Livre Blanc

Sécuriser l'IoMT* : Guide pratique des certificats SSL/TLS à l'usage des services biomédicaux

* **Internet of Medical Things** (Internet des Objets Médicaux)

Convergence Santé
www.inkkreation.com

Introduction : Le DM est devenu un objet réseau

Il y a dix ans, un dispositif médical (DM) était une île : on le poussait, on l'allumait, il fonctionnait. Aujourd'hui, un moniteur de surveillance ou un automate de biologie qui n'est pas "sur le réseau" est un dispositif amputé de sa valeur.

Cette connectivité (IoMT) apporte une fluidité vitale aux soins, mais elle crée une vulnérabilité majeure : la donnée de santé circule. Si cette circulation n'est pas protégée par des "tunnels" sécurisés et des "cartes d'identité" numériques (les certificats SSL/TLS), le DM devient la porte d'entrée des cyberattaques hospitalières.

Ce livre blanc a un but unique : Donner aux techniciens et ingénieurs biomédicaux les clés pour comprendre, gérer et exiger une connexion sécurisée pour leurs dispositifs.

Partie 1 : Comprendre l'invisible (La vulgarisation)

1.1 Qu'est-ce qu'un certificat SSL/TLS ?

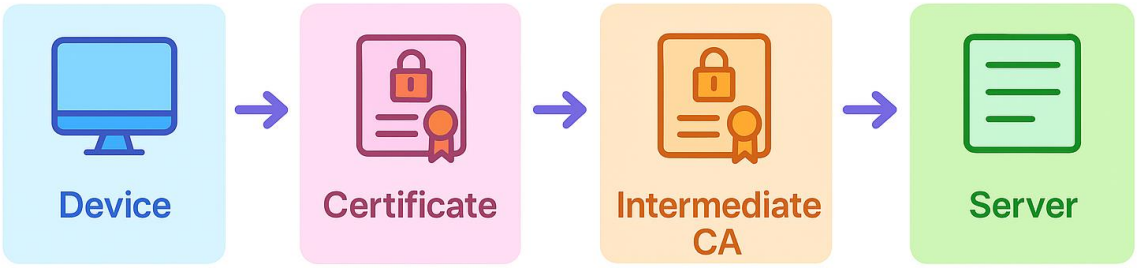
Imaginez que votre DM doive envoyer un résultat d'examen au serveur de l'hôpital.

- Le SSL/TLS, c'est l'enveloppe scellée et le tunnel blindé dans lequel voyage le courrier.
- Le Certificat, c'est le tampon officiel sur l'enveloppe qui prouve que l'expéditeur est bien le DM "Échographe n°4" et non un pirate informatique.

1.2 La Chaîne de Confiance : Le rôle de l'Autorité de Certification (CA)

Pour qu'un certificat soit valide, il doit être signé par une entité de confiance, c'est le certificat Racine (ROOT) qui le permet.

- L'analogie du passeport : Vous avez un passeport (le certificat). La police aux frontières (le serveur de l'hôpital) vous laisse passer parce que c'est l'État (la CA) qui a délivré le document.
- Le problème des certificats "auto-signés" : C'est comme si vous dessiniez votre propre passeport. Le serveur de l'hôpital va probablement bloquer la connexion en disant : *"Je ne connais pas cet émetteur, connexion refusée"*.



1.3 Le "Handshake" (La poignée de main)

Avant d'échanger la moindre donnée patient, le DM et le serveur effectuent une « danse » en trois étapes :

1. Présentation : "Bonjour, voici mon certificat."
2. Vérification : "Est-il périmé ? Est-il signé par la DSI ?"
3. Cryptage : "Ok, tout est bon. Voici une clé secrète pour que nous soyons les seuls à comprendre nos messages."

Partie 2 : Les enjeux critiques pour le biomédical

2.1 La continuité des soins : Le piège de l'expiration

C'est le risque n°1. Un certificat a une date de péremption (souvent 1 ou 2 ans mais cela dépend de l'institution).

