International Journal of Academic Health and Medical Research (IJAHMR)
ISSN: 2643-9824
Vol. 10 Issue 7 July - 2026, Pages: 111-115

Le certificat SSL/TLS au service de la vie privée des patients : Étude de la confidentialité des échanges de données médicales entre établissements de santé

Jacques KIZA DIMANDJA

Assistant Deuxime Mandat
Email: Jacques.kiza.dimandja@uka.ac.cd
University : Our Lady of Kasayi University (U.KA),

Licencié en Sciences Informatiques (Orientation: Conception des systèmes Informatiques) , Assistant Scientifque à l'Université Notre-Dame du Kasayi (U.KA), Kasaï Central, Kananga(RDC)

***Abstract**: The transmission of sensitive Electronic Health Records (EHR) during critical inter-hospital transfers requires robust mechanisms to preserve patient privacy and data confidentiality. When medical directors or senior nurses transfer critical patient cases across Wide Area Networks (WAN), unencrypted communication channels expose medical histories to unauthorized eavesdropping, data alteration, and phishing-based identity spoofing. This paper presents an in-depth study on the deployment of SSL/TLS protocol certificates as a core mechanism for privacy protection in online health data exchanges. We demonstrate how transport-layer encryption (TLS 1.3) combined with mutual TLS authentication (mTLS) and Extended Validation (EV) certificates prevents phishing attacks, mitigates Man-in-the-Middle (MitM) interceptions, and ensures strict medical secrecy.*

Keywords: ***SSL/TLS Certificates, Patient Privacy, Confidentiality, Inter-hospital Data Transfer, Phishing Prevention, Electronic Health Records, mTLS***

***Résumé* :** *Lors du transfert d'un patient critique d'un hôpital vers un autre, la transmission rapide du Dossier Médical Informatisé (DMI) par les Médecins Directeurs ou Infirmiers Titulaires s'effectue à travers des réseaux étendus (WAN). Sans protection adéquate, l'exposition des données de santé compromet la vie privée du patient et ouvre la voie à des attaques par hameçonnage (phishing) ciblées.*

Cet article étudie le rôle du protocole SSL/TLS dans la garantie de la confidentialité des échanges de données médicales entre établissements de santé. Nous démontrons comment le chiffrement bout en bout, l'authentification mutuelle (mTLS) et l'analyse des certificats à validation étendue (EV) permettent d'assurer une étanchéité totale de la vie privée en ligne tout en contrecarrant les tentatives d'usurpation d'identité et de hameçonnage.

Mots-clés: ***Certificat SSL/TLS, Vie privée du patient, Confidentialité médicale, Transferts interhospitaliers, Lutte contre l'hameçonnage, mTLS, Dossier Médical Informatisé.***

1. Le Transit des Données Critiques sur Réseau WAN

Dans une chaîne de soins interconnectée, lorsqu'un cas médical devient critique, le Médecin Directeur ou l'Infirmier Titulaire de l'établissement émetteur (Hôpital A) doit transmettre en urgence le dossier complet du patient (constantes vitales, imagerie DICOM, bilans biologiques, traitements en cours) à l'établissement récepteur (Hôpital B).

Le réseau étendu (WAN) reliant ces établissements est par nature non sécurisé. Le problème fondamental est double :

1. **Atteinte à la vie privée :** Un tiers interceptant le flux réseau peut accéder à l'identité, au diagnostic et à l'historique pathologique du patient, violant le secret médical.

2. **Attaques par hameçonnage et usurpation:** Un pirate informatique peut concevoir un faux portail web récepteur (faux Hôpital B) ou intercepter la communication pour détourner le transfert et récupérer des données de santé à des fins malveillantes.

2. Protection de la Vie Privée des Patients en Ligne via SSL/TLS

Le protocole **SSL/TLS** (*Transport Layer Security*) garantit la protection de la vie privée des patients lors des transferts numériques grâce à trois mécanismes cryptographiques fondamentaux :

2.1 Le Chiffrement Point à Point (Confidentialité Absolue)

Lorsque le transfert est initié sous HTTPS (TLS 1.3), les données médicales sont chiffrées à l'aide d'un algorithme symétrique fort (ex. AES-256-GCM).

