ÉCHANTILLON : Vérification de préparation quantique-sûre, un rapport d'échantillon complet et identifié (FR)

> **ÉCHANTILLON. Ce n'est pas le rapport d'un client.** Chaque section ci-dessous est un échantillon identifié et garde sa propre mention. Les sections viennent de trois sources différentes (le dossier d'échantillon d'un client fictif, une sonde réelle des domaines d'Adwaizer et des données de test fictives) ; elles ne forment pas un seul mandat. Ce document ne constitue ni une certification, ni une opinion d'audit, ni un avis juridique, et il ne garantit pas la sûreté quantique.

#	Section du rapport livré	Dans cet échantillon	Fichier source
1	Page couverture : note de préparation, sommaire, période de vérification ; Portée (`:115` - `:153`)	absent de cet échantillon	aucun
2	Lettre d'Attestation (`:155`)	absent de cet échantillon	aucun
3	Clauses applicables et réponses (`:159`)	oui	`qsafe examples/sample-pack/answer-sheet-fr.md @ f662b0d`
4	Profil cryptographique vérifié : points d'accès (`:171` - `:182`)	oui, avec la CBOM	`2026-10-30-sample-endpoint-section.fr.md`
4	Profil cryptographique vérifié : modules cryptographiques (`:183` - `:193`)	absent de cet échantillon	aucun
5	Écarts et plan de correction (`:196`)	absent de cet échantillon	aucun
6	Énoncé d'agilité cryptographique (`:206`)	absent de cet échantillon	aucun
7	Fournisseurs en amont (`:220`) ; Décisions consignées (`:212`) s'il y en a	absent de cet échantillon	aucun
8	Méthodologie et limites (`:228`)	absent de cet échantillon	aucun
9	Signatures et Vérification (`:240` , `:246`)	absent de cet échantillon	aucun
Annexe APM	Champs du portefeuille d'applications (APM) de la SPIN 6.2.3 (`:257` , seulement quand la clause est visée)	absent de cet échantillon	aucun
Annexe	Courriel en transit (instantané gratuit, `snapshot_show.html:31` - `:45`)	oui	`2026-10-30-sample-mail-transit-section.fr.md`

1. Note de préparation, sommaire, période de vérification et portée

```
absent de cet échantillon
```

2. Attestation

```
absent de cet échantillon
```

3. Clauses applicables et réponses

Échantillon identifié : Northbridge Software Inc. et son produit sont fictifs ; les points d'accès du dossier étaient les domaines d'Adwaizer, à la place de ceux d'un client, sondés le 18 oct. 2026 ; le dossier a été émis le 26 oct. 2026, ses lignes de points d'accès précèdent donc la sonde du 30 oct. de la section 4.

ADW-QSR-SAMPLE-002 · 2026-10-26 · grade C

Second réviseur : pas encore désigné

Clause	Source	Statut	Réponse	Preuve
CA-SPIN-6.3.1	SPIN, section 6.3.1 (procurement clauses)	Engagé (2026-12-31)	Non satisfait à ce jour ; engagement du client à le satisfaire d'ici le 2026-12-31 (déclaration du client, vérifiée par Adwaizer à cette date).	Key establishment hybrid today; signatures by 15 Dec 2026; FIPS 140-3 module migration by 31 Dec 2026
CA-ITSM00501-2.1.1-KE	ITSM.00.501, section 2.1.1 (recommended cryptographic algorithms)	Conforme (mesuré)	Conforme, mesuré sur l'environnement déployé ; voir la preuve.	adwaizer.com:443: X25519MLKEM768; www.adwaizer.com:443: X25519MLKEM768
CA-ITSM00501-2.1.1-DS	ITSM.00.501, section 2.1.1 (recommended cryptographic algorithms)	Engagé (2026-12-15)	Non satisfait à ce jour ; engagement du client à le satisfaire d'ici le 2026-12-15 (déclaration du client, vérifiée par Adwaizer à cette date).	Vendor roadmap: ML-DSA-65 code signing in release 4.2 (Q4 2026)
CA-ITSM00501-2.1.2	ITSM.00.501, section 2.1.2 (cryptographic agility)	Conforme (attesté)	Conforme selon la preuve du client (document ou entrevue), non mesuré par Adwaizer ; voir la preuve.	Cipher suites, groups and key sizes configurable in the edge policy; application signing algorithm selectable per environment; updates signed with Cosign
CA-ITSM00501-2.1.3	ITSM.00.501, sections 2.1.3 and 2.2.3 (cryptographic certification)	Écart	Non conforme à ce jour ; correctif planifié (voir les écarts).	OpenSSL FIPS Provider 3.0.8 (application TLS): CMVP #4282 FIPS 140-2 Historical; Seagate SSG5 SED (storage encryption): CMVP #5552 FIPS 140-3 Active; Vendor HSM (key wrapping): CMVP certificate pending
CA-ITSM00501-2.2	ITSM.00.501, section 2.2 (service providers and cloud services)	Écart	Non conforme à ce jour ; correctif planifié (voir les écarts).	adwaizer.com:443: versions TLSv1/TLSv1.1/TLSv1.2/TLSv1.3; www.adwaizer.com:443: versions TLSv1/TLSv1.1/TLSv1.2/TLSv1.3
CA-SSC-CSIAAS2024-CP	CS-IAAS-2024, Cryptographic Protection, clauses (1) to (7)	Engagé (2026-12-31)	Non satisfait à ce jour ; engagement du client à le satisfaire d'ici le 2026-12-31 (déclaration du client, vérifiée par Adwaizer à cette date).	Clause (5) active CMVP certification: see modules; (3) and (7) configurable algorithms and agility: see crypto-agility statement