Scénario noir : Un automate de biochimie s'arrête de transmettre ses résultats à 2h du matin parce que son certificat a expiré. Pour le technicien d'astreinte, la machine semble fonctionner, mais le "tuyau" informatique est fermé.

2.1.1 Exemples concrets de DM concernés par les certificats SSL/TLS

1. Imagerie médicale

Échographes modernes
→ Ils utilisent des interfaces web internes pour exporter des images ou communiquer avec des serveurs PACS.
Un certificat expiré peut bloquer l'envoi des examens DICOM.

Scanners & IRM
→ Beaucoup disposent de consoles distantes, de portails web internes ou d'intégrations RIS/PACS nécessitant TLS pour authentifier les flux DICOMweb, HL7 ou FHIR.

2. Monitorage patient

Moniteurs multiparamétriques en réanimation
→ Communication en temps réel avec un serveur central.
Sans certificat valide, la centrale de monitorage peut refuser la connexion, provoquant une perte d'affichage des tendances.

Stations de télémétrie cardiaque
→ Transmission chiffrée obligatoire afin de protéger des données physiologiques sensibles (ECG en continu).

3. Laboratoire et biologie médicale

Automates d'hématologie ou de biochimie
→ Utilisent généralement des API, du HTTPS ou TLS pour envoyer les résultats au SIL (Système d'Information Laboratoire).
Un certificat invalide bloque la remontée des résultats.

Analyseurs de gaz du sang
→ Certains modèles transmettent leurs résultats via HTTPS vers un serveur intermédiaire. SSL est souvent requis pour la conformité réglementaire.

4. Anesthésie & blocs opératoires

Respirateurs de bloc opératoire
→ Connexion sécurisée aux systèmes de supervision de bloc et aux dossiers per-opératoires.

Stations d'anesthésie connectées
→ Certains constructeurs imposent TLS 1.2 pour la transmission des données anesthésiques en temps réel.

5. Cardiologie & dispositifs connectés

ECG numériques / systèmes d'épreuve d'effort
→ Transmission chiffrée vers le serveur de cardiologie.

Échographes cardiaques
→ Certains exigent l'import du Root CA de l'hôpital pour valider leur certificat serveur interne.

6. Automates *de stérilisation & endoscopie*

Laveurs-désinfecteurs et autoclaves connectés
→ Ils génèrent des rapports de cycle envoyés automatiquement au logiciel de traçabilité. TLS est parfois obligatoire pour la conformité ISO.

Tours vidéo d'endoscopie
→ Export d'images via HTTPS vers PACS/VNA.

7. Dispositifs de perfusion & pompes intelligentes

Pompes à perfusion connectées (IV Smart Pumps)
→ Mise à jour des bibliothèques de médicaments via le réseau hospitalier, nécessitant une connexion chiffrée et authentifiée.

8. Dispositifs de lit & IoMT général

Literie intelligente ou lits connectés
→ Transmission des alarmes et de la présence patient via API sécurisée.

Capteurs IoMT (pression, chute, mobilité)
→ Souvent basés sur des gateways avec certificats embarqués.

2.2 La responsabilité

Le technicien biomédical est garant du bon fonctionnement du dispositif. Si une fuite de données survient car le chiffrement était désactivé ou obsolète (ex: vieux protocole TLS 1.0), la responsabilité du service biomédical peut être engagée aux côtés de la DSI.

2.3 Référentiels et normes applicables à la sécurité des dispositifs médicaux connectés

La gestion des certificats SSL/TLS dans les dispositifs médicaux s'inscrit dans un paysage réglementaire en pleine évolution. Plusieurs normes internationales soulignent que la sécurité des communications n'est plus un simple choix technique, mais une exigence de sécurité patient.

- L'**IEC 81001-5-1** introduit le concept d'"hygiène numérique" et impose des pratiques de protection des données échangées, notamment via le chiffrement et le contrôle des identités machines.