- **Analogie Médicale :** L'envoi du dossier ne se fait plus sous forme d'une lettre ouverte, mais à l'intérieur d'un **coffre-fort numérique itinérant**.
- **Résultat en ligne :** Même si un paquet réseau est capturé par un pirate sur le WAN, le contenu reste une suite d'octets indéchiffrables. La vie privée et le secret médical du patient sont préservés.

2.2 L'Intégrité des Données de Santé

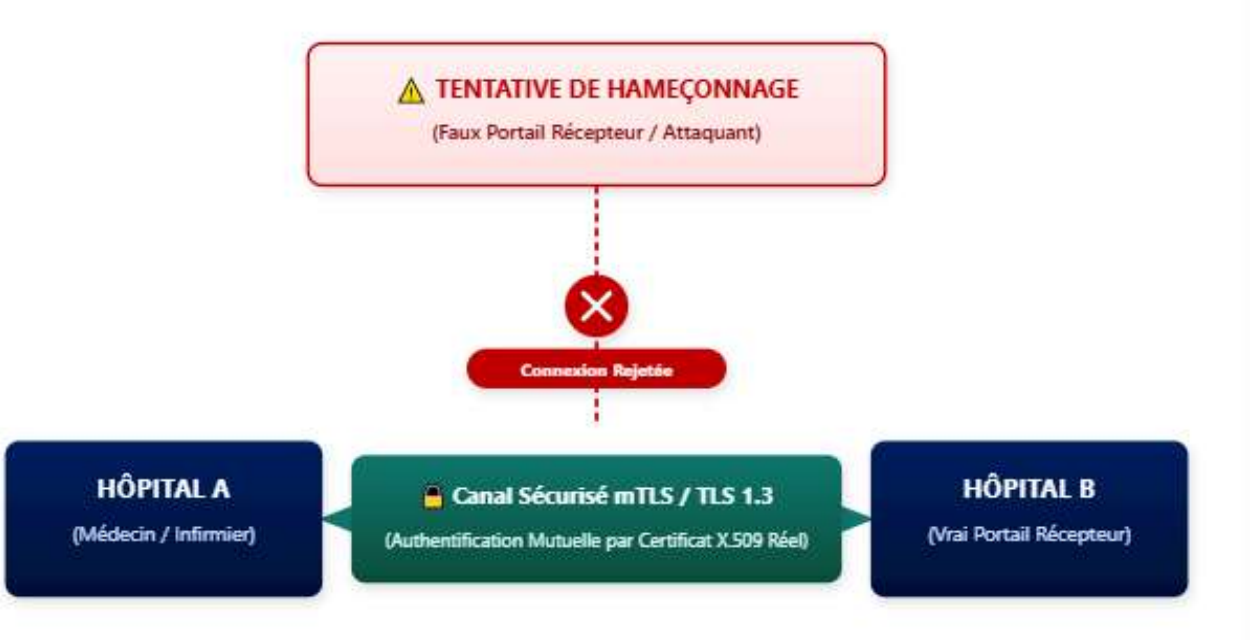
Le protocole utilise des fonctions de hachage cryptographique (ex. HMAC-SHA256) pour sceller chaque message.

- **Résultat en ligne :** Si un attaquant tente d'altérer une donnée médicale en transit (ex. modifier le groupe sanguin ou la dose d'un médicament), l'empreinte numérique recalculée par l'Hôpital B sera discordante. Le transfert est immédiatement rejeté, éliminant tout risque d'erreur médicale induite.

3. Mesures de Sécurité pour Contrer les Attaques par Hameçonnage (*Phishing*)

L'hameçonnage dans le secteur médical cible souvent les soignants (Médecins Directeurs, Infirmiers) via de faux formulaires de transfert ou de faux portails interhospitaliers destinés à voler des identifiants et des dossiers médicaux. Les certificats SSL/TLS offrent des réponses techniques et opérationnelles strictes contre ce risque.