Clause	Source	Statut	Réponse	Preuve
CA-SPIN-6.2.3	SPIN, section 6.2.3 (application portfolio records)	Conforme (attesté)	Conforme selon la preuve du client (document ou entrevue), non mesuré par Adwaizer ; voir la preuve.	APM record fields supplied in the appendix: components, algorithms, hosting, dependencies, versions, contract expiry 2028-03-31, refresh 2027, contact, priority High
AU-ASD-VENDORQ	ASD vendor questions (16 Jul 2026) and AUSCERT questionnaire v1.0 (Aug 2026)	Conforme (attesté)	Conforme selon la preuve du client (document ou entrevue), non mesuré par Adwaizer ; voir la preuve.	Board-approved quantum readiness plan (Sep 2026); CBOM available on request; no SHA-1 or 3DES in the service chain

4. Profil cryptographique vérifié

Montré au prospect :

> **Échantillon identifié.** Il s'agit d'une exécution réelle de la sonde de points de terminaison Quantum-Safe et de la fusion CBOM, sur deux domaines dont Adwaizer est propriétaire : adwaizer.com et acuarela.adwaizer.com. Ce n'est pas le rapport d'un client. Exécutée le 30 oct. 2026 à 11 h 46 UTC (heure de la sonde), sur le Mac d'Adwaizer avec OpenSSL 3.6.4 et une connexion TLS directe (sans proxy), à partir d'adwaizer-qsafe-pipeline au commit `f662b0d`.

Profil des points de terminaison

Hôte	Note	Échange de clés (par défaut)	Versions TLS	Clé du certificat feuille	Constats
adwaizer.com:443	A	hybride X25519MLKEM768, TLSv1.3, TLS_AES_256_GCM_SHA384	TLSv1.3 et TLSv1.2 oui ; TLSv1 et TLSv1.1 non	EC-256 (secp256r1), signée ecdsa-with-SHA384 par Let's Encrypt YE1	**faible** `cert-classical-key` (clause CA-ITSM00501-2.1.1-DS)
acuarela.adwaizer.com:443	A	hybride X25519MLKEM768, TLSv1.3, TLS_AES_256_GCM_SHA384	TLSv1.3 et TLSv1.2 oui ; TLSv1 et TLSv1.1 non	EC-256 (secp256r1), signée ecdsa-with-SHA384 par Let's Encrypt YE1	**faible** `cert-classical-key` (clause CA-ITSM00501-2.1.1-DS)

Les deux hôtes présentent le même certificat feuille (`CN=adwaizer.com`, noms `*.adwaizer.com` et `adwaizer.com`, SHA-256 `29a60d45…64fa`), valide jusqu'au 24 janv. 2027 (85 jours restants lors de l'exécution), avec une chaîne de quatre certificats jusqu'à ISRG Root X1.

Nomenclature cryptographique (CBOM)

2 CBOM (une par hôte) fusionnées en 7 composants, CycloneDX 1.6 valide : l'échange de clés X25519MLKEM768 (accord de clés, niveau de sécurité quantique NIST 3), une entrée de protocole TLSv1.3 par hôte, et les quatre certificats de la chaîne commune.