- De son côté, la série **IEC 62443**, largement utilisée pour les environnements industriels et hospitaliers, recommande le recours aux certificats pour authentifier les composants et segmenter les communications critiques.

- Enfin, les autorités sanitaires renforcent également leurs exigences :

    - la **FDA** (États-Unis) demande depuis 2023 que les DM incluent des mécanismes de gestion du chiffrement et des certificats dans leur cycle de vie,

    - l'**ENISA** (Union européenne) identifie la validation des certificats et la synchronisation temporelle comme des prérequis essentiels dans les "Smart Hospitals".

Pour les services biomédicaux, cela signifie que la gestion des certificats n'est plus optionnelle : elle fait partie intégrante de la conformité réglementaire, de la sécurité du patient et de la protection de l'institution.

2.4 Référentiels suisses applicables à la cybersécurité des dispositifs médicaux connectés

En Suisse, plusieurs organismes publient des cadres de référence essentiels pour sécuriser les infrastructures de santé, y compris les dispositifs médicaux connectés.

- L'**Office fédéral de la cybersécurité (OFCS)** recommande un ensemble d'exigences minimales destinées à tous les prestataires du secteur de la santé, couvrant la protection des communications, la gestion des certificats et la sécurisation des systèmes techniques et organisationnels. Ces recommandations constituent aujourd'hui le socle national de bonnes pratiques en matière de cybersécurité.

- Dans le contexte plus large de la numérisation, la **Stratégie Cybersanté Suisse 2.0** pilotée par la Confédération et les cantons met également l'accent sur l'interopérabilité, la sécurité des données et la confiance numérique, éléments clés pour garantir des échanges de santé fiables et sécurisés, notamment via des mécanismes comme le TLS et la gestion des certificats associés.

- Enfin, la **FMH** établit des exigences minimales visant à renforcer la sécurité informatique dans les cabinets et institutions médicales, soulignant que la protection des données sensibles exige l'utilisation de mécanismes de chiffrement robustes et la gestion appropriée de certificats de sécurité au sein des infrastructures de soins.

Ces référentiels rappellent que, dans le système de santé suisse, la cybersécurité n'est pas seulement un enjeu technique : elle fait partie intégrante de la protection des patients, de la continuité des soins et de la conformité réglementaire.

Partie 3 : Guide pratique de gestion (Le "How-to")

3.1 Générer un certificat : Le CSR

En général pour obtenir un certificat, le DM doit générer une CSR (Certificate Signing Request). C'est un fichier contenant l'identité de la machine.

- Conseil : Ne transmettez jamais la "clé privée" associée. Elle doit rester dans le DM, comme le code PIN de votre carte bleue.

Cette étape peut aussi être différente et « externalisée » dans un autre processus de demande de certificats SSL.

3.2 Comprendre les formats et extensions de fichiers (.pem, .cer, .key, .pfx)

Une fois que la DSI ou l'autorité de certification vous renvoie le certificat, il peut se présenter sous différentes extensions qu'il est essentiel de ne pas confondre pour réussir l'installation sur le DM.

- Le format **.PEM** (ou .CRT), très polyvalent et courant dans le milieu hospitalier, est un fichier texte lisible avec un bloc-notes pouvant contenir aussi bien un certificat seul que la chaîne complète de confiance.

- Il est souvent accompagné d'un fichier **.KEY** qui contient exclusivement la **clé privée** du dispositif, laquelle doit rester strictement confidentielle et stockée de manière sécurisée sur le DM.

- L'extension **.CER** (ou .DER / .CRT) désigne généralement un certificat seul (partie publique) sans la clé privée, format souvent utilisé pour transmettre le certificat "racine" de l'hôpital nécessaire à l'établissement de la confiance.

- Enfin, le format **.PFX** (ou .P12), très utilisé sur les systèmes Windows, est un "conteneur" binaire protégé par mot de passe regroupant le certificat, la clé privée et

les certificats racines ; son importation sur un DM nécessitera systématiquement le mot de passe défini lors de sa création.

