République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire

En vue de l'obtention du diplôme de Master professionnel en Informatique

Option

Administration et sécurité des réseaux

Thème

Analyse et validation du protocole d'authentification EAP-AKA' dans les systèmes de santé connectés.

Présenté par :

M^lle CHEMACHE Soulaf
M^lle ZAOUCHE Soulaf

Encadré par :

Mr Sadi Mustafa U. A/Mira Béjaia.

Soutenu le 01 juillet 2025 devant le jury composé de :

Présidente	*M^lle* Battat	Nadia	U. A/Mira Béjaia.
Examinatrice	*M^lle* Houha	Amel	U. A/Mira Béjaia.
Examinateur	*Mr* Chekrid	Mohamed	U. A/Mira Béjaia.
Examinateur	*Mr* Moktefi	Mohand	U. A/Mira Béjaia.

Année universitaire : 2024/2025

* *Remerciements* *

Au nom de Dieu, le Clément, le Miséricordieux, que les louanges soient adressées à Allah, le Tout-Puissant.

Nous souhaitons exprimer notre profonde et sincère gratitude à l'ensemble des personnes qui, de près ou de loin, ont contribué à la concrétisation de ce travail de recherche.

Nous adressons nos remerciements les plus respectueux à *Monsieur SADI Mustapha*, *notre encadrant, pour la qualité de son accompagnement, la pertinence de ses orientations, ainsi que pour sa disponibilité constante. Ses conseils judicieux et son soutien indéfectible ont été d'une aide précieuse tout au long de l'élaboration de ce mémoire.*

Nos remerciements s'adressent également à l'ensemble des enseignants et membres du jury, dont les enseignements rigoureux et les observations constructives ont grandement enrichi notre réflexion et contribué à la maturation de notre démarche scientifique.

Nous tenons également à exprimer notre reconnaissance envers nos collègues et amis, pour leur présence bienveillante, leur soutien moral et les échanges intellectuellement stimulants dont nous avons pu bénéficier.

Nos pensées les plus sincères vont à notre famille, et plus particulièrement à nos parents, pour leur patience, leur dévouement et leur appui inconditionnel. Leur affection et leur constante sollicitude ont constitué un pilier essentiel dans notre parcours académique.

Enfin, nous remercions chaleureusement toutes celles et ceux qui, par leur bienveillance, leur aide ou leur inspiration, ont participé à la réussite de ce mémoire et à l'accomplissement de notre formation.

** Dédicaces **

C'est avec grand plaisir et fierté que je dédie ce modeste travail aux êtres les plus précieux à mes yeux, à ceux que je n'arriverais jamais à leurs exprimer mon amour sincère.

Particulièrement à mes parents, qui ont fait de moi ce que je suis aujourd'hui. Pour leur immense amour, leur compréhension et leur dévouement. Que Dieu les garde et les protège. C'est à eux que je dois ma réussite. Aucune dédicace ne saurait exprimer tout l'amour et la gratitude que je leur porte.

À mes chers frères et sœurs, merci pour votre affection sincère, votre soutien fidèle et vos encouragements continus.À Sofiane et Yassmina, en particulier, pour leur présence bienveillante, leurs précieux conseils et leur soutien indéfectible tout au long de mes études.

À la mémoire de mon cher frère Foudil, Puisse son âme repose en paix.Il etait un accompagnon qui ne lache pas ma main quoi qu'il arrive. J'espère que ce modeste travail lui parvienne comme un témoignage sincère de mon amour et de ma profonde reconnaissance.Ton souvenir restera gravé à jamais dans mon cœurs, et tes valeurs continueront de vivre en moi.

À tous mes chers neveux Ayoub, Youva, Aksel, Djessim, M-Amine,Mehrez, Djaouad, Melina, Tasnim, Issraa et Sadil.

À ma chère cousine et amie Zohra CHEMACHE, une femme exceptionnelle et une doctorante exemplaire. Merci de m'avoir soutenue, écoutée et encouragée, dans les moments les plus difficiles. Ta bienveillance et ta générosité resteront gravées dans mon cœur.

À toute personne qui a contribué de près ou de loin à la réalisation de ce travail.

Soulaf Chemache

**** Dédicaces ****

Je rends grâce à Celui qui éclaire les cœurs et guide les pas, source de sagesse, de paix et de patience, pour la force qu'Il m'a accordée dans chaque moment de doute et d'espérance.

À mes parents, piliers silencieux de mon existence, dont l'amour inconditionnel, les sacrifices et les prières ont porté ce chemin avec tant de courage et de tendresse. À mes sœurs, à mon frère, pour leur affection sincère, leur présence apaisante et les sourires partagés qui ont toujours réchauffé le cœur.

Et une pensée toute particulière à mon petit chouchou « Dylan », cette tendre étoile dans notre ciel familial.
A mes amis, pour leur présence fidèle, leurs mots simples et vrais, et les éclats de rire qui ont illuminé ce parcours, je dis merci.

Soulaf Zaouche

Résumé : Les dispositifs médicaux connectés jouent un rôle essentiel dans la transformation numérique de la santé. Cependant, la sécurité des échanges de données sensibles reste un défi majeur. Ce mémoire s'intéresse à l'analyse du protocole EAP-AKA', utilisé dans les réseaux 5G, pour sécuriser l'authentification des dispositifs de télésurveillance médicale. Le protocole repose sur des étapes clés telles que l'identification, l'échange de défi et la dérivation de clés de session. Malgré sa robustesse, certaines failles comme les attaques par rejeu subsistent. Des améliorations ont été proposées, et une validation formelle via l'outil AVISPA a confirmé l'efficacité du protocole renforcé. Ce travail contribue ainsi à renforcer la confidentialité, l'intégrité et la fiabilité des systèmes de santé connectée.

Mots clés : EAP-AKA', Dispositifs médicaux connectés, Authentification, Sécurité, Analyse, Validation formelle, Réseaux 5G

Abstract : Connected medical devices play a key role in the digital transformation of healthcare. However, ensuring the security of sensitive data exchanges remains a major challenge. This thesis focuses on the analysis of the EAP-AKA' protocol, used in 5G networks, to secure authentication in remote medical monitoring systems. The protocol relies on essential steps such as identity verification, challenge-response exchange, and session key derivation. Despite its robustness, certain vulnerabilities—like replay attacks—persist. Technical enhancements were proposed, and formal validation using the AVISPA tool confirmed the effectiveness of the improved protocol. This work contributes to strengthening the confidentiality, integrity, and reliability of connected healthcare systems.

Keywords : EAP-AKA', Connected medical devices, Authentication, Security, Analysis, Formal verification, 5G networks

Table des matières

Table des figures

Liste des abréviations

3G 3rd Generation
3GPP 3rd Generation Partnership Project
4G 4th Generation
5G 5th Generation
ABBA Anti-Bidding down Between Architectures
AI Artificial Intelligence
ARPF Authentication credential Repository and Processing Function
AUTN Authentication Token
AUSF Authentication Server Function
AV Authentication Vector
AVISPA Automated Validation of Internet Security Protocols and Applications
CAS+ Constraint-based Analysis of Security Protocols
CHAP Challenge-Handshake Authentication Protocol
CK Ciphering Key
CK' Cipher Key prime
CL-AtSe Constraint-Logic-based Attack Searcher
DL Deep Learning (Apprentissage profond)
DoS Denial of Service
E-mail Electronic Mail
EAP Extensible Authentication Protocol
EAP-AKA Extensible Authentication Protocol Authentication and Key Agreement
EAP-AKA' Extensible Authentication Protocol Authentication and Key Agreement prime
eSIM embedded SIM (SIM intégrée)
FDA Food and Drug Administration
GSM Global System for Mobile Communications
HLPSL High-Level Protocol Specification Language
HLPSL2IF HLPSL to IF Translator
HMAC Hash-based Message Authentication Code
HMAC-SHA-256 Hash-based Message Authentication Code-Secure Hash Algorithm 256-bit
HNID Home Network Identifier

IETF Internet Engineering Task Force
IDS Intrusion Detection System
IF Intermediate Format
IK Integrity Key
IK' Integrity Key prime
IMD Implantable Medical Device
IoMT Internet of Medical Things
IoWD Internet of Wearable Devices
KDF Key Derivation Function
KSEAF Key for Security Anchor Function
MAC Message Authentication Code
MAC2 Second Message Authentication Code
Mac_failure MAC Verification Failure
MFA Authentification Multi-Facteur
MitM Man-in-the-Middle
ML Machine Learning (Apprentissage automatique)
NAI Network Access Identifier
ngKSI Next Generation Key Set Identifier
OFMC On-the-Fly Model-Checker
PPP Point-to-Point Protocol
RAND Random Challenge
RES Response
RFC 3748 Request for Comments 3748
SATMC SAT-based Model-Checker
SEAF Security Anchor Function
SHA-1 Secure Hash Algorithm 1
SHA-256 Secure Hash Algorithm 256-bit
SIEM Security Information and Event Management
SIM Subscriber Identity Module
SMS Short Message Service
SNN Serving Network Name
SPAN Security Protocol Animator
SQN Sequence Number
SUCI Subscription Concealed Identifier
SUPI Subscription Permanent Identifier
Synch_failure Synchronization Failure
TA4SP Tree Automata based on Automatic Approximations for the Analysis of Security Protocols
UDM Unified Data Management
UE User Equipment

USIM Universal Subscriber Identity Module
Wi-Fi Wireless Fidelity
XRES Expected Response
XOR Exclusive OR (OU exclusif)

Introduction Générale

L'émergence des technologies de l'Internet des Objets (IoT) a profondément transformé le domaine de la santé. Les dispositifs médicaux connectés, capables de collecter, transmettre et analyser des données cliniques en temps réel, offrent des perspectives inédites pour le suivi à distance des patients, la télémédecine, la prévention et l'amélioration de la qualité des soins. Toutefois, cette avancée technologique soulève de nombreux défis, notamment en matière de sécurité des données médicales, qui sont par nature sensibles, confidentielles et critiques.

Dans ce contexte, la sécurisation des communications entre les dispositifs de santé connectés et les infrastructures médicales devient une exigence majeure. Il est indispensable de garantir l'authenticité, la confidentialité, l'intégrité et la disponibilité des échanges afin de préserver la confiance des utilisateurs et de répondre aux exigences réglementaires. Parmi les mécanismes de sécurité, l'authentification forte joue un rôle fondamental en permettant de vérifier l'identité des entités en communication et d'empêcher les accès non autorisés.

Le protocole EAP-AKA' (Extensible Authentication Protocol - Authentication and Key Agreement prime), largement utilisé dans les réseaux mobiles de nouvelle génération (4G, 5G) et les environnements IoT, s'impose comme une solution prometteuse pour sécuriser les dispositifs médicaux. Toutefois, malgré ses améliorations par rapport à EAP-AKA, le protocole EAP-AKA' présente encore certaines limites, notamment en matière de résistance aux attaques par rejeu, aux risques liés à la gestion des clés. Ces vulnérabilités peuvent compromettre la sécurité globale des systèmes de santé connectés.

Face à ces constats, ce mémoire s'inscrit dans une problématique centrale : le protocole EAP-AKA' est-il suffisamment robuste pour répondre aux exigences de sécurité des systèmes de santé connectés modernes, en particulier dans un environnement 5G ? Afin d'apporter des éléments de réponse à cette question, notre étude propose une approche structurée reposant d'abord sur une analyse approfondie du protocole EAP-AKA', de ses mécanismes d'authentification et de son fonctionnement dans les réseaux mobiles 5G. Cette analyse est complétée par une mise en œuvre concrète du protocole dans un scénario de télésurveillance médicale, permettant d'observer son comportement dans un cadre d'application réaliste et d'évaluer sa pertinence face aux exigences du domaine.

L'étude se poursuit par une analyse critique des limitations du protocole, visant à identifier les vulnérabilités qui persistent malgré les mécanismes de sécurité existants. Pour renforcer la rigueur de notre démarche, nous procédons enfin à une validation formelle de la sécurité du protocole à l'aide de l'outil AVISPA, un environnement de simulation permettant d'évaluer sa

résistance face à divers scénarios de menace.

Ce mémoire se structure autour de quatre chapitres complémentaires. Le premier introduit la notion de santé connectée, présente les principaux types de dispositifs médicaux intelligents et pose les fondements de la sécurité dans ces systèmes. Le deuxième se consacre à l'étude détaillée du protocole EAP-AKA', en explorant ses principes, son architecture et son intégration dans les réseaux 5G. Le troisième s'appuie sur une étude de cas concrète autour d'un système de télésurveillance intégrant le protocole. Enfin, le quatrième chapitre propose une validation formelle du protocole à l'aide d'AVISPA, afin de confronter ses mécanismes aux menaces théoriques identifiées.

Par cette approche intégrée, notre objectif est de contribuer à une meilleure compréhension des enjeux de sécurité dans le domaine de la santé connectée, tout en apportant une évaluation rigoureuse, contextualisée et appliquée de l'efficacité du protocole EAP-AKA' dans un environnement aussi critique que celui des dispositifs médicaux modernes.

Chapitre 1

Généralités sur la santé connectée

1.1 Introduction

Face à l'augmentation continue des maladies chroniques et au vieillissement de la population, les systèmes de santé traditionnels montrent leurs limites. Il devient indispensable d'adopter des solutions intelligentes et connectées pour répondre efficacement aux besoins croissants en soins. Si la prévention reste essentielle à travers une bonne hygiène de vie, elle ne suffit pas à elle seule à contenir l'aggravation de pathologies complexes.

C'est dans ce contexte que la santé connectée prend tout son sens. Elle repose notamment sur l'usage croissant des objets connectés médicaux, tels que les pacemakers intelligents, les glucomètres connectés, ou encore les dispositifs de surveillance cardiaque à distance, qui permettent un suivi continu et automatisé de l'état de santé des patients, y compris en dehors du cadre hospitalier.

Cependant, cette transition vers une médecine plus numérique s'accompagne de nouveaux défis, notamment en matière de sécurité et de protection des données de santé. En effet, les dispositifs connectés collectent, transmettent et stockent des informations médicales sensibles, ce qui en fait des cibles potentielles pour des attaques informatiques. Assurer la confidentialité, l'intégrité et la disponibilité de ces données devient donc une priorité stratégique, afin de préserver la confiance des patients et garantir la continuité des soins.

1.2 Santé connectée

La santé connectée désigne l'utilisation des technologies numériques et des objets intelligents (dispositifs) pour améliorer la prise en charge médicale. Elle permet notamment de collecter, transmettre et analyser des données de santé à distance, en facilitant la prévention, le diagnostic et le suivi des patients en dehors des structures de soins traditionnelles[1].

1.3 Type de dispositifs médicaux connectés

La santé connectée repose sur un ensemble de technologies numériques conçues pour améliorer la prévention, le diagnostic, le traitement et le suivi médical. Ces dispositifs se déclinent en plusieurs catégories, en fonction de leur usage, de leur mode de fonctionnement et de leur niveau d'implication médicale[2].

- **Les objets connectés de santé / bien-être** : Ce sont des appareils équipés de capteurs capables de mesurer certaines données physiologiques (fréquence cardiaque, activité physique, qualité du sommeil, tension artérielle, glycémie, etc.) et de les transmettre à une application ou à un professionnel de santé. Ils sont utilisés tant par des personnes en bonne santé (dans une logique de bien-être) que par des patients chroniques. Exemples : montre connectée, tensiomètre Bluetooth, balance intelligente, pilulier électronique.
- **Les dispositifs médicaux implantables ou portables** : Ils comprennent les technologies plus avancées qui assurent un suivi médical actif, parfois en continu. On y retrouve

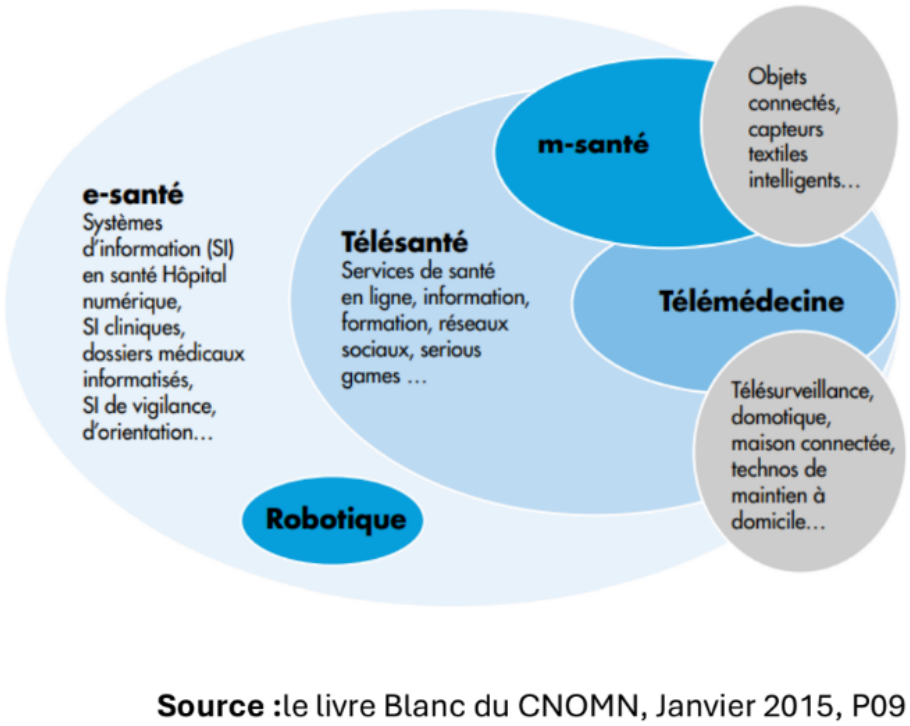


Figure 1.1 – Typologie des dispositifs médicaux connectées dans la santé numérique[2].

des capteurs intégrés dans le corps ou portés sur soi (comme les patchs de surveillance ou les pacemakers intelligents). Ces dispositifs sont souvent couplés à un système de télésurveillance médicale, comme le CardioMessenger dans le cas de certains implants cardiaques, permettant une transmission sécurisée des données aux professionnels de santé.