Ce que les constats signifient pour vous

- **Échange de clés hybride X25519MLKEM768 sur les deux hôtes.** Le trafic vers ces sites est déjà chiffré avec un échange de clés qui combine une méthode classique et une méthode post-quantique (ML-KEM) ; cette méthode est conçue pour que le trafic enregistré aujourd'hui ne puisse pas être déchiffré plus tard par un ordinateur quantique. Il suffit de le garder activé.
- **[faible]** `cert-classical-key` **sur les deux hôtes.** Le certificat qui prouve l'identité des sites utilise encore une clé classique EC-256, qu'un grand ordinateur quantique futur pourrait en principe contrefaire ; il s'agit d'usurpation d'identité plus tard, pas de lecture du trafic d'aujourd'hui. La sonde recommande de « planifier des certificats ML-DSA dès que l'autorité de certification les prend en charge » ; l'action est donc un plan daté avec l'autorité de certification, pas une correction d'urgence.

Cet échantillon n'est ni une certification, ni une opinion d'audit, ni un avis juridique, et il ne garantit pas la sécurité quantique.

Modules cryptographiques

`absent de cet échantillon`

5. Écarts et plan de correction

`absent de cet échantillon`

6. Énoncé d'agilité cryptographique

`absent de cet échantillon`

7. Fournisseurs en amont

`absent de cet échantillon`

8. Méthodologie et limites

`absent de cet échantillon`

9. Signatures et vérification

`absent de cet échantillon`

Annexe : champs du portefeuille d'applications (APM) de la SPIN 6.2.3

`absent de cet échantillon`

Annexe : Courriel en transit (instantané gratuit)

Ce n'est pas une section de l'attestation livrée : c'est ce qu'affiche la page de l'instantané gratuit.

Exemple tiré des données de test. Chaque valeur ci-dessous vient du domaine fictif `example.ca` des tests versionnés du pipeline. Aucun domaine réel n'a été interrogé, et rien n'a été publié ni envoyé.

Ce que lit la vérification

Seulement les enregistrements DNS du domaine de l'acheteur, en lecture. La vérification ne se connecte jamais aux serveurs de courriel sur le port 25 et ne télécharge jamais le fichier de politique MTA-STS (`src/qsafe/ingest/dns.py:91-:93`; `tests/test_mail_transport.py:48-:49`). La phrase de la page pour l'acheteur : « Si le courriel qui vous est envoyé est protégé en chemin, lu uniquement dans votre DNS public. » (`src/qsafe/web/i18n.py:110`).

Exemple A : les quatre sont publiés

Données `ALL` (`tests/test_mail_transport.py:25-:31`), vérifiées par `test_all_four_present` (`:34-:39`).

Vérification	La page affiche	Ce que cela veut dire pour l'acheteur	Référence (qsafe @ f662b0d)
MX	présent `10 mx1.example.ca` `20 mx2.example.ca`	Le domaine nomme deux serveurs de courriel, par ordre de préférence. Ce sont les hôtes visés par les trois autres vérifications. Un MX nul (`0 .`, « ce domaine ne reçoit pas de courriel ») compte comme aucun hôte.	`src/qsafe/ingest/dns.py:95-:101`; `tests/test_mail_transport.py:36`, `:64-:68`; `src/qsafe/web/templates/snapshot_show.html:39`
MTA-STS	présent `id=20261027T000000`	Le domaine publie l'enregistrement TXT `_mta-sts`, qui annonce aux serveurs d'envoi qu'une politique TLS existe. Seul l'enregistrement est lu. L'instantané ne vérifie pas si le fichier de politique dit `enforce` ou `testing`.	`src/qsafe/ingest/dns.py:102`, `:107`; `tests/test_mail_transport.py:37`; `src/qsafe/web/templates/snapshot_show.html:40`