Le conseil du tech : Si votre DM demande un format spécifique que vous n'avez pas, des outils (souvent gérés par la DSI) permettent de convertir ces formats (par exemple un .pfx en .pem) selon les besoins spécifiques de votre équipement. L'important est de toujours savoir si la **clé privée** est incluse ou non dans votre fichier avant toute manipulation.

3.3 Astuce technique : Identifier le contenu avec le "Bloc-notes"

En cas de doute sur la nature d'un fichier reçu, vous pouvez l'ouvrir avec un éditeur de texte (type Bloc-notes) pour vérifier ses balises :

- **Certificat Public :** Vous lirez -----BEGIN CERTIFICATE-----. C'est le document que vous pouvez partager sans crainte avec la DSI.
- **Clé Privée :** Vous lirez -----BEGIN PRIVATE KEY-----. **Attention :** Ce fichier ne doit jamais être transmis par e-mail ; il doit être manipulé avec la plus grande prudence et rester sur le dispositif.
- **Fichier illisible :** Si vous ne voyez que des symboles incohérents, il s'agit d'un format binaire (comme le **.pfx**). Il ne peut être lu que par l'interface du dispositif médical ou un logiciel spécialisé.

3.4 Diagnostic : Pourquoi ça ne communique pas ?

Si vous voyez un message "SSL Error" ou "Certificate Invalid", vérifiez toujours ces trois points de base :

1. L'heure du DM : Si l'horloge du DM est décalée de 10 minutes, il peut croire que le certificat n'est pas encore valide ou déjà périmé.
2. La chaîne de certification : Le DM possède-t-il le certificat "racine" de l'hôpital ?
3. Le nom (FQDN : *Fully Qualified Domain Name* ou nom de domaine entièrement qualifié ou encore hostname) : Le nom inscrit dans le certificat doit correspondre exactement à l'adresse réseau du DM.

Partie 4 : Dialogue avec la DSI et Achats

4.1 Questions à poser aux fournisseurs (Appels d'offres)

Ne demandez plus seulement si le DM est "connectable", demandez :

- *"Le DM supporte-t-il l'import de certificats tiers (CA hospitalière) ?"*
- *"Quelle est la version de TLS supportée ? (Exiger TLS 1.2 minimum, idéalement 1.3)"*
- *"Le DM dispose-t-il d'une alerte d'expiration de certificat 30 jours avant l'échéance ?"*

Attention ceci est à modifier et compléter selon les exigences de votre institution en termes de connectivité réseau.

4.2 La frontière de maintenance

Il est crucial de définir un Document de Stratégie de Maintenance (DSM) :

- Biomed : Gère l'inventaire des dates d'expiration et l'accès physique/logiciel au DM.
- DSI : Fournit les fichiers de certificats signés et gère l'infrastructure de confiance.

Conclusion : De la maintenance mécanique à la maintenance numérique

Le métier de technicien biomédical vit une mutation sans précédent. Historiquement garant de l'intégrité physique des dispositifs, il ne peut plus aujourd'hui se contenter de vérifier la pression des fluides, l'usure des batteries ou la précision des capteurs. Dans un hôpital interconnecté, un dispositif médical qui ne communique plus — ou qui communique mal — est un dispositif inopérant, voire dangereux.

Désormais, la **"confiance numérique"** devient un paramètre de maintenance au même titre que la sécurité électrique. S'assurer qu'un certificat SSL/TLS est à jour, c'est garantir que le lien vital entre le patient et son dossier médical n'est pas rompu. C'est s'assurer qu'une alerte critique ne sera pas interceptée ou bloquée par un serveur de sécurité.

Cette évolution impose un changement de paradigme :

- **La cybersécurité n'est plus une option technique**, c'est une composante intrinsèque de la **sécurité du patient**. Un DM vulnérable est un risque clinique potentiel.
- **Le dialogue est la nouvelle clé.** Le technicien biomédical devient le traducteur indispensable entre le monde du soin, les exigences de la DSI et les contraintes des constructeurs.

