec possibilité de monter à un niveau supérieur selon la politique et l'exigence (Top Secret).
- Conservation de la forward secrecy dans tous les modes hybrides.
- Résistance du 0-RTT aux attaques de rejeu grâce à la validation obligatoire de la preuve ZKP pour les transactions critiques.
- Absence de régression de sécurité par rapport à TLS 1.3 classique sur les propriétés fondamentales (authentification, confidentialité, intégrité).

Ces résultats doivent être appuyés par des analyses cryptographiques, des tests d'intrusion ciblés et la préparation des vecteurs ACVP pour les primitives sous-jacentes.

3. Résultats de sécurité attendus

LE PROTOCOLE DOIT GARANTIR LES PROPRIÉTÉS DE SÉCURITÉ SUIVANTES



RÉSISTANCE AUX ATTAQUES QUANTIQUES D'AU MOINS LE NIVEAU NIST 1

avec possibilité de monter à un niveau supérieur selon la politique et l'exigence **(TOP SECRET)**



CONSERVATION DE LA FORWARD SECRECY

dans tous les modes hybrides.



RÉSISTANCE DU 0-RTT AUX ATTAQUES DE REJEU

grâce à la validation obligatoire de la preuve **ZKP** pour les transactions critiques.



ABSENCE DE RÉGRESSION DE SÉCURITÉ

par rapport à TLS 1.3 classique sur les propriétés fondamentales **(AUTHENTIFICATION, CONFIDENTIALITÉ, INTÉGRITÉ)**

SUPPORTÉ PAR



ANALYSES CRYPTOGRAPHIQUES

Preuves et réductions de sécurité rigoureuses.



TESTS D'INTRUSION CIBLÉS

Scénarios avancés et adversaires quantiques.



PRÉPARATION DE VECTEURS ACVP

Pour les primitives sous-jacentes et la validation automatisée.

4. Résultats d’intégration attendus

L’intégration technique doit produire les résultats suivants :

- Interopérabilité complète avec les piles TLS 1.3 standards via des extensions documentées, sans modification invasive de la couche transport.
- Intégration fonctionnelle et stable du module QSA comme fournisseur des primitives post-quantiques.
- Interface multi-algorithmes prête pour les tests ACVP, avec documentation et vecteurs de test automatisables destinés aux laboratoires accrédités.
- Comportement dégradé contrôlé et traçable en cas de signalisation absente ou malformée.

Ces résultats garantissent que le protocole peut être déployé de manière progressive et non disruptive sur des infrastructures existantes.

4. Résultats d'intégration attendus



1

Interopérabilité complète

avec les piles TLS 1.3 standards via des extensions documentées, **sans modification invasive de la couche transport.**



2

Intégration fonctionnelle et stable

du module QSA comme **fournisseur des primitives post-quantiques.**



3

Interface multi-algorithmes

prête pour les tests ACVP, avec documentation et vecteurs de test automatisables destinés aux **laboratoires accrédités.**



4

Comportement dégradé contrôlé

et traçable en cas de signalisation **absente ou malformée.**



Ces résultats garantissent que le protocole peut être déployé de manière **progressive et non disruptive** sur les infrastructures existantes.



5. Résultats d’usage attendus

Sur les cas d’usage prioritaires, des gains concrets doivent être démontrés :

- **Capteur de centrale / réseau électrique** : fonctionnement stable en mode hybride allégé avec réduction mesurable de la consommation par rapport à un mode PQ maximal.
- **Frigo connecté (chaîne du froid)** : prolongation significative de l’autonomie grâce à l’adaptation maximale en situation de batterie faible.
- **Contrôle de trafic aérien / terrestre** : application du mode hybride maximal avec validation ZKP obligatoire, sans dégradation inacceptable de la latence.
- **Reprise 0-RTT** : ouverture immédiate de session pour des transactions critiques, avec preuve ZKP validée et absence de round-trip supplémentaire.

5. Résultats d’usage attendus

CAS D’USAGE PRIORITAIRES

1



CAPTEUR DE CENTRALE RÉSEAU ÉLECTRIQUE



Fonctionnement stable en mode hybride allégé avec réduction mesurable de la consommation par rapport à un mode PQ maximal.

2



FRIGO CONNECTÉ (CHAÎNE DU FROID)



Prolongation significative de l’autonomie grâce à l’adaptation maximale en situation de batterie faible.

3



CONTRÔLE DE TRAFIC AÉRIEN / TERRESTRE



Application du mode hybride maximal avec validation ZKP obligatoire, sans dégradation inacceptable de la latence.

4



REPRISE 0-RTT



Ouverture immédiate de session pour des transactions critiques, avec preuve ZKP validée et absence de round-trip supplémentaire.

ANALYSE DÉTAILLÉE

Protocole TLS Hybride Post-Quantique Adaptatif pour l'IoT



ANALYSE DETAILLEE
Chapitre 1

AGENDA Chapitre 1 – Introduction et Contexte

- 1.1 Contexte des infrastructures critiques et de leur connectivité
- 1.2 Incidents récents et limites des protocoles de sécurité classiques
- 1.3 Enjeux post-quantiques et contraintes énergétiques spécifiques à l'IoT
- 1.4 Positionnement du projet : une couche réseau chiffrée du futur
- 1.5 Vision de l'outil ouvert et complémentarité avec l'existant

1.1 Contexte des infrastructures critiques et de leur connectivité croissante

Les infrastructures critiques (production et distribution d'énergie, réseaux d'eau, centrales nucléaires ou thermiques, chaîne du froid industrielle et commerciale, contrôle du trafic aérien et terrestre) sont devenues fortement dépendantes de systèmes cyber-physiques. Ces systèmes reposent de plus en plus sur des réseaux d'objets connectés (IoT) pour la supervision, la commande et la maintenance.

Cette connectivité permet des gains d'efficacité majeurs (optimisation énergétique, maintenance prédictive, pilotage en temps réel), mais elle expose simultanément des actifs stratégiques à des risques de cybersécurité. Les équipements concernés sont souvent des capteurs et actionneurs contraints : faible puissance de calcul, autonomie limitée, débit radio restreint et conditions environnementales difficiles. Toute solution de sécurité doit donc tenir compte de ces contraintes matérielles sous peine de devenir inutilisable sur le terrain.

1.1 Contexte des infrastructures critiques et de leur connectivité croissante

INFRASTRUCTURES CRITIQUES

- PRODUCTION / DISTRIBUTION D'ÉNERGIE
- RÉSEAUX D'EAU
- CENTRALES NUCLÉAIRES / THERMIQUES
- CHAÎNE DU FROID INDUSTRIELLE / ET COMMERCIALE
- CONTRÔLE DU TRAFIC AÉRIEN ET TERRESTRE

SYSTÈMES CYBER-PHYSIQUES & RÉSEAUX IoT

SUPERVISION • COMMANDE • MAINTENANCE

GAINS D'EFFICACITÉ

- OPTIMISATION ÉNERGÉTIQUE
- MAINTENANCE PRÉDICTIVE
- CONTRÔLE EN TEMPS RÉEL

RISQUES CYBERNÉTIQUES

- ATTEINTES AUX ACTIFS STRATÉGIQUES
- CYBERATTAQUES & SABOTAGES
- IMPACTS POTENTIELS MAJEURS

CAPTEURS / ACTIONNEURS CONTRAINTS

- FAIBLE PUISSANCE DE CALCUL
- AUTONOMIE LIMITÉE
- DÉBIT RADIO RESTREINT
- CONDITIONS ENVIRONNEMENTALES DIFFICILES

TOUTE SOLUTION DE SÉCURITÉ DOIT PRENDRE EN COMPTE CES CONTRAINTES MATÉRIELLES.

SOUS PEINE D'ÊTRE INUTILISABLE SUR LE TERRAIN.

1.2 Incidents récents et limites des protocoles de sécurité classiques

Les incidents observés ces dernières années (compromission de frigos connectés dans la grande distribution, attaques ciblées sur des centrales électriques, notamment en Inde) illustrent les faiblesses des approches actuelles. Les protocoles de sécurité classiques (TLS 1.2/1.3 avec cryptographie asymétrique pré-quantique, tunnels VPN classiques, mécanismes d'authentification statiques) présentent plusieurs limites structurelles :

- vulnérabilité à moyen/long terme face aux ordinateurs quantiques (algorithmes de Shor et Grover) ;
- coût computationnel et énergétique élevé des handshakes complets, particulièrement pénalisant pour les capteurs à batterie ;
- absence de prise en compte dynamique de l'état du terminal (niveau de batterie, qualité du lien radio, criticité de la transaction) ;
- faiblesse du 0-RTT classique face aux attaques de rejeu et à l'absence de forward secrecy post-quantique.

Ces limites rendent les solutions existantes inadaptées aux environnements IoT industriels critiques, où l'on doit simultanément garantir un niveau de sécurité élevé et préserver l'autonomie des équipements.

1.2 Incidents récents et limites des protocoles de sécurité classiques

INCIDENTS RÉCENTS



COMPROMISSION DE FRIDGES CONNECTÉS

Réseaux de bots via IoT domestique



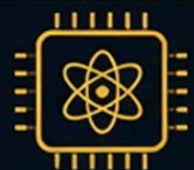
ATTAQUES DE CENTRALES ÉLECTRIQUES

Intrusions via accès distants et chaînes d'approvisionnement

INCIDENTS RÉELS, CONSÉQUENCES CRITIQUES.

Les protocoles classiques ne suffisent plus.

LIMITES STRUCTURELLES DES PROTOCOLES CLASSIQUES



VULNÉRABLES AUX ORDINATEURS QUANTIQUES

TLS 1.2/1.3 pré-quantique affaibli par Shor et Grover



COÛT ÉLEVÉ DES FULL HANDSHAKES

Consommation computationnelle et énergétique pénalisante pour capteurs sur batterie



AUCUNE PRISE EN COMPTE DYNAMIQUE DE L'ÉTAT DES TERMINAUX

Batterie, radio, criticité non considérées



FAIBLESSE DU 0-RTT CLASSIQUE

Sensible aux replay attacks et sans post-quantique forward secrecy

SOLUTIONS EXISTANTES NON ADAPTÉES AU IIOT CRITIQUE HAUTE SÉCURITÉ + AUTONOMIE

Il faut plus que des protocoles classiques.

SÉCURITÉ RENFORCÉE

AUTONOMIE ÉLEVÉE

IIOT CRITIQUE

1.3 Enjeux post-quantiques et contraintes énergétiques spécifiques à l'IoT

La transition vers la cryptographie post-quantique (PQC) est devenue une nécessité stratégique pour protéger les infrastructures critiques sur plusieurs décennies. Les algorithmes standardisés ou en cours de standardisation (KEM et signatures) offrent une résistance quantique, mais ils sont généralement plus coûteux en taille de clés, en calcul et en bande passante que leurs équivalents pré-quantiques.

Dans un contexte IoT basse consommation, cette surcharge est particulièrement problématique :

- chaque millijoule compte pour l'autonomie des capteurs ;
- les liens radio (LoRaWAN, NB-IoT, 5G RedCap, etc.) sont limités en débit et en énergie d'émission ;
- un handshake non optimisé peut consommer une part significative du budget énergétique quotidien d'un équipement.

Il est donc indispensable de concevoir une approche hybride et adaptative qui n'applique le niveau de protection post-quantique maximal que lorsque cela est justifié par le contexte (criticité de la donnée, état de la batterie, qualité du réseau).

1.3 Enjeux post-quantiques et contraintes énergétiques spécifiques à l'IoT

AUJOURD'HUI
Menace quantique émergente

TRANSITION PROGRESSIVE
10 – 20 ANS

ADOPTION PQC
GÉNÉRALISÉE

PQC COMME NÉCESSITÉ STRATÉGIQUE
pour les infrastructures critiques

ÉNERGIE · SANTÉ · TRANSPORT · GOUVERNEMENT · INDUSTRIE

PQC : RÉSISTANCE QUANTIQUE, MAIS PLUS COÛTEUX

PRÉ-QUANTIQUE (CLASSIQUE)
TAILLE DES CLÉS · CALCUL · BANDE PASSANTE

PQC : KEM (EX. KYBER)

PQC : SIGNATURES (EX. DILITHIUM)

COÛT RELATIF (vs CLASSIQUE)
x 4 – 10
x 3 – 20 REPMEENTE (cycles CPU)
x 2 – 5 REDWINIDI (octets échangés)

⚠ Plus de sécurité quantique = plus de ressources consommées.

DANS L'IoT BASSE CONSOMMATION : CHAQUE MILLIPOULE COMPTE

AUTONOMIE DES CAPTEURS
Chaque mJ compte

LIENS RADIO CONTRAINTS
LoRaWAN · 5G NB-IoT · 5G RedCap

FAIBLE DÉBIT
ÉNERGIE D'ÉMISSION LIMITÉE

HANDSHAKE NON OPTIMISÉ
peut consommer une part significative du budget énergétique quotidien

APPROCHE HYBRIDE ADAPTATIVE

Appliquer la protection PQ maximale uniquement quand le contexte le justifie

CRITICITÉ DES DONNÉES
Sensibles / Réglementées

ÉTAT DE LA BATTERIE
Critique / Faible / Bonne

QUALITÉ DU RÉSEAU
Débit / Latence / Fiabilité

SÉCURITÉ MAXIMALE QUAND C'EST JUSTIFIÉ
PERFORMANCE & AUTONOMIE PRÉSERVÉES SINON

SÉCURITÉ POST-QUANTIQUE INTELLIGENTE. DURABLE. ADAPTÉE À L'IoT.

1.4 Positionnement du projet : une couche réseau chiffrée du futur

Le projet propose de développer une couche réseau chiffrée spécifiquement conçue pour l'IoT industriel critique. Son cœur est un protocole TLS hybride post-quantique dont le handshake est hyper-adaptatif. Cette architecture concilie trois exigences jusqu'ici difficiles à satisfaire simultanément :

- la sécurité post-quantique, en s'appuyant sur le module QSA existant et sur une interface multi-algorithmes ;
- les contraintes matérielles des équipements IoT (autonomie, faible trafic, possibilité de compression) ;
- la réduction drastique des allers-retours réseau grâce à un mécanisme de 0-RTT rendu sûr par des preuves à divulgation nulle de connaissance (ZKP) ultra-rapides.

L'adaptation dynamique repose sur une signalisation du client (niveau de batterie, exigence de sécurité – Top Secret / Secret / Confidentiel –, qualité de réseau perçue) permettant au serveur de choisir le niveau de chiffrement hybride le plus approprié. Cette approche constitue une réponse directe aux incidents observés sur les infrastructures critiques et vise à offrir une protection durable sans sacrifier la viabilité opérationnelle des capteurs.

1.4 Positionnement du projet : une couche réseau chiffrée du futur

COUCHE RÉSEAU CHIFFRÉE

spécialement conçue pour l'IoT industriel critique



Réponse directe aux incidents des infrastructures critiques

Protection durable sans sacrifier la viabilité des capteurs

ADAPTATION DYNAMIQUE

Le serveur choisit le niveau hybride adapté selon la signalisation du client

- **BATTERIE** (autonomie)
- **NIVEAU DE SÉCURITÉ** Top Secret / Secret / Confidentiel
- **QUALITÉ RÉSEAU** (latence, pertes)

CHOIX DU NIVEAU HYBRIDE

TOP SECRET · SECRET · CONFIDENTIEL

PROTOCOLE TLS HYBRIDE POST-QUANTIQUE HYPER-ADAPTATIF

CŒUR DU PROTOCOLE

3 EXIGENCES CONCILIÉES

SÉCURITÉ POST-QUANTIQUE

Via le module QSA et une interface multi-algorithmes

INTERFACE MULTI-ALGORITHMES

ML-KEM · FN-DSA · + AUTRES

CONTRAINTES MATÉRIELLES IoT

Autonomie, trafic minimal, compression

AUTONOMIE · FAIBLE TRAFIC · COMPRESSION

RÉDUCTION DRASTIQUE DES ALLERS-RETOURS

Grâce au 0-RTT sécurisé par ZKP ultra-rapide

0-RTT → ZKP ULTRA-RAPIDE

PROTOCOLE EN ACTION : HANDSHAKE ADAPTATIF

CLIENT → 0-RTT + PREUVE ZKP ULTRA-RAPIDE → SERVEUR DÉDIÉ INFRASTRUCTURE CRITIQUE → CONNEXION SÉCURISÉE ADAPTÉE

Moins d'allers-retours, latence minimale, sécurité maximale

PROTÉGER L'ESSENTIEL. | GARDER LES CAPTEURS EN VIE.