Vérification	La page affiche	Ce que cela veut dire pour l'acheteur	Référence (qsafe @ f662b0d)
TLS-RPT	présent `mailto:tlsrpt@example.ca`	Le domaine demande aux serveurs d'envoi de signaler les échecs TLS, et la page montre où vont ces rapports. Sans cet enregistrement, une livraison chiffrée qui échoue passe inaperçue.	`src/qsafe/ingest/dns.py:103, :108`; `tests/test_mail_transport.py:38`; `src/qsafe/web/templates/snapshot_show.html:41`
DANE	présent `mx1.example.ca (2 TLSA) mx2.example.ca (1 TLSA)`	Chaque serveur de courriel publie des enregistrements TLSA, qui épinglent son certificat dans le DNS, et la page les compte par serveur. L'instantané compte seulement les TLSA. Il ne valide pas DNSSEC, sur lequel DANE repose.	`src/qsafe/ingest/dns.py:104, :109`; `tests/test_mail_transport.py:39`; `src/qsafe/web/templates/snapshot_show.html:42`

Exemple B : publié en partie

Données `ALL`, modifiées comme dans deux tests : le TXT `_mta-sts` n'a pas `v=STSv1` (`test_mta_sts_txt_without_version_is_missing`, `tests/test_mail_transport.py:52-:55`), et `mx2` n'a aucun TLSA (`test_one_of_two_mx_hosts_with_tlsa, :58-:61`).

Vérification	La page affiche	Ce que cela veut dire pour l'acheteur	Référence (qsafe @ f662b0d)
MX	présent `10 mx1.example.ca 20 mx2.example.ca`	Les deux mêmes serveurs que dans A.	`src/qsafe/ingest/dns.py:95-:101`; `src/qsafe/web/templates/snapshot_show.html:39`

Vérification	La page affiche	Ce que cela veut dire pour l'acheteur	Référence (qsafe @ f662b0d)
MTA-STS	absent	Un TXT sans la balise de version `v=STSv1` n'est pas un enregistrement MTA-STS : les serveurs d'envoi l'ignoreraient, et la page indique absent.	`src/qsafe/ingest/dns.py:42-:46, :102; tests/test_mail_transport.py:54`
TLS-RPT	présent `mailto:tlsrpt@example.ca`	Les rapports fonctionnent quand même, indépendamment du reste.	`tests/test_mail_transport.py:55; src/qsafe/web/templates/snapshot_show.html:41`
DANE	présent `mx1.example.ca (2 TLSA)`	DANE est « présent » dès qu'un seul serveur a des TLSA. La page ne liste que les serveurs qui en ont : `mx2.example.ca` n'est pas couvert, et seule son absence de la liste le montre. Le courriel qui passe par `mx2` n'a aucun épinglage DANE.	`src/qsafe/ingest/dns.py:104, :109; tests/test_mail_transport.py:61; src/qsafe/web/templates/snapshot_show.html:42 (if n)`

Exemple C : rien de publié, ou DNS illisible

Cas	La page affiche	Ce que cela veut dire pour l'acheteur	Référence (qsafe @ f662b0d)
Rien de publié (données `{}`)	MX absent · MTA-STS absent · TLS-RPT absent · DANE absent	Aucun serveur de courriel n'est nommé, donc aucune recherche TLSA n'a lieu. Un acheteur dont le courriel passe par un autre domaine voit ce résultat pour le domaine qu'il a saisi.	`tests/test_mail_transport.py:42-:49; src/qsafe/web/templates/snapshot_show.html:37, :39-:42`
Erreur du résolveur (`SERVFAIL`)	« Votre DNS de courriel n'a pas pu être lu : SERVFAIL »	Un échec DNS est affiché comme tel. Il ne fait jamais échouer l'instantané ni ses notes TLS.	`src/qsafe/web/app.py:270-:273; tests/test_mail_transport.py:77-:86; src/qsafe/web/i18n.py:113`

Ce que la section ne dit pas

- Elle ne donne aucune note et aucun résultat réussi ou échoué pour le courriel. Elle indique présent ou absent pour chaque enregistrement (`src/qsafe/web/templates/snapshot_show.html:37`).
- Elle lit seulement le DNS. Elle ne teste pas qu'un serveur de courriel offre vraiment TLS sur le port 25, et elle ne lit pas le mode de la politique MTA-STS (`src/qsafe/ingest/dns.py:92` – `:93`).
- Elle ne dit rien de l'échange de clés post-quantique pour le courriel. La note d'échange de clés hybride de l'instantané porte sur les points d'accès HTTPS, plus haut sur la page (`src/qsafe/web/i18n.py:106`).

ÉCHANTILLON. Ce n'est pas le rapport d'un client. Ce document ne constitue ni une certification, ni une opinion d'audit, ni un avis juridique, et il ne garantit pas la sûreté quantique.