Mode Opératoire

Architecture PKI interne et HTTPS des services

Code : MO-SEC-006
Version : 1.2
Date : 21 septembre 2026
Auteur : Cédric LEGRAND
Classification : USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	14/09/2026	Création initiale, validée par la mise en production effective du jour : batterie d'acceptation 12/12 côté Traefik et contrôle `curl -cacert` de chaque hôte.
1.1	14/09/2026	Distribution de la racine aux postes hors domaine via le portail (tuile dédiée, page d'instructions, script Linux, stratégie Firefox ImportEnterpriseRoots).
1.2	21/09/2026	Réémission du wildcard (ID 13) avec SAN IP `172.31.250.20` supplémentaire (VLAN PLT, MO-NET-009) — remplace l'ID 5.

1 Objet

Ce document décrit l'**architecture de la PKI interne et du HTTPS des services** de l'infrastructure BTS SIO, mise en production le 14 septembre 2026. C'est un document d'architecture et d'exploitation : il explique la chaîne de confiance, justifie les décisions prises, dresse l'état des lieux et fixe les règles d'exploitation et de sécurité.

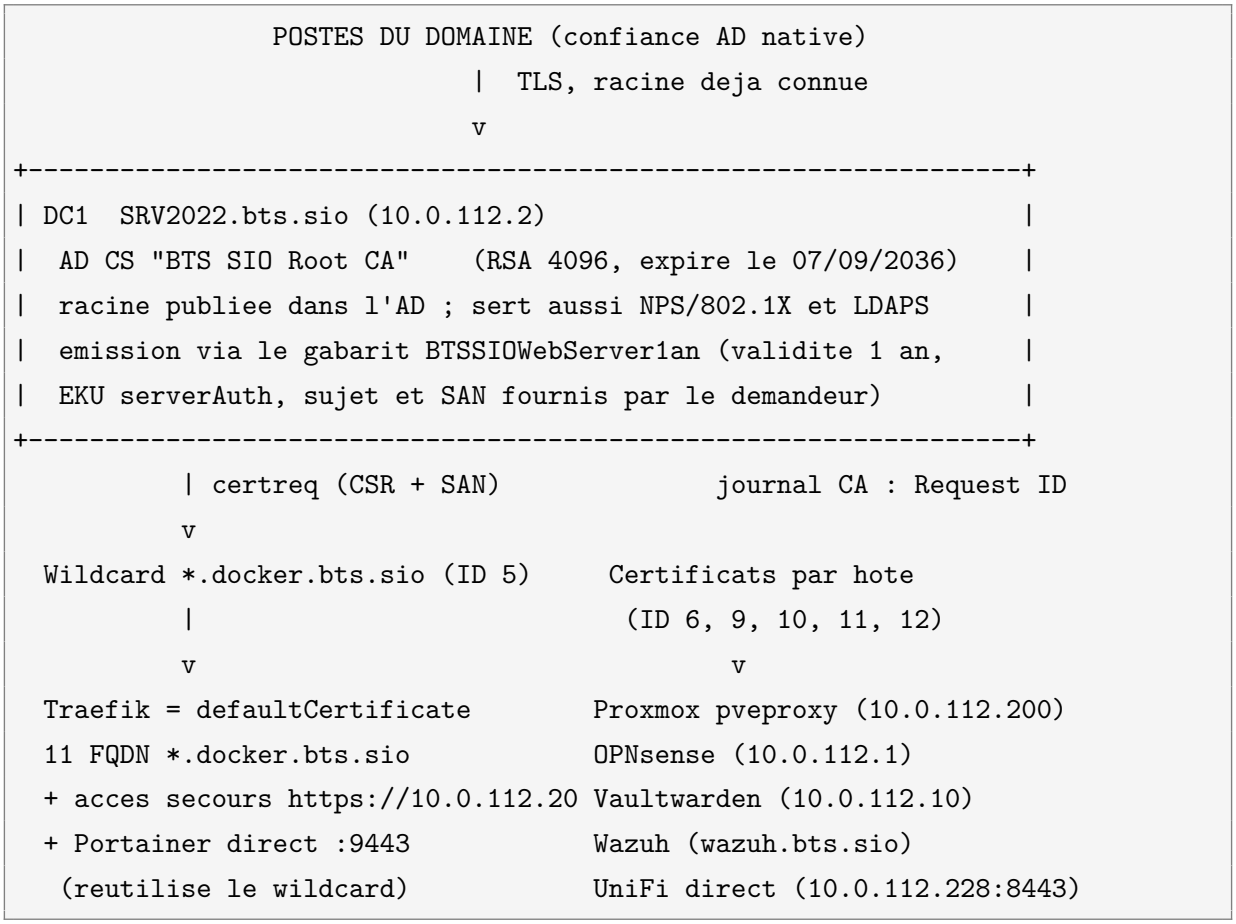
La procédure opérationnelle (émission, déploiement, renouvellement d'un certificat) relève du **MO-SEC-005**, document compagnon du présent MOP. La spécification d'origine du chantier figure dans le dépôt : `docs/superpowers/specs/2026-09-14-https-services-docker-design.md`.