1.5 Vision de l'outil ouvert et complémentarité avec l'existant

L'outil est conçu comme une brique ouverte, multi-algorithmes et extensible. Il prévoit dès sa conception :

- le support de plusieurs algorithmes post-quantiques validés ou en cours de validation NIST (avec interface préparée pour les tests ACVP réalisés par des laboratoires accrédités) ;
- une architecture modulaire permettant d'intégrer le module QSA comme première implémentation des primitives cryptographiques ;
- une complémentarité naturelle avec les produits et modules de sécurité déjà développés, en se positionnant comme la couche réseau sécurisée du futur.

Cette approche ouverte vise à faciliter l'adoption par les acteurs industriels des secteurs vitaux, tout en garantissant la possibilité d'évolution face aux évolutions des standards post-quantiques et des contraintes opérationnelles. Elle répond ainsi à un besoin stratégique de souveraineté et de résilience pour l'ensemble des infrastructures critiques connectées.

1.5 Vision de l'outil ouvert et complémentarité avec l'existant

BRIQUE OUVERTE, MULTI-ALGORITHMES ET EXTENSIBLE

OUVERT & OPEN SOURCE

Transparence, audits, communauté

MULTI-ALGORITHMES

Support des algorithmes post-quantiques validés ou en validation par le NIST

- KYBER
- DILITHIUM
- FALCON
- SPHINCS+

Interopérabilité et agilité cryptographique

EXTENSIBLE

Interface ACVP-ready pour tests et certification

ACVP READY

ARCHITECTURE MODULAIRE

Intégration native du module QSA comme première implémentation de primitives cryptographiques

- GESTION & ORCHESTRATION
- MODULE QSA — Primitives cryptographiques PQ
- ABSTRACTION & API UNIFIÉES
- INTÉGRATIONS & EXTENSIONS

COMPLÉMENTARITÉ NATURELLE

Complète les produits et modules de sécurité existants

PARE-FEU & PASSERELLES + HSM & PKI + VPN & SD-WAN

COUCHE RÉSEAU SÉCURISÉE POST-QUANTIQUE

Interopérable et incrémentale

FACILITE L'ADOPTION INDUSTRIELLE

Dans les secteurs vitaux

ÉVOLUTIVITÉ

S'adapte à l'évolution des standards PQ

CONTRAINTES OPÉRATIONNELLES

Performance, intégration, maintien en conditions

SOUVERAINETÉ & RÉSILIENCE

Maîtrise technologique et résilience des infrastructures connectées

INFRASTRUCTURES CRITIQUES

Énergie, Transports, Santé, Eau, Télécoms, Industrie

OUVERT • MODULAIRE • ÉVOLUTIF • SÉCURISÉ • SOUVERAIN

ANALYSE DETAILLEE
Chapitre 2

AGENDA Chapitre 2 – Objectifs du Projet

- 2.1 Objectif de négociation TLS hybride post-quantique adaptative
- 2.2 Signalisation dynamique des contraintes et exigences du client
- 2.3 Adaptation du niveau de chiffrement hybride côté serveur
- 2.4 Sécurisation du 0-RTT par validation de tickets via ZKP
- 2.5 Interface multi-algorithmes post-quantiques et complémentarité avec le module QSA

2.1 Objectif de négociation TLS hybride post-quantique adaptative

L'objectif central est de concevoir et de fournir une négociation TLS hybride post-quantique spécifiquement adaptée aux équipements IoT à basse consommation. Contrairement aux implémentations classiques de TLS 1.3 ou aux approches post-quantiques statiques, cette négociation doit être capable de moduler dynamiquement le niveau de protection selon le contexte réel du terminal et de la transaction.

Cette adaptativité vise à éviter l'application systématique d'algorithmes post-quantiques lourds lorsque le contexte ne l'exige pas, tout en garantissant une résistance quantique dès que le niveau de criticité ou les conditions le justifient. L'objectif est donc double : maintenir un niveau de sécurité post-quantique crédible et rendre le protocole viable sur des capteurs contraints en énergie et en ressources.

2.1 Objectif de négociation
TLS hybride post-quantique adaptative

APPROCHES CLASSIQUES

TLS 1.3 CLASSIQUE
Sécurité pré-quantique statique et rigide

✕

POST-QUANTIQUE STATIQUE
Algorithmes PQ lourds appliqués systématiquement

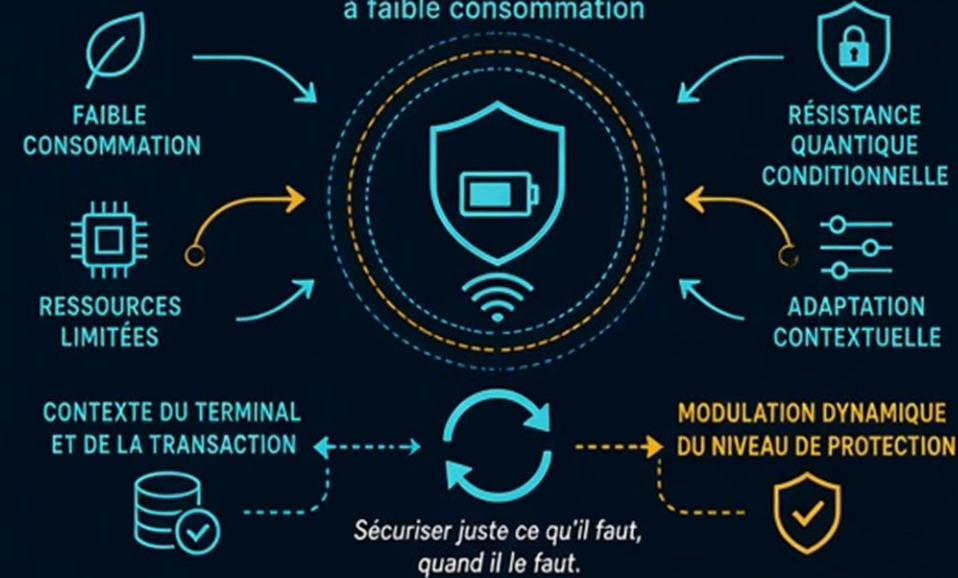
✕

SURCONSOMMATION ÉNERGÉTIQUE
et surcharge inutile sur les équipements contraints

OBJECTIF CENTRAL

NÉGOCIATION TLS HYBRIDE POST-QUANTIQUE ADAPTATIVE

spécifiquement adaptée aux équipements IoT à faible consommation



ÉVITE LES ALGORITHMES PQ LOURDS SYSTÉMATIQUES *lorsqu'ils ne sont pas nécessaires.*

NOTRE APPROCHE

NÉGOCIATION ADAPTATIVE
Protection modulée selon le contexte réel

✓

HYBRIDE ET CONTEXTUEL
Classique (léger) par défaut post-quantique activé si criticité

✓

SÉCURITÉ CRÉDIBLE
seulement quand c'est justifié.

DOUBLE OBJECTIF

MAINTENIR UN NIVEAU DE SÉCURITÉ POST-QUANTIQUE CRÉDIBLE
Résistance quantique garantie lorsque la criticité l'exige.

RENDRE LE PROTOCOLE VIABLE SUR LES CAPTEURS CONTRAINTS
Efficacité énergétique et empreinte légère pour l'IoT.

2.2 Signalisation dynamique des contraintes et exigences du client

Un objectif majeur est de permettre au client IoT de signaler, de manière dynamique et standardisée, les paramètres essentiels qui influencent le choix du niveau de sécurité :

- son niveau de batterie (ou un indicateur discret d'état énergétique) ;
- ses exigences de sécurité exprimées selon une classification claire (Top Secret / Secret / Confidentiel) ;
- une estimation de la qualité du réseau (latence, débit disponible, taux d'erreur ou état du lien radio).

Cette signalisation, transportée idéalement dans une extension du ClientHello ou dans un mécanisme équivalent, constitue la base informationnelle sur laquelle le serveur pourra prendre une décision éclairée. Elle doit être légère, fiable et résistante aux manipulations malveillantes afin de ne pas introduire de nouveaux vecteurs d'attaque.

2.2 Signalisation dynamique des contraintes et exigences du client



LÉGÈRE • FIABLE • RÉSISTANTE AUX MANIPULATIONS MALVEILLANTES

LÉGÈRE

Faible empreinte (quelques octets) et impact minimal sur la batterie et la bande passante.

FIABLE

Format normalisé, parsing robuste et transmission garantie (intégrité & authenticité).

RÉSISTANTE AUX ATTAQUES

Conçue pour éviter les nouveaux vecteurs d'attaque : validation stricte, anti-rejeu, anti-tampering

UNE SIGNALISATION FIABLE AUJOURD'HUI, DES INFRASTRUCTURES SÉCURISÉES DEMAIN.

2.3 Adaptation du niveau de chiffrement hybride côté serveur

Le serveur doit être en mesure d'adapter le niveau de chiffrement hybride (combinaison d'algorithmes classiques et post-quantiques, paramètres de clés, choix des primitives) en fonction des informations reçues du client et de sa propre politique de sécurité. L'objectif est d'économiser l'énergie et le trafic côté client tout en restant résistant aux menaces quantiques.

Cette adaptation peut se traduire par :

- le choix d'un algorithme post-quantique plus léger ou plus robuste ;
- la réduction ou l'augmentation de la taille des clés et des paramètres ;
- le recours à un mode hybride minimal, standard ou maximal selon la criticité annoncée et l'état énergétique du terminal.

L'objectif est de garantir que la sécurité ne soit jamais inférieure au niveau requis, tout en évitant une sur-protection coûteuse en énergie lorsque le contexte le permet.

2.3 Adaptation du niveau de chiffrement hybride côté serveur

ENTRÉES

SIGNAUX CLIENT
État d'énergie du terminal
Capacités & préférences

POLITIQUE DE SÉCURITÉ
Niveau de criticité des données
Exigences de conformité

Évite la sur-protection coûteuse
Adapte intelligemment selon le contexte

DÉCISION SERVEUR
Évalue & adapte le niveau hybride



GARANTIE : Sécurité jamais inférieure au niveau requis

ADAPTATION DU NIVEAU HYBRIDE

MINIMAL (léger)
Faible criticité + terminal contraint
→ PRIMITIVES
PQ Light (Kyber-512)
Classique (AES-128)

STANDARD (équilibré)
Criticité moyenne + autonomie modérée
→ PRIMITIVES
PQ Standard (Kyber-768)
Classique (AES-256)

MAXIMAL (robuste)
Haute criticité + terminal capable
→ PRIMITIVES
PQ Robuste (Kyber-1024)
Classique (AES-256) + HMAC-SHA384

OBJECTIF

ÉCONOMIES CLIENT
Moins d'énergie consommée
Moins de trafic réseau

ÉCONOMIE

- jusqu'à **40%** d'énergie
- jusqu'à **30%** de trafic

SÉCURITÉ QUANTIQUE

Résistant aux ordinateurs quantiques grâce à la combinaison classique + post-quantique

ADAPTATIF • CONTEXTUEL • SÉCURISÉ • EFFICIENT

2.4 Sécurisation du 0-RTT par validation de tickets via ZKP

Un objectif stratégique est de rendre le mécanisme 0-RTT sûr à 100 % pour les transactions critiques, y compris dans un contexte post-quantique. Cela passe par la mise en place d'un protocole de validation des tickets de session reposant sur des preuves à divulgation nulle de connaissance (ZKP) ultra-rapides.

L'objectif est double :

- permettre la reprise de session sans round-trip supplémentaire (gain de latence et d'énergie) ;
- garantir l'authenticité du ticket, la résistance aux attaques de rejeu et la préservation des propriétés de sécurité post-quantique, même en 0-RTT.

La vérification de la preuve ZKP doit être suffisamment performante pour ne pas annuler les bénéfices du 0-RTT, tout en offrant une garantie cryptographique forte.

2.4 Sécurisation du 0-RTT par validation de tickets via ZKP

OBJECTIF STRATÉGIQUE

Rendre le

0-RTT

100% SÉCURISÉ

pour les transactions critiques,
y compris post-quantique

via validation ultra-rapide des tickets de session par **ZKP**

Confidentialité + Intégrité + Disponibilité même en 0-RTT

0-RTT
Reprise de session immédiate sans aller-retour

TICKET DE SESSION
Ticket chiffré et lié à la session

PREUVE ZKP
Preuve de possession du ticket (sans rien révéler)

VÉRIFICATION INSTANTANÉE
Validation ultra-rapide par le serveur

DOUBLE OBJECTIF

1. REPRISE SANS ALLER-RETOUR

- zéro latence ajoutée
- économie d'énergie

2. GARANTIES CRYPTOGRAPHIQUES

- ✓ AUTHENTICITÉ du ticket et de l'émetteur
- ✓ ANTI-REJEU par construction
- ✓ POST-QUANTIQUE résistant aux attaques quantiques

Sécurité forte, même dans les échanges 0-RTT

ZKP : ULTRA-PERFORMANTE

La vérification doit être hautement performante

LATENCE minimale

ÉNERGIE réduite

GARANTIE CRYPTOGRAPHIQUE maximale

Sans pénaliser les bénéfices du 0-RTT

0-RTT + ZKP = RAPIDE | SÉCURISÉ | POST-QUANTIQUE | EFFICIENT

2.5 Interface multi-algorithmes post-quantiques et complémentarité avec le module QSA

L'objectif est de fournir une interface ouverte et standardisée permettant d'intégrer plusieurs algorithmes post-quantiques validés ou en cours de validation par le NIST. Cette interface doit être conçue pour faciliter les tests ACVP réalisés par des laboratoires accrédités et pour s'appuyer prioritairement sur le module QSA existant comme première implémentation des primitives cryptographiques.

Cet objectif inclut également les ambitions secondaires du projet :

- réduction du trafic réseau inutile grâce à l'adaptation et à la compression éventuelle ;
- compatibilité avec les exigences industrielles des secteurs vitaux (énergie, eau, froid, transport) ;
- conception d'un outil ouvert, extensible et complémentaire des produits de sécurité déjà développés.

L'ensemble vise à positionner le protocole comme une brique réseau durable, évolutive et industrialisable pour les infrastructures critiques.