- **Les applications mobiles de santé** : Téléchargeables sur smartphones ou tablettes, ces applications offrent de nombreuses fonctionnalités : suivi des traitements, rappels de prise de médicaments, conseils personnalisés, journal de symptômes, etc. Certaines sont destinées au bien-être général, d'autres relèvent d'un usage médical, et peuvent alors être considérées comme des dispositifs médicaux à part entier.
- **Les outils de communication et d'aide à la décision** : Ils comprennent les logiciels de gestion des données de santé, les systèmes d'alerte médicale, ou encore les outils d'intelligence artificielle qui assistent les professionnels dans leurs décisions cliniques. Ces outils sont souvent interconnectés avec les autres dispositifs pour former un véritable écosystème numérique de soins.
- **Les plateformes de télémédecine** : Ce sont des systèmes numériques permettant des échanges à distance entre patients et professionnels de santé. Elles regroupent des services comme la téléconsultation, la téléexpertise, la télésurveillance médicale et la téléassistance. Ces plateformes sécurisées facilitent le suivi à domicile, l'ajustement de traitements et la détection précoce d'éventuelles complications.

1.4 Fonctionnement générale d'un système de télémédecine

La télémédecine regroupe plusieurs modalités d'intervention médicale à distance, rendues possibles grâce aux technologies numériques. Elle permet de connecter un patient et un professionnel de santé, ou plusieurs professionnels entre eux, sans nécessité de présence physique simultanée[29].

- **Téléconsultation** : consultation entre un médecin et un patient à distance, avec ou sans accompagnement d'un professionnel de santé. Elle est accessible à tous les médecins et facturée comme une consultation classique.
- **Téléexpertise** : échange entre médecins pour obtenir un avis spécialisé sur un dossier médical, avec l'accord du patient. Elle permet d'accélérer les diagnostics et la prise en charge.
- **Téléassistance** : Cette modalité concerne l'assistance à distance apportée par un médecin à l'un de ses confrères lors de la réalisation d'un acte médical ou chirurgical. Elle permet de mobiliser des compétences spécifiques sans que le médecin assistant soit physiquement présent.
- **Régulation médicale** : Réalisée par les médecins régulateurs des services d'urgence, elle consiste à évaluer par téléphone la situation d'un appelant afin d'établir un premier diagnostic et de décider de la réponse la plus adaptée, qu'elle soit médicale ou logistique.
- **Télésurveillance médicale** : Elle permet à un médecin de suivre à distance l'état de santé d'un patient, en analysant des données cliniques ou biologiques transmises régulièrement par le patient lui-même ou un professionnel de santé. Cette méthode est souvent utilisée pour le suivi de pathologies chroniques.

Un exemple courant de dispositif de télésurveillance médicale est le système Biotronik Home Monitoring, utilisé pour le suivi à distance de patients cardiaques.

1.5 Avantages et limites de la santé connectée

La santé connectée apporte de nombreux bénéfices, mais elle présente aussi certaines limites. Cette section propose un aperçu de ses principaux avantages et inconvénients[3][4][5] :

1.5.1 Avantages de la santé connectée

La santé connectée présente plusieurs avantages qui impactent positivement la vie de l'homme dans différents aspects. On peut citer, entre autres :

- **Amélioration de l'accès aux soins** : La santé connectée facilite l'accès aux soins, en particulier pour les populations éloignées ou rencontrant des difficultés de mobilité, permettant des consultations à distance.

- **Optimisation du parcours de soins** : Le partage d'informations entre professionnels améliore la coordination des soins, réduisant les examens redondants et limitant les erreurs médicales.
- **Autonomisation des patients** : Les objets connectés et applications permettent aux patients de mieux gérer leurs pathologies chroniques, augmentant ainsi leur autonomie dans le suivi médical.
- **Réduction des coûts de santé** : En réduisant les hospitalisations évitables et en optimisant les ressources, la santé connectée contribue à la baisse des dépenses de santé.
- **Prévention et suivi en temps réel** : La télésurveillance permet un suivi continu des patients, facilitant la détection précoce des complications et la prévention des rechutes.
- **Réduction des déplacements** : La téléconsultation et la télémédecine limitent les déplacements, un atout majeur pour les personnes âgées ou en situation de handicap.

1.5.2 Limites

Malgré ses apports, la santé connectée présente plusieurs limites :

- **Limites économiques** : La certification des dispositifs est coûteuse et difficile d'accès pour les start-ups. Beaucoup privilégient donc des objets non médicaux moins encadrés mais plus simples à commercialiser.
- **Risques éthiques** : Certaines entreprises peuvent exploiter les données de santé à des fins commerciales. L'accès aux données en temps réel, sans accompagnement, peut aussi générer stress ou dépenses inutiles. De plus, ces technologies risquent d'amplifier les inégalités d'accès aux soins.
- **Enjeux juridiques** : Le droit ne s'adapte pas encore totalement aux objets connectés. Il manque un cadre spécifique pour encadrer la collecte et l'usage des données personnelles en santé.
- **Risques techniques et industriels** : Les failles de cybersécurité et l'absence de standards techniques homogènes freinent le déploiement sécurisé de ces outils. Beaucoup d'innovations restent à l'état de prototypes.

1.6 Technologie de communication utilisé

Dans les systèmes de santé connectés, la communication joue un rôle fondamental pour assurer la transmission des données médicales entre les patients, les professionnels de santé et les infrastructures numériques. Plusieurs technologies sont utilisées selon les besoins et les contextes[6][7][8] .

Le GSM reste une solution fiable pour la transmission de données simples, comme des alertes ou des mesures de suivi, notamment dans les zones où les infrastructures modernes sont limitées. Le Wi-Fi et le Bluetooth sont souvent utilisés en milieu hospitalier ou à domicile pour connecter

localement les appareils médicaux aux plateformes de gestion. La 4G, quant à elle, a permis de fluidifier l'échange de données médicales plus lourdes, comme les images ou les vidéos.

Plus récemment, l'arrivée de la 5G ouvre de nouvelles perspectives pour la santé connectée, grâce à sa rapidité, sa fiabilité et sa capacité à connecter simultanément un grand nombre de dispositifs médicaux.

- **Carte SIM (Subscriber Identity Module)**

La carte SIM est un petit circuit intégré utilisé dans les appareils mobiles pour identifier l'utilisateur sur un réseau mobile. Elle contient des informations essentielles comme l'identité de l'abonné (IMSI), les clés de chiffrement pour la sécurité, et permet l'authentification et la connexion au réseau de l'opérateur. Elle joue un rôle central dans la transmission sécurisée des données, notamment dans les dispositifs de santé connectée.

Parmi les évolutions de la carte SIM, on distingue deux modèles :

— USIM (Universal SIM) : c'est une version améliorée de la SIM classique, utilisée dans les réseaux 3G, 4G et 5G. Elle offre des capacités de stockage plus importantes et renforce la sécurité des échanges grâce à des algorithmes de chiffrement plus avancés.

— eSIM (embedded SIM) : il s'agit d'une carte SIM intégrée directement dans l'appareil, sans format physique amovible. Elle permet une gestion à distance (activation, changement d'opérateur) et est particulièrement adaptée aux objets connectés comme les dispositifs médicaux miniaturisés.

1.6.1 Apports de la 5G dans la santé connectée

La technologie 5G présente des atouts majeurs pour le développement de la santé connectée, en particulier lorsqu'elle est associée à l'Internet des objets médicaux (IoMT). Grâce à son haut débit et à sa faible latence, la 5G facilite plusieurs usages clés dans le domaine médical[8] :

- **Surveillance à distance des patients** : La 5G permet un suivi en temps réel grâce à des dispositifs médicaux portables connectés, facilitant la prise en charge rapide et la personnalisation des soins.
- **Développement de la télésanté** : Elle rend les consultations médicales à distance plus fluides et fiables, tout en réduisant les coûts et les déplacements pour les patients.
- **Partage instantané des données** : Le transfert rapide et sécurisé des données médicales améliore la coordination entre professionnels de santé et accélère le diagnostic.
- **Appui au diagnostic par l'intelligence artificielle** : Grâce à sa faible latence, la 5G permet aux systèmes d'IA d'analyser rapidement les données de santé, améliorant la précision des diagnostics et l'efficacité des traitements.

1.7 Architecture des systèmes IoMT

La plupart des systèmes IoMT actuels sont généralement divisés en quatre couches comme illustré sur la figure 2.1. Ces couches couvrent toutes les étapes de traitement des données, en commençant par la collecte biométrique des informations de l'individu jusqu'à leur transfert sur le réseau, pour être ensuite visualisées et analysées par un professionnel de santé. Avec les avancées récentes des dispositifs médicaux implantables (IMD) et des dispositifs portables (IoWD), ces derniers partagent en grande partie la même architecture, dans la mesure où les IMD peuvent communiquer avec les passerelles, comme l'illustre un pacemaker[11].

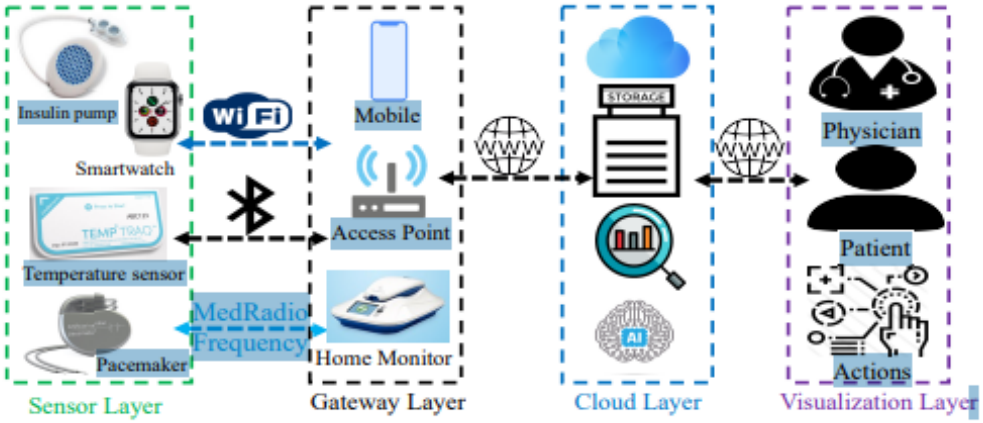


Figure 1.2 – Architecture de système IoMT[11].

- **Couche des capteurs** : Cette couche regroupe les capteurs portables ou implantés chez le patient, chargés de collecter des données de santé telles que la fréquence cardiaque, la température corporelle ou encore le taux d'oxygène dans le sang. Ces informations biométriques sont ensuite transmises à la couche supérieure à l'aide de technologies de communication sans fil à courte portée telles que le Wi-Fi, le ZigBee ou le Bluetooth.
- **Couche passerelle** : Étant donné les capacités limitées des dispositifs IoMT en matière de traitement et de stockage, cette couche repose sur des appareils intermédiaires plus puissants comme les smartphones ou les montres connectées. Ces derniers jouent le rôle de passerelles, assurant un prétraitement minimal des données avant de les transférer vers l'infrastructure réseau pour un traitement plus approfondi.
- **Couche réseau** : Cette couche est responsable du transfert, du stockage et de l'analyse avancée des données de santé. Des technologies telles que le machine learning (ML) et le deep learning (DL) sont utilisées pour extraire des informations pertinentes à partir des données recueillies. Toutefois, la latence due à la congestion du réseau peut nuire à la réactivité du système, ce qui est critique pour les applications médicales. Pour y remédier, des approches comme l'edge computing ou la blockchain sont envisagées pour renforcer la sécurité et réduire les délais de traitement.
- **Couche de visualisation (ou couche applicative)** : Cette couche permet aux professionnels de santé et aux patients d'accéder aux résultats via des interfaces adaptées. Les

médecins peuvent y consulter les données, poser des diagnostics, émettre des recommandations ou prescrire des traitements. Les patients, quant à eux, peuvent suivre l'évolution de leur état de santé en temps réel et recevoir des conseils personnalisés.

1.8 Principes fondamentaux de la sécurité des dispositifs IoMt

La sécurité de l'Internet des Objets médicaux (IoMT) vise à protéger les dispositifs médicaux connectés, ainsi que les réseaux hospitaliers auxquels ils sont associés, contre les menaces et vulnérabilités informatiques. Cela implique la détection, la surveillance et la correction proactive des failles de sécurité susceptibles de compromettre l'intégrité des systèmes de santé et la confidentialité des données des patients. En l'absence de mesures de sécurité adéquates, ces dispositifs peuvent devenir des portes d'entrée pour les cybercriminels.

Par exemple[13][14], en 2019, la société Medtronic, spécialisée dans les dispositifs médicaux, a été confrontée à une faille critique affectant plusieurs modèles de ses pompes à insuline connectées, utilisés par des patients diabétiques pour administrer automatiquement de l'insuline, communiquaient sans fil avec d'autres appareils, mais sans chiffrement ni authentification. Cette vulnérabilité permettait à un attaquant situé à proximité (moins de deux mètres) d'intercepter les signaux, voire de modifié à distance les doses d'insuline délivrées. Une injection incorrecte pouvait entraîner de graves conséquences pour le patient, telles qu'une hypoglycémie sévère ou une hyperglycémie. Bien qu'aucune attaque réelle n'ait été signalée, la faille était exploitable, poussant la FDA (Food and Drug Administration) à émettre une alerte de sécurité et à recommander de retirer ces dispositifs du marché. Cet incident souligne l'importance cruciale de la La sécurité informatique dans la conception des dispositifs médicaux connectés.

Les principes fondamentaux de la sécurité des dispositifs IoT incluent[10][11] :

- **Surveillance continue :** Il est essentiel de déployer des mécanismes de surveillance en temps réel afin de détecter toute activité suspecte ou comportement inhabituel sur les dispositifs IoT médicaux et les réseaux auxquels ils sont connectés. Cela peut inclure l'utilisation de systèmes de détection d'intrusion (IDS) et de solutions de gestion des événements et informations de sécurité (SIEM) pour analyser les flux de données et réagir rapidement en cas d'anomalie.
- **Correction des vulnérabilités :** Il est crucial d'appliquer régulièrement des mises à jour logicielles et des correctifs de sécurité afin de traiter les vulnérabilités identifiées. Les fabricants de dispositifs IoT ainsi que les fournisseurs de services doivent faire preuve de réactivité et de rigueur dans la diffusion de ces correctifs pour garantir la sécurité continue de leurs équipements et logiciels.
- **Authentification et autorisation :** Il est essentiel de mettre en place des mécanismes d'authentification solides afin de s'assurer que seuls les utilisateurs légitimes peuvent accéder aux dispositifs IoT et aux données qu'ils traitent. Par ailleurs, la gestion des droits

d'accès doit être strictement contrôlée, en appliquant le principe du moindre privilège, afin de limiter les risques d'abus ou d'exploitation malveillante.

- **Chiffrement des données :** Il est indispensable d'utiliser des techniques de chiffrement pour sécuriser les données sensibles, aussi bien lors de leur transmission entre les dispositifs IoT et les serveurs que lors de leur stockage local. Ainsi, même en cas d'interception, les informations restent illisibles et protégées contre toute tentative d'exploitation non autorisée.
- **Gestion des accès** : Il est important d'établir des politiques de contrôle d'accès afin de déterminer précisément qui peut interagir avec les dispositifs IoT et accéder aux données qu'ils produisent. Cela inclut la gestion des identités, l'attribution de rôles selon les responsabilités des utilisateurs, ainsi que la révocation rapide des droits d'accès en cas de besoin ou de changement de statut.

1.9 Conclusion

En somme, si la santé connectée ouvre la voie à une médecine plus réactive, personnalisée et accessible, elle soulève également des enjeux cruciaux en matière de sécurité numérique. La protection des données médicales, la sécurisation des communications entre dispositifs et infrastructures de santé, ainsi que la fiabilité des systèmes d'authentification sont désormais au cœur des préoccupations. Face à ces défis, il devient essentiel de mettre en place des mécanismes robustes et adaptés aux contraintes du domaine médical. C'est dans le chapitre prochain de ce mémoire qu'on s'intéresse particulièrement aux protocoles d'authentification, et notamment au rôle stratégique du protocole EAP-AKA′ dans les réseaux 5G, qui constituent une brique fondamentale pour garantir la sécurité des dispositifs médicaux connectés et la confiance dans les systèmes de santé de demain.

Chapitre 2

Le protocole d'authentification EAP-AKA'

2.1 Introduction

Le protocole EAP-AKA' (Extensible Authentication Protocol – Authentication and Key Agreement prime) est une méthode d'authentification largement utilisée dans les réseaux mobiles 3G, 4G et 5G. Il repose sur le mécanisme d'authentification et d'accord de clés (AKA) défini pour les réseaux mobiles de troisième génération[15].