Aucun secret dans ce document

Les identifiants et secrets sont référencés par leur entrée dans le coffre Vaultwarden de l'équipe (`https://10.0.112.10`), jamais recopiés ici.

2 Vue d'ensemble

2.1 Chaîne de confiance



2.2 Rôle de chaque brique

— **AD CS « BTS SIO Root CA »** (DC1) : autorité de certification d'entreprise, déjà publiée dans l'AD — les postes joints au domaine (dont les PC enseignants) lui font confiance **sans aucune GPO supplémentaire**.

— **Gabarit `BTSSIOWebServer1an`** : gabarit d'émission unique des certificats de services web (validité 1 an, clé min. 2048, exportable, EKU *Server Authentication*, sujet fourni par le demandeur).

— **Traefik v2.11** (CT 200, `docker-srv`) : **terminaison TLS centralisée** des onze FQDN `*.docker.bts.sio` via le *wildcard* déclaré en `defaultCertificate` — un seul certificat à déployer et renouveler pour tout le parc de services conteneurisés.

— **Certificats par hôte** : les services hors Traefik (Proxmox, OPNsense, Vaultwarden, Wazuh) et les accès directs (Portainer `:9443`, UniFi `:8443`) reçoivent chacun leur certificat à SAN IP (Portainer réutilise le *wildcard*, même IP).

— **Accès de secours** : l'accès HTTPS par IP (`https://10.0.112.20`) est couvert par le SAN IP du *wildcard* ; les accès de secours **HTTP par `IP:port` (LAN)** demeurent inchangés, de même que les accès VPN.

3 Décisions d'architecture

3.1 Choix de l'autorité : ADCS plutôt que step-ca ou Let's Encrypt

Option	Arbitrage
ADCS « BTS SIO Root CA » (retenu)	Déjà déployée sur DC1 (NPS, LDAPS) et **déjà distribuée aux postes du domaine par l'AD** : couverture immédiate sans GPO ni nouveau service critique à maintenir.
step-ca interne + ACME	Renouvellement automatisé séduisant, mais nouveau service critique, distribution d'une seconde racine en doublon d'ADCS, complexité sans bénéfice immédiat. Réévaluable si le parc de certificats internes grossit.
Let's Encrypt (DNS-01)	Impossible : `bts.sio` n'est pas un TLD public et `lurcat.fr` est hors contrôle direct (EuroDNS, API non supportée par lego/Traefik). Aucune CA publique ne signe d'ailleurs d'IP privée — l'accès de secours par IP resterait en alerte.

3.2 Décisions de paramétrage

— **Gabarit dédié, validité 1 an** : le gabarit intégré « Web Server » émet pour 2 ans, au-delà de la limite de 398 jours acceptée par Safari et Chrome. La duplication `BTSSIOWebServer1an` fixe la validité à 1 an (renouvellement annuel via MO-SEC-005) sans toucher au gabarit d'origine.

— **ACE « Enroll » dédiée à `BTS\Administrateur`** sur ce gabarit uniquement : autorise les soumissions `certreq` scriptées (WinRM depuis le poste d'administration) sans déléguer l'inscription sur les autres gabarits ; action réversible par simple retrait de l'ACE.

— **`EDITF_ATTRIBUTESUBJECTALTNAME2` sur la CA** (`EditFlags` `0x11014e` → `0x15014e`) : la CA accepte les SAN portés par le CSR — indispensable, les CSR OpenSSL fournissent DNS et IP.