2.5 Interface multi-algorithmes post-quantiques et complémentarité avec le module QSA

INTERFACE MULTI-ALGORITHMES POST-QUANTIQUES

ouverte · standardisée · interopérable

PLUSIEURS ALGORITHMES NIST VALIDÉS OU EN VALIDATION

- **Kyber** — NIST ✓
- **Dilithium** — NIST ✓
- **Falcon** — EN VALIDATION
- **SPHINCS+** — EN VALIDATION
- **ML-KEM / ML-DSA** — EN VALIDATION

NIST

CONÇUE POUR LES TESTS ACVP PAR LABORATOIRES ACCRÉDITÉS

CONFORMITÉ · AUDIT · ACCREDITATION

MODULE QSA

PREMIÈRE IMPLÉMENTATION DE RÉFÉRENCE

- INTERFACE STANDARD OUVERTE
- INTÉGRATION QSA comme socle initial + PLUSIEURS ALGORITHMES post-quantiques

COMPLÉMENTARITÉ

- ÉVOLUTION CONTINUE
- CHOIX AGILE
- RÉSILIENCE ACCRUE

AMBITIONS SECONDAIRES

RÉDUCTION DU TRAFIC RÉSEAU INUTILE
via adaptation et compression contextuelles

COMPATIBILITÉ INDUSTRIELLE
répond aux exigences des systèmes critiques

ÉNERGIE · EAU · FROID · TRANSPORT

OUTIL OUVERT ET EXTENSIBLE
brique complémentaire évolutive et collaborative

BRIQUE RÉSEAU DURABLE, ÉVOLUTIVE ET INDUSTRIALISABLE
pour les infrastructures critiques

ÉNERGIE · EAU · FROID · TRANSPORT

BRIQUE RÉSEAU DURABLE · ÉVOLUTIVE · INDUSTRIALISABLE

POUR LA SÉCURITÉ DES INFRASTRUCTURES CRITIQUES

ANALYSE DETAILLEE
Chapitre 3
Périmètre et Acteurs

AGENDA Chapitre 3 – Périmètre et Acteurs

- 3.1 Éléments inclus dans le périmètre fonctionnel
- 3.2 Éléments hors périmètre à ce stade
- 3.3 Acteurs principaux et leurs rôles
- 3.4 Interactions et flux entre acteurs
- 3.5 Justification du périmètre et alignement avec les objectifs

3.1 Éléments inclus dans le périmètre fonctionnel

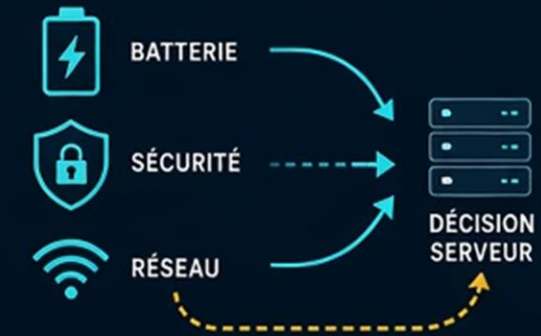
Le périmètre du projet couvre l'ensemble des mécanismes nécessaires à la mise en œuvre d'un handshake TLS hybride post-quantique adaptatif. Sont explicitement inclus :

- le handshake hybride adaptatif, comprenant la signalisation des paramètres côté client (batterie, exigence de sécurité, qualité réseau) et la logique de décision côté serveur ;
- la sélection dynamique des algorithmes post-quantiques parmi plusieurs primitives disponibles ;
- le protocole de validation des tickets de session par preuves à divulgation nulle de connaissance (ZKP) ;
- l'interface d'intégration avec le module QSA, permettant d'appeler les primitives cryptographiques de manière standardisée ;
- la gestion des niveaux de sécurité (Top Secret / Secret / Confidentiel) et des contraintes énergétiques associées.

Ces éléments constituent le cœur fonctionnel du protocole et doivent être spécifiés, conçus et validés dans le cadre du projet.

3.1 Éléments inclus dans le périmètre fonctionnel

1 Handshake hybride adaptatif



SIGNALISATION CLIENT + DÉCISION SERVEUR

2 Sélection dynamique des algorithmes post-quantiques



SÉLECTION DYNAMIQUE

ADAPTATIF & POST-QUANTIQUE

CŒUR FONTIONNEL DU PROTOCOLE À SPÉCIFIER, CONCEVOIR ET VALIDER

3 Protocole de validation des tickets par ZKP



VALIDATION SANS RÉVÉLATION

4 Interface d'intégration avec le module QSA



INTÉGRATION SÉCURISÉE

5 Gestion des niveaux de sécurité et contraintes énergétiques

- TOP SECRET
- SECRET
- CONFIDENTIEL

CONTRAINTES ÉNERGÉTIQUES

OPTIMISATION AUTONOME

ADAPTATION NIVEAU × ÉNERGIE

CES 5 ÉLÉMENTS FORMENT LE CŒUR FONCTIONNEL DU PROTOCOLE | SPÉCIFIER | CONCEVOIR | VALIDER

3.2 Éléments hors périmètre à ce stade

Certains aspects sont volontairement exclus du périmètre actuel afin de concentrer les efforts sur les innovations propres au projet. Sont hors périmètre :

- l'implémentation complète de la couche transport : le protocole s'appuie sur TLS existant (extensions et mécanismes standards) sans en réécrire la pile ;
- la certification ACVP finale : l'interface et les vecteurs de test sont préparés, mais la certification elle-même est réalisée par des laboratoires accrédités ;
- le déploiement matériel spécifique : le projet ne couvre pas le portage sur des plateformes matérielles particulières ni l'intégration industrielle complète chez les opérateurs.

Cette délimitation permet de livrer une brique logicielle ouverte et réutilisable, tout en laissant les phases de certification et d'intégration matérielle aux acteurs spécialisés.

3.2 Éléments hors périmètre à ce stade

1.
Implémentation complète de la couche transport



s'appuie sur TLS existant, extensions et mécanismes standards, **sans réécrire la pile**



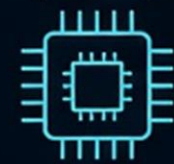
2.
Certification ACVP finale



interface et vecteurs de test préparés, mais certification réalisée par **laboratoires accrédités**



3.
Déploiement matériel spécifique



pas de portage sur plateformes matérielles particulières ni intégration industrielle complète





CETTE DÉLIMITATION PERMET DE LIVRER
UNE BRIQUE LOGICIELLE OUVERTE ET RÉUTILISABLE
en laissant la certification et l'intégration matérielle à des **acteurs spécialisés.**



OUVERTE ET INTEROPÉRABLE



RÉUTILISABLE PAR LA COMMUNAUTÉ



FOCUS SUR LE LOGICIEL, PAS SUR LA CERTIFICATION OU LE MATÉRIEL

DÉLIMITATION CLAIRE • RESPONSABILITÉS PARTAGÉES • IMPACT MAXIMAL

3.3 Acteurs principaux et leurs rôles

Les acteurs intervenant dans le système sont les suivants :

- **Client IoT** : capteur, actionneur ou équipement critique qui initie la connexion, signale son état (batterie, exigence de sécurité, qualité réseau) et applique les décisions d'adaptation ;
- **Serveur / Gateway réseau** : entité qui reçoit la signalisation, applique la politique d'adaptation, sélectionne les algorithmes et valide les tickets de session via ZKP ;
- **Module QSA** : fournisseur des primitives post-quantiques (KEM, signatures, etc.), appelé via l'interface multi-algorithmes ;
- **Opérateur d'infrastructure critique** : responsable de la définition des politiques de sécurité, du déploiement et de la supervision opérationnelle ;
- **Laboratoire d'évaluation (ACVP)** : organisme accrédité chargé de valider la conformité des implémentations post-quantiques selon les procédures NIST.

Chaque acteur dispose d'un rôle clairement délimité afin de garantir la séparation des responsabilités et la traçabilité des décisions.

3.3 Acteurs principaux et leurs rôles

1 Client IoT



- Initie la connexion
- Signale son état (batterie, sécurité, réseau)
- Applique les adaptations

Rôle : émetteur de signaux et exécutant des adaptations

2 Serveur / Gateway réseau



- Reçoit les signalements
- Applique la politique d'adaptation
- Sélectionne les algorithmes
- Valide les tickets via ZKP

Rôle : décideur d'adaptation et validateur de tickets

3 Module QSA



- Fournit les primitives post-quantiques (KEM, signatures)
- Via une interface multi-algorithmes
- Garantit l'abstraction cryptographique

Rôle : fournisseur de primitives post-quantiques

4 Opérateur d'infrastructure critique



- Définit les politiques de sécurité
- Déploie les configurations
- Supervise l'exploitation et les incidents

Rôle : stratège et superviseur opérationnel

5 Laboratoire d'évaluation ACVP



- Valide la conformité des implémentations post-quantiques
- Selon les procédures NIST (ACVP)

Rôle : valideur indépendant de conformité

RÔLES CLAIREMENT DÉLIMITÉS | **SÉPARATION DES RESPONSABILITÉS** | **TRAÇABILITÉ DES DÉCISIONS** | **CONFORMITÉ ET CONFIANCE**

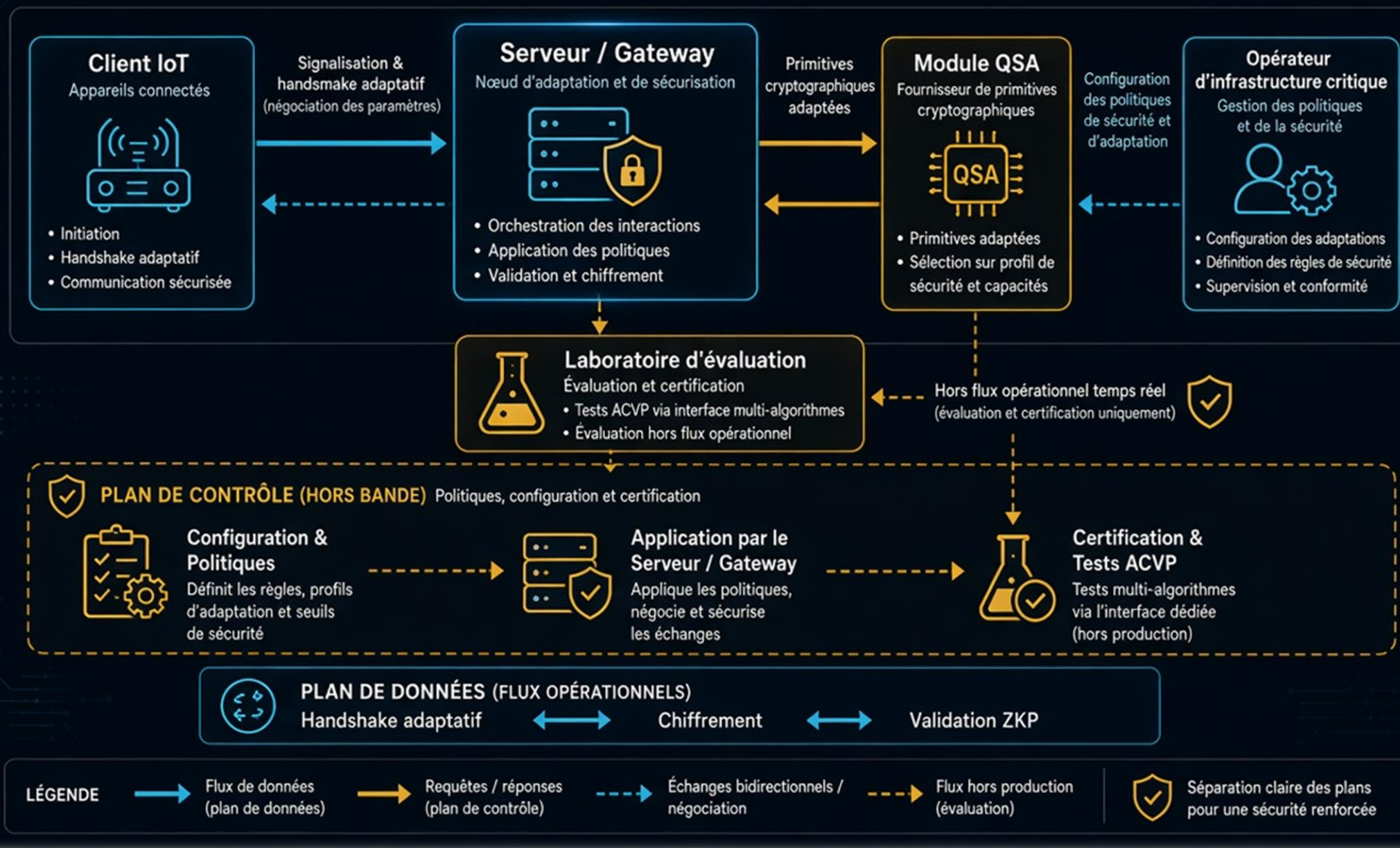
3.4 Interactions et flux entre acteurs

Les interactions principales se déroulent comme suit :

- le Client IoT communique avec le Serveur / Gateway via le handshake adaptatif (signalisation + négociation) ;
- le Serveur interroge le Module QSA pour obtenir les primitives cryptographiques adaptées au niveau choisi ;
- l'Opérateur d'infrastructure critique configure les politiques d'adaptation et de sécurité appliquées par le Serveur ;
- le Laboratoire d'évaluation interagit avec l'interface multi-algorithmes pour réaliser les tests ACVP, sans intervenir dans le flux opérationnel temps réel.

Ces flux permettent une séparation nette entre le plan de contrôle (politiques, certification) et le plan de données (handshake, chiffrement, validation ZKP).

3.4 Interactions et flux entre acteurs



3.5 Justification du périmètre et alignement avec les objectifs

Le périmètre défini est volontairement focalisé sur les innovations différenciantes du projet : adaptativité du handshake, sélection dynamique d'algorithmes, sécurisation du 0-RTT par ZKP et intégration ouverte du module QSA. En excluant la réécriture de la couche transport, la certification finale et le déploiement matériel, le projet reste réalisable dans des délais maîtrisés tout en livrant une brique réutilisable et complémentaire des produits existants.

Cette délimitation est cohérente avec les objectifs du Chapitre 2 : elle permet de concentrer les efforts sur la négociation adaptative, la signalisation client, l'adaptation serveur, la sécurisation du 0-RTT et l'interface multi-algorithmes, tout en préparant les conditions d'une adoption industrielle et d'une validation externe. Elle garantit ainsi que le protocole puisse être intégré dans les infrastructures critiques sans imposer de rupture technologique majeure.

3.5 Justification du périmètre et alignement avec les objectifs

FOCUS : INNOVATIONS DIFFÉRENCIANTES

ADAPTATIVITÉ DU HANDSHAKE

Négociation dynamique du handshake selon le contexte et les capacités.

SÉLECTION DYNAMIQUE D'ALGORITHMES

Choix optimisé de l'algorithme en temps réel selon la politique et le risque.

SÉCURISATION DU 0-RTT PAR ZKP

Preuves à divulgation nulle pour garantir la sécurité des échanges 0-RTT.

INTÉGRATION OUVERTE DU MODULE QSA

API et standards ouverts pour une intégration modulaire et interopérable.

SÉCURITÉ RENFORCÉE → PERFORMANCE ADAPTÉE → CONÇU POUR L'INTEROPÉRABILITÉ

HORS PÉRIMETRE (EXCLUSIONS)

COUCHE TRANSPORT

Hors scope : TCP, UDP, QUIC, TLS transport

CERTIFICATION FINALE

Hors scope : évaluation et certification finale.

DÉPLOIEMENT MATÉRIEL

Hors scope : intégration matérielle et fabrication

EXCLUSIONS CIBLÉES POUR RESTER ATTEIGNABLE, MAÎTRISER LES DÉLAIS ET LIVRER DE LA VALEUR RAPIDEMENT.

ALIGNEMENT AVEC LES OBJECTIFS DU CHAPITRE 2

- **SÉCURITÉ RENFORCÉE PAR DESIGN** — Innovations fondées sur des primitives cryptographiques modernes. ✓
- **PERFORMANCE ET ADAPTABILITÉ** — Réduction de la latence et adaptation au contexte opérationnel. ✓
- **INTEROPÉRABILITÉ ET EXTENSIBILITÉ** — Conception modulaire et ouverte pour intégrer et faire évoluer. ✓
- **MAÎTRISE DES RISQUES ET DES DÉLAIS** — Périmètre focalisé pour une réalisation incrémentale et maitrisée. ✓

BRIQUE COMPLÉMENTAIRE RÉUTILISABLE

Un composant modulaire, ouvert et réutilisable dans de multiples systèmes et cas d'usage.