Conçu pour exploiter les cartes SIM (USIM) comme ancrage de confiance, EAP-AKA′ permet une authentification mutuelle entre l'utilisateur et le réseau, tout en générant des clés de session cryptographiques pour sécuriser les communications.

En raison de sa compatibilité structurelle avec les architectures médicales préexistantes et de son aptitude à opérer dans des environnements fortement contraints en ressources, le protocole EAP-AKA' s'impose comme un mécanisme d'authentification de prédilection pour les dispositifs médicaux connectés, où la confidentialité et l'intégrité des données de santé revêtent une importance capitale.

L'évolution vers EAP-AKA′ a introduit des améliorations en termes de protection de la vie privée et de résistance aux attaques, notamment en liant les clés dérivées au nom du réseau d'accès.

De nombreux opérateurs et acteurs technologiques ont adopté ce protocole comme élément fondamental de l'infrastructure d'authentification mobile, en particulier pour assurer la sécurité et l'intégrité des communications dans les réseaux mobiles.

2.2 Définition de protocole d'authentification

Un protocole d'authentification est un ensemble de règles et de procédures permettant de vérifier l'identité d'un utilisateur ou d'un appareil cherchant à accéder à un système, un réseau ou une ressource numérique. Il s'agit d'une étape fondamentale pour garantir la sécurité des systèmes informatiques, en empêchant les accès non autorisés et en protégeant les données sensibles[27].

Le protocole impose un langage et des étapes précises que chaque entité (utilisateur, serveur, application) doit respecter lors de la communication, afin d'assurer que l'identité présentée est bien celle de la personne ou de l'appareil qui tente de se connecter[28].

2.3 Le protocole EAP(Extensible Authentification Protocol)

Le protocole EAP (Extensible Authentication Protocol) est une norme définie par l'IETF (Internet Engineering Task Force) dans le document RFC 3748. Il fournit un cadre flexible permettant aux clients et aux serveurs d'authentification d'utiliser différentes méthodes d'authentification, existantes ou futures.

À l'origine, EAP a été conçu comme une extension du protocole PPP (Point-to-Point Protocol), un protocole de liaison de données utilisé pour établir une connexion directe entre deux nœuds réseau, notamment dans les connexions Internet par modem ou entre routeurs afin de permettre l'intégration de mécanismes d'authentification variés. Contrairement à des protocoles comme CHAP, qui utilisent une méthode fixe, EAP permet de négocier dynamiquement une méthode d'authentification au moment de l'établissement de la connexion.

Une fois cette méthode choisie, EAP facilite un échange de messages entre le client et le serveur, sous forme de requêtes et de réponses, afin de vérifier l'identité de l'utilisateur. Le type de méthode EAP sélectionné détermine alors la nature et la durée de cet échange.

Le protocole EAP spécifie quatre types de paquets pouvant être échangés entre le client et le serveur d'authentification[17] :

- **Requete :**émis par le serveur d'authentification, ce paquet demande au client une information d'identification ou une preuve d'identité, selon une méthode d'authentification précise par le serveur (mot de passe, certificat électronique, etc.).
- **Réponse :** envoyée par le client, elle contient l'information demandée. Si le client ne prend pas en charge la méthode proposée, il peut en informer le serveur et proposer d'autres méthodes. Le serveur peut alors en choisir une autre. Si aucune méthode n'est compatible, l'authentification échoue.
- **Succès :** le serveur envoie ce message pour confirmer que l'authentification a réussi. Le client est alors autorisé à accéder au réseau.
- **Échec :** envoyé par le serveur pour signaler que l'authentification a échoué.

Grâce à son architecture modulaire et évolutive, EAP s'adapte facilement à des environnements variés, notamment ceux reposant sur les technologies sans fil, les objets médicaux connectés (IoMT) et les infrastructures à forte exigence de sécurité.

2.4 Présentation de AKA

Le terme « Authentication and Key Agreement » (AKA) désigne le principal protocole d'authentification et d'établissement de clés utilisé par les réseaux mobiles 3GPP depuis la troisième génération (3G) et dans les générations suivantes.

Bien que des versions ultérieures aient ajouté de nouvelles fonctionnalités, le fonctionnement fondamental du protocole reste identique. Ce protocole repose sur un mécanisme de défi-réponse et utilise la cryptographie symétrique. Contrairement aux protocoles des réseaux GSM plus anciens, AKA propose des clés de plus grande longueur et assure une authentification mutuelle entre le terminal et le réseau. Il est exécuté au niveau de la USIM (Universal Subscriber Identity Module), une application sécurisée pouvant résider sur une carte SIM physique ou intégrée[18].

2.4.1 Fonctionnement du protocole AKA

AKA fonctionne de la manière suivante[18] :

— Le client commence le processus en envoyant son identité au serveur d'authentification.

— Le serveur vérifie si le client a les droits d'accès au réseau, puis génère les éléments cryptographiques nécessaires (clés, paramètres de défi).

— Le serveur envoie ensuite un message de challenge au client, contenant les informations nécessaires à l'authentification.

— À la réception, le client vérifie la validité des paramètres, notamment en comparant le nom du réseau attendu avec celui reçu. En cas d'incohérence, le processus est interrompu.

— Si toutes les vérifications sont correctes, le client effectue les calculs cryptographiques, génère une réponse d'authentification, et la renvoie au serveur.

— Le serveur compare la réponse reçue avec celle qu'il a lui-même calculée. Si elles correspondent, l'authentification est validée.

— Le serveur envoie alors un message de confirmation au client.

— Une session sécurisée peut alors débuter entre le client et le serveur.

2.5 Le protocole EAP-AKA′ :

Dans le cadre de l'intégration du protocole AKA à EAP, le traitement de l'authentification est pris en charge par le réseau domestique de l'opérateur. Ce dernier génère les vecteurs d'authentification nécessaires. Le serveur du réseau joue le rôle de serveur EAP, tandis que l'équipement de l'utilisateur, composé de la USIM et du téléphone mobile, agit en tant que client.[19]

2.5.1 Description de protocole EAP-AKA′ :

Le protocole EAP-AKA′ est une version améliorée d'EAP-AKA, développée pour renforcer la sécurité des procédures d'authentification dans les réseaux mobiles modernes. Il repose sur les mêmes principes que son prédécesseur, tout en introduisant des mécanismes plus robustes pour assurer la confidentialité et l'intégrité des échanges entre le terminal et le réseau.

L'une des principales évolutions apportées par EAP-AKA′ est l'introduction d'un mécanisme qui associe les clés de sécurité au nom du réseau d'accès, renforçant ainsi la protection contre certaines attaques, comme les redirections malveillantes qui peuvent exposer les utilisateurs à des sites dangereux. En plus de cette amélioration, le protocole intègre des fonctions cryptographiques mises à jour, en remplaçant SHA-1, une fonction de hachage qui produit une empreinte numérique unique par SHA-256, une version plus robuste offrant une meilleure résistance aux collisions et HMAC, un algorithme de vérification de l'intégrité et de l'authenticité des messages basé sur une clé secrète par HMAC-SHA-256, une version plus sécurisée.Ce protocole garantit

une protection accrue des données personnelles de l'utilisateur et une authentification mutuelle fiable entre le terminal et l'infrastructure réseau comme le montre le schéma suivant :

2.5.2 Fonctionnement générale de EAP-AKA′

Le protocole EAP-AKA′ repose sur une série d'échanges structurés entre le client (doté d'une USIM) et le serveur d'authentification du réseau. Chaque étape vise à assurer une authentification mutuelle fiable et à établir un canal sécurisé pour les communications futures.

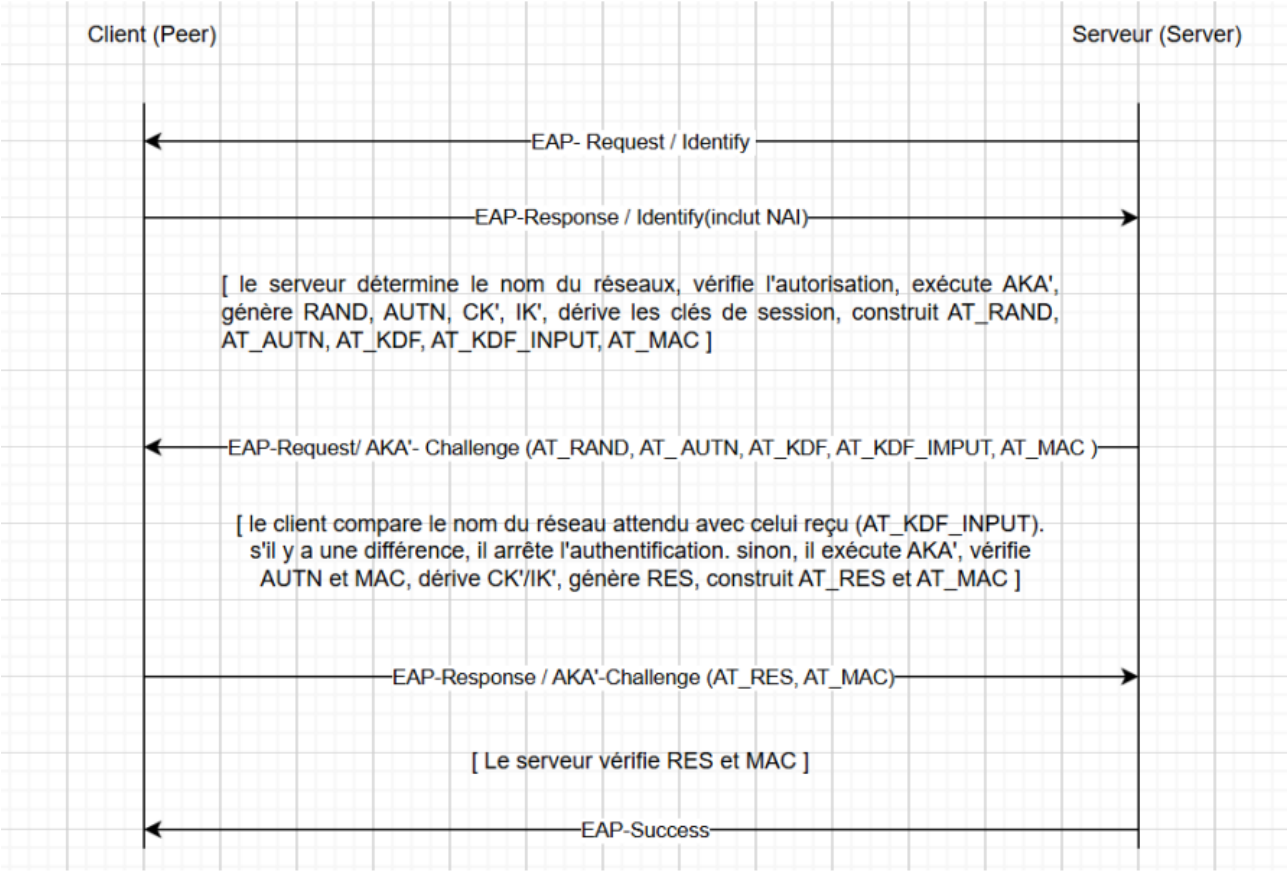


Figure 2.1 – Processus d'authentification EAP-AKA′

Ci-dessous sont décrites les principales étapes du déroulement de l'authentification via EAP-AKA′ :

- **EAP-Request/Identity :** Le serveur demande l'identité du client.
- **EAP-Response/Identity :** Le client envoie son identité, généralement sous la forme d'un NAI (Network Access Identifier), qui est un identifiant normalisé permettant de reconnaître de manière unique un utilisateur sur le réseau. Il se présente souvent sous la forme d'une adresse similaire à un email, comme utilisateur@domaine.com, et permet de diriger la requête d'authentification vers le bon opérateur ou domaine.
- **Exécution côté serveur :** Le serveur vérifie les droits d'accès, exécute AKA', dérive les clés, et construit les attributs nécessaires (AT_RAND, AT_AUTN, etc.).

- **EAP-Request/AKA′-Challenge :** Le serveur envoie le défi au client.

- **Traitement côté client :** Le client vérifie l'identité du réseau, exécute AKA, dérive les clés et renvoie la réponse (RES).
- **Vérification :** Le serveur compare RES et XRES. Si c'est correct, il envoie un message de succès.
- **EAP-Success :** L'authentification est validée et la session peut débuter.

2.5.3 Objectifs de protocole EAP-AKA′

Le protocole EAP-AKA' vise à renforcer la sécurité et la confidentialité dans les environnements de communication modernes, en particulier ceux propres à la 5G. Ses objectifs principaux peuvent être résumés comme suit[19] :

— Garantir la confidentialité des données sensibles afin d'empêcher toute divulgation d'informations critiques en cas d'écoute passive.

— Assurer l'intégrité des échanges pour éviter toute modification non autorisée des messages durant la communication.

— Fournir une authentification mutuelle fiable entre les parties impliquées dans l'authentification, en s'appuyant sur des mécanismes cryptographiques robustes.

— Prévenir les attaques par par rejeu grâce à des mécanismes de synchronisation et de hachage, assurant l'unicité des sessions.

— Protéger les clés de session en veillant à ce qu'elles ne soient jamais réutilisées, et en conservant leur secret tout au long de leur cycle de vie.

— Renforcer la vie privée des utilisateurs à travers des mesures d'anonymat, de non-traçabilité et de dissociation entre les sessions.

— Garantir l'indépendance des sessions pour empêcher toute forme de corrélation entre différentes communications. Offrir une résistance accrue aux attaques connues, telles que les attaques de désynchronisation, de surveillance ou de localisation.

— S'intégrer de manière sécurisée avec des protocoles de transport protégés afin d'assurer des communications fiables sur le long terme.

2.5.4 Avantages et Inconvénients protocole EAP-AKA′

Voici les avantages et inconvénients du protocole EAP-AKA′ [19][20][21] :

2.5.4.1 Avantages

- **Sécurité renforcée :** EAP-AKA′ utilise SHA-256 pour la dérivation des clés, offrant une sécurité supérieure à EAP-AKA qui repose sur SHA-1.

  La liaison des clés au nom du réseau d'accès réduit aussi l'impact d'une compromission locale.

- **Authentification mutuelle robuste :** Le protocole assure l'authentification mutuelle entre le terminal et le réseau, ce qui limite les risques d'attaques d'usurpation.
- **Protection contre la réutilisation des clés compromises :** Grâce à la liaison des clés au réseau d'accès, une clé compromise sur un réseau ne peut pas être réutilisée sur un autre, ce qui limite la portée des attaques.
- **Compatibilité avec les infrastructures existantes :** EAP-AKA′ reste compatible avec les infrastructures EAP-AKA, facilitant la migration vers la 5G.[20][21]
- **Utilisation dans le Wi-Fi et la 5G :** Il est utilisé pour l'authentification sur les réseaux Wifi et les réseaux 5G, offrant une expérience d'authentification unifiée.

2.5.4.2 Inconvénients

- **Complexité accrue :** L'ajout de la liaison des clés au réseau d'accès et l'utilisation de SHA-256 augmentent la complexité du protocole par rapport à EAP-AKA.
- **Surcharge potentielle de gestion des clés :** La nécessité de gérer des clés spécifiques à chaque réseau d'accès peut entraîner une surcharge administrative et technique dans certains environnements.
- **Support variable selon les équipements :** Bien que largement pris en charge, certains équipements anciens peuvent ne pas être compatibles avec EAP-AKA' ou ses extensions avancées.
- **Performance légèrement impactée :** L'utilisation de SHA-256 et des mécanismes de sécurité avancés peut entraîner une légère augmentation de la consommation de ressources par rapport à EAP-AKA, bien que cela reste généralement négligeable dans les infrastructures modernes.

2.6 Analyse de sécurité

Cette section présente une évaluation des points forts de sécurité offertes parEAP-AKA′, ainsi que ses Limitations et vulnérabilités potentielles[19][30].

2.6.1 Points forts

- **Authentification mutuelle :** Le protocole permet de vérifier que chaque partie est bien celle qu'elle prétend être. L'utilisateur est authentifié par le réseau, et réciproquement, le réseau est validé par l'utilisateur grâce à des échanges d'informations sécurisées. Cette authentification mutuelle est essentielle pour établir une relation de confiance entre les parties.
- **Sécurité des clés :** Les clés de session générées sont spécifiques à chaque session et incluent des paramètres uniques qui empêchent leur réutilisation. Cela garantit que les communications sont protégées contre les attaques utilisant des clés compromises ou réutilisées.

- **Confidentialité et protection de la vie privée :** L'identité de l'utilisateur est protégée tout au long du processus, notamment grâce à des mécanismes qui cachent ou anonymisent ces informations sensibles. Le protocole assure que ces données confidentielles ne sont pas exposées lors des échanges.
- **Résilience aux attaques :** Le protocole est conçu pour empêcher des attaques où un tiers tenterait de se faire passer pour une des parties ou de partager une clé secrète à l'insu des autres. Même si une clé de session passée est compromise, la confidentialité des sessions en cours est maintenue. Cependant, la protection contre la compromission à long terme (forward secrecy) n'est pas garantie, ce qui signifie qu'une clé compromise pourrait exposer des communications passées ou futures

2.6.2 Limitations et vulnérabilités potentielles du protocole EAP-AKA′

- **Gestion des clés faible ou compromise :**

Même si EAP-AKA′ repose sur des mécanismes cryptographiques robustes, une mauvaise gestion des clés côté opérateur, serveur ou dispositif peut introduire des vulnérabilités. Parmi les scénarios critiques :

— Fuite ou réutilisation de clés : Si des clés issues de sessions précédentes sont compromises (par exemple à cause d'une mauvaise suppression ou d'une fuite mémoire), un attaquant peut tenter une attaque par récupération de clé.