International Journal of Academic Health and Medical Research (IJAHMR)
ISSN: 2643-9824
Vol. 10 Issue 7 July - 2026, Pages: 111-115



3.1 Authentification Mutuelle (mTLS - Mutual TLS)

Pour contrer le hameçonnage par redirection ou faux site web, l'architecture d'échange entre hôpitaux ne s'appuie pas sur un simple mot de passe (facilement piégeable par un faux mail), mais sur le **mTLS** :

- **Principe :** L'Hôpital A et l'Hôpital B possèdent chacun un certificat numérique $X.509$ unique et signé par une Autorité de Certification (AC) de santé officielle.
- **Contre-mesure anti-phishing :** Si un soignant est redirigé vers une plateforme fantôme ou si un pirate tente de se faire passer pour l'Hôpital B, la poignée de main cryptographique (*TLS Handshake*) échoue immédiatement car le pirate ne possède pas le certificat privé valide d'un établissement agréé. Le transfert est bloqué à la racine.

3.2 Certificats à Validation Étendue (EV) et Épinglage de Certificat (*Certificate Pinning*)

- **Validation Étendue (EV) :** L'identité juridique de l'hôpital destinataire est soumise à une vérification stricte avant la délivrance du certificat, garantissant au soignant l'identité réelle du destinataire.
- **Certificate Pinning :** Les applications d'échange d'informations de santé intègrent en dur la clé publique du serveur destinataire. Si le trafic est détourné vers un serveur malveillant muni d'un faux certificat, l'application refuse la connexion instantanément.

3.3 Tableau Synthétique des Menaces d'Hameçonnage et Réponses SSL/TLS

Type de Menace / Hameçonnage	Risque pour le Patient / Soignant	Solution SSL/TLS / Protection
Site Miroir / Faux Portail Récepteur	Le soignant envoie le dossier critique sur un faux serveur géré par un pirate.	**mTLS + Certificat $X.509$:** Le faux serveur est incapable de prouver son identité cryptographique ; le transfert est refusé.
Attaque Man-in-the-Middle (MitM)	Interception du flux sur le réseau WAN et vol du dossier en temps réel.	**Chiffrement TLS 1.3 (AES-256) :** Les données interceptées sont illisibles et inexploitables.
Usurpation d'Identité du Soignant	Un pirate se fait passer pour le Médecin Directeur pour demander un dossier.	**Clé Privée liée au Certificat Soignant :** L'authentification requiert la clé cryptographique propre au poste ou au badge du cadre médical.

4. Étapes de Mise en Œuvre de l'Architecture Sécurisée

Pour mettre en place cette solution au sein du réseau d'échange interhospitalier, la démarche méthodologique suivante est appliquée :

1. **Cartographie des accès et rôles :** Définition stricte des profils habilités à initier le transfert (Médecins Directeurs et Infirmiers Titulaires).

2. **Déploiement d'une PKI de Santé (Infrastructure à Clés Publiques)** : Génération et distribution des certificats numériques $X.509$ sur les serveurs d'échange des hôpitaux partenaires.

3. **Configuration du protocole mTLS et TLS 1.3** : Désactivation des versions obsolètes (SSL v3, TLS 1.0, TLS 1.1) sur les passerelles Web pour neutraliser les attaques par rétrogradation (**downgrade attacks**).

4. **Sensibilisation et formation des cadres médicaux** : Entraînement du personnel soignant aux indicateurs de sécurité (vérification des certificats, alerte en cas d'erreur TLS) pour éviter les pièges d'ingénierie sociale.

Conclusion

L'intégration du protocole SSL/TLS et de l'authentification mutuelle (mTLS) garantit la protection de la vie privée des patients lors des transferts de dossiers médicaux critiques sur les réseaux publics. En neutralisant les risques d'interception et en barrant la route aux attaques par hameçonnage et usurpation d'identité, ces mécanismes cryptographiques offrent un cadre de confiance indispensable aux Médecins Directeurs et Infirmiers Titulaires pour l'exercice de leurs fonctions dans le respect du secret médical.

Références Bibliographiques

- Chappe, S. et Bideau, E. (2021). *Sécurité informatique et réseaux : Cours et exercices corrigés*, 2e éd., Paris.

- Kiza Dimandja, J. (2024). *SQL Injection Attack Prevention Methodology: Best Practices and Strategies*, International Journal of Academic Multidisciplinary Research (IJAMR), Vol. 8, N° 5.
- Kleppmann, M. (2018). *Concevoir des applications intensives en données : Les principes fondamentaux des systèmes fiables, évolutifs et maintenables*, Paris.
- Laudon, K. et Laudon, J. (2020). *Management des systèmes d'information*, 16e éd., Paris.
- Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3*, RFC 8446, IETF.