INTÉGRATION DANS LES SYSTÈMES EXISTANTS → RÉUTILISABLE DANS PLUSIEURS DOMAINES → ÉVOLUTIF ET EXTENSIBLE

COHÉRENT AVEC LE CHAPITRE 2.

INTÉGRABLE DANS LES INFRASTRUCTURES CRITIQUES SANS RUPTURE TECHNOLOGIQUE MAJEURE.



ANALYSE DETAILLEE
Chapitre 4
Exigences Fonctionnelles

AGENDA Chapitre 4 – Exigences Fonctionnelles

- 4.1 Signalisation adaptative client et décision d’adaptation serveur
- 4.2 Support multi-algorithmes post-quantiques et intégration du module QSA
- 4.3 Validation des tickets de session par ZKP et sécurisation du 0-RTT
- 4.4 Gestion des niveaux de sécurité et optimisation énergétique
- 4.5 Ouverture, extensibilité et compatibilité TLS

4.1 Signalisation adaptative client et décision d'adaptation serveur (EF-01 & EF-02)

EF-01 – Signalisation adaptative client (Priorité : Haute)

Le client IoT doit transmettre, dans le ClientHello ou via une extension dédiée, trois informations essentielles à l'adaptation :

- son niveau de batterie (valeur continue ou état discret : critique / bas / normal / élevé) ;
- son exigence de sécurité (Top Secret / Secret / Confidentiel) ;
- une estimation de la qualité du réseau (latence, débit disponible, taux d'erreur ou état du lien radio).

Cette signalisation doit être légère, authentifiée et résistante aux manipulations. Elle constitue la base informationnelle permettant au serveur de prendre une décision éclairée sans imposer un handshake complet systématique.

EF-02 – Décision d'adaptation serveur (Priorité : Haute)

Le serveur choisit dynamiquement la combinaison hybride (algorithmes classiques + post-quantiques) ainsi que les paramètres associés (taille de clé, nombre de rounds, niveau de robustesse) en fonction des signaux reçus et de sa politique de sécurité.

La décision doit garantir que le niveau de protection n'est jamais inférieur à l'exigence annoncée, tout en optimisant la consommation énergétique et le trafic lorsque le contexte le permet. La politique doit être configurable par l'opérateur d'infrastructure critique et traçable pour les audits.

4.1 Signalisation adaptative client et décision d'adaptation serveur (EF-01 & EF-02)

EF-01 SIGNALISATION ADAPTATIVE CLIENT

PRIORITÉ HAUTE

Le client transmet dans ClientHello ou une extension dédiée :

NIVEAU DE BATTERIE
Critique / Faible / Normal / Élevé

EXIGENCE DE SÉCURITÉ
Top Secret / Secret / Confidentiel

ESTIMATION RÉSEAU
Latence • Bande passante • Taux d'erreur

LÉGÈRE (faible overhead) | **AUTHENTIFIÉE** | **RÉSISTANTE AUX MANIPULATIONS**

EF-02 DÉCISION D'ADARTATION SERVEUR

PRIORITÉ HAUTE

Le serveur choisit dynamiquement :



Combinaison hybride (classique + post-quantique)
et paramètres adaptés selon les signaux et la politique de sécurité.

GARANTIT une protection jamais inférieure à l'exigence

OPTIMISE énergie et trafic lorsque possible.

POLITIQUE configurable par l'opérateur

TRAÇABLE pour audits

CLIENT émet ses signaux → **SERVEUR** évalue et décide → **ADAPTATION HYBRIDE** appliquée → **CONFORMITÉ & OPTIMISATION** garanties

4.2 Support multi-algorithmes post-quantiques et intégration du module QSA (EF-03 & EF-04)

EF-03 – Multi-algorithmes post-quantiques (Priorité : Haute)

Le protocole doit supporter au moins plusieurs algorithmes KEM et signatures post-quantiques validés ou en cours de validation NIST. L'interface doit être interchangeable afin de permettre l'ajout ou le remplacement d'algorithmes sans modification du cœur du handshake.

Cette exigence prépare les tests ACVP réalisés par des laboratoires accrédités et garantit l'évolutivité face aux futures évolutions des standards post-quantiques.

EF-04 – Intégration QSA (Priorité : Haute)

Le module QSA fournit les primitives cryptographiques post-quantiques. Le protocole les appelle via une interface standardisée, découplée de l'implémentation concrète.

Cette architecture permet d'utiliser QSA comme première implémentation tout en restant ouvert à d'autres bibliothèques ou modules. L'interface doit être documentée, stable et conçue pour faciliter les validations externes.

4.2 Support multi-algorithmes post-quantiques et intégration du module QSA (EF-03 & EF-04)

EF-03 Multi-algorithmes post-quantiques

PRIORITÉ HAUTE

Support multi-algorithmes PQ
KEM et signatures validés NIST (ou en validation)

Interface interchangeable
Ajout/remplacement d'algorithmes sans modifier le cœur du handshake

Prépare les tests ACVP
Évolutivité garantie et ready pour les validations et audits

NIST **Préparation ACVP**
Tests officiels de conformité

EF-04 Intégration QSA

PRIORITÉ HAUTE

QSA **Module QSA : primitives PQ**
Fournit les briques cryptographiques post-quantiques

Appels via interface standardisée
Découplé de l'implémentation concrète, ouvert à d'autres bibliothèques/modules

Interface documentée & stable
Conçue pour validations externes et audits indépendants

Interface standardisée, stable et auditable.

Multi-algorithmes post-quantiques | Interface interchangeable | Module QSA | NIST / ACVP | Interface standardisée

4.3 Validation des tickets de session par ZKP et sécurisation du 0-RTT (EF-05 & EF-06)

EF-05 – Validation de tickets par ZKP (Priorité : Haute)

Les tickets de session sont validés au moyen d'une preuve à divulgation nulle de connaissance (ZKP) ultra-rapide. Cette preuve garantit l'authenticité du ticket et la résistance quantique du mécanisme 0-RTT sans introduire de round-trip supplémentaire.

La génération et la vérification de la preuve doivent être suffisamment performantes pour ne pas annuler les bénéfices du 0-RTT (objectif : vérification en quelques microsecondes à quelques millisecondes maximum).

EF-06 – 0-RTT sûr pour les transactions critiques (Priorité : Haute)

Le 0-RTT n'est autorisé que si la preuve ZKP est valide et que le niveau de sécurité demandé le permet. Pour les transactions classées Top Secret ou critiques, la validation ZKP est obligatoire.

Cette exigence transforme le 0-RTT d'un mécanisme fragile en un outil utilisable de manière sûre, y compris dans un environnement post-quantique, tout en préservant les propriétés de forward secrecy et de résistance aux rejeux.

4.3 Validation des tickets de session par ZKP et sécurisation du 0-RTT (EF-05 & EF-06)



EF-05

Validation de tickets par ZKP

(Priorité Haute)

Les tickets de session sont validés par une preuve ZKP ultra-rapide garantissant authenticité et résistance quantique du 0-RTT sans aller-retour supplémentaire.

AUTHENTICITÉ GARANTIE
Preuve d'authenticité du ticket

RÉSISTANCE QUANTIQUE
Sécurisé contre les attaques quantiques

HAUTE PERFORMANCE
Génération & vérification en quelques microsecondes à millisecondes max*

Conçu pour ne pas annuler les bénéfices du 0-RTT

≤ quelques µs à ms max*



EF-06

0-RTT sûr pour transactions critiques

(Priorité Haute)

Le 0-RTT n'est autorisé que si la preuve ZKP est valide et si le niveau de sécurité le permet. Obligatoire pour les transactions Top Secret ou critiques.

AUTORISATION CONDITIONNELLE
Uniquement si ZKP valide et niveau de sécurité autorisé

OBLIGATOIRE POUR LE CRITIQUE
Requis pour Top Secret et transactions critiques

SÉCURITÉ RENFORCÉE
Post-quantique, confidentialité persistante et anti-replay

TRANSFORME LE 0-RTT
D'un mécanisme fragile à un outil sécurisé et utilisable

CONFIDENTIALITÉ PERSISTANTE
Préserve le secret forward

ANTI-REPLAY INTÉGRÉ
Protection efficace contre les rejeux

POST-QUANTIQUE
Prêt pour aujourd'hui et demain

ZKP + 0-RTT = SÉCURITÉ HAUTE PERFORMANCE • RÉSISTANCE QUANTIQUE • CONFIANCE ZÉRO

4.4 Gestion des niveaux de sécurité et optimisation énergétique (EF-07 & EF-08)

EF-07 – Gestion des niveaux de sécurité (Priorité : Moyenne)

Un mapping clair doit être défini et appliqué :

- Top Secret → hybride maximal (algorithmes PQ les plus robustes, paramètres élevés) ;
- Secret → hybride allégé (compromis performance/sécurité) ;
- Confidentiel → hybride minimal ou classique renforcé, selon la politique et l'état énergétique.

Ce mapping doit être documenté, configurable et vérifiable. Il constitue le cadre décisionnel du serveur lors de l'adaptation.

EF-08 – Optimisation énergétique (Priorité : Haute)

L'adaptation doit réduire significativement la consommation CPU et radio du client IoT par rapport à un handshake post-quantique non adaptatif.

Des métriques de référence (énergie par handshake, taille des messages, temps de calcul côté client) doivent être définies et mesurées. L'optimisation ne doit jamais compromettre le niveau de sécurité minimal requis par l'exigence annoncée.

4.4 Gestion des niveaux de sécurité et optimisation énergétique (EF-07 & EF-08)

EF-07
GESTION DES NIVEAUX DE SÉCURITÉ

PRIORITÉ MOYENNE

MAPPING DOCUMENTÉ, CONFIGURABLE ET VÉRIFIABLE

TOP SECRET
Niveau maximal → **HYBRID MAXIMAL**
PQ le plus robuste
Paramètres élevés

SECRET
Niveau standard → **HYBRID LIGHT**
Compromis performance et sécurité

CONFIDENTIEL
Niveau opérationnel → **HYBRID MINIMAL**
Ou classique renforcé selon politique et état énergétique

CONSTITUE LE CADRE DE DÉCISION DU SERVEUR

EF-08
OPTIMISATION ÉNERGÉTIQUE

PRIORITÉ HAUTE

ADAPTATION = MOINS DE CONSOMMATION

SANS ADAPTATION (PQ CLASSIQUE)

AVEC ADAPTATION (NIVEAU ADAPTÉ)



MÉTRIQUES DE RÉFÉRENCE DÉFINIES ET MESURÉES

- ÉNERGIE PAR HANDSHAKE
- TAILLE DES MESSAGES
- TEMPS DE CALCUL CLIENT

L'OPTIMISATION N'ALTÈRE JAMAIS LE NIVEAU DE SÉCURITÉ MINIMAL REQUIS

SÉCURITÉ ADAPTATIVE • PERFORMANCE INTELLIGENTE • AUTONOMIE RENFORCÉE

4.5 Ouverture, extensibilité et compatibilité TLS (EF-09 & EF-10)

EF-09 – Ouverture et extensibilité (Priorité : Moyenne)

L'architecture doit permettre l'ajout d'algorithmes post-quantiques sans modification du cœur du handshake. Les interfaces (sélection d'algorithmes, appel des primitives, politique d'adaptation) doivent être stables, documentées et conçues pour une évolution future.

Cette exigence garantit que le protocole reste ouvert et complémentaire des produits existants, tout en facilitant l'intégration de nouvelles primitives validées par le NIST.

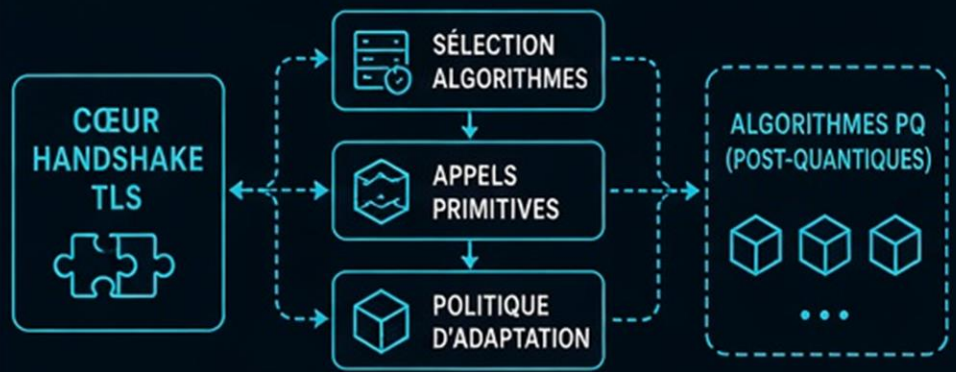
EF-10 – Compatibilité TLS (Priorité : Haute)

Le protocole s'appuie sur TLS 1.3 via des extensions standards ou clairement documentées afin de rester interopérable avec les piles TLS existantes.

Aucune réécriture de la couche transport n'est requise. Les mécanismes d'adaptation, de signalisation et de validation ZKP doivent s'intégrer de manière non disruptive, permettant un déploiement progressif sur les infrastructures critiques.

4.5 Ouverture, extensibilité et compatibilité TLS (EF-09 & EF-10)

EF-09
Ouverture et extensibilité
(Priorité Moyenne)



Interfaces stables, documentées et pensées pour l'évolution future.

Ouvert et complémentaire aux produits existants.
Facilite l'intégration de nouvelles primitives validées par le NIST.

EF-10
Compatibilité TLS
(Priorité Haute)



Extensions standard ou clairement documentées

Déploiement progressif et sans rupture sur les infrastructures critiques.

Ouverture aujourd'hui. Compatibilité garantie. Sécurité durable.

EXTENSIBLE | INTEROPÉRABLE | PRÊT POUR L'AVENIR

ANALYSE DETAILLEE
Chapitre 5
Architecture Fonctionnelle

AGENDA Chapitre 5 – Architecture Fonctionnelle

- 5.1 Module de signalisation client
- 5.2 Moteur de décision adaptative (serveur)
- 5.3 Couche d’abstraction multi-algorithmes post-quantiques
- 5.4 Moteur ZKP de validation de tickets
- 5.5 Gestionnaire de politique de sécurité et d’énergie

5.1 Module de signalisation client

Le module de signalisation client est le point d'entrée du handshake adaptatif. Il collecte et transmet, de manière légère et sécurisée, les informations de contexte nécessaires à la décision serveur :

- niveau de batterie (ou état discret : critique / bas / normal / élevé) ;
- exigence de sécurité (Top Secret / Secret / Confidentiel) ;
- qualité du réseau estimée (latence, débit, taux d'erreur ou état du lien radio).

Ces données sont encapsulées dans une extension du ClientHello (ou mécanisme équivalent compatible TLS 1.3). Le module doit garantir l'intégrité et l'authenticité de la signalisation afin d'éviter toute manipulation malveillante. Il est conçu pour rester minimal en termes de taille de message et de consommation énergétique, afin de ne pas pénaliser les équipements IoT contraints. Une fois la signalisation émise, le client attend la décision du serveur avant de poursuivre l'établissement des clés.