— **`RequestExtensionList = 2.5.29.37`** sur la CA : l'extension EKU est reprise du CSR. Exigence d'OPNsense, qui refuse un certificat sans EKU *serverAuth* explicite (deux émissions refusées le 14/09/2026 avant ce réglage : Request ID 7 et 8).

— ***Wildcard* en `defaultCertificate` Traefik** : un certificat unique pour les onze FQDN, pris en charge par le *provider file* (rechargement à chaud de la configuration dynamique ; un seul redémarrage pour la suppression de l'ancien `defaultGeneratedCert` auto-signé).

4 État des lieux au 14/09/2026

4.1 Certificats émis (journal de la CA)

Toutes les émissions du jour utilisent le gabarit `BTSSIOWebServer1an` ; expiration au **14/09/2027** (sauf le wildcard réémis le 21/09/2026, expiration **21/09/2027**).

Request ID	Cible	SANs	État
5	*Wildcard* Traefik	DNS `docker.bts.sio`, `*.docker.bts.sio` ; IP `10.0.112.20`	**Remplacé** par l'ID 13 (21/09/2026)
13	*Wildcard* Traefik	DNS `docker.bts.sio`, `*.docker.bts.sio` ; IP `10.0.112.20` + `172.31.250.20`	**Déployé** 21/09/2026 (Traefik + Portainer `:9443`) — expire **21/09/2027**
6	Proxmox	IP `10.0.112.200`	**Déployé** (`pveproxy`)
7, 8	OPNsense	IP `10.0.112.1`	**Inertes** : émis sans EKU (avant `RequestExtensionList`), refusés par OPNsense, jamais exportés ni déployés
9	OPNsense	IP `10.0.112.1`	**Déployé** (avec EKU)
10	Vaultwarden	IP `10.0.112.10`	**Déployé**
11	Wazuh	DNS `wazuh.bts.sio` ; IP `10.0.112.103`	**Déployé** (dashboard)
12	UniFi	DNS `unifi.docker.bts.sio` ; IP `10.0.112.228`	**Déployé** (keystore)

4.2 Services couverts

Accès	Certificat servi
11 FQDN Traefik (`homer`, `portainer`, `kuma`, `netbox`, `grafana`, `prometheus`, `auth`, `unifi`, `pihole`, `cadvisor`, `traefik` en `.docker.bts.sio`)	*Wildcard* (ID 5) via `defaultCertificate`
`https://10.0.112.20` (secours)	*Wildcard* (ID 5), SAN IP
`https://10.0.112.20:9443` (Portainer direct)	*Wildcard* (ID 5), réutilisé
`https://10.0.112.200:8006` (Proxmox)	ID 6
`https://10.0.112.1` (OPNsense)	ID 9
`https://10.0.112.10` (Vaultwarden)	ID 10
`https://wazuh.bts.sio` (Wazuh dashboard)	ID 11
`https://10.0.112.228:8443` (UniFi direct)	ID 12

Acceptation du jour : batterie `curl -cacert` des onze FQDN et de l'IP de secours **12/12 OK**, plus un contrôle individuel par hôte. Validation terrain (navigateur sur poste du domaine) demandée en clôture de chantier.

5 Exploitation

5.1 Renouvellement annuel

Expiration de tout le parc au **14/09/2027**. La procédure complète (même gabarit, mêmes configurations `.cnf` — en y ajoutant `extendedKeyUsage = serverAuth` pour le *wildcard* et Proxmox —, redémarrage des services concernés) est décrite au **MO-SEC-005 § 7**.

5.2 Supervision des expirations — point ouvert

Supervision Kuma en attente

Au 14/09/2026, la supervision est en place : 23 moniteurs Uptime Kuma (17 préexistants + 6 ajoutés : Wazuh HTTPS, Pi-hole, UniFi, Authentik, cAdvisor, Traefik) dont tous les moniteurs HTTPS en validation TLS stricte (racine ADCS montée dans le conteneur via `NODE_EXTRA_CA_CERTS`) avec notification d'expiration activée (J-30). Le mot de passe admin Kuma, perdu, a été régénéré par la procédure de récupération du conteneur et consigné au coffre (item « Uptime Kuma (kuma.docker.bts.sio) »).

5.3 Points d'attention

— **Portainer** : pas de rechargement TLS à chaud — tout renouvellement impose un redémarrage du conteneur ; les flags `-sslcert`/`-sslkey` sont dépréciés en 2.41 (migrer vers `-tlscert`/`-tlskey` plus tard).

— **UniFi** : le certificat vit dans un keystore Java (`aircontrolenterprise`, alias `unifi`) ; l'import se fait en PKCS12 via `keytool` et exige le `chown 1000:1000` final (MO-SEC-005 § 6.7).

— **Postes hors domaine** : la racine est distribuée par le portail lui-même — tuile « Racine ADCS » menant à `https://homer.docker.bts.sio/assets/hors-domaine.html` (page d'instructions par OS, empreinte SHA-256 de référence, script Linux `install-ca-btssio.sh`). Amorçage sans alerte depuis le LAN : `http://10.0.112.20:8088/assets/hors-domaine.html`. Un seul geste par poste. Sous Linux, le script couvre les trois familles de navigateurs : magasin système (curl/outils), base NSS partagée `/.pki/nssdb` (Brave/Chrome/Chromium — ils ne lisent ni `/etc/ssl/certs` ni les stratégies pour les CA), et Firefox via la stratégie `Certificates → Install` (`/etc/firefox/policies/policies.json`) — `ImportEnterpriseRoots` étant sans effet sous Linux. Sous Windows, `certutil -addstore` couvre Chrome/Edge/Brave, et Firefox par stratégie équivalente.

— **Wazuh** : ne jamais toucher au `root-ca.pem` interne de l'indexer — seuls les deux `wazuh-dashboard*.pem` relèvent de cette PKI.

— **Rollback** : chaque remplacement s'appuie sur une copie `.bak-<date>` de l'ancien fichier (MO-SEC-005 § 6).

6 Sécurité

6.1 Localisation des clés privées

Principe : **la clé privée est générée sur l'hôte qui l'utilise et n'en sort jamais** — seuls les CSR (publics) circulent vers DC1.

Hôte	Fichier	Droits
CT 200 (`docker-srv`)	`/opt/docker/traefik/certs/wildcard.key`	`0600 root:root`
Proxmox	`/etc/pve/local/pveproxy-ssl.key`	`0600 root:root`
CT 127 (Vaultwarden)	`/opt/vaultwarden/ssl/key.pem`	`0600 root:root`
CT 103 (Wazuh)	`/etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem`	`0400 wazuh-dashboard`
CT 200 (UniFi)	keystore `/opt/docker/unifi/config/data/keystore`	UID/GID 1000 (conteneur)
OPNsense	magasin interne de l'appliance (import via l'UI)	géré par OPNsense

Exception documentée : la clé OPNsense a été générée sur le poste d'administration (l'appliance n'offre pas d'OpenSSL opérationnel pour préparer un CSR), importée via l'interface web, puis **détruite du poste** en fin de chantier.

6.2 Traçabilité et hygiène

— **Journal de la CA** : chaque émission est tracée côté DC1 (`certutil -view`) ; les Request ID 5 à 12 correspondent au chantier du 14/09/2026, dont les ID 7 et 8 inertes (conservés comme trace d'un paramétrage incomplet, corrigé depuis).
— **Fichiers temporaires** : CSR et `.cer` ne contiennent aucune clé privée ; le dossier `C:\adcs` de DC1 et les sauvegardes `.bak-https-20260914` sont purgés après validation complète du chantier.
— **Aucune clé privée dans git** : seuls les fichiers de configuration OpenSSL (`.cnf`) et le script de préparation ADCS sont versionnés, dans `modes-operatoires/securite/MO-SEC-005_certificats-adcs-services/files/`.
— **Surface d'attaque** : aucun flux pare-feu modifié, aucun port supplémentaire ouvert ; les accès de secours HTTP par `IP:port` (LAN) demeurent.

7 Références

— **MO-SEC-005** — Certificats ADCS des services (émission, déploiement, renouvellement ; configurations et script versionnés)
— **MO-PLT-012** — Se connecter à Uptime Kuma (supervision des expirations)
— **MO-NET-008** — Architecture du Wi-Fi pédagogique (la même CA sert NPS/802.1X)
— Spécification (dépôt) : `docs/superpowers/specs/2026-09-14-https-services-docker-design.md`
— Plan d'implémentation (dépôt) : `docs/superpowers/plans/2026-09-14-https-services-docker.md`