— Faiblesses dans le stockage local : Si le dispositif médical ou la passerelle locale (comme un smartphone) ne stocke pas correctement les secrets (ex. K, CK, IK), un attaquant ayant un accès physique ou logiciel pourrait les extraire.

— Attaques liées aux KDF (Key Derivation Function) : Bien que EAP-AKA′ utilise des KDF basées sur SHA-256, une mauvaise implémentation peut réduire leur efficacité.

- **Accords faibles entre les entités :**

La robustesse du protocole repose sur un bon alignement (synchronisation) entre le réseau, le client, et les serveurs d'authentification. Cependant :

— Desynchronisation : Un attaquant actif peut injecter de faux messages ou provoquer un décalage dans les séquences SQN, entraînant une désynchronisation entre l'UE et le réseau. Cela pourrait forcer l'échec de l'authentification, entraînant un déni de service (DoS).

— Absence de confirmation explicite : Même si EAP-AKA′ améliore l'authentification mutuelle, certaines implémentations peuvent ne pas vérifier explicitement tous les champs d'un message d'accord, ouvrant la voie à des attaques de downgrade ou de falsification.

— Manque de robustesse en cas de perte de connectivité : Dans certains environnements critiques où la connexion réseau peut être intermittente ou instable, une perte de synchronisation entre les entités peut dégrader la qualité de service, voire entraîner des risques pour la sécurité des opérations.

2.6.3 Mesures d'atténuation proposées :

- **Renforcement de la gestion des clés :** Il est essentiel d'assurer une gestion rigoureuse des clés cryptographiques afin de prévenir toute compromission. Cela inclut notamment l'implémentation de techniques telles que la rotation régulière des clés et le stockage sécurisé des secrets cryptographiques.
- **Amélioration des mécanismes de surveillance :** Des systèmes de détection et de réponse robustes doivent être déployés pour identifier rapidement les activités suspectes, telles que les tentatives d'authentification non autorisées ou les comportements anormaux lors des échanges de données.
- **Mises à jour régulières :** Le protocole doit être constamment maintenu à jour par l'application systématique des correctifs de sécurité et des mises à jour logicielles. Ceci permet de corriger les vulnérabilités détectées et de renforcer la résistance du système face aux nouvelles menaces.

2.7 Déploiement de protocole EAP-AKA′ dans l'authentification des dispositifs de santé connecté

Le protocole EAP-AKA′ (Extensible Authentication Protocol – Authentication and Key Agreement prime) joue un rôle central dans la sécurisation des dispositifs médicaux connectés (IoMT), en particulier dans le contexte des réseaux 5G. Ces dispositifs sont au cœur de la télésurveillance et de la télémédecine, domaines où les transferts de données sur réseau sont fréquents et portent sur des informations de santé hautement sensibles, telles que les constantes vitales, les diagnostics ou les historiques médicaux. Toute compromission de ces données pourrait avoir des conséquences graves sur la vie privée des patients. Dès lors, une authentification forte et une dérivation sécurisée des clés cryptographiques sont indispensables pour s'assurer que seuls les acteurs autorisés puissent accéder aux dispositifs, interagir avec les capteurs ou transmettre des données vers les plateformes de soins. EAP-AKA' répond à ces exigences en garantissant la confidentialité, l'intégrité et l'authenticité des communications, tout en réduisant les risques liés à l'usurpation d'identité, à l'interception ou à la manipulation des données. Il constitue ainsi un socle de confiance essentiel pour les environnements médicaux connectés, où la sécurité des échanges conditionne directement la sécurité des patients et la continuité des soins à distance.

2.7.1 Attaques atténuées par EAP-AKA′ dans les dispositifs médicaux connectés

Le protocole EAP-AKA' (Extensible Authentication Protocol – Authentication and Key Agreement prime) est conçu pour fournir une authentification forte, la dérivation de clés sécurisées et la protection de la confidentialité dans des environnements tels que les réseaux 5G, y

compris pour les dispositifs IoT médicaux (IoMT). Voici les attaques qui peuvent être limitées ou atténuées par l'utilisation d'EAP-AKA′[19] [22] :

- **Usurpation d'identité (Spoofing) :**

L'attaquant se fait passer pour un dispositif ou un utilisateur légitime afin d'accéder à des ressources, intercepter des données sensibles ou perturber le système.

EAP-AKA′ repose sur une authentification mutuelle forte entre le dispositif (UE) et le réseau. Cela permet de s'assurer que seules les entités autorisées peuvent participer à la communication, empêchant un attaquant de se faire passer pour un dispositif ou un serveur.

- **Attaque par rejeu (Replay Attack) :**

Un attaquant capture des messages d'authentification valides puis les retransmet plus tard pour tromper le système et se faire authentifier illicitement.

Le protocole utilise un numéro de séquence (SQN) et un mécanisme de synchronisation pour vérifier la fraîcheur des messages. Cela permet de rejeter les messages déjà vus et rend les attaques par rejeu inefficaces.

- **Attaque de désynchronisation :**

Un attaquant tente de perturber le mécanisme d'authentification en injectant des messages falsifiés, dans le but de rompre la coordination entre le dispositif et le système d'authentification, ce qui peut entraîner un blocage du service ou un échec de connexion.

Le protocole EAP-AKA′ améliore les mécanismes de cohérence et de vérification au sein du processus d'authentification, rendant plus difficile la manipulation des échanges pour provoquer une désynchronisation. Cela renforce la résilience des dispositifs contre les tentatives de perturbation visant à les rendre inaccessibles.

- **Attaque de l'homme du milieu (Man-in-the-Middle – MitM) :**

L'attaquant intercepte, observe ou modifie les échanges entre le dispositif médical et le serveur distant sans que celles-ci ne s'en aperçoivent.

Le protocole génère des clés de session dérivées de secrets partagés et applique des mécanismes de confirmation implicite des clés. Cela protège l'échange contre les interceptions ou altérations, rendant les attaques MitM inefficaces.

- **Surveillance passive et atteinte à la vie privée :**

Un attaquant écoute les communications réseau pour collecter des informations sensibles (identifiants, données médicales, comportements).

EAP-AKA′ cache les identifiants permanents comme le SUPI (identifiant d'abonné) en le remplaçant par le SUCI (identifiant chiffré). Il garantit également la confidentialité des messages échangés, protégeant l'anonymat et la traçabilité de l'utilisateur.

- **Vol de clé ou génération de clés faibles :**

Un attaquant tente de déduire ou de voler les clés utilisées pour sécuriser les échanges, par exemple à partir de clés partagées faibles ou mal dérivées dans le but d'accéder aux informations médicales.

Le protocole repose sur des fonctions de dérivation de clés (KDF) robustes basées sur SHA-256, considéré comme une fonction pseudo-aléatoire sécurisée. Cela rend impraticable la déduction des clés ou l'utilisation de techniques de force brute.

2.7.2 Apports du déploiement de EAP-AKA′ dans la santé connectée

- **Sécurité native à la 5G sans dépendance à des solutions tierces :** EAP-AKA′ est intégré nativement dans l'architecture 5G, offrant une authentification mutuelle forte sans nécessiter de logiciels supplémentaires. Cela simplifie le déploiement et renforce la sécurité des dispositifs médicaux connectés.
- **Réduction des risques de vol de données ou d'intrusion :** Grâce à la dérivation de clés robustes et à la protection contre les attaques par rejeu, EAP-AKA′ limite les risques d'accès non autorisé aux données sensibles des patients.
- **Meilleure gestion de la confidentialité (SUPI/SUCI) :** Le protocole masque l'identité permanente de l'utilisateur (SUPI) en la remplaçant par une identité chiffrée (SUCI), renforçant ainsi la protection de la vie privée des patients.
- **Interopérabilité avec les réseaux cellulaires existants :** EAP-AKA′ est compatible avec les infrastructures 4G et 5G, facilitant la transition et l'intégration dans les systèmes de santé existants.

2.8 Conclusion

Dans ce chapitre, nous avons tout d'abord présenté le protocole EAP-AKA', en exposant ses principes fondamentaux ainsi que ses principaux avantages et inconvénients. Cette introduction a permis de mieux comprendre les enjeux liés à son utilisation dans les réseaux modernes, notamment les réseaux 5G. Nous avons ensuite effectué une analyse approfondie de la sécurité du protocole, en mettant en lumière ses points forts, mais aussi ses limites et vulnérabilités potentielles. Afin de pallier ces faiblesses, plusieurs mesures d'atténuation ont été proposées, renforçant ainsi la robustesse du protocole face aux menaces. Enfin, nous avons exploré le déploiement concret de EAP-AKA' dans le domaine de la santé connectée, en détaillant les attaques qu'il permet d'atténuer et en soulignant les apports majeurs qu'il offre pour sécuriser les dispositifs médicaux connectés. Cette approche globale montre que, malgré certaines limites, EAP-AKA' reste un protocole pertinent et adapté pour répondre aux besoins de sécurité spécifiques à la santé connectée. Le chapitre suivant approfondira ces aspects à travers une étude de cas pratique, illustrant son implémentation dans un réseau 5G dédié aux dispositifs médicaux.

Chapitre 3

Etude de cas : Authentification sécurisée en home monitoring via EAP-AKA′ en 5G

3.1 Introduction

Avec l'évolution des technologies de communication et l'avènement des réseaux mobiles de nouvelle génération, la santé connectée s'est imposée comme un pilier fondamental dans la transformation numérique du secteur médical. Parmi ses composantes les plus critiques figure la télésurveillance médicale à domicile (home monitoring), qui permet le suivi continu de patients porteurs de dispositifs médicaux implantables tels que des pacemakers, défibrillateurs, ou capteurs physiologiques. Ces dispositifs, une fois implantés, sont souvent associés à un terminal de transmission situé au domicile du patient. Ce terminal assure la collecte des données cliniques, leur transmission automatique via des réseaux mobiles (3G, 4G, 5G), et leur envoi vers une plateforme sécurisée consultée par les professionnels de santé. Ce modèle réduit les visites hospitalières inutiles, permet des diagnostics plus précoces, et améliore la qualité de vie des patients. Cependant, cette architecture soulève d'importants enjeux de sécurité. Les données médicales transmises sont hautement sensibles, et toute faille dans le processus d'authentification ou dans la confidentialité des échanges pourrait exposer le patient à des risques graves (usurpation d'identité, interception des données, falsification des signaux, etc.). En particulier, l'utilisation de réseaux mobiles publics pour transporter ces informations introduit de nouvelles vulnérabilités.

3.2 Contexte de notre travail

Dans l'article[19], les auteurs formalisent et évaluent le protocole EAP-AKA′ dans le cadre de la sécurité d'accès aux réseaux 5G. Leur étude propose une modélisation rigoureuse du protocole à l'aide de méthodes formelles, permettant de vérifier ses propriétés de sécurité telles que la confidentialité, l'authentification mutuelle et la résistance aux attaques de rejeu. À travers l'analyse avec des outils de vérification automatisés, les auteurs mettent en évidence certaines vulnérabilités potentielles ainsi que les conditions nécessaires pour garantir un niveau de sécurité élevé dans des scénarios d'accès réseau sensibles, notamment pour les dispositifs mobiles ou connectés. Ces travail souligne l'importance d'une validation formelle pour renforcer la confiance dans les mécanismes de sécurité des réseaux 5G. Dans cette partie, nous allons étudié l'application du protocole EAP-AKA′ dans un contexte de santé connectée, en particulier dans les systèmes de télésurveillance médicale (home monitoring) via les réseaux 5G. Nous allons analysé ces vulnérabilités face aux attaques par rejeu. Enfin, nous allons proposé des améliorations du protocole EAP-AKA′ afin de renforcer sa robustesse face à ces menaces spécifiques.

3.3 Fonctionnement général d'un système de Home Monitoring médical

Pour assurer un suivi médical continu en dehors des établissements de soins, les systèmes de télésurveillance médicale à domicile se basent sur une architecture technique permettant

la collecte automatique des données de santé. Ces données, générées par des dispositifs médicaux portés ou implantés chez le patient, sont transmises à distance à l'équipe soignante via une passerelle de communication et une plateforme sécurisée. Cette section présente les différents composants de ce système et décrit le rôle de chacun dans le processus global de télésurveillance[9].

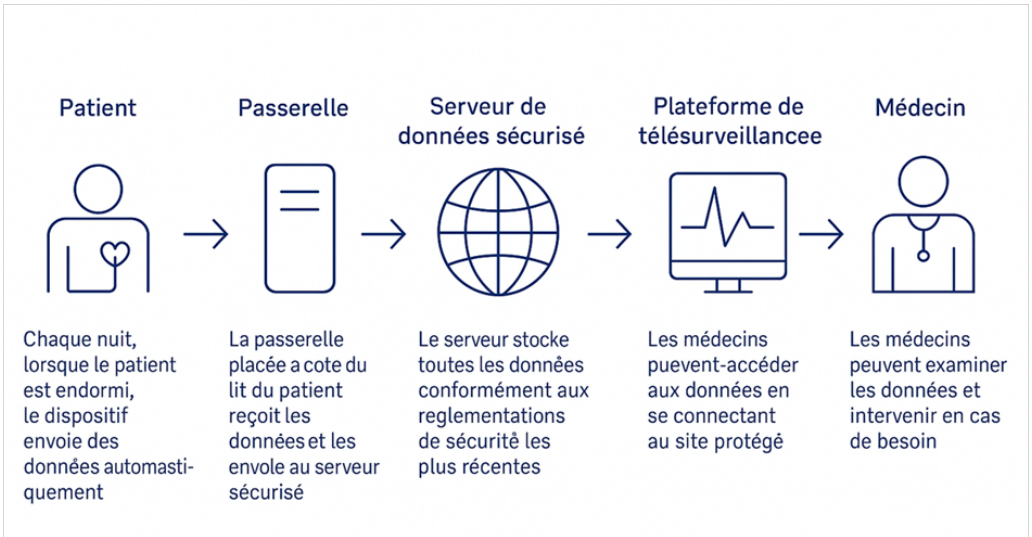


Figure 3.1 – Architecture de home monitoring[9].

- **Patient :** Porte un dispositif médical connecté (comme un capteur ou une montre) qui mesure en continu ses paramètres vitaux tels que le rythme cardiaque ou la tension artérielle. Ces données sont transmises automatiquement, généralement via Bluetooth ou radio (RF), à une passerelle locale.
- **Passerelle :** Peut être un smartphone ou un petit boîtier dédié équipé d'une carte SIM, se charge ensuite d'envoyer les informations vers les serveurs médicaux à distance en utilisant une connexion 4G/5G ou Wi-Fi.
- **Serveur de données sécurisé :** Le serveur de la plateforme médicale qui centralise, enregistre et sécurise les données de santé tout en assurant leur confidentialité et leur protection contre tout accès non autorisé
- **Centre de télésurveillance plateforme médicale :** Les professionnels de santé autorisés peuvent accéder à ces données en temps réel ou en différé à travers une interface sécurisée (portail web, application médicale dédiée).
- **Médecin :** Il consulte les données du patient à distance, reçoit des alertes si des anomalies sont détectées, et peut adapter le traitement ou intervenir rapidement si nécessaire.

3.3.1 Enjeux de l'authentification de la passerelle de télésurveillance

Dans un tel environnement distribué, où les données transitent via des réseaux publics, la sécurité est un enjeu central. L'usage de protocoles d'authentification forte comme EAP-AKA'

permet de garantir l'identité de la passerelle de télésurveillance, la confidentialité des échanges, et la protection contre les attaques de type usurpation,interception, ou rejeu. Ce protocole repose sur une carte USIM sécurisée, une clé partagée et une vérification mutuelle entre le terminal et l'infrastructure réseau

Parmi les principaux enjeux liés à l'authentification, on retrouve :

- **Vérification de l'identité de la passerelle :** Il est essentiel que le réseau (ou la plateforme médicale) s'assure que la passerelle est bien autorisée à transmettre des données de santé. Sans une authentification forte, un appareil frauduleux pourrait usurper l'identité d'une passerelle légitime et injecter de fausses données médicales.
- **Garantie d'origine des données médicales :** L'authentification de la passerelle garantit que les données cliniques reçues proviennent bien du bon patient via le bon dispositif. Cela empêche les erreurs médicales dues à une association incorrecte entre les données et le patient.
- **Protection contre les attaques de type "man-in-the-middle" ou usurpation :** L'authentification de la passerelle protège contre les attaques comme l'interception, la falsification ou la réutilisation de messages. Sans cette vérification, une passerelle non sécurisée peut devenir une cible facile pour des attaques de type "man-in-the-middle" ou servir de point d'entrée à un attaquant, compromettant ainsi la confidentialité et la fiabilité des données médicales.
- **Établissement de canaux sécurisés (clés de session) :** L'authentification, avec des protocoles comme EAP-AKA′, permet d'établir des clés de session entre la passerelle et le réseau. Ces clés sont utilisées pour chiffrer les échanges, garantissant ainsi la confidentialité, l'intégrité des données et la preuve que les messages ont bien été envoyés par les bons acteurs.
- **Fiabilité et continuité des soins** : Une authentification fiable est essentielle pour garantir la continuité des soins. Sans elle, la plateforme médicale risque de rejeter des connexions légitimes ou, au contraire, d'accepter des connexions malveillantes. Cela peut entraîner des interruptions dans le suivi du patient, des alertes manquées ou des retards dans les traitements.