5.1 Module de signalation client

Point d'entrée de la négociation adaptative

MODULE CLIENT

NIVEAU BATTERIE
Critique / Faible / Normal / Élevé

EXIGENCE DE SÉCURITÉ
Top Secret / Secret / Confidentiel

QUALITÉ RÉSEAU ESTIMÉE
Latence • Bande passante
• Taux d'erreur •
• Liaison radio

Début de la négociation adaptative

Transmission légère et sécurisée

CLIENTHELLO EXTENSION
(ou équivalent TLS 1.3 compatible)

Contexte client | Intégrité | Authenticité

Données encapsulées et protégées

INTÉGRITÉ & AUTHENTICITÉ GARANTIES

Vérification de l'intégrité
Détection de toute modification

Authenticité assurée
Origine client vérifiée

Empêche la manipulation malveillante

SERVEUR
Décision adaptative basée sur le contexte reçu

Le client attend la décision du serveur avant de poursuivre l'établissement des clés

Négociation adaptative sécurisée et efficace

EMPREINTE MINIMALE
Taille de message minimale

CONSOMMATION ÉNERGÉTIQUE OPTIMISÉE
Conçu pour les IoT contraints

CONÇU POUR L'IoT
Léger • Sécurisé • Efficace

5.2 Moteur de décision adaptative (serveur)

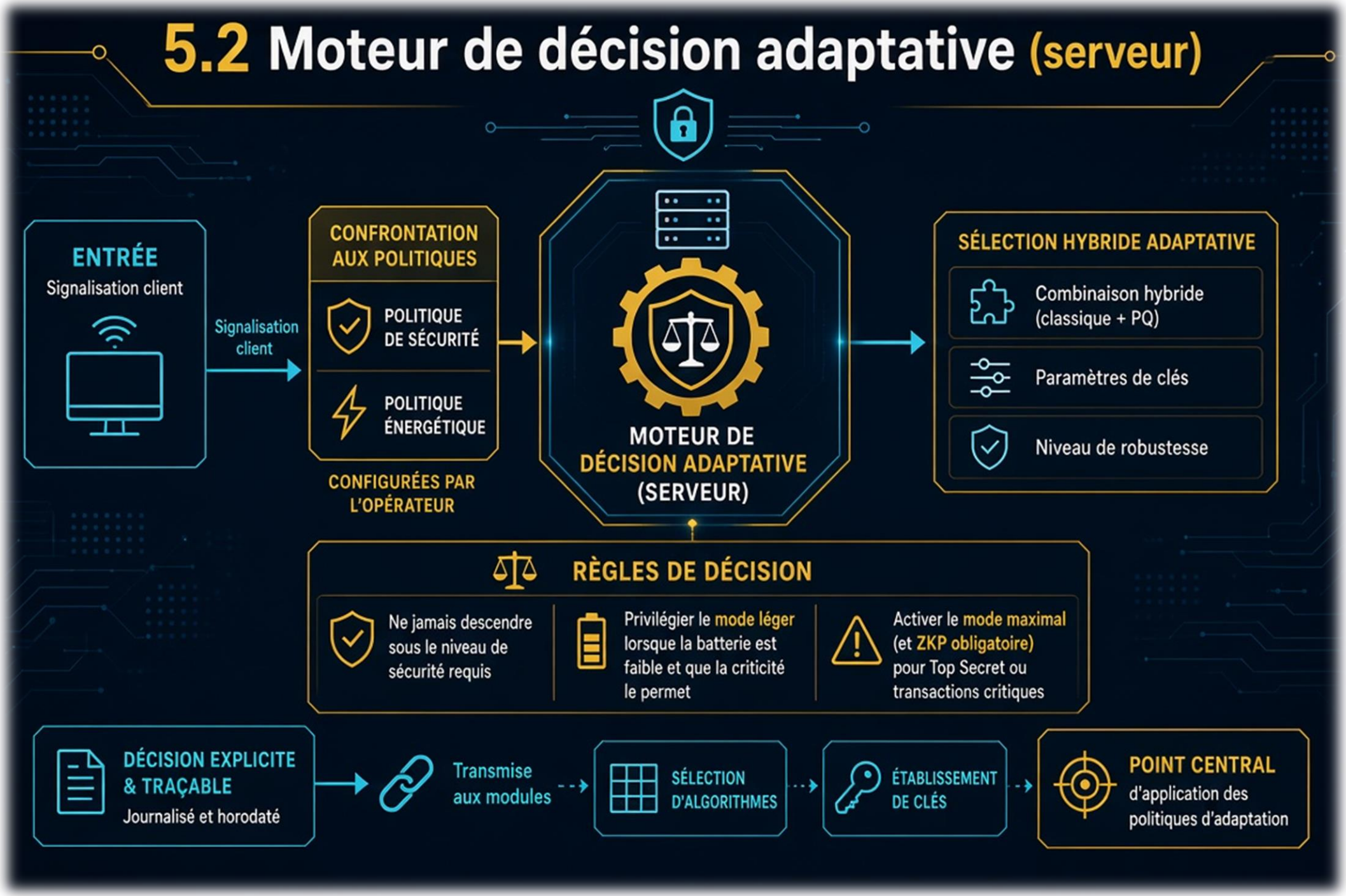
Le moteur de décision adaptative est le cœur logique côté serveur. Il reçoit la signalisation du client, la confronte à la politique de sécurité et d'énergie configurée par l'opérateur, puis sélectionne la combinaison hybride appropriée (algorithmes classiques + post-quantiques, paramètres de clés, niveau de robustesse).

La décision doit respecter les règles suivantes :

- ne jamais descendre en dessous du niveau de sécurité exigé ;
- privilégier un mode allégé lorsque la batterie est faible et que la criticité le permet ;
- activer le mode maximal (et la validation ZKP obligatoire) pour les exigences Top Secret ou les transactions critiques.

Le moteur produit une décision explicite et traçable qui est ensuite transmise aux modules de sélection d'algorithmes et d'établissement des clés. Il constitue le point central d'application des politiques d'adaptation.

5.2 Moteur de décision adaptative (serveur)



5.3 Couche d’abstraction multi-algorithmes post-quantiques

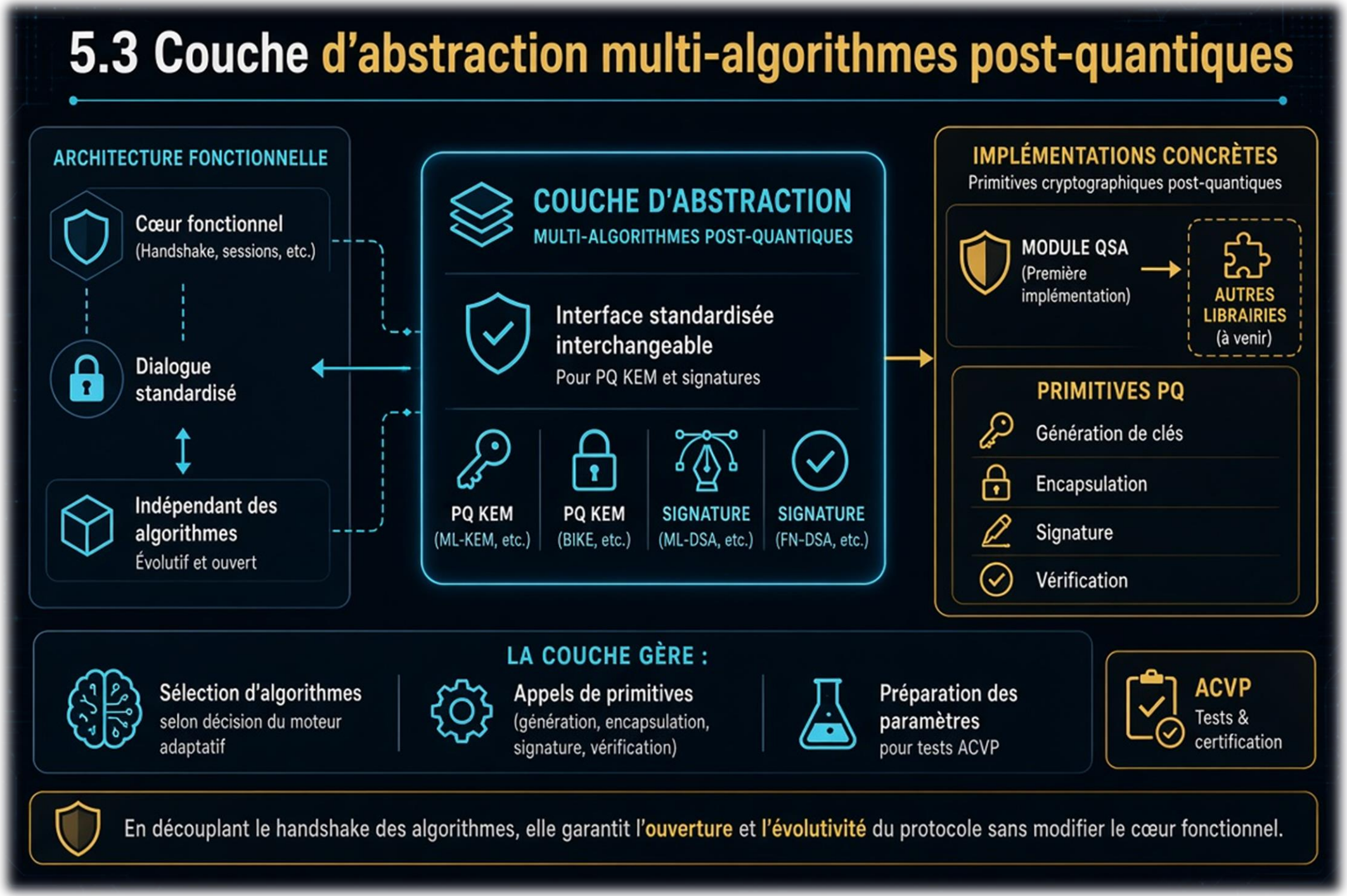
La couche d’abstraction multi-algorithmes post-quantiques isole le reste de l’architecture des implémentations concrètes des primitives cryptographiques. Elle offre une interface standardisée permettant d’appeler plusieurs algorithmes KEM et signatures post-quantiques de manière interchangeable.

Cette couche dialogue directement avec le module QSA (première implémentation) et peut accueillir d’autres bibliothèques. Elle gère :

- la sélection de l’algorithme selon la décision du moteur adaptatif ;
- l’appel des primitives (génération de clés, encapsulation, signature, vérification) ;
- la préparation des paramètres pour les tests ACVP.

En découplant le handshake des algorithmes, elle garantit l’ouverture et l’évolutivité du protocole sans modification du cœur fonctionnel.

5.3 Couche d'abstraction multi-algorithmes post-quantiques



5.4 Moteur ZKP de validation de tickets

Le moteur ZKP de validation de tickets est responsable de la sécurisation du 0-RTT. Lors de la création d'un ticket de session, il génère une preuve à divulgation nulle de connaissance prouvant la possession de la clé de session et l'intégrité du ticket, sans la révéler.

Lors d'une reprise 0-RTT, le client présente le ticket accompagné de la preuve. Le moteur vérifie cette preuve de manière ultra-rapide (objectif : quelques microsecondes à quelques millisecondes). Si la preuve est valide et que le niveau de sécurité le permet, le 0-RTT est accepté sans round-trip supplémentaire, y compris pour les transactions critiques. Ce module garantit ainsi l'authenticité, la résistance aux rejeux et la compatibilité post-quantique du mécanisme 0-RTT.

5.4 Moteur ZKP de validation de tickets

Sécurisation du 0-RTT avec preuves à divulgation nulle

CRÉATION DU TICKET DE SESSION



Génère une preuve ZKP :

- ✓ possession de la clé de session
- ✓ intégrité du ticket
- ✓ sans rien révéler

PREUVE ZKP →



MOTEUR ZKP

Validation ultra-rapide

µs à ms

→ VÉRIFICATION

REPRISE 0-RTT



Le client présente :

- ticket
- preuve ZKP

VÉRIFICATION ULTRA-RAPIDE
(quelques microsecondes à millisecondes)

NIVEAU DE SÉCURITÉ AUTORISÉ

0-RTT ACCEPTÉ
sans aller-retour supplémentaire
y compris pour les transactions critiques

GARANTIES

AUTHENTICITÉ
Preuves cryptographiques infalsifiables

ANTI-REJEU
Protection forte contre les attaques de replay

COMPATIBILITÉ POST-QUANTIQUE
Résistant aux ordinateurs quantiques

Confidentialité • Intégrité • Performance

5.5 Gestionnaire de politique de sécurité et d'énergie

Le gestionnaire de politique de sécurité et d'énergie fournit le cadre décisionnel utilisé par le moteur de décision adaptative. Il définit et applique le mapping entre les exigences de sécurité et les modes hybrides :

- Top Secret → hybride maximal ;
- Secret → hybride allégé ;
- Confidentiel → hybride minimal ou classique renforcé.

Il intègre également les contraintes énergétiques (seuils de batterie, objectifs de réduction de consommation CPU/radio) et les règles d'activation de la validation ZKP. Ce gestionnaire est configurable par l'opérateur d'infrastructure critique et permet d'ajuster le comportement du protocole selon les secteurs (énergie, froid, trafic, etc.) sans modifier le code du handshake. Il assure la cohérence globale entre sécurité, performance et autonomie des équipements IoT.

5.5 Gestionnaire de politique de sécurité et d'énergie

GESTIONNAIRE DE POLITIQUE

Fournit le cadre de décision

CADRE DE DÉCISION

Fourni au moteur de décision adaptatif

MOTEUR DE DÉCISION ADAPTATIF

MAPPING DE SÉCURITÉ

Top Secret	HYBRID MAXIMAL
Secret	HYBRID LIGHT
Confidentiel	HYBRID MINIMAL OU CLASSIQUE RENFORCÉ

CONTRAINTES ÉNERGÉTIQUES

- Seuils batterie (critiques / bas / moyen)
- Réduction CPU (objectifs)
- Réduction radio (objectifs)

ACTIVATION ZKP

RÈGLES D'ACTIVATION

Conditions de niveau de sécurité, d'énergie et de contexte

CONFIGURABLE PAR L'OPÉRATEUR D'INFRASTRUCTURES CRITIQUES

Ajuste le comportement des protocoles par secteur sans modifier le code du handshake

ÉNERGIE · FROID · TRAFFIC · AUTRES SECTEURS

ASSURE LA COHÉRENCE GLOBALE

entre sécurité, performance et autonomie des équipements IoT

SÉCURITÉ · PERFORMANCE · AUTONOMIE

ANALYSE DETAILLEE
Chapitre 6
Description des Fonctions Principales

AGENDA Chapitre 6 – Description des Fonctions Principales

- 6.1 Handshake Hybride Adaptatif
- 6.2 Interface Multi-Algorithmes Post-Quantiques
- 6.3 Protocole de Validation de Tickets par ZKP
- 6.4 Optimisation Énergétique et Réduction du Trafic
- 6.5 Gestion des Politiques et Mapping des Niveaux de Sécurité

6.1 Handshake Hybride Adaptatif

La fonction de handshake hybride adaptatif constitue le mécanisme central du protocole. Le client IoT envoie, dans une extension du ClientHello, une signalisation contenant :

- le niveau de batterie (pourcentage ou état discret : critique / bas / normal / élevé) ;
- l'exigence de sécurité (Top Secret / Secret / Confidentiel) ;
- une estimation de la qualité du réseau (latence, bande passante disponible, taux de perte de paquets).

Le serveur applique une politique configurable pour choisir la combinaison d'algorithmes et les paramètres associés. À titre d'exemple : un mode Kyber-512 + AES-GCM peut être retenu si la batterie est faible et l'exigence est Secret ; un mode Kyber-1024 + Dilithium + AES-GCM est sélectionné si l'exigence est Top Secret et que la batterie est correcte.

Cette fonction garantit que le niveau de protection post-quantique n'est jamais inférieur à l'exigence annoncée, tout en optimisant la taille des messages et la charge computationnelle côté client. Elle s'appuie sur TLS 1.3 via des extensions afin de rester interopérable.