En maîtrisant la gestion des certificats et les protocoles de sécurisation, le service biomédical ne fait pas que protéger des données ; il protège la continuité des soins et l'institution hospitalière dans son ensemble.

L'ère de la maintenance hybride est arrivée : elle est à la fois mécanique, électronique et numérique. Soyons-en les acteurs.

Annexe 1 : Exemple de Check-list de Maintenance Préventive Numérique

1. État des Certificats et Sécurité TLS

- [ ] **Validité temporelle :** Relever la date d'expiration du certificat. Si l'échéance est à moins de 90 jours, planifier le renouvellement avec la DSI.
- [ ] **Algorithme de signature :** Vérifier que le certificat n'utilise pas un algorithme obsolète (ex: bannir le SHA-1 au profit du SHA-256).
- [ ] **Version du protocole :** S'assurer que les versions non sécurisées (SSLv2, SSLv3, TLS 1.0, TLS 1.1) sont désactivées dans les réglages du DM si le constructeur le permet.

2. Configuration Système & Temps

- [ ] **Synchronisation Horloge :** Vérifier l'heure et le fuseau horaire. Si le DM n'est pas sur un serveur NTP, recaler l'heure à la seconde près (un décalage de quelques minutes brise la validation SSL).
- [ ] **Statut du Client NTP :** Vérifier que l'adresse IP du serveur de temps de l'hôpital est bien renseignée et que la synchronisation est "Active".

3. Gestion des Accès et Identités

- [ ] **Identifiants par défaut :** Confirmer que les mots de passe "usine" (ex: admin/admin, 1234) ont été remplacés par des mots de passe robustes.
- [ ] **Comptes obsolètes :** Supprimer les comptes créés pour des prestataires externes dont l'intervention est terminée.
- [ ] **Interface d'administration :** Vérifier que l'accès à la configuration réseau du DM est protégé par un mot de passe différent de celui de l'interface utilisateur "soignant".

4. Intégrité et Connectivité

- [ ] **Journal d'erreurs (Logs) :** Consulter les logs système du DM pour détecter des tentatives de connexion SSL échouées répétitives.
- [ ] **Ports ouverts :** S'assurer que seuls les ports nécessaires à la fonction médicale sont ouverts (désactiver Telnet, FTP ou HTTP non sécurisé si possible).
- [ ] **Sauvegarde de configuration :** Effectuer une sauvegarde des paramètres réseau (incluant les certificats) sur un support sécurisé avant toute modification.

5. Inventaire et Documentation

- [ ] **Mise à jour de la base GMAO :** Renseigner la version du firmware et la date de fin de validité du certificat dans la fiche de l'équipement.
- [ ] **Étiquetage physique (Optionnel) :** Apposer une pastille ou un QR Code sur le DM indiquant la date de la dernière vérification de cybersécurité.

Annexe 2 : Guide de diagnostic rapide des erreurs SSL/TLS

À utiliser lorsqu'un dispositif médical (DM) affiche une erreur de connexion réseau sécurisée.

La règle d'or : Toujours vérifier **l'heure et la date** de l'équipement en premier. 80% des pannes SSL en biomédical proviennent d'une dérive de l'horloge interne (souvent due à une pile de sauvegarde CMOS fatiguée sur les anciens dispositifs).