3.4 Application du protocole EAP-AKA' pour l'authentification de la passerelle en environnement 5G

3.4.1 Entités principales de l'authentification EAP-AKa' dans un système de télésurveillance médicale (home monitoring) dans un réseau 5G

L'authentification sécurisée entre la passerelle et l'infrastructure médicale est essentielle. Le protocole EAP-AKA', conçu pour les réseaux 5G, constitue une solution robuste pour assurer

une authentification mutuelle, la confidentialité, et l'intégrité des communications. Ce protocole permet à l'infrastructure médicale (réseau de santé) de vérifier l'identité de la passerelle de télésurveillance utilisé par le patient, tout en lui permettant de s'assurer qu'il communique bien avec un réseau médical légitime et permet l'établissement de clés de session pour sécuriser la transmission des données médicales sensibles.. Cela garantit une connexion sécurisée, même lorsqu'elle s'effectue sur un canal sans fil exposé, comme dans un environnement de home monitoring.

Quatre entités principales participent au processus d'authentification :

- **UE (User Equipment) – Passerelle mobile du patient :** C'est l'appareil (boîtier ou smartphone) qui envoie automatiquement les données médicales collectées vers le réseau. Il contient une carte SIM sécurisée et initie le processus d'authentification avec le réseau.
- **SEAF(Security Anchor Function) – Point d'accès réseau :** Il fait le lien entre la passerelle et le réseau. Il transmet les messages d'authentification et participe à l'établissement des clés de sécurité.
- **AUSF (Authentication Server Function) – Serveur d'authentification :** Situé dans le cœur du réseau, il traite les demandes d'authentification et décide si la passerelle est autorisée ou non à accéder au service.
- **ARPF/UDM – Gestionnaire des identifiants :** C'est l'entité qui génère les données nécessaires à l'authentification (vecteurs, clés, identifiants) et stocke les informations liées à l'abonnement du patient.

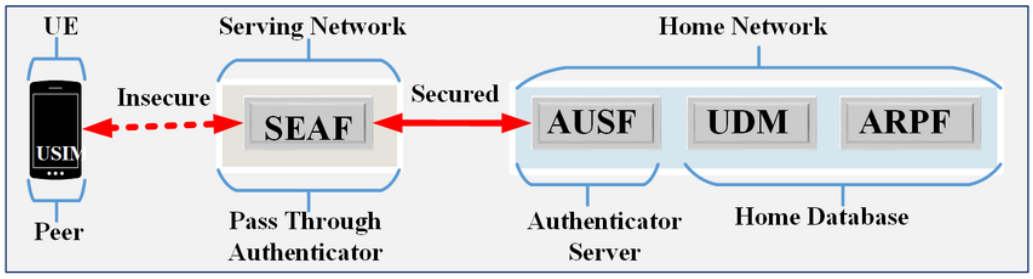


Figure 3.2 – Les entités d'authentification EAP dans les réseaux 5G[19].

3.4.2 Processus d'authentification

Le processus du protocole EAP-AKA′ est divisé en trois étapes principales, reposant sur l'utilisation de vecteurs d'authentification (AV) et l'échange de messages entre les différentes entités du réseau.

3.4.2.1 Étape 1 : Initialisation et négociation de la méthode d'authentification :

Lorsque la passerelle, connectée au dispositif implanté, détecte une connexion réseau mobile (ex. après collecte de données cardiaques), il déclenche une session sécurisée avec la plateforme de télésurveillance médicale, comme illustrée sur la figure suivante :

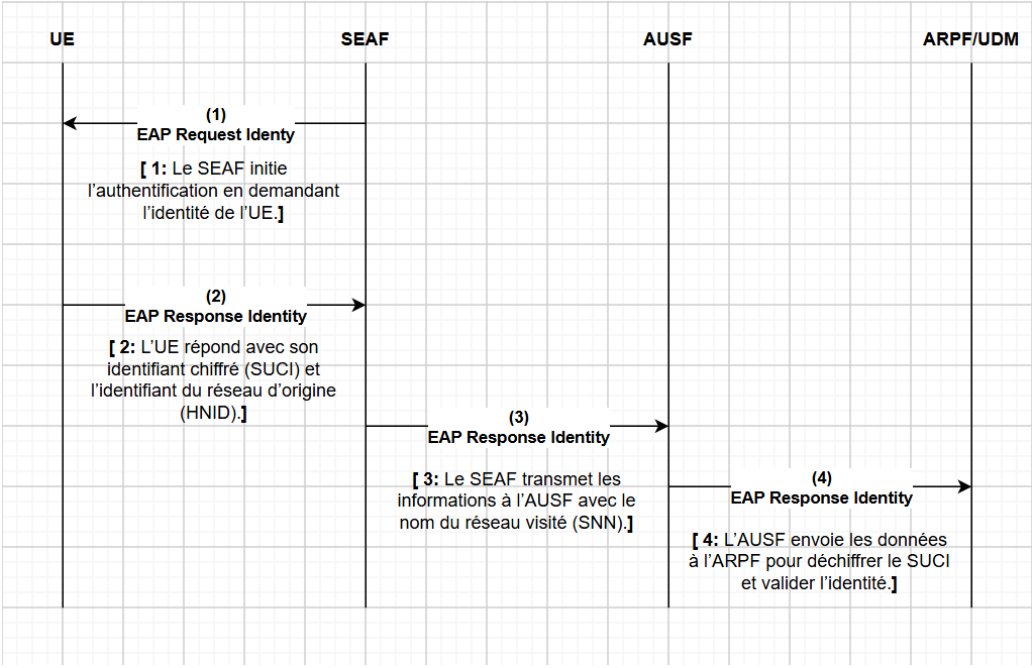


Figure 3.3 – Initialisation et négociation de la méthode d'authentification

- **Message 1 : (SEAF →UE) : EAP-Request/Identity**

  Le SEAF, situé dans l'infrastructure réseau du fournisseur de services de santé, initie une requête d'identité en demandant à la passerelle de lui fournir son identité.

- **Message 2 : (UE→ SEAF) : SUCI, HNID**

  Le dispositif répond en envoyant un identifiant chiffré appelé SUCI, dérivé de sa carte SIM (eSIM), ce qui garantit l'anonymat de l'utilisateur. Il transmet également l'identifiant du réseau domestique (HNID).

- **Message 3 : (SEAF → AUSF) : SUCI, SNN**

  Le SEAF transmet ces informations au serveur d'authentification AUSF, en incluant le SNN (Serving Network Name), c'est-à-dire le nom ou l'identifiant du réseau de desserte. Le réseau de desserte désigne ici le réseau mobile local auquel le dispositif est actuellement connecté. C'est le réseau qui prend en charge l'utilisateur pendant la session d'authentification et assure l'accès aux services de l'opérateur.

- **Message 4 : (AUSF → ARPF) : SUCI, SNN**

  L'AUSF transmet ensuite le SUCI et le SNN au serveur ARPF (ou UDM dans le cœur de réseau 5G), qui déchiffre le SUCI pour retrouver l'identité réelle de l'utilisateur (SUPI). Ce serveur valide ensuite l'authentification initiale.

3.4.2.2 Étape 2 : Déroulement du protocole EAP-AKA'

Une fois la méthode EAP-AKA' sélectionnée, un échange défi-réponse cryptographique est engagé, cette figure si dessus illustre les différents messages échangées.

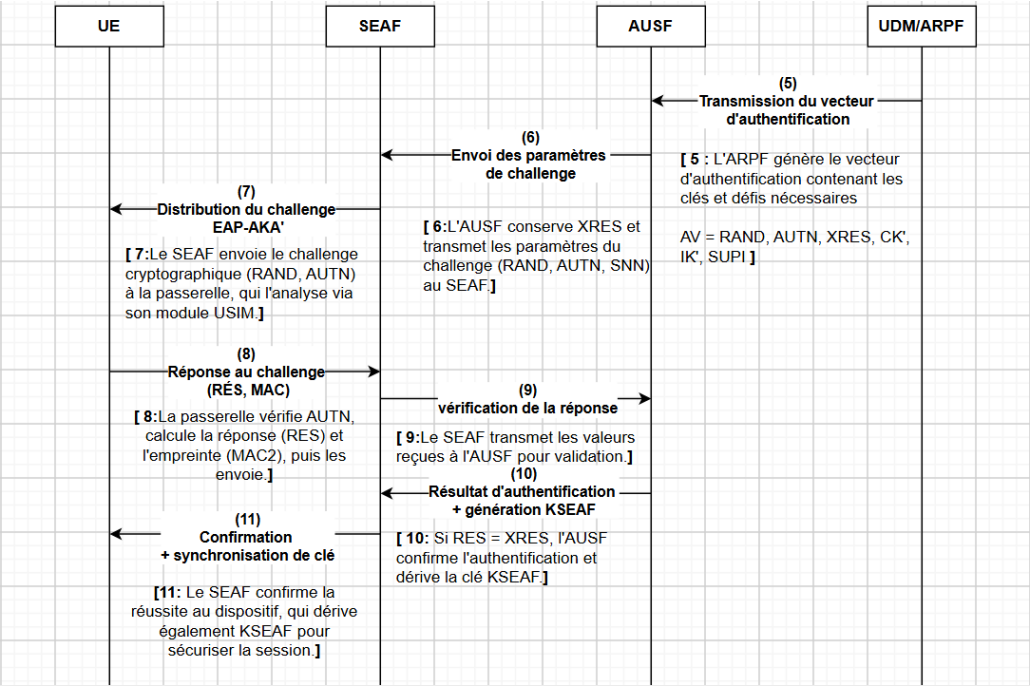


Figure 3.4 – Déroulement du protocole EAP-AKA'

- **Message 5 : (ARPF → AUSF) : AV = RAND, AUTN, XRES, CK', IK', SUPI**

  L'ARPF génère un vecteur d'authentification contenant les clés et défis nécessaires :

  — RAND(Random Challenge) : C'est une valeur aléatoire générée par le serveur pour chaque tentative d'authentification.Elle rend chaque authentification unique.

  — AUTN (Authentication Token) : C'est un jeton d'authentification qui contient : Le numéro de séquence (SQN), Le code d'authentification de message (MAC), D'autres éléments cryptographiques.

  — XRES (Expected Response) : la réponse que l'UE devra produire pour réussir l'authentification.

  — CK', IK'(Cipher Key', Integrity Key') : les clés de chiffrement et d'intégrité nécessaires à la sécurisation des échanges.

  — SUPI : l'identité réelle de l'utilisateur.

- **Message 6 : (AUSF → SEAF) : RAND, AUTN, SNN**

  L'AUSF conserve la réponse attendue (XRES) pour la comparaison future, et transmet les autres éléments au SEAF.

- **Message 7 : (SEAF →UE) : RAND, AUTN, ngKSI, ABBA**

  La passerelle reçoit le défi et le traite à l'aide de son module sécurisé USIM où :

  — gKSI(Next Generation Key Set Identifier) : identifiant de la clé cryptographique à utiliser.

  — ABBA(Additional Parameters for Binding Authentication) : Ce sont des paramètres additionnels de sécurité utilisés pour renforcer l'authentification et l'intégrité des

messages. Parfois, ils permettent aussi des ajustements ou extensions spécifiques selon l'opérateur.

- **Message 8 : (UE→ SEAF) : RES, MAC2**

La passerelle vérifie la validité de l'AUTN, Cette vérification permet de s'assurer que le challenge provient bien d'un serveur légitime. calcule la réponse(RES), Cette réponse est unique pour ce challenge et prouve que l'UE détient bien les clés correctes et calcule un code d'intégrité MAC2 puis lest ransmet.

- **Message 9 : (SEAF → AUSF) : RES, MAC2**
  Le SEAF transmet les réponses au serveur d'authentification.
- **Message 10 : (AUSF → SEAF) : EAP-Success, K_{SEAF}, SUPI**
  Si RES = XRES, l'authentification est validée et la clé K_{SEAF} est générée.
- **Message 11 : (SEAF →UE) : EAP-Success, ngKSI, ABBA**
  La passerelle reçoit la confirmation et dérive également la mêmeK_{SEAF}, établissant ainsi un canal sécurisé avec les serveurs de la plateforme de télésurveillance médicale.

3.4.2.3 Étape 3 : Ré-synchronisation

Dans un système de surveillance médicale à distance, il peut arriver que le compteur de séquence (SQN) entre la passerelle mobile du patient (UE) et le réseau de l'opérateur (HN) ne soit plus synchronisé. Cela peut se produire, par exemple, après une période prolongée sans connexion. Lors de l'authentification, si la carte USIM du patient détecte une incohérence dans le message d'authentification (AUTN), elle peut signaler soit une erreur de message (MAC failure), soit une désynchronisation (Synch failure).Voici les différents messages décrits sur cette figure :

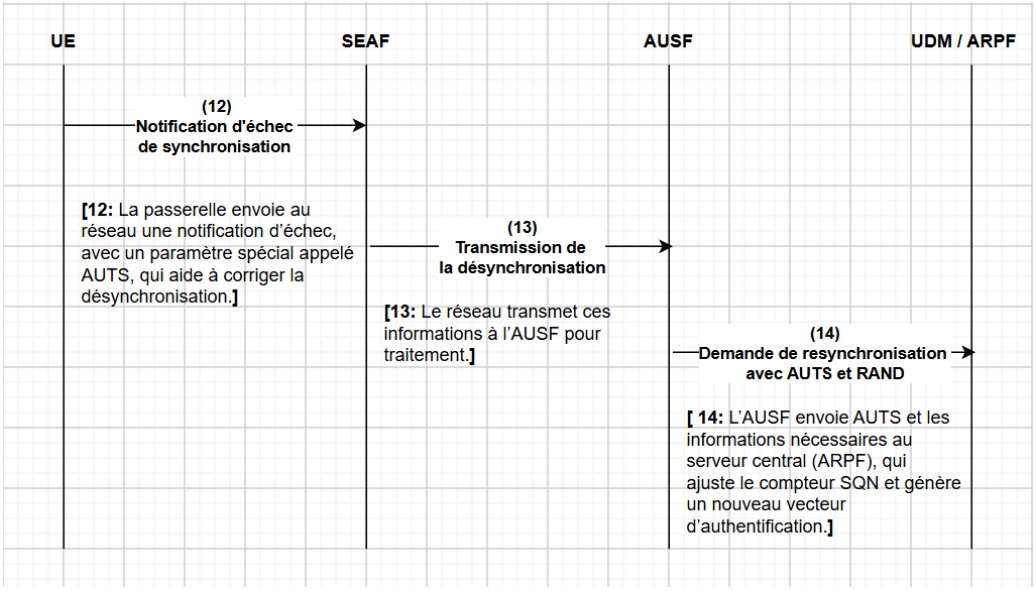


Figure 3.5 – Ré-synchronisation

- **Message 12 (UE → SEAF) : (Mac_failure, Synch_failure, AUTS)**
  La passerelle envoie au réseau une notification d'échec, avec un paramètre spécial appelé AUTS, qui aide à corriger la désynchronisation.
- **Message 13 (SEAF → AUSF) : (Synch_failure, AUTS)**
  Le réseau transmet ces informations à l'AUSF pour traitement.
- **Message 14 (AUSF → ARPF) : (Synch_failure, AUTS, Rand)**
  L'AUSF envoie AUTS et les informations nécessaires au serveur central (ARPF), qui ajuste le compteur SQN et génère un nouveau vecteur d'authentification.

Cette phase permet au système de se réajuster automatiquement, garantissant une authentification correcte et continue du dispositif médical connecté, sans intervention manuelle, assurant ainsi la fiabilité de la télésurveillance même en cas de coupure ou de décalage temporel.

3.4.3 Établissement d'un canal sécurisé après authentification

À l'issue des trois phases d'authentification du protocole EAP-AKA′, la passerelle médicale est reconnue comme un dispositif légitime par l'infrastructure réseau. Une clé de session sécurisée (K_{SEAF}) est alors dérivée à la fois du côté de la passerelle et du réseau, permettant la création d'un canal de communication chiffré. Ce canal garantit que toutes les données de santé échangées entre la passerelle et la plateforme médicale ne peuvent être ni interceptées ni altérées. Grâce à cette connexion sécurisée, les données collectées sont transmises en toute sécurité. Le médecin, via une interface sécurisée, peut alors consulter ces informations, recevoir des alertes en temps réel, et adapter les traitements selon l'évolution de l'état du patient.

3.5 Analyse des attaques par rejeu dans le protocole EAP-AKA′ utilisé en 5G

Il demeure vulnérable à certaines attaques de rejeu, susceptibles de compromettre la confidentialité des utilisateurs. Ci-dessous, une analyse détaillée de ce type d'attaque ainsi que de ses conséquences potentielles :

3.5.1 Fonctionnement de l'attaque de rejeu

L'attaque de rejeu est une technique utilisée par un attaquant pour intercepter des messages valides, puis les renvoyer ultérieurement afin de tromper le système d'authentification comme illustré sur la figure 3.6. Cette attaque ne nécessite pas forcément de modifier les messages, mais repose sur leur répétition dans un contexte différent. Dans le cadre des protocoles de sécurité comme EAP-AKA′, ce type d'attaque peut compromettre la fiabilité de l'authentification si aucune mesure de protection contre la réutilisation des messages n'est en place.