6.1 Handshake Hybride Adaptatif

CLIENT IoT

SIGNALISATION DANS
ClientHello (EXTENSION)

NIVEAU DE BATTERIE
32%
CRITIQUE / FAIBLE

EXIGENCE DE SÉCURITÉ
SECRET

QUALITÉ RÉSEAU (ESTIMATION)

LATENCE	BANDE PASSANTE	PERTE PAQUETS
120 ms	MOYENNE	2%

ENVOI DANS EXTENSION
ClientHello

HANDSHAKE HYBRIDE ADAPTATIF

ADAPTÉ AU CONTEXTE DU CLIENT

SERVEUR : POLITIQUE CONFIGURABLE

POLITIQUE ADAPTATIVE

- NIVEAU BATTERIE
- EXIGENCE DE SÉCURITÉ
- QUALITÉ RÉSEAU

CHOIX DE LA COMBINAISON HYBRIDE ET DES PARAMÈTRES

COMBINAISONS HYBRIDES EXEMPLES

FAIBLE BATTERIE ET SECRET
↓
Kyber-512 + AES-GCM

TOP SECRET ET BATTERIE CORRECTE
↓
Kyber-1024 + Dilithium + AES-GCM

PROTECTION POST-QUANTIQUE JAMAIS INFÉRIEURE À L'EXIGENCE ANNONCÉE

OPTIMISE LA TAILLE DES MESSAGES ET LA CHARGE CALCUL CLIENT

ÉQUILIBRE SÉCURITÉ, PERFORMANCE ET AUTONOMIE

REPOSE SUR TLS 1.3

VIA EXTENSIONS POUR UNE INTEROPÉRABILITÉ MAXIMALE

EXTENSIBLE | INTEROPÉRABLE | RÉTROCOMPATIBLE | STANDARD TLS 1.3

6.2 Interface Multi-Algorithmes Post-Quantiques

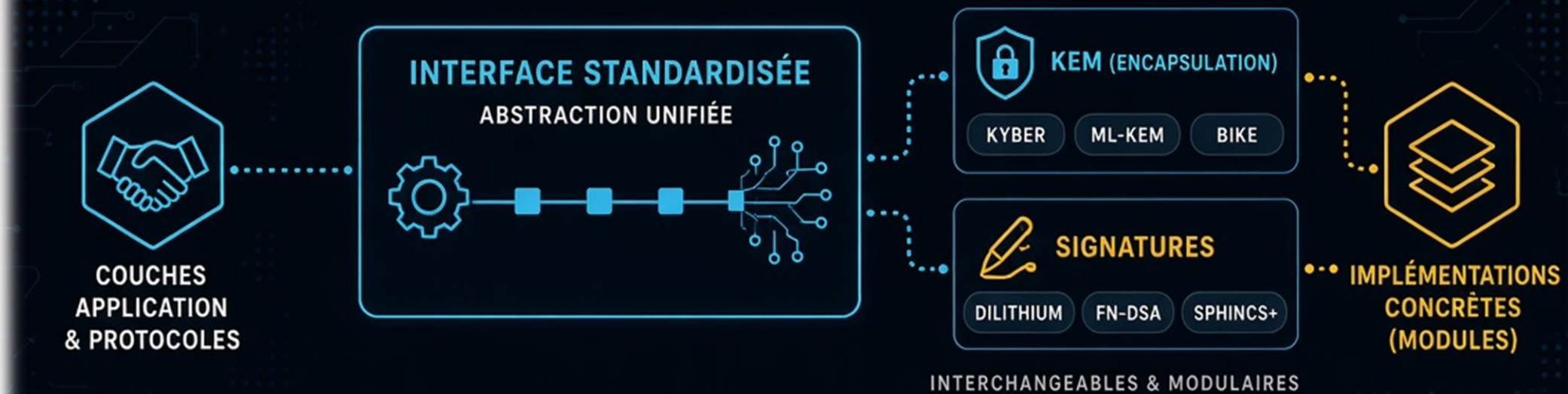
L'interface multi-algorithmes post-quantiques fournit une couche d'abstraction permettant de brancher plusieurs KEM et signatures de manière interchangeable. Elle découple le handshake des implémentations concrètes des primitives cryptographiques.

Les caractéristiques principales sont :

- support d'au moins plusieurs algorithmes validés ou en cours de validation NIST ;
- interface standardisée prévue pour faciliter les tests ACVP réalisés par des laboratoires accrédités ;
- le module QSA constitue la première implémentation ; d'autres bibliothèques ou modules peuvent être ajoutés sans modification du cœur du protocole.

Cette fonction assure l'ouverture et l'évolutivité du système face aux futures évolutions des standards post-quantiques, tout en permettant une intégration immédiate avec les outils déjà développés.

6.2 Interface Multi-Algorithmes Post-Quantiques



CONÇUE POUR LA CONFORMITÉ, L'OUVERTURE ET L'ÉVOLUTIVITÉ

SUPPORT MULTI-ALGORITHMES
NIST validés ou en validation

INTERFACE NORMALISÉE
Conçue pour les tests ACVP par laboratoires accrédités

QSA EN PREMIER
Module de référence extensible. Ajout de nouvelles bibliothèques sans modifier le cœur du protocole.

OUVERTURE & ÉVOLUTIVITÉ
Prêt pour les futures normes post-quantiques sans refonte de l'architecture.

INTÉGRATION IMMÉDIATE
Compatible avec les outils et développements existants dès aujourd'hui.

SÉCURITÉ POST-QUANTIQUE • INTEROPÉRABILITÉ • ÉVOLUTIVITÉ • CONFORMITÉ

6.3 Protocole de Validation de Tickets par ZKP

La fonction de validation de tickets par preuves à divulgation nulle de connaissance (ZKP) sécurise le mécanisme 0-RTT. Lors de la création d'un ticket de session, une preuve ZKP est générée. Elle prouve la possession de la clé de session et l'intégrité du ticket sans la révéler.

Lors d'une reprise de session, le client présente le ticket accompagné de la preuve. Le serveur vérifie cette preuve de manière ultra-rapide (objectif : quelques microsecondes à quelques millisecondes). Si la preuve est valide, le 0-RTT est accepté sans round-trip supplémentaire, y compris pour les transactions critiques.

Cette fonction garantit l'authenticité du ticket, la résistance aux attaques de rejeu et la préservation des propriétés de sécurité post-quantique, transformant le 0-RTT en un mécanisme utilisable de manière sûre dans un environnement quantique.

6.3 Protocole de Validation de Tickets par ZKP

1 CRÉATION DU TICKET DE SESSION



Preuve ZKP générée
Prouve la possession de la clé de session et l'intégrité du ticket sans les révéler

Le ticket reste opaque et protégé

2 REPRISE DE SESSION



VÉRIFICATION ULTRA-RAPIDE
Quelques microsecondes à millisecondes

Preuve valide → 0-RTT accepté
Sans aller-retour supplémentaire, même pour les transactions critiques



GARANTIES DE SÉCURITÉ

AUTHENTICITÉ DU TICKET
Preuve cryptographique infalsifiable

ANTI-REJEU
Protection forte contre les attaques de rejeu

SÉCURITÉ POST-QUANTIQUE
Résistant aux attaques quantiques

0-RTT SÉCURISÉ
Transforme le 0-RTT en mécanisme utilisable en environnement quantique

ZKP + TICKETS = 0-RTT SÉCURISÉ ET POST-QUANTIQUE

Preuve rapide • Confidentialité préservée • Résistance quantique • Utilisable en production

6.4 Optimisation Énergétique et Réduction du Trafic

Cette fonction vise à réduire significativement la consommation CPU et radio du client IoT ainsi que le trafic réseau inutile. Elle s'appuie sur les décisions du handshake adaptatif pour :

- sélectionner des algorithmes et des paramètres plus légers lorsque le contexte (batterie faible, exigence modérée) le permet ;
- limiter la taille des messages de handshake et des échanges cryptographiques ;
- activer, le cas échéant, des mécanismes de compression des données applicatives.

Des métriques de référence (énergie par handshake, taille des messages, temps de calcul côté client) sont définies pour mesurer les gains. L'optimisation ne doit jamais compromettre le niveau de sécurité minimal requis. Cette fonction est essentielle pour rendre le protocole viable sur des capteurs à autonomie limitée déployés dans les infrastructures critiques.

6.4 Optimisation Énergétique et Réduction du Trafic



Fonction : réduire fortement la consommation du client IoT ainsi que le trafic réseau inutile

OPTIMISATION ÉNERGÉTIQUE





Moins de CPU et radio
→ plus d'autonomie

RÉDUCTION DU TRAFIC



Moins de trafic réseau
→ moins de congestion

S'appuie sur des décisions de handshake adaptatives

ALGORITHMES ET PARAMÈTRES ALLÉGÉS

Sélectionne des algorithmes et paramètres plus légers quand le contexte le permet (batterie faible, exigence modérée).

TAILLE MAÎTRISÉE

Limite la taille des messages de handshake et des échanges cryptographiques.

COMPRESSION DES DONNÉES

Active la compression des données applicatives lorsque applicable.

MÉTRIQUES DE RÉFÉRENCE POUR MESURER LES GAINS

ÉNERGIE PAR HANDSHAKE
↓ gain

TAILLE DES MESSAGES
↓ gain

TEMPS DE CALCUL CLIENT
↓ gain

L'OPTIMISATION NE COMPROMET JAMAIS LE NIVEAU MINIMAL DE SÉCURITÉ REQUIS

ESSENTIEL POUR RENDRE LE PROTOCOLE VIABLE SUR DES CAPTEURS À AUTONOMIE LIMITÉE DANS LES INFRASTRUCTURES CRITIQUES.

6.5 Gestion des Politiques et Mapping des Niveaux de Sécurité

La fonction de gestion des politiques définit et applique le mapping entre les exigences de sécurité, l'état énergétique et les modes hybrides :

- Top Secret → hybride maximal (algorithmes PQ les plus robustes, paramètres élevés, ZKP obligatoire pour le 0-RTT) ;
- Secret → hybride allégé (compromis performance/sécurité) ;
- Confidentiel → hybride minimal ou classique renforcé, selon la politique et l'état de la batterie.

Cette fonction est configurable par l'opérateur d'infrastructure critique. Elle alimente le moteur de décision adaptative et assure la cohérence globale entre sécurité, performance et autonomie. Elle permet d'adapter le comportement du protocole aux spécificités des différents secteurs (énergie, chaîne du froid, contrôle de trafic) sans modifier le code du handshake, garantissant ainsi une industrialisation progressive et maîtrisée.

6.5 Gestion des Politiques et Mapping des Niveaux de Sécurité

GESTION DES POLITIQUES

Définit et applique le mapping entre
exigences de sécurité, état énergétique et modes hybrides

TOP SECRET →	HYBRID MAXIMAL	PQ le plus robuste, paramètres élevés, ZKP obligatoire pour 0-RTT
SECRET →	HYBRID LIGHT	Compromis performance / sécurité
CONFIDENTIEL →	HYBRID MINIMAL ou CLASSIQUE RENFORCÉ	Selon politique et état de la batterie

CONFIGURABLE
par l'opérateur d'infrastructure critique

MOTEUR DE DÉCISION ADAPTATIF
Alimenté par les politiques et états temps réel

Cohérence globale
Sécurité • Performance • Autonomie

COHÉRENCE GARANTIE
Entre sécurité, performance et autonomie à chaque décision

ADAPTÉ AUX SECTEURS
energy, cold chain, traffic control

- ÉNERGIE
- CHAÎNE DU FROID
- CONTRÔLE DU TRAFIC

ADAPTATION SANS MODIFICATION
Adapte le comportement du protocole aux spécificités sectorielles **sans toucher au code du handshake**

INDUSTRIALISATION PROGRESSIVE ET CONTRÔLÉE

- Déploiement par politique
- Maîtrise des risques
- Évolutivité sécurisée

ANALYSE DETAILLEE
Chapitre 7
Contraintes Techniques et Non-Fonctionnelles

AGENDA Chapitre 7 – Contraintes Techniques et Non-Fonctionnelles

- 7.1 Contraintes de performance réseau
- 7.2 Contraintes énergétiques
- 7.3 Contraintes de sécurité
- 7.4 Interopérabilité et maintenabilité
- 7.5 Robustesse et comportement en mode dégradé

7.1 Contraintes de performance réseau

La performance réseau est une contrainte critique pour le déploiement sur des équipements IoT et des infrastructures critiques. Le handshake adaptatif doit présenter une latence inférieure ou égale à celle d'un handshake TLS 1.3 classique, augmentée d'un overhead minimal lié à la signalisation et à la sélection hybride.

La vérification de la preuve ZKP, élément clé de la sécurisation du 0-RTT, doit être réalisée en moins de 1 milliseconde. Cet objectif garantit que le mécanisme 0-RTT conserve son intérêt (absence de round-trip supplémentaire) même pour des transactions critiques.

Des mesures de référence (temps de handshake complet, temps de vérification ZKP, taille des messages) doivent être définies et suivies tout au long du développement afin de valider le respect de ces contraintes dans des conditions réseau représentatives (liens stables, liens dégradés, réseaux contraints).

7.1 Contraintes de performance réseau



LA PERFORMANCE RÉSEAU EST UNE CONTRAINTE CRITIQUE POUR LE DÉPLOIEMENT SUR IOT ET INFRASTRUCTURES CRITIQUES

Garantir des échanges rapides, légers et fiables dans des conditions réseau variées.



IOT ET INFRASTRUCTURES CRITIQUES
(INDUSTRIE, ÉNERGIE, TRANSPORT, VILLES, SANTÉ...)

HANDSHAKE ADAPTATIF

LATENCE ≤ HANDSHAKE TLS 1.3 CLASSIQUE
+ SURCOÛT MINIMAL DE SIGNALISATION
ET DE SÉLECTION HYBRIDE



TLS 1.3 — HANDSHAKE ADAPTATIF

MÊME LATENCE, EMPREINTE LÉGÈRE

VÉRIFICATION ZKP (POUR 0-RTT)

< 1 ms

PRÉSERVE L'INTÉRÊT DU 0-RTT
AUCUN ALLER-RETOUR SUPPLÉMENTAIRE,
MÊME POUR LES TRANSACTIONS CRITIQUES

MESURES DE RÉFÉRENCE DÉFINIES ET SUIVIES

POUR VALIDER LES CONTRAINTES DANS DES CONDITIONS RÉSEAU REPRÉSENTATIVES

TEMPS DE HANDSHAKE COMPLET	TEMPS DE VÉRIFICATION ZKP	TAILLE DES MESSAGES
MESURÉ DE BOUT EN BOUT	< 1 ms	SURCOÛT MINIMAL

RÉSEAUX STABLES ----------> RÉSEAUX DÉGRADÉS ----------> LIENS CONTRAINTS

MESURES RÉFÉRENCES → DÉVELOPPEMENT → VALIDATION CONTINUE

7.2 Contraintes énergétiques

L'optimisation énergétique constitue une exigence non-fonctionnelle majeure. L'adaptation du handshake doit produire une réduction mesurable de la consommation CPU et radio du client IoT par rapport à un handshake post-quantique non adaptatif.

Cette réduction doit être quantifiée selon des métriques claires : énergie consommée par handshake, durée d'activité radio, charge de calcul côté client. Les gains doivent être significatifs dans les scénarios où la batterie est faible ou moyenne et où le niveau de sécurité le permet (modes Secret ou Confidentiel).

La contrainte énergétique ne doit jamais être satisfaite au détriment du niveau de sécurité minimal requis. Des campagnes de mesures sur des plateformes représentatives des capteurs industriels sont nécessaires pour valider les objectifs d'autonomie.

7.2 Contraintes énergétiques

L'adaptation de la poignée de main doit produire une réduction mesurable de la consommation CPU et radio du client IoT

VS Poignée de main post-quantique non adaptative

QUANTIFIÉ PAR DES MÉTRIQUES CLÉS

ÉNERGIE CONSOMMÉE PAR POIGNÉE DE MAIN
µJ
(microjoules)

DURÉE D'ACTIVITÉ RADIO
ms
(millisecondes)

CHARGE DE CALCUL CÔTÉ CLIENT
% CPU
(moyenne)

SCÉNARIOS BATTERIE

FAIBLE MOYENNE

GAINS SIGNIFICATIFS
si le niveau de sécurité le permet

SECRET CONFIDENTIEL

SÉCURITÉ D'ABORD

LA CONTRAINTE ÉNERGÉTIQUE N'EST JAMAIS SATISFAITE AU DÉTRIMENT DU NIVEAU MINIMAL DE SÉCURITÉ REQUIS

CAMPAGNES DE MESURE

SUR PLATEFORMES REPRÉSENTATIVES DE CAPTEURS INDUSTRIELS POUR VALIDER LES OBJECTIFS D'AUTONOMIE



L'OPTIMISATION ÉNERGÉTIQUE : UNE EXIGENCE NON FONCTIONNELLE MAJEURE

7.3 Contraintes de sécurité

Les contraintes de sécurité portent sur trois axes principaux :

- **Résistance quantique** : le protocole doit offrir une résistance aux attaques quantiques d'au moins le niveau NIST 1, ou supérieur selon la politique appliquée et l'exigence de sécurité (Top Secret pouvant requérir un niveau plus élevé).
- **Forward secrecy** : les propriétés de forward secrecy doivent être conservées, y compris dans les modes hybrides allégés.
- **Sécurité du 0-RTT** : le mécanisme 0-RTT doit être résistant aux attaques de rejeu grâce à la validation par preuve ZKP. Aucune reprise de session critique ne doit être acceptée sans preuve valide.

Ces contraintes doivent être vérifiées par des analyses cryptographiques et des tests d'intrusion ciblés, en complément des validations ACVP des primitives sous-jacentes.

7.3 Contraintes de sécurité

Trois axes principaux

1 Résistance quantique

Au moins **NIST level 1,** ou supérieur selon la politique et les exigences

Top Secret : potentiellement supérieur

2 Forward secrecy

Propriétés **conservées,** y compris dans les modes hybrides légers

3 Sécurité du 0-RTT

Résistant aux attaques de réplication grâce à la validation de preuve **ZKP**

Aucune reprise de session critique **sans preuve valide**

Vérifiés par :

- Analyses cryptographiques
- Tests d'intrusion ciblés
- En complément des validations **ACVP** des primitives sous-jacentes

7.4 Interopérabilité et maintenabilité

Interopérabilité

Le protocole doit s'appuyer sur des extensions TLS standards ou clairement documentées afin de rester compatible avec les piles TLS 1.3 existantes. Aucune modification invasive de la couche transport n'est autorisée. Les mécanismes de signalisation, de décision adaptative et de validation ZKP doivent pouvoir être déployés de manière progressive et non disruptive.

Maintenabilité

Le code doit être ouvert, les interfaces stables et documentées. Les tests ACVP doivent être automatisables afin de faciliter les validations externes par des laboratoires accrédités. L'architecture modulaire (abstraction multi-algorithmes, gestionnaire de politiques) doit permettre l'évolution des primitives post-quantiques sans remise en cause du cœur du handshake. Ces exigences garantissent la pérennité et l'adoptabilité industrielle du protocole.

7.4 Interopérabilité et maintenabilité

INTEROPÉRABILITÉ

Protocole s'appuyant sur des extensions TLS standard ou clairement documentées pour rester compatible avec les piles TLS 1.3 existantes.

TLS 1.3

Aucune modification invasive de la couche transport n'est autorisée.

COUCHE TRANSPORT

Mécanismes de signalisation, décision adaptative et validation ZKP déployables progressivement et de manière non disruptive.

SIGNALISATION → DÉCISION ADAPTATIVE → VALIDATION ZKP

MAINTENABILITÉ

Code ouvert, interfaces stables et documentées.

INTERFACES STABLES & DOCUMENTÉES

Tests ACVP automatisables pour validations externes par des laboratoires accrédités.

ACVP

ACVP
TESTS AUTOMATISABLES

Architecture modulaire : abstraction multi-algorithmes et gestionnaire de politiques permettent l'évolution des primitives PQ sans remettre en cause le cœur du handshake.



Ces exigences garantissent **DURABILITÉ** et **ADOPTABILITÉ INDUSTRIELLE.**

7.5 Robustesse et comportement en mode dégradé

Le protocole doit présenter un comportement robuste et prévisible en cas d'anomalie. Si la signalisation client est absente, incomplète ou malformée, le système doit adopter un comportement dégradé contrôlé : application d'une politique par défaut sécurisée (par exemple mode hybride standard ou refus du 0-RTT critique) sans provoquer d'échec non maîtrisé de la connexion.

Les cas d'erreur (preuve ZKP invalide, algorithme non supporté, dépassement de seuils énergétiques) doivent être explicitement gérés, journalisés et traçables. Cette robustesse est essentielle pour un déploiement sur des infrastructures critiques où la continuité de service et la prévisibilité du comportement sont prioritaires. Des tests de robustesse (fuzzing de la signalisation, injection d'erreurs) doivent être intégrés au plan de validation.

7.5 Robustesse et comportement en mode dégradé

Le protocole adopte un comportement robuste et prévisible en cas d'anomalie.

COMPORTEMENT NORMAL

Signalisation client présente, complète et valide

Connexion sécurisée et optimisée

ABSENCE, SIGNALISATION INCOMPLÈTE OU MALFORMÉE

Détection d'anomalie

MODE DÉGRADÉ CONTRÔLÉ

Application d'une politique par défaut sécurisée (ex. mode hybride standard)

Refus du 0-RTT critique

sans échec de connexion incontrôlé

GESTION EXPLICITE DES ERREURS

Preuve ZKP invalide
Rejet + journalisation + alerte

Algorithme non supporté
Négociation sécurisée ou refus explicite

Seuil d'énergie dépassé
Limitation ou refus + journalisation

JOURNALISATION ET TRAÇABILITÉ
Événements horodatés, contextes conservés, audits facilités

ESSENTIEL POUR LES INFRASTRUCTURES CRITIQUES

Continuité de service et comportement prévisible en toutes circonstances.

DISPONIBILITÉ · PRÉVISIBILITÉ · CONFIANCE

TESTS DE ROBUSTESSE INTÉGRÉS AU PLAN DE VALIDATION

FUZZING DE SIGNALISATION → INJECTION D'ERREURS → SCÉNARIOS DE DÉGRADATION → MÉTRIQUE & RAPPORTS

Validation continue pour garantir robustesse et prédictibilité

Robustesse • Prévisibilité • Sécurité • Traçabilité : les piliers d'un protocole prêt pour le monde réel.

ANALYSE DETAILLEE
Chapitre 8
Cas d’Usage Principaux

AGENDA Chapitre 8 – Cas d’Usage Principaux

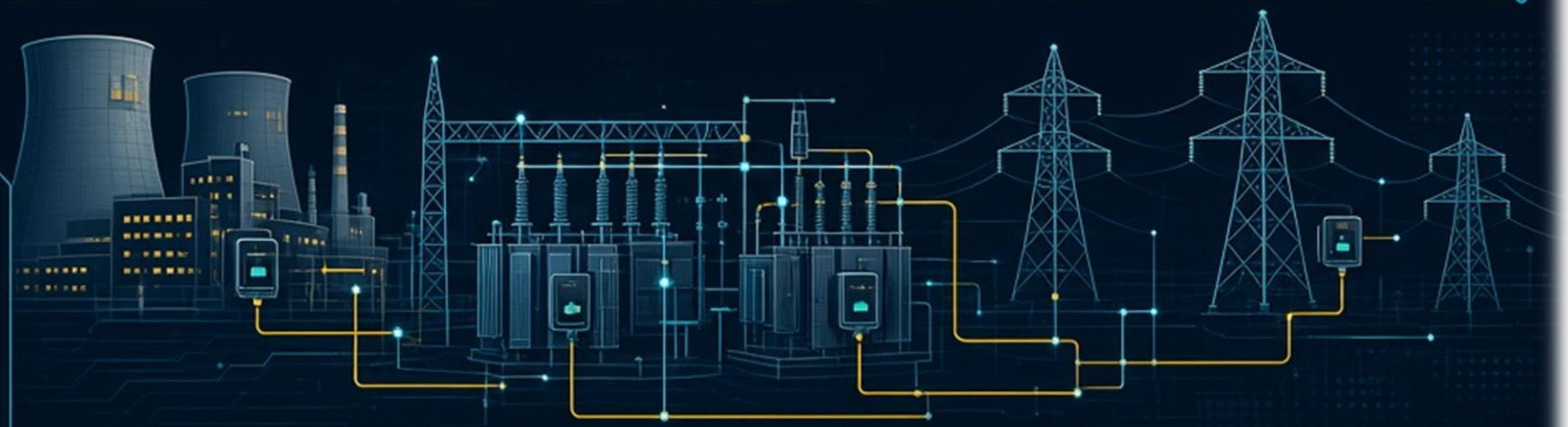
- 8.1 Cas d’usage : Capteur de centrale / réseau électrique
- 8.2 Cas d’usage : Frigo connecté (chaîne du froid)
- 8.3 Cas d’usage : Contrôle de trafic aérien / terrestre
- 8.4 Cas d’usage : Reprise de session 0-RTT sécurisée
- 8.5 Synthèse transversale et enseignements des cas d’usage

8.1 Cas d’usage : Capteur de centrale / réseau électrique

Ce cas concerne des capteurs déployés sur des infrastructures électriques (centrales, postes de transformation, réseaux de distribution). Le contexte type est le suivant : batterie moyenne, exigence de sécurité « Secret », réseau relativement stable.

Dans ce scénario, le handshake adaptatif conduit à un mode hybride allégé. Le client signale un niveau de batterie intermédiaire et une exigence Secret. Le serveur sélectionne alors une combinaison post-quantique de niveau intermédiaire (par exemple un KEM plus léger couplé à une primitive classique robuste) afin de réduire la consommation énergétique et la taille des messages, tout en conservant une résistance quantique adaptée au niveau de criticité. Ce choix permet de maintenir une supervision fiable sans épuiser prématurément l’autonomie des capteurs, tout en protégeant les données de pilotage et de mesure contre les menaces actuelles et futures.

8.1 Cas d'usage : Capteur de centrale / réseau électrique



CONTEXTE TYPIQUE

- Batterie Moyenne
- Exigence de sécurité **Secret**
- Réseau Stable

ÉCHANGE ADAPTATIF

Négociation sécurisée des capacités et algorithmes

MODE HYBRIDE LÉGER

Combinaison optimale pour performance et sécurité

PQ KEM (Intermédiaire) + Crypto classique robuste

BÉNÉFICES CLÉS

CONSOMMATION RÉDUITE

Moins d'énergie par message

TAILLE DE MESSAGE RÉDUITE

Messages compacts pour réseaux contraints

SUPERVISION FIABLE SANS DRAINER L'AUTONOMIE

Surveillance continue avec une batterie moyenne

PROTECTION DURABLE

Données de commande et de mesure protégées contre les menaces actuelles et futures

Équilibre optimal : légèreté, **sécurité renforcée, résilience quantique.**

8.2 Cas d’usage : Frigo connecté (chaîne du froid)

Ce cas illustre les contraintes maximales d’autonomie, typiques des équipements de la chaîne du froid (frigos industriels, chambres froides, conteneurs frigorifiques connectés). Le contexte est caractérisé par une batterie faible et une exigence de sécurité « Confidentiel ».

L’adaptation est ici poussée au maximum : le serveur privilégie le mode hybride le plus léger autorisé pour ce niveau de confidentialité, voire un renforcement classique optimisé lorsque le risque quantique immédiat est jugé acceptable. L’objectif prioritaire est de préserver l’autonomie du capteur afin d’éviter toute interruption de la chaîne du froid. La signalisation de batterie faible déclenche explicitement cette stratégie d’économie d’énergie, tout en maintenant un niveau de protection suffisant contre les compromissions observées sur ce type d’équipements. Ce cas démontre la capacité du protocole à rester opérationnel dans des conditions énergétiques très contraintes.

8.2 Cas d'usage : Frigo connecté (chaîne du froid)

ÉQUIPEMENTS DE LA CHAÎNE DU FROID



ARMOIRE FRIGORIFIQUE
Capteurs IoT : température, porte, énergie



CHAMBRE FROIDE
Capteurs IoT : température, humidité, accès



CONTENEUR / CAMION FRIGORIFIQUE
Capteurs IoT : température, GPS, énergie, choc

CONTEXTE

BATTERIE FAIBLE
Niveau d'énergie limité
Autonomie à préserver

EXIGENCE DE SÉCURITÉ
CONFIDENTIEL
Données sensibles : températures, alertes, localisations, accès.

ADAPTATION MAXIMALE

MODE HYBRIDE ALLÉGÉ
Sécurité minimale requise + chiffrement léger, filtrage essentiel, rapports optimisés

RENFORCEMENT CLASSIQUE OPTIMISÉ
Paramétrage fin et contextuel pour maintenir la protection tout en minimisant la conso

PRIORITÉ : ÉCONOMIE D'ÉNERGIE TOUT EN MAINTENANT UNE PROTECTION SUFFISANTE

CONTINUITÉ DE LA CHAÎNE DU FROID : UNE PRIORITÉ ABSOLUE

- Préserve l'autonomie
- Maintient la sécurité
- Évite toute rupture du froid

8.3 Cas d’usage : Contrôle de trafic aérien / terrestre

Ce cas porte sur des systèmes de contrôle du trafic (aérien ou terrestre) où la criticité est maximale. L’exigence de sécurité est « Top Secret », la batterie est correcte et la disponibilité ainsi que l’intégrité des données sont primordiales.

Le handshake aboutit à un mode hybride maximal : sélection des algorithmes post-quantiques les plus robustes, paramètres de clés élevés et activation systématique de la validation par ZKP pour tout 0-RTT critique. Aucune économie d’énergie n’est priorisée au détriment de la sécurité. Le protocole garantit ainsi une résistance quantique complète et une protection forte contre les attaques de rejeu ou de manipulation, indispensables pour des applications où une compromission pourrait avoir des conséquences humaines ou opérationnelles graves. Ce cas valide la capacité du système à monter en niveau de protection lorsque les exigences le justifient.

8.3 Cas d'usage : Contrôle de trafic aérien / terrestre

CONTEXTE

TOP SECRET
Exigence de sécurité maximale

BATTERIE CORRECTE / BONNE
Alimentation fiable et surveillée

CRITICITÉ MAXIMALE
Impacts catastrophiques en cas de défaillance

DISPONIBILITÉ & INTÉGRITÉ DES DONNÉES
Primordiales et non négociables



MODE HYBRIDE MAXIMAL

Configuration la plus robuste

ALGORITHMES POST-QUANTIQUES LES PLUS ROBUSTES
Lattice-based, Hash-based, MPC-friendly.

PARAMÈTRES DE CLÉS ÉLEVÉS
Sécurité maximale, marges renforcées.

ZKP SYSTÉMATIQUE
Validation obligatoire pour toute donnée critique 0-RTT.

CRITICITÉ ÉLEVÉE
Capteurs & systèmes critiques haute priorité.

GARANTIES DE SÉCURITÉ

AUCUNE ÉCONOMIE D'ÉNERGIE AU DÉTRIMENT DE LA SÉCURITÉ
Performance et sécurité : priorité absolue à la sécurité.

RÉSISTANCE QUANTIQUE COMPLÈTE
Sécurisé contre les attaques quantiques actuelles et futures.

PROTECTION FORTE CONTRE REPLAY & MANIPULATION
Détection et prévention systématiques

AUCUN COMPROMIS. SÉCURITÉ MAXIMALE. DISPONIBILITÉ TOTALE. INTÉGRITÉ GARANTIE.

TOP SECRET | HYBRIDE MAXIMAL | ZKP OBLIGATOIRE | CRITICITÉ MAXIMALE

8.4 Cas d’usage : Reprise de session 0-RTT sécurisée

Ce cas se concentre sur la reprise de session sans round-trip supplémentaire, y compris pour des transactions critiques et dans un environnement post-quantique. Le client présente un ticket de session accompagné d’une preuve ZKP valide.