Symptôme / Message d'erreur	**Cause probable**	**Action corrective (Niveau Biomédical)**
"Certificate Expired" ou **"Date Invalid"**	Le certificat du DM ou du serveur a dépassé sa date de validité.	1. Vérifier la date d'expiration dans l'interface réseau du DM. 2. Si expiré : Demander un nouveau certificat à la DSI.
"Handshake Failed" ou **"Protocol Version Mismatch"**	Incompatibilité de version (ex: le serveur exige TLS 1.3 mais le DM ne connaît que le vieux TLS 1.0).	1. Vérifier si une mise à jour logicielle du DM est disponible. 2. Contacter la DSI pour savoir si un protocole obsolète a été banni du réseau.
"Untrusted Root" ou **"Unknown CA"**	Le DM ne reconnaît pas l'autorité qui a signé le certificat du serveur.	1. Importer le "Certificat Racine" (Root CA) de l'hôpital dans le trousseau de clés du DM. 2. Vérifier que le DM n'est pas configuré en "Auto-signé".
"Time / Clock Skew Error"	L'horloge interne du DM n'est pas à l'heure.	1. Régler l'heure et la date du DM à la seconde près.

Symptôme / Message d'erreur	Cause probable	Action corrective (Niveau Biomédical)
		2. **Conseil :** Activer la synchronisation NTP (Network Time Protocol) si disponible.
"Hostname Mismatch"	Le nom inscrit dans le certificat (ex: *ecm-01.local*) ne correspond pas à l'IP ou au nom réel du DM.	1. Vérifier que le nom réseau (Hostname) n'a pas été modifié après l'installation du certificat. 2. Regénérer une demande de certificat (CSR) avec le bon nom.
"Connection Reset" (juste après le Hello)	Le certificat est présent mais le chiffrement est bloqué par un pare-feu ou un antivirus réseau.	1. Tester la connexion sur un port non sécurisé (si possible) pour isoler le problème. 2. Vérifier si le port standard (souvent le **443**) est bien celui configuré sur le DM 3. Solliciter la DSI pour vérifier l'ouverture des flux (Pare-feu).

Annexe 3 : Petit Lexique du Biomédical Connecté (SSL/TLS)

Ce glossaire traduit le jargon informatique en concepts concrets pour le terrain biomédical.

Terme	Définition simple	Ce qu'il faut retenir pour le DM
CA (Autorité de Certification)	L'organisme (externe ou interne à l'hôpital) qui signe les certificats.	C'est le "notaire" qui valide que votre DM est bien celui qu'il prétend être.
CSR (Certificate Signing Request)	Un fichier de demande de certificat généré par le DM.	C'est le "formulaire de demande de passeport" que vous envoyez à la DSI.
Clé Privée (Private Key)	Un fichier secret stocké à l'intérieur du DM.	**Crucial :** Elle ne doit jamais sortir de l'appareil. Si elle est perdue ou volée, la sécurité est rompue.
Clé Publique (Public Key)	Une clé partagée avec tout le monde pour chiffrer les données.	Elle fonctionne en duo avec la clé privée : ce que l'une verrouille, seule l'autre peut le déverrouiller.
FQDN (Fully Qualified Domain Name)	Le nom complet du DM sur le réseau (ex: *scanner01.hopital.fr*).	Le certificat est souvent lié à ce nom précis. Si vous changez le nom du DM, le certificat devient invalide.
Handshake (Poignée de main)	Phase de négociation initiale entre le DM et le serveur.	C'est le moment où les erreurs SSL apparaissent le plus souvent (incompatibilité de version).
NTP (Network Time Protocol)	Protocole qui permet de synchroniser l'heure des machines sur le réseau.	Un DM mal synchronisé rejettera systématiquement un certificat valide. **C'est la cause n°1 des pannes.**
PKI (Public Key Infrastructure)	L'ensemble des serveurs et processus qui gèrent les certificats dans l'hôpital.	C'est "l'usine à certificats" gérée par votre DSI.

Terme	Définition simple	Ce qu'il faut retenir pour le DM
Root Certificate (Certificat Racine)	Le certificat "père" qui permet de faire confiance à tous les autres.	Pour qu'un DM communique, il doit souvent avoir le "Certificat Racine" de l'hôpital installé dans sa mémoire.
TLS / SSL	Protocoles de sécurisation des échanges.	SSL est l'ancien nom, **TLS** est le nom moderne. Aujourd'hui, on exige généralement le **TLS 1.2** ou **1.3**.