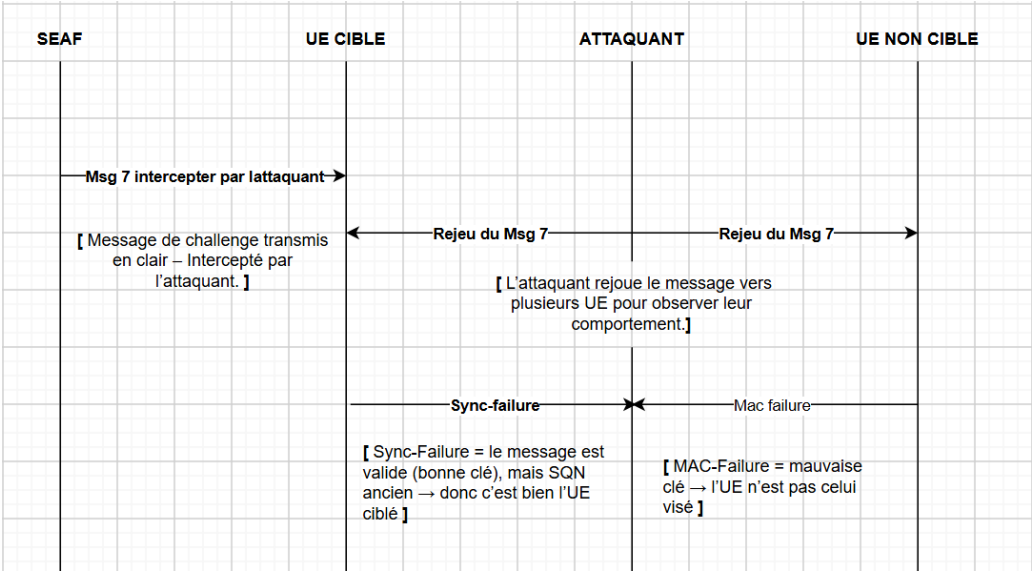


Figure 3.6 – Attaque de rejeu

3.5.1.1 Interception et rejeu du message de challenge

Un attaquant peut intercepter le message de challenge spécifiquement le message 7 transmis du SEAF vers l'UE, contenant les éléments (RAND, AUTN, ngKSI, ABBA) envoyé en clair. En enregistrant ce message, l'attaquant est ensuite en mesure de le rejouer ultérieurement. Ce rejeu permet notamment de vérifier si l'UE ciblé est présent dans une zone donnée, compromettant ainsi la confidentialité de sa localisation.

3.5.2 Différences de comportement entre l'UE ciblé et les autres dispositifs lors de la réception d'un message rejoué

- **Dispositifs non ciblés :** Lorsqu'un dispositif non ciblé reçoit un message rejoué, il tente de vérifier le code MAC en utilisant sa propre clé d'authentification. Cependant, puisque le MAC du message a été généré avec une clé partagée exclusivement entre le HN (Home Network) et l'UE ciblé, cette vérification échoue. En conséquence, le dispositif retourne une erreur de type MAC_failure.
- **Dispositifs ciblé :** Si le message rejoué parvient au véritable UE ciblé, la vérification du MAC réussit, car la clé utilisée pour générer le MAC correspond à celle détenue par l'UE. Toutefois, le message contient un ancien numéro de séquence (SQN). L'UE, ayant déjà avancé son propre SQN, détecte un décalage, ce qui entraîne une erreur de synchronisation signalée par une réponse 'sync_failure'.

3.5.3 Détection de la présence de l'UE ciblé :

Un attaquant peut exploiter les réponses à des messages rejoués pour déterminer si l'UE ciblé est présent dans une zone donnée. En surveillant les réponses, une erreur de type sync-failure indique que le message a été accepté par un dispositif qui possède la clé correcte, mais

que le numéro de séquence (SQN) est désynchronisé. Cela ne peut survenir que si le véritable UE ciblé est présent, révélant ainsi sa localisation. Ce comportement constitue une atteinte à la vie privée.

3.5.3.1 Étude des comportements de connexion de l'utilisateur ciblé (UE) :

En rejouant plusieurs fois le même message de challenge à différents moments, un attaquant peut recueillir des réponses du UE ciblé contenant des valeurs dérivées du numéro de séquence (SQN). Ces valeurs sont généralement masquées. En comparant les réponses obtenues à chaque tentative, l'attaquant peut observer les variations dans la valeur masquée du SQN. Cela lui permet d'estimer à quelle fréquence le SQN évolue, ce qui reflète la fréquence de connexion ou d'authentification du dispositif. Ainsi, sans jamais déchiffrer les données, l'attaquant peut déduire des informations sensibles sur le comportement d'utilisation du UE ciblé, comme sa régularité de connexion, ce qui constitue une atteinte à la vie privée.

3.6 Renforcement du Protocole EAP-AKA′ :

Pour faire face aux vulnérabilités identifiées dans le protocole EAP-AKA′, notamment celles liées aux attaques de rejeu, plusieurs contre-mesures peuvent être envisagées. Celles-ci visent à renforcer l'authentification, garantir l'intégrité des échanges et protéger la confidentialité des utilisateurs :

3.6.1 Chiffrement des Messages de Challenge :

Protection des éléments sensibles (RAND, AUTN) : En chiffrant les messages de challenge, on empêche leur réutilisation en cas d'interception.

Ce chiffrement peut être réalisé à l'aide de clés de session temporaires ou de techniques de chiffrement symétrique, assurant ainsi la confidentialité des informations même sur un canal exposé.

3.6.2 Ajout d'un Code MAC aux Messages Sensibles :

Intégrité des échanges : Chaque message échangé entre l'UE (dispositif utilisateur) et le SEAF doit inclure un Message Authentication Code (MAC) calculé à partir du contenu du message et d'une clé partagée.

Vérification systématique : À la réception, chaque entité vérifie la validité du MAC. Si celui-ci ne correspond pas, le message est rejeté, ce qui empêche toute falsification ou altération des messages.

3.6.3 Utilisation de Timestamps (horodatage) :

Vérification de la fraîcheur des messages : L'inclusion d'un timestamp dans chaque message de challenge permet à l'UE de vérifier que le message est récent.

Si le timestamp est trop ancien ou hors d'une plage temporelle acceptable, le message est ignoré, empêchant ainsi la réutilisation de messages obsolètes.

3.6.4 Amélioration de la Synchronisation :

Mécanisme de resynchronisation renforcé : Le processus de réinitialisation du compteur de séquence (SQN) doit être sécurisé pour ne pas révéler d'informations sensibles. Cela peut passer par l'utilisation de nonces temporaires ou de mécanismes de masquage avancés pour dissimuler la véritable valeur du SQN.

Timestamps complémentaires : Leur intégration permet également d'éviter le traitement de messages anciens, contribuant à la sécurisation de la synchronisation.

3.6.5 Détection et Réaction face aux Attaques de Rejeu :

Surveillance des anomalies : Le réseau peut surveiller les occurrences de messages de type sync-failure. Une augmentation anormale peut indiquer une attaque de rejeu en cours.

Limitation des tentatives : Imposer une limite au nombre de tentatives de resynchronisation dans un intervalle donné permet de prévenir les attaques par force brute ou essais répétés.

3.6.6 Authentification Multi-Facteur (MFA) :

Renforcement de l'identité : Ajouter un second facteur d'authentification (code de confirmation via SMS, e-mail sécurisé, ou biométrie) renforce la sécurité. Cette méthode permet d'introduire un facteur non rejouable, rendant les attaques par rejeu bien plus difficiles, voire inopérantes.

L'intégration de ces contre-mesures dans le protocole EAP-AKA′ contribuerait significativement à en réduire la surface d'attaque. En protégeant les messages critiques, en assurant l'intégrité des échanges et en détectant les comportements suspects, les réseaux 5G peuvent offrir une authentification robuste, respectueuse de la confidentialité des utilisateurs, et adaptée à des usages sensibles comme la télésurveillance médicale.

3.6.7 Conclusion

Dans ce chapitre, nous avons exploré en détail l'application du protocole EAP-AKA′ dans un contexte de télésurveillance médicale (home monitoring), en mettant en lumière les mécanismes d'authentification au sein d'un réseau 5G sécurisé.

Après avoir décrit le fonctionnement général d'un système de home monitoring médical. Le processus d'authentification EAP-AKA′, articulé autour d'un échange cryptographique sécurisé, garantit l'identité mutuelle des entités et établit des clés de session pour sécuriser la transmission des données médicales sensibles. Toutefois, nous avons également mis en évidence des limites potentielles, notamment la possibilité d'attaques par rejeu en cas de désynchronisation des compteurs de séquence (SQN). Des mécanismes de resynchronisation et des pistes d'amélioration ont été proposés afin de renforcer la robustesse du protocole dans des environnements médicaux à haute exigence de fiabilité.

Le prochain chapitre sera consacré à la vérification formelle du protocole EAP-AKA′ à l'aide de l'outil de vérification AVISPA (Automated Validation of Internet Security Protocols and Applications). En modélisant les différentes étapes du protocole dans le langage HLPSL.

Chapitre 4

Vérification de protocole avec l'outil Avispa

4.1 Introduction

La vérification de la sécurité des protocoles cryptographiques repose généralement sur deux approches complémentaires : la recherche d'éventuelles attaques et la démonstration formelle de leur robustesse. Ces démarches permettent non seulement d'identifier des vulnérabilités potentielles, mais aussi de s'assurer que les protocoles respectent des propriétés de sécurité essentielles telles que la confidentialité, l'authentification et l'intégrité.

Parmi les outils dédiés à cette vérification automatique, la plateforme AVISPA (Automated Validation of Internet Security Protocols and Applications) se distingue comme l'une des plus reconnues. Elle permet de modéliser et d'analyser un large éventail de protocoles (au total 79), et son efficacité a été largement démontrée à travers l'étude de protocoles récemment standardisés, notamment par l'IETF. En permettant de détecter et de corriger les failles avant le déploiement opérationnel, la vérification formelle constitue ainsi un levier essentiel pour garantir la fiabilité et la sécurité des communications dans les systèmes informatiques modernes[24].

Ce chapitre est consacré à la vérification de protocole d'authentification EAP-AKA' à l'aide de la plateforme SPAN/AVISPA, en s'appuyant sur le langage de spécification HLPSL. L'intégration de cette plateforme permet d'effectuer une analyse formelle des propriétés de sécurité du protocole, assurant ainsi sa robustesse et sa fiabilité.

4.2 Définition de l'outil Avispa

AVISPA est un outil conçu pour la validation automatique des protocoles et des applications sensibles à la sécurité sur Internet. Il s'appuie sur un langage formel à la fois modulaire et expressif, permettant de décrire précisément les protocoles ainsi que leurs propriétés de sécurité. L'outil intègre plusieurs moteurs d'analyse (back-ends) qui mettent en œuvre différentes techniques d'analyse automatisée de pointe afin de vérifier la conformité de ces protocoles aux objectifs de sécurité définis[32]. Lorsqu'une vulnérabilité est identifiée dans un protocole, AVISPA est capable de la représenter à travers un diagramme de séquence de messages. Cette visualisation permet de mieux comprendre la nature de la faille et le déroulement de son exploitation potentielle[25].

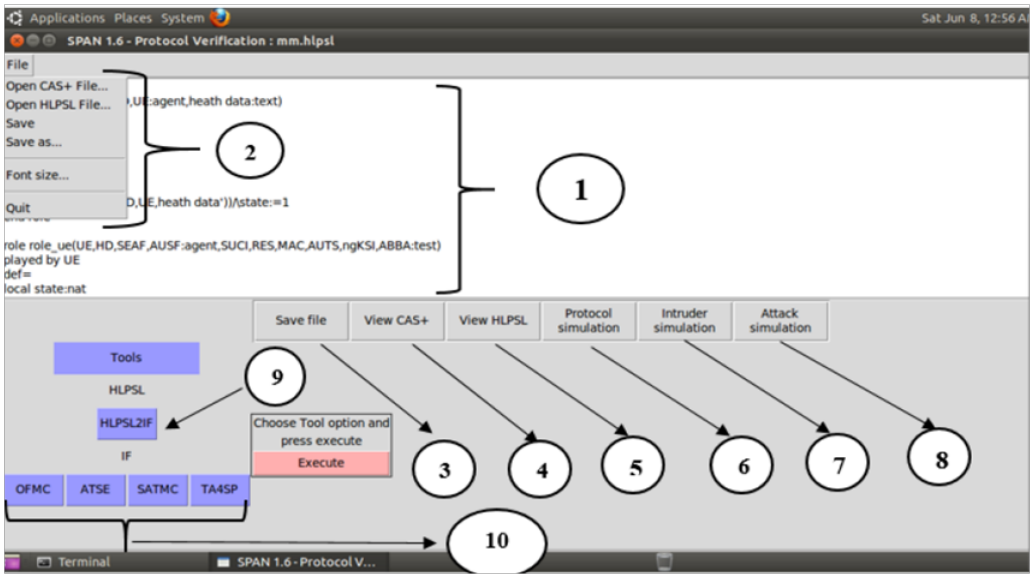


Figure 4.1 – Interface principale de l'outil SPAN AVISPA

— 1 :Zone de modélisation graphique du protocole HLPSL

— 2 : ouvrir ou d'enregistrer une spécification de protocole au format HLPSL ou CAS+ ou quitter l'application.

— 3 :Permet de sauvegarder les modifications faites dans le fichier HLPSL édité.

— 4 :Permet d'afficher la version CAS+ (le langage intermédiaire utilisé par AVISPA) du fichier HLPSL.

— 5 :Affiche le fichier HLPSL modélisé, utile pour revoir le code sans passer par l'éditeur.

— 6 :Lance une simulation du protocole sans attaque pour vérifier s'il fonctionne correctement en conditions normales.

— 7 :Lance une simulation avec la présence d'un intrus passif ou actif, selon le modèle Dolev-Yao. Cela permet de voir comment un attaquant peut intercepter, modifier ou rejouer les messages.

— 8 :Effectue une analyse complète de sécurité en simulant diverses attaques (rejeu, usurpation, etc.).

— 9 :Transforme le code HLPSL en une représentation intermédiaire (IF) utilisée par les moteurs de vérification.

— 10 :Outils de vérification (OFMC, CL-AtSe, SATMC, TA4SP)

4.3 Architecture de Avispa

L'architecture de l'outil AVISPA s'appuie sur une démarche systématique pour l'analyse formelle des protocoles de sécurité, en intégrant trois composants clés. Tout d'abord, la spécification s'effectue en HLPSL, un langage haut niveau modulaire et expressif permettant de décrire les rôles des participants, les opérations cryptographiques ainsi que leurs propriétés algébriques, les modèles de menace, et enfin les propriétés de sécurité à vérifier, sans nécessiter de

simplifications préalables du protocole. Ensuite, le module HLPSL2IF traduit automatiquement ces spécifications HLPSL dans un format intermédiaire (IF) qui représente le protocole sous la forme d'un système de transitions à états infinis, adapté à l'analyse formelle automatisée. Enfin, AVISPA met à disposition quatre moteurs d'analyse (back-ends) spécialisés, utilisant différentes techniques pour explorer l'espace d'états et détecter automatiquement les vulnérabilités[26].

AVISPA intègre quatre back-ends, chacun offrant une méthode unique de vérification[25] :

- **OFMC (On-the-fly Model-Checker) :** Est un outil qui cherche des attaques en résolvant des contraintes logiques. Il utilise des techniques pour simplifier les calculs et éviter de répéter les mêmes vérifications. IL vérifie que chaque message reçu est bien du type attendu et vérifier la manière dont les messages sont combinés dans le protocole.
- **CL-AtSe (Constraint-Logic-based Attack Searcher) :** Est un moteur d'analyse de protocoles de sécurité qui s'appuie sur la résolution de contraintes, enrichie par des heuristiques avancées de simplification et des méthodes d'élimination des redondances. Sa conception modulaire facilite son extension pour intégrer la gestion des propriétés algébriques des opérateurs cryptographiques. CL-AtSe prend en charge la détection des erreurs de type (type-flaw) et gère l'associativité dans la concaténation des messages.
- **SATMC (SAT-based Model-Checker) :** Est un outil qui modélise le protocole sous forme d'une formule logique limitée dans le temps. Grâce à un solveur SAT, il vérifie si cette formule permet de violer une propriété de sécurité. Si une violation est détectée, SATMC fournit un scénario d'attaque complet, permettant une analyse détaillée.
- **TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols) :** Est un outil d'analyse de protocoles de sécurité qui vérifie leur robustesse sans limite sur le nombre de sessions. Il estime les connaissances possibles d'un attaquant à l'aide d'approximations automatiques basées sur des langages réguliers sur arbres et des techniques de modélisation symbolique. TA4SP permet de prouver qu'un protocole est vulnérable ou sécurisé pour un nombre quelconque de sessions.

Cette architecture offre ainsi une solution complète, allant de la modélisation jusqu'à la vérification formelle, tout en garantissant expressivité et rigueur méthodologique.

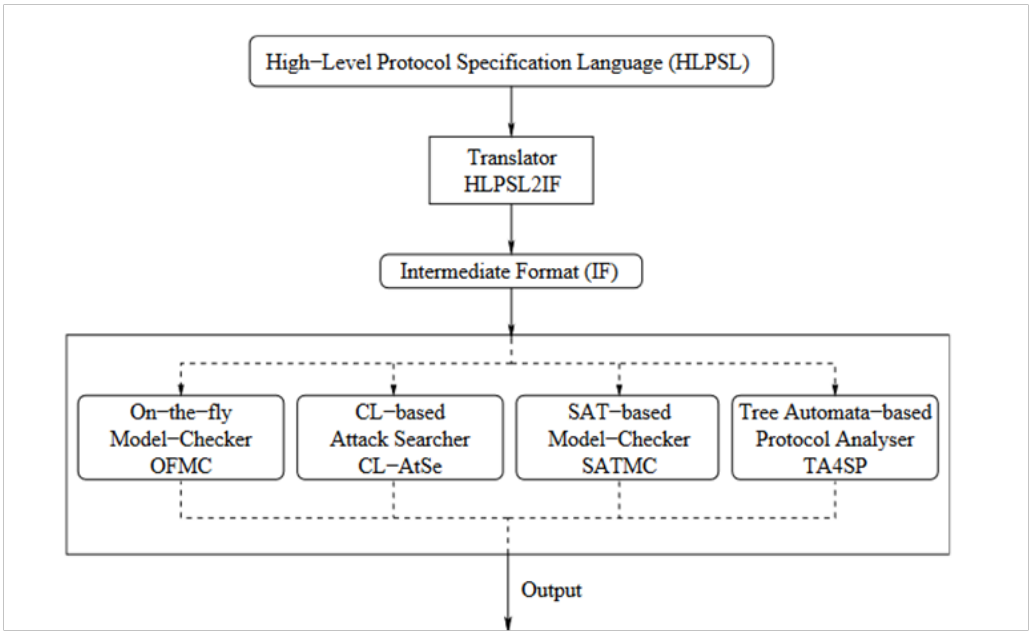
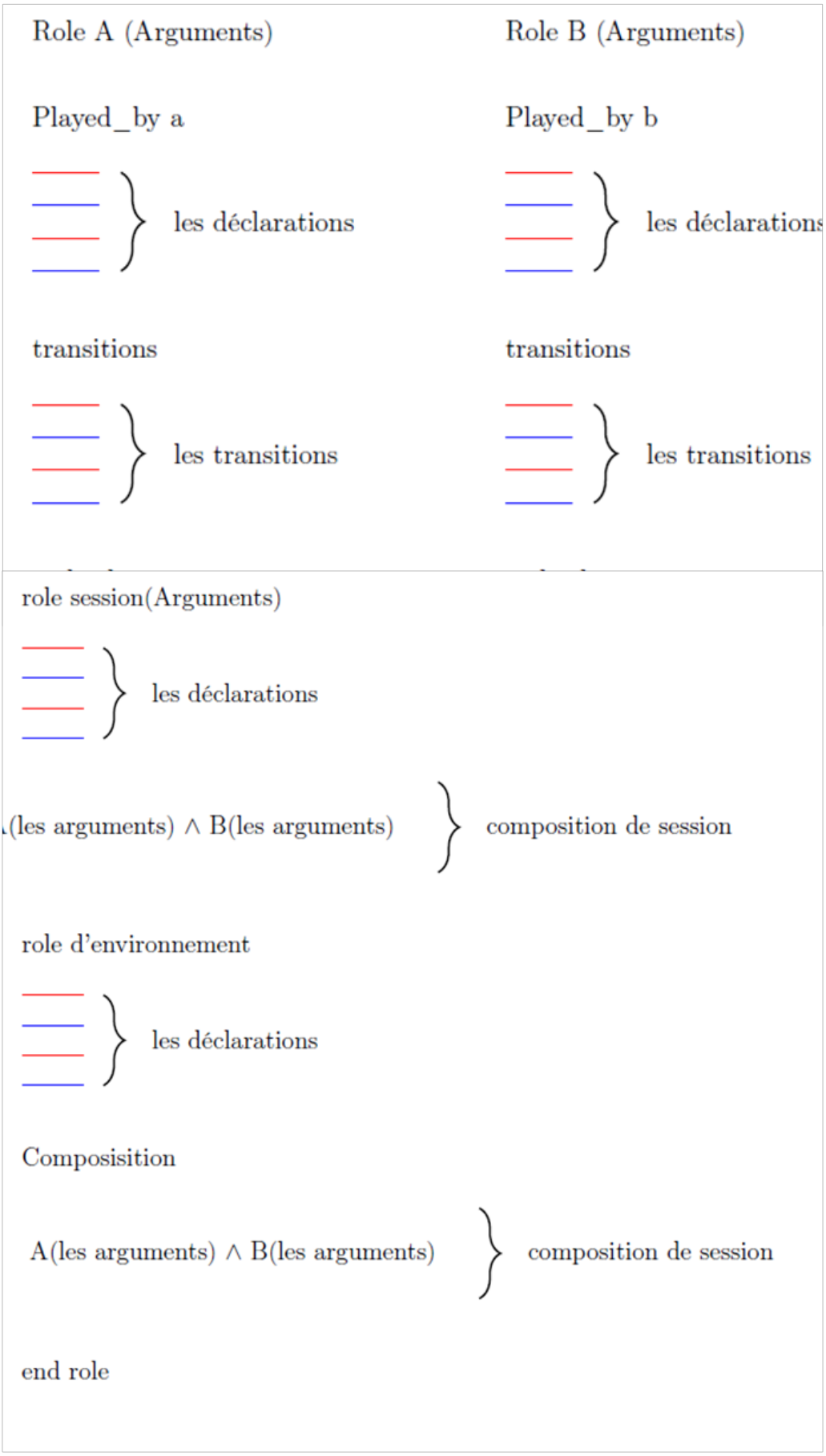


Figure 4.2 – Architecture d'AVISPA[26].

4.4 Définition de HLPSL

HLPSL (High-Level Protocol Specification Language) est un langage formel conçu pour spécifier et analyser des protocoles de sécurité de manière modulaire et structurée. Il repose sur une modélisation par rôles, permettant de décrire les différentes entités impliquées (comme les clients, serveurs ou autorités de certification) ainsi que leurs interactions. Le langage intègre un ensemble de primitives cryptographiques, incluant les clés symétriques, asymétriques et les fonctions de hachage, tout en prenant en compte leurs propriétés algébriques (telles que le XOR ou l'exponentiation). L'objectif principal d'HLPSL est de vérifier formellement des propriétés de sécurité fondamentales, comme l'authentification et la confidentialité, en représentant les protocoles sous forme de systèmes à états et transitions. Cette représentation facilite leur analyse à l'aide de logiques temporelles, notamment la logique temporelle linéaire (LTL). Les spécifications HLPSL se divisent en deux catégories : les rôles de base, qui décrivent les comportements individuels des agents, et les rôles de composition, qui modélisent des scénarios complexes impliquant plusieurs acteurs[26].

4.4.1 Structuration du HLPSL



4.5 Vérification du protocole EAP-AKA′

Dans un premier temps, nous avons modélisé le protocole EAP-AKA' dans l'environnement AVISPA afin d'analyser sa robustesse face aux attaques. Cette analyse a permis de mettre en évidence une vulnérabilité de type rejeu ciblant le message 7, dans lequel l'attaquant peut rejouer un ancien challenge (RAND, AUTN) pour tromper l'UE. Suite à cette observation, nous avons implémenté des améliorations proposé dans le modèle HLPSL afin de renforcer la protection contre ce type d'attaque. La version améliorée du protocole a ensuite été soumise à une nouvelle vérification à l'aide de l'outil OFMC, pour confirmer la correction des failles détectées.

4.5.1 Modelisation de l'attaque par rejeu sur le message 7 : SEAF →UE(RAND, AUTN, ngKSI, ABBA)

Cette section présente la modélisation HLPSL de la version vulnérable du protocole, suivie d'une vérification automatique avec AVISPA.

4.5.1.1 Analyse du comportement de SEAF :

- **Etape 1 :** le serveur SEAF envoie le message de challenge vers l'UE qui contient :RAND, AUTN, ngKSI, ABBA.
- **Etape 2 :** Il attend une réponse :

— soit une réponse d'authentification (RES)

— soit une notification d'erreur(sync_failure)

Le code HLPSL :

```
role SEAF(UE, SEAF_ID, RAND, AUTN, ngKSI, ABBA, RES) played_by SEAF
 def=
  local
    State : nat
  init
    State := 0
  transition
    % SEAF envoie le message de challenge
    1. State = 0 =>
       send(SEAF, UE, (RAND, AUTN, ngKSI, ABBA))
       State := 1

    % SEAF reçoit la réponse ou un sync_failure
    2. State = 1 /\ (recv(UE, RES) \/ recv(UE, sync_failure)) =>
       State := 2
end role
```

Figure 4.3 – Rôle de SEAF

4.5.1.2 Analyse du comportement de UE :

le dispositif de l'utilisateur répond au challenge reçu du SEAF. Il vérifie la validité du message et la synchronisation du compteur SQN.

- **Étape 1 :** L'UE reçoit le message de challenge provenant du SEAF.
- **Étape 2 :**L'UE vérifie la synchronisation du numéro de séquence (SQN) :

— Si le message est ancien ou rejoué (désynchronisé), l'UE envoie une réponse d'erreur sync_failure.

— Si le message est valide et synchronisé, l'UE envoie la réponse d'authentification RES.

Le code hlpsl :

```
role UE(AUSF, SEAF, UE_ID, RAND, AUTN, RES, SQN, sync_failure) played_by UE
 def=
  local
    State : nat
  init
    State := 0
  transition
    % L'UE reçoit le message de challenge
    1. State = 0 /\ recv(SEAF, (RAND, AUTN, ngKSI, ABBA)) =>
       State := 1

    % L'UE vérifie la synchronisation du SQN
    2. State = 1 =>
       if not_synced(SQN) then
         send(UE, SEAF, sync_failure)
       else
         send(UE, SEAF, RES)
       endif
       State := 2
end role
```

Figure 4.4 – Rôle de passrelle(UE)

4.5.1.3 Analyse du comportement de l'attaquant :

L'attaquant par rejeu intercepte un message légitime et le rejoue à l'UE dans le but de détecter la présence de l'utilisateur ciblé grâce à la réponse fournie par le dispositif.

- **Étape 1 :** L'attaquant intercepte le message de challenge initialement destiné à l'UE.
- **Étape 2 :** L'attaquant rejoue ce même message vers l'UE pour provoquer une réponse.
- **Étape 3 :** L'attaquant écoute la réponse de l'UE :

— Une réponse sync_failure signifie que l'UE ciblé est présent (preuve d'une désynchronisation sur un message légitime).

— Une réponse RES peut également être observée dans certains cas.

Le code hlpsl :

```
role attacker_replay(UE, SEAF, RAND, AUTN, ngKSI, ABBA, RES, sync_failure) played_by I
 def=
  local
    State : nat
  init
    State := 0
  transition
    % L'attaquant intercepte le message de challenge
    1. State = 0 =>
       recv(SEAF, UE, (RAND, AUTN, ngKSI, ABBA))
       State := 1

    % L'attaquant rejoue le message intercepté vers l'UE
    2. State = 1 =>
       send(I, UE, (RAND, AUTN, ngKSI, ABBA))
       State := 2

    % L'attaquant observe la réponse RES ou sync_failure
    3. State = 2 /\ (recv(UE, RES) \/ recv(UE, sync_failure)) =>
       State := 3
end role
```

FIGURE 4.5 – Rôle de l'attaquant

4.5.2 Execution du protocole

il suffit de cliquer sur "File", puis sur "Open HLPSL file" pour charger le fichier. Ensuite, parmi les quatre moteurs de vérification proposés par AVISPA, nous sélectionnons l'outil OFMC, puis cliquons sur "Exécuter" pour lancer la vérification du protocole.

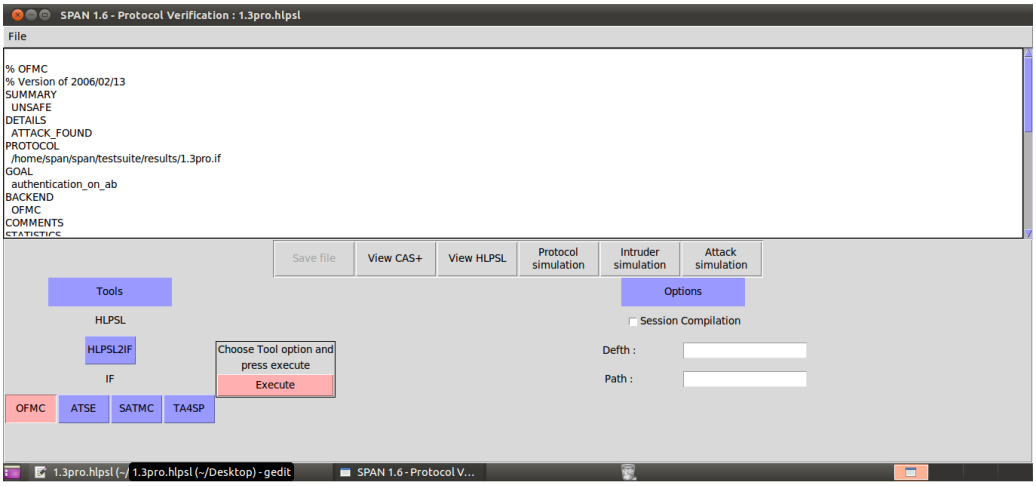


FIGURE 4.6 – résultat d'execution

4.5.2.1 Interprétation des résultats

— La section SUMMARY indique que le protocole est vulnérable, avec le résultat UNSAFE(n'est pas sûr).

— la section DETAILS indique que la verification formelle a pu détecter l'attaque par rejeu par le résultat ATTACK_FOUND.

4.5.3 Verification de protocole amélioré

Après avoir identifié des vulnérabilités dans la version initiale du protocole, notamment une attaque par rejeu sur le message 7, nous avons appliquée les améliorations proposée pour le renforcement du Protocole EAP-AKA'. Les modifications apportées visent à renforcer l'authentification mutuelle, assurer la fraîcheur des messages échangés, et protéger les valeurs critiques contre toute manipulation ou réutilisation par un attaquant. Afin de valider l'efficacité de ces améliorations, une nouvelle vérification du protocole a été réalisée à l'aide de l'outil OFMC dans l'environnement AVISPA.

- **Le code hlpsl :**

```
role ue(
    UE, SEAF : agent,
    K_UE_SEAF : symmetric_key)
played_by UE

vars
    SUCI, RAND, AUTN, ngKSI, ABBA, RES, MAC2, Timestamp, AUTS : text
    State : nat

init
    State := 0

transition
    1. State = 0 /
       recv(SEAF, {"EAP-Request/Identity"}_(K_UE_SEAF)) =|>
       SUCI' := new() /
       send(SEAF, {SUCI', "HNID"}_(K_UE_SEAF)) /
       State' := 1

    2. State = 1 /
       recv(SEAF, {RAND, AUTN, ngKSI, ABBA, Timestamp}_(K_UE_SEAF)) =|>
       is_fresh(Timestamp) = true /
       State' := 2 /
       RES' := new() /
       MAC2' := h(RES', K_UE_SEAF) /
       NewTimestamp' := new() /
       send(SEAF, {RES', MAC2', NewTimestamp'}_(K_UE_SEAF))

    3. State = 2 /
       recv(SEAF, {"EAP-Success", ngKSI, ABBA}_(K_UE_SEAF)) =|>
       State' := 3

    4. State = 2 /
       recv(SEAF, {"Sync-Failure-Request"}_(K_UE_SEAF)) =|>
       AUTS' := new() /
       send(SEAF, {"MAC_Failure", "Sync_Failure", AUTS'}_(K_UE_SEAF)) /
       State' := 4

end role
```

Figure 4.7 – Rôle de UE

```
role seaf(
    SEAF, UE, AUSF : agent,
    K_UE_SEAF : symmetric_key)
played_by SEAF

vars
    SUCI, RAND, AUTN, ngKSI, ABBA, RES, MAC2, Timestamp, XRES, AUTS : text
    State : nat

init
    State := 0

transition
    1. State = 0 =|>
       send(UE, {"EAP-Request/Identity"}_(K_UE_SEAF)) /
       State' := 1

    2. State = 1 /
       recv(UE, {SUCI, "HNID"}_(K_UE_SEAF)) =|>
       send(AUSF, {SUCI, "SNN"}_(K_UE_SEAF)) /
       State' := 2

    3. State = 2 /
       recv(AUSF, {RAND, AUTN, XRES, ngKSI, ABBA}_(K_UE_SEAF)) =|>
       Timestamp' := new() /
       send(UE, {RAND, AUTN, ngKSI, ABBA, Timestamp'}_(K_UE_SEAF)) /
       State' := 3

    4. State = 3 /
       recv(UE, {RES, MAC2, Timestamp}_(K_UE_SEAF)) =|>
       is_fresh(Timestamp) = true /
       MAC2 = h(RES, K_UE_SEAF) =|>
       send(AUSF, RES) /
       State' := 4

    5. State = 4 /
       recv(AUSF, XRES) =|>
       if (XRES = RES) then
           send(UE, {"EAP-Success", ngKSI, ABBA}_(K_UE_SEAF)) /
           State' := 5
       else
           send(UE, {"Sync-Failure-Request"}_(K_UE_SEAF)) /
           State' := 6

    6. State = 6 /
       recv(UE, {"MAC_Failure", "Sync_Failure", AUTS}_(K_UE_SEAF)) =|>
       send(AUSF, {"Sync_Failure", AUTS}_(K_UE_SEAF)) /
       State' := 7

end role
```