Si la preuve est vérifiée avec succès, la session est ouverte immédiatement. Le mécanisme ZKP assure l’authenticité du ticket, empêche les rejeux et préserve les propriétés de sécurité post-quantique sans introduire de latence supplémentaire. Ce cas d’usage est particulièrement important pour les équipements IoT qui doivent transmettre des données critiques de manière réactive (alarmes, commandes urgentes) tout en limitant la consommation radio. Il démontre que le 0-RTT peut devenir un outil sûr et non plus un compromis de sécurité.

8.4 Cas d'usage : Reprise de session 0-RTT sécurisée

CLIENT



Présente :

- Ticket de session (opaque, pré-partagé)
- Preuve ZKP valide (zéro connaissance)

1. Ticket de session + preuve ZKP →

SERVEUR

Vérification instantanée de la preuve ZKP

- Authenticité confirmée
- Session ouverte immédiatement

2. Vérification instantanée →

RÉSULTAT

Session 0-RTT ouverte sans aller-retour supplémentaire

- Aucune latence ajoutée

0-RTT

ZKP garantit l'authenticité
Preuve d'identité sans révéler de secret

Prévention des attaques de rejeu
Chaque preuve est unique et non réutilisable

Sécurité post-quantique préservée
Résistant aux attaques quantiques

Zéro latence ajoutée
Aucun aller-retour supplémentaire



CRITIQUE POUR LES DISPOSITIFS IoT

Données réactives critiques : alarmes, commandes urgentes

- Alarmes
- Commandes urgentes
- Transmission rapide + faible consommation radio

0-RTT : UN OUTIL SÉCURISÉ, PLUS UN COMPROMIS

Grâce à la preuve ZKP :

- ✓ Sécurisé
- ✓ Rapide
- ✓ Post-quantique

8.5 Synthèse transversale et enseignements des cas d'usage

Les quatre cas d'usage illustrent la flexibilité du protocole face à des contextes industriels très différents. Ils montrent que l'adaptation dynamique (batterie, exigence de sécurité, qualité réseau) permet de couvrir un spectre allant de l'économie maximale d'énergie (frigo) à la protection maximale (trafic aérien), tout en rendant le 0-RTT viable pour les transactions critiques grâce aux ZKP.

Ces scénarios confirment la pertinence de l'approche pour les infrastructures critiques : elle répond à la fois aux incidents observés (frigos compromis, centrales ciblées) et aux contraintes opérationnelles réelles des capteurs. Ils constituent également une base solide pour la définition des politiques d'adaptation, des jeux de tests et des critères de validation énergétique et de sécurité. Enfin, ils soulignent l'intérêt d'une interface multi-algorithmes (s'appuyant sur le module QSA) capable de supporter ces différents niveaux de protection de manière ouverte et évolutive.

8.5 Synthèse transversale et enseignements des cas d'usage

SPECTRE DES CAS D'USAGE : DU MAXIMUM D'ÉCONOMIES ÉNERGÉTIQUES À LA PROTECTION MAXIMALE

ÉCONOMIES ÉNERGÉTIQUES MAXIMALES
Faible conso. batterie
Confidentialité modérée

PROTECTION MAXIMALE
Consommation plus élevée
Confidentialité très forte



1. Chaîne du froid (Frigorifique)
Économies d'énergie max.
Batterie faible

CONFIDENTIEL

2. Centrale électrique (Capteurs)
Équilibre économies et sécurité

SENSIBLE

3. Trafic aérien (0-RTT sécurisé par ZKP)
Faible latence + preuves de validité sans données

SECRET

4. Trafic terrestre (Critique au sol)
Protection maximale et résilience

TOP SECRET

FLEXIBILITÉ DU PROTOCOLE : ADAPTATION DYNAMIQUE

Le protocole s'adapte en continu selon trois facteurs clés

BATTERIE
Niveau d'énergie disponible
→ Ajustement des mécanismes

NIVEAU DE SÉCURITÉ
Exigence de confidentialité
→ Choix des algorithmes et force

QUALITÉ RÉSEAU
Bande passante, latence, pertes
→ Adaptation des échanges

ADAPTATION DYNAMIQUE ET CONTEXTUELLE

ENSEIGNEMENTS CLÉS

1. PERTINENCE POUR LES INFRASTRUCTURES CRITIQUES
Répond à des incidents réels et contraintes opérationnelles :

- Pannes & pannes
- Contraintes terrain
- Exigences réglementaires

2. BASE SOLIDE POUR LES POLITIQUES D'ADAPTATION
Le spectre guide les décisions d'adaptation dynamiques selon le contexte et les risques.

3. TESTS ET CRITÈRES DE VALIDATION
Définir des scénarios, métriques et seuils pour valider l'équilibre énergie / sécurité / performance.

4. INTÉRÊT DE L'INTERFACE MULTI-ALGORITHMES
Le module QSA active le bon algorithme au bon moment pour des niveaux de protection ouverts et évolutifs.

ANALYSE DETAILLEE
Chapitre 9
Impacts et Bénéfices

AGENDA Chapitre 9 – Impacts et Bénéfices

- 9.1 Impact en matière de sécurité post-quantique
- 9.2 Bénéfices énergétiques et réduction du trafic réseau
- 9.3 Souveraineté technologique et ouverture
- 9.4 Complémentarité avec les produits et modules existants
- 9.5 Impact mondial sur les secteurs vitaux

9.1 Impact en matière de sécurité post-quantique

Le principal bénéfice du protocole réside dans la protection post-quantique des infrastructures critiques tout en conservant des performances compatibles avec l'IoT. Contrairement aux approches statiques qui appliquent systématiquement des algorithmes lourds, l'adaptation dynamique permet de maintenir une résistance quantique (au moins niveau NIST 1, voire supérieur selon la politique) uniquement lorsque le contexte l'exige.

Cette approche réduit le risque de compromission à long terme des systèmes de supervision et de commande (centrales, réseaux d'eau, contrôle de trafic) face aux futurs ordinateurs quantiques. Elle répond directement aux limites des protocoles classiques face aux menaces observées, tout en préservant la forward secrecy et en sécurisant le 0-RTT grâce aux preuves ZKP. Le résultat est une couche de sécurité durable, crédible et opérationnellement viable pour les secteurs vitaux.

9.1 Impact en matière de sécurité post-quantique



PROTECTION POST-QUANTIQUE
DES INFRASTRUCTURES CRITIQUES

+



PERFORMANCES
COMPATIBLES IoT

APPROCHE STATIQUE → ADAPTATION DYNAMIQUE



ALGORITHMES LOURDS APPLIQUÉS
SYSTÉMATIQUEMENT

>



ADAPTATION DYNAMIQUE : RÉSISTANCE QUANTIQUE
ACTIVÉE UNIQUEMENT QUAND LE CONTEXTE L'EXIGE

RÉDUCTION DU RISQUE
de compromission à long terme des systèmes de supervision et de commande (centrales, réseaux d'eau, contrôle du trafic) face aux ordinateurs quantiques futurs.

RÉPOND AUX LIMITES DES PROTOCOLES CLASSIQUES
Préserve la confidentialité persistante et sécurise le 0-RTT via ZKP.

COUCHE DE SÉCURITÉ DURABLE, CRÉDIBLE ET OPÉRATIONNELLEMENT VIABLE

POUR LES SECTEURS VITAUX
Énergie, Eau, Transports, Industries critiques

RÉSULTAT : Une sécurité durable, crédible et opérationnellement viable pour les secteurs vitaux.

9.2 Bénéfices énergétiques et réduction du trafic réseau

L'adaptation du handshake produit des gains concrets en énergie et en trafic. En sélectionnant des modes hybrides allégés lorsque la batterie est faible ou moyenne et que l'exigence de sécurité le permet, le protocole prolonge significativement l'autonomie des capteurs. La réduction de la charge CPU et de l'activité radio diminue la consommation énergétique par rapport à un handshake post-quantique non adaptatif.

Parallèlement, la limitation de la taille des messages et l'optimisation des échanges réduisent le trafic réseau inutile. Ces bénéfices sont particulièrement importants pour les déploiements massifs d'équipements contraints (chaîne du froid, capteurs de réseau électrique, systèmes de transport). Ils permettent de maintenir la disponibilité opérationnelle des infrastructures tout en maîtrisant les coûts énergétiques et la charge des réseaux radio.

9.2 Bénéfices énergétiques et réduction du trafic réseau

ADAPTATION DU HANDSHAKE PQ
sécurisé & intelligent

→

BATTERIE FAIBLE OU MOYENNE

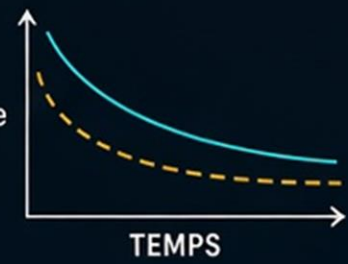
→

EXIGENCE DE SÉCURITÉ AUTORISÉE

→

MODES HYBRIDES LÉGERS SÉLECTIONNÉS

autonomie des capteurs significativement prolongée



MOINS DE CHARGE CPU ET MOINS D'ACTIVITÉ RADIO

→ CONSOMMATION ÉNERGÉTIQUE RÉDUITE



VS NON-ADAPTATIF
MOINS D'ÉNERGIE

TAILLE DES MESSAGES LIMITÉE ET ÉCHANGES OPTIMISÉS

→ TRAFIC RÉSEAU RÉDUIT



MOINS DE DONNÉES INUTILES

CRUCIAL POUR LES DÉPLOIEMENTS MASSIFS D'ÉQUIPEMENTS CONTRAINTS

CHAÎNE DU FROID

RÉSEAU ÉLECTRIQUE

SYSTÈMES DE TRANSPORT

MAINTIENT LA DISPONIBILITÉ OPÉRATIONNELLE DES INFRASTRUCTURES
TOUT EN MAÎTRISANT LES COÛTS ÉNERGÉTIQUES ET LA CHARGE DES RÉSEAUX RADIO.

9.3 Souveraineté technologique et ouverture

Le protocole est conçu comme un outil ouvert et multi-algorithmes, compatible avec les processus de validation NIST et les tests ACVP réalisés par des laboratoires accrédités. Cette ouverture favorise la souveraineté technologique : les opérateurs et intégrateurs peuvent maîtriser les primitives cryptographiques utilisées, les faire évoluer et les auditer de manière indépendante.

L'interface standardisée permet d'intégrer plusieurs algorithmes post-quantiques sans dépendance à une implémentation unique. En s'appuyant en priorité sur le module QSA tout en restant extensible, le projet offre une solution maîtrisée, auditable et alignée sur les standards internationaux. Cette approche renforce la confiance des acteurs industriels et publics dans la transition post-quantique.

9.3 Souveraineté technologique et ouverture



QSA
MODULE PRINCIPAL

INTERFACE STANDARD OUVERTE

- CRYSTALS-Kyber +
- CRYSTALS-Dilithium +
- FALCON +
- SPHINCS+ +

NIST ACVP

TESTS ACVP

LABORATOIRES ACCRÉDITÉS

OUVERTURE ET SOUVERAINETÉ

L'ouverture favorise la souveraineté : maîtrise, évolution et audit indépendants des primitives cryptographiques.

INTÉGRATION MULTI-ALGORITHMES

Une interface standardisée permet d'intégrer plusieurs algorithmes PQ sans dépendance à une implémentation unique.

AUDITABILITÉ ET EXTENSIBILITÉ

Priorité sur QSA, extensible et ouvert : une solution maîtrisée, auditable et alignée sur les standards internationaux.

MAÎTRISÉ AUDITABLE STANDARDISÉ

Renforce la confiance des acteurs industriels et publics dans la transition post-quantique.

9.4 Complémentarité avec les produits et modules existants

Le protocole s'intègre naturellement aux produits de sécurité déjà développés grâce au module QSA et à l'interface multi-algorithmes adaptable. Il ne se substitue pas aux solutions existantes mais les complète en apportant la couche réseau chiffrée adaptative manquante.

Cette complémentarité facilite l'adoption progressive : les organisations peuvent déployer le handshake hybride en s'appuyant sur les primitives QSA déjà en place, tout en conservant la possibilité d'ajouter d'autres algorithmes validés. Le caractère modulaire et ouvert réduit les coûts d'intégration et permet une montée en puissance maîtrisée sur les infrastructures critiques, sans rupture technologique majeure.

9.4 Complémentarité avec les produits et modules existants

PRODUITS ET MODULES EXISTANTS

- Pare-feu & Segmentation
- EDR / XDR
- Modules de chiffrement
- PKI & Gestion des identités

Solutions déjà développées et validées.

MODULE QSA

QSA

INTERFACE MULTI-ALGORITHMES ADAPTABLE

S'intègre naturellement grâce au module QSA et à son interface multi-algorithmes adaptable.

COUCHE RÉSEAU CHIFFRÉE ADAPTATIVE

La brique manquante qui complète, sans se substituer.

Complète les solutions existantes en apportant la couche réseau chiffrée adaptative manquante.

+ P + {#} ...

ADOPTION PROGRESSIVE

Déployez le handshake hybride en vous appuyant sur les primitives QSA déjà en place, tout en gardant la possibilité d'ajouter d'autres algorithmes validés.

MODULARITÉ OUVERTE

Une architecture modulaire et ouverte réduit les coûts d'intégration et permet un ramp-up maîtrisé.

SÉCURITÉ MAÎTRISÉE

Préserve les investissements existants et évite les ruptures technologiques majeures.

IDÉAL POUR LES INFRASTRUCTURES CRITIQUES

Intégration progressive, sécurisée et évolutive, sans refonte complète.

COMPLÉTER AUJOURD'HUI. ÉVOLUER DEMAIN. SÉCURISER DURABLEMENT.

9.5 Impact mondial sur les secteurs vitaux

Le projet apporte une réponse concrète aux menaces observées sur les secteurs vitaux (énergie, eau, chaîne du froid, transport aérien et terrestre). Les incidents récents (frigos connectés compromis, centrales ciblées) illustrent les risques d'une connectivité croissante sans adaptation des mécanismes de sécurité.

En offrant une protection post-quantique compatible avec les contraintes énergétiques des capteurs, le protocole contribue à renforcer la résilience des infrastructures critiques à l'échelle mondiale. Il permet aux opérateurs de sécuriser durablement leurs systèmes cyber-physiques tout en préservant l'autonomie et la disponibilité des équipements. Cet impact dépasse le cadre technique : il participe à la protection des services essentiels et à la réduction des risques systémiques liés à la transition numérique et quantique des infrastructures vitales.

9.5 Impact mondial sur les secteurs vitaux

MENACES OBSERVÉES



FRIGOS CONNECTÉS COMPROMIS
RISQUE POUR LA CHAÎNE DU FROID

CENTRALES ÉLECTRIQUES CIBLÉES
RISQUE D'INDISPONIBILITÉ MASSIVE

Une connectivité croissante sans adaptation de la sécurité augmente les risques.

NOTRE PROTOCOLE APPORTE UNE RÉPONSE CONCRÈTE

Post-quantique, compatible avec les contraintes énergétiques des capteurs



SECTEURS VITAUX PROTÉGÉS

- ÉNERGIE
- EAU
- CHAÎNE DU FROID
- TRANSPORT AÉRIEN
- TRANSPORT TERRESTRE

RÉSILIENCE RENFORCÉE

Sécurise les infrastructures critiques à l'échelle mondiale. mondiale.

IMPACT GLOBAL

Réduit les risques systémiques liés à la transition numérique et quantique.

SERVICES ESSENTIELS

Protège les services essentiels au quotidien et préserve autonomie et disponibilité des équipements.

UN IMPACT QUI DÉPASSE LE CADRE TECHNIQUE : PROTÉGER L'ESSENTIEL, RÉDUIRE LES RISQUES, PRÉSERVER L'AVENIR.