Figure 4.8 – Rôle de SEAF

```
role ausf(
    AUSF, SEAF, ARPF : agent,
    K_UE_SEAF : symmetric_key)
played_by AUSF

vars
    SUCI, SNN, RAND, AUTN, XRES, ngKSI, ABBA, RES, AUTS : text
    State : nat

init
    State := 0

transition
    1. State = 0 /
       recv(SEAF, {SUCI, SNN}_(K_UE_SEAF)) =|>
       send(ARPF, {SUCI, SNN}_(K_UE_SEAF)) /
       State' := 1

    2. State = 1 /
       recv(ARPF, {RAND, AUTN, XRES, ngKSI, ABBA}_(K_UE_SEAF)) =|>
       send(SEAF, {RAND, AUTN, XRES, ngKSI, ABBA}_(K_UE_SEAF)) /
       State' := 2

    3. State = 2 /
       recv(SEAF, RES) =|>
       send(SEAF, XRES) /
       State' := 3

    4. State = 3 /
       recv(SEAF, {"Sync_Failure", AUTS}_(K_UE_SEAF)) =|>
       send(ARPF, {"Sync_Failure", AUTS}_(K_UE_SEAF)) /
       State' := 4

end role
```

Figure 4.9 – Rôle de AUSF

```
role arpf(
    ARPF, AUSF : agent,
    K_UE_SEAF : symmetric_key)
played_by ARPF

vars
    SUCI, SNN, RAND, AUTN, XRES, ngKSI, ABBA, AUTS : text
    State : nat

init
    State := 0

transition
    1. State = 0 /
       recv(AUSF, {SUCI, SNN}_(K_UE_SEAF)) =|>
       RAND' := new() /
       AUTN' := new() /
       XRES' := new() /
       ngKSI' := new() /
       ABBA' := new() /
       send(AUSF, {RAND', AUTN', XRES', ngKSI', ABBA'}_(K_UE_SEAF)) /
       State' := 1

    2. State = 1 /
       recv(AUSF, {"Sync_Failure", AUTS}_(K_UE_SEAF)) =|>
       % Resynchronisation logic can be expanded here
       State' := 2

end role
```

Figure 4.10 – Rôle de ARPF

4.5.3.1 Execution du protocole

Le backend utilisé pour la vérification est OFMC

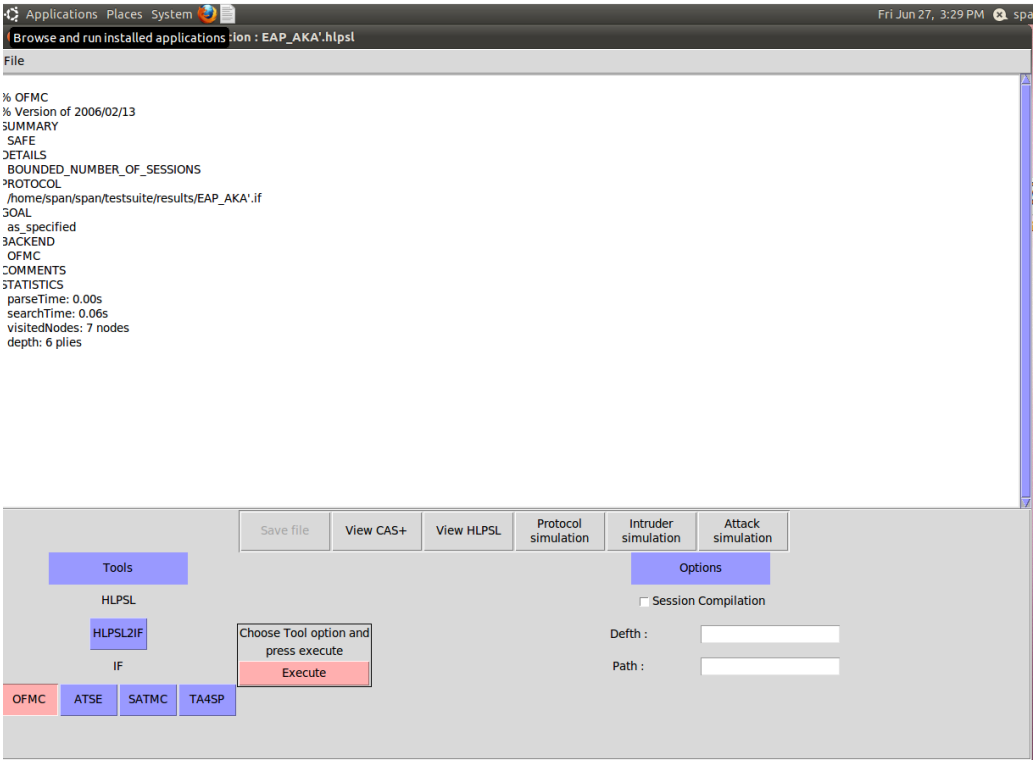


Figure 4.11 – Résultat d'execution

4.5.3.2 Interprétation des résultats

— Le résultat "SAFE" dans la section SUMMARY indique que le protocole est sécurisé.

— GOAL as_specified : Cela indique que les objectifs spécifiés dans le fichier HLPSL (comme l'authentification ou la confidentialité) ont été vérifiés.

L'évaluation formelle du protocole a permis de vérifier qu'il respecte les propriétés de sécurité spécifiées, telles que l'authentification, la confidentialité et l'intégrité. Cette vérification renforce la confiance dans la robustesse du protocole face aux attaques modélisées.

4.6 Conclusion

Ce chapitre a porté sur la vérification formelle du protocole EAP-AKA' à l'aide de la plateforme AVISPA et du langage HLPSL. Une vulnérabilité critique a été identifiée : une attaque par rejeu sur le message 7, dans laquelle un attaquant, ayant détecté l'identité de l'UE cible, peut réutiliser un ancien challenge (RAND, AUTN) pour compromettre l'authentification.

Cette attaque a été modélisée et validée automatiquement à l'aide du backend OFMC. les améliorations proposées ont été ensuite intégrées au modèle HLPSL, puis vérifiées avec succès, prouvant leur efficacité.

Cette démarche met en lumière l'importance de l'analyse formelle pour anticiper les failles de sécurité et renforcer la robustesse des protocoles avant leur mise en œuvre. L'utilisation d'AVISPA s'est révélée essentielle pour évaluer la résistance du protocole EAP-AKA', en assurant les propriétés fondamentales de confidentialité, d'intégrité et d'authentification dans les communications sécurisées.

Conclusion et Perspectives

Ce mémoire s'est inscrit dans le contexte croissant de la numérisation du secteur de la santé et de l'émergence des dispositifs médicaux connectés. À travers une exploration approfondie des enjeux de sécurité propres à ces systèmes, nous avons mis en évidence la nécessité d'un protocole d'authentification robuste afin de garantir la confidentialité, l'intégrité et l'authenticité des échanges entre dispositifs et infrastructures médicales.

Le protocole EAP-AKA', issu des réseaux mobiles 5G, s'est révélé être une solution adaptée aux contraintes spécifiques des environnements médicaux connectés, en assurant une authentification mutuelle forte et en intégrant des mécanismes cryptographiques avancés.

Toutefois, notre étude a également mis en lumière certaines limites, notamment la vulnérabilité du protocole face aux attaques par rejeu, les risques induits par une gestion imparfaite des clés, ainsi que les difficultés liées aux désynchronisations pouvant entraîner des dénis de service. Ces failles, bien que ciblées, soulignent l'importance de renforcer la mise en œuvre d'EAP-AKA' par des mécanismes complémentaires. Des solutions comme l'intégration de timestamps pour contrer les rejets d'anciennes requêtes, une meilleure gestion du cycle de vie des clés cryptographiques, ou encore une synchronisation plus robuste entre les entités en communication apparaissent comme des pistes essentielles à explorer.

En mobilisant une approche formelle de validation à l'aide de l'outil AVISPA, nous avons pu confirmer la robustesse générale du protocole tout en identifiant des vecteurs d'attaque potentiels. Cette étape de validation a permis non seulement de consolider notre analyse, mais également de dégager des perspectives concrètes d'amélioration. Elle confirme, par ailleurs, l'importance d'une vigilance constante dans la conception, le test et le déploiement des protocoles de sécurité dans un domaine aussi sensible que celui de la santé connectée, où la fiabilité des échanges conditionne directement la protection des patients et la qualité des soins dispensés.

Dans cette optique, plusieurs perspectives d'évolution se dessinent pour renforcer la sécurité des protocoles d'authentification, à commencer par l'intégration de l'intelligence artificielle. En exploitant les capacités du machine learning, il serait possible de mettre en place des systèmes capables de détecter en temps réel des comportements anormaux ou suspects, tels que les attaques par rejeu ou les intrusions. L'authentification pourrait également devenir plus contextuelle, en s'appuyant sur l'analyse des habitudes des utilisa-

teurs ou des patients pour ajuster dynamiquement le niveau de sécurité requis en fonction du risque perçu.

Parallèlement, l'usage de la blockchain représente un axe complémentaire prometteur. Cette technologie, en offrant une infrastructure décentralisée et immuable, permettrait d'assurer une gestion transparente et traçable des identités des dispositifs médicaux, tout en réduisant les risques d'usurpation ou de falsification des accès. En horodatant les transactions et les échanges, la blockchain pourrait également renforcer la résistance aux attaques par rejeu et offrir une meilleure résilience globale du système. L'auditabilité native des blockchains constitue un atout supplémentaire dans les environnements soumis à des exigences réglementaires strictes.

Ces approches innovantes devront cependant être envisagées dans le cadre plus large de l'évolution des réseaux de communication, notamment avec l'émergence progressive de la 6G. Les futurs réseaux ultra-rapides et massivement distribués, qui accueilleront un nombre croissant d'objets connectés médicaux (IoMT), imposeront une refonte partielle des protocoles actuels. Il sera essentiel d'adapter EAP-AKA', voire de concevoir de nouveaux protocoles plus légers, plus réactifs et compatibles avec les exigences de latence extrêmement faibles. De plus, la montée en puissance de l'informatique quantique appelle à intégrer dès maintenant des mécanismes de chiffrement post-quantiques afin de garantir la pérennité des systèmes face aux menaces futures.

En conclusion, ce mémoire a démontré qu'EAP-AKA' constitue une solution solide pour l'authentification sécurisée dans le domaine de la santé connectée. Néanmoins, pour répondre pleinement aux exigences d'un écosystème médical en constante évolution, il apparaît nécessaire de le faire évoluer en combinant vérification formelle, intelligence artificielle et technologies décentralisées comme la blockchain. Cette combinaison pourrait permettre la construction de systèmes médicaux connectés à la fois performants, résilients et inviolables.

Les prochaines étapes logiques de ce travail consisteraient à prototyper les améliorations proposées, à collaborer avec des industriels pour tester ces solutions dans des environnements réels, et à engager des démarches de standardisation auprès des organismes compétents afin d'ancrer ces bonnes pratiques dans un cadre normatif reconnu. La sécurité des dispositifs médicaux connectés n'est pas un luxe, mais une nécessité vitale, et les perspectives ouvertes par ce travail s'inscrivent pleinement dans cette exigence de confiance, de rigueur et d'innovation au service de la santé de demain.

Bibliographie

[1] CHU de Lille, “La santé connectée, c’est quoi ?”, CHU Lille, consulté le 27 juin 2025. [En ligne]. Disponible : https ://santeconnectee.chu-lille.fr/le-programme

[2] Conseil National de l’Ordre des Médecins, *Le Livre Blanc de la santé connectée*, 2025. [En ligne]. Consulté le : 7 mars 2025. Disponible : https ://www.conseil-national.medecin.fr/sites/default/files/external-package/edition/lu5yh9/medecins-sante-connectee.

[3] EHESP. La santé connectée. École des Hautes Études en Santé Publique, 2021. Disponible sur : https ://documentation.ehesp.fr

[4] French Healthcare. Chronolife et Garmin Health s’associent pour un meilleur télésuivi des patients. 2021. Disponible sur : https ://frenchhealthcare.fr

[5] A. Gaudin, "E-Health, the Internet of Things and Telemedicine," Correspondances en Onco-Hématologie, vol. 11, no. 2, pp. 120–124, 2016

[6] Carte SIM pour la santé connectée : connectivité cellulaire, Synox, 2025.Disponible : https ://www.synox.io/cat-sante-connectee/carte-sim-sante-connectee/[Consulté le 08 mars 2025]

[7] Vie-publique.fr. La télémédecine : une solution pour faciliter l’accès aux soins, https ://www.vie-publique.fr/eclairage/18473-la-telemedecine-une- solution pourfaciliterl’acces aux soins, April 2023

[8] Télésanté : connecter la ville et l’offre de santé grâce à la 5G https ://www.orange business.com/fr/magazine/5g telesante-connecter-ville-et-offre-sante, 2023.

[9] BIOTRONIK SECo.KG, *La Téléc@rdiologie – BIOTRONIK Home Monitoring® : Informations pour les patients et leurs proches*, Berlin, Allemagne : BIOTRONIK SE Co. KG, 2011.

[10] “Sécurité internet des objets | IoT Journey,” 2024. [Online]. Available : https ://iotjourney.orange.com/fr-FR/explorer/les-solutions-iot/securite-internet-des-objets

[11] “Qu’est-ce que la sécurité des IoT ? | Fortinet,” 2024. [Online]. Available : https ://www.fortinet.com/fr/resources/cyberglossary/iot-security

[12] CYBER COVER contact@cyber cover.fr. 5G : quels sont les enjeux de cybersécurité ?https ://www.cyber-cover.fr/cyber-documentation/cyber-securite/quels-sontles-veritables-enjeux-de-cybersecurite-poses-par-larrivee-de-la-5g.

[13] U.S. Food and Drug Administration, Cybersecurity Vulnerabilities Affecting Medtronic MiniMed Insulin Pumps, FDA Safety Communication, Jun. 27, 2019. [Online]. Available : https ://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-minimed-insulin-pumps-fda-safety-communication

[14] MITRE, “CVE-2019-10964,” Common Vulnerabilities and Exposures, 2019. [Online]. Available : https ://cve.mitre.org/cgi-bin/cvename.cgi ?name=CVE-2019-10964

[15] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC 4187, Jan. 2006. [Online]. Available : https ://datatracker.ietf.org/doc/html/rfc4187.

[16] J. Arkko, V. Lehtovirta, and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA’)," RFC 5448, May 2009. [Online]. Available : https ://datatracker.ietf.org/doc/html/rfc5448

[17] L. Blunk and J. Vollbrecht, Extensible Authentication Protocol (EAP), RFC 3748, IETF, June 2004. [Online]. Available : https ://datatracker.ietf.org/doc/html/rfc3748

[18] J. Arkko and M. Naslund, Forward Secrecy Extension to the Improved Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA’ FS), RFC 9678, Internet Engineering Task Force (IETF), Dec. 2022. [En ligne]. Disponible https ://datatracker.ietf.org/doc/rfc9678/

[19] E. K. K. Edris, M. Aiash, and J. Loo, “Formalization and evaluation of EAP-AKA protocol for 5G network access security,” Array, vol. 16, p. 100254, 2022

[20] Enea, « EAP SIM Authentication Server », Enea, [En ligne]. Disponible sur : https ://www.enea.com/solutions/service-provider-wifi/aptilo-smp-wifi-service-management/aptilo-eap-sim-authentication-server/. [Consulté le : 25 mai 2025]

[21] Enea, « EAP and Seamless Access with SIM Authentication », Enea, [En ligne]. Disponible sur : https ://www.enea.com/insights/eap-and-seamless-access-with-sim-authentication/. [Consulté le : 25 mai 2025].

[22] J. Arkko and V. Lehtovirta, Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'), RFC 9048, June 2021. [Online]. Available : https ://doi.org/10.17487/RFC9048

[23] J. Arkko and H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), RFC 4187, January 2006. [Online]. Available : https ://doi.org/10.17487/RFC4187

[24] N. Chikouche, U. de M'sila, and M. Benmohammed, "Vérification automatique des protocoles d'authentification des systèmes RFID.

[25] A. Armando and al, "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications," in Computer Aided Verification, 2005, series Title : Lecture Notes in Computer Science. [Online]. Available : http ://link.springer.com/10.1007/1151398827

[26] "AVISPA v1.1 User Manual," Jun. 2006. [Online]. Available : https ://www.avispa-project.org/package/user-manual

[27] Okta, Protocoles d'authentification – Identity 101, Okta, [En ligne]. Disponible : https ://www.okta.com/fr-fr/identity-101/authentication-protocols/. [Consulté le : 20 avril 2025].

[28] Ping Identity, Protocoles d'authentification et d'autorisation, Ping Identity, [En ligne]. Disponible : https ://www.pingidentity.com/fr/resources/identity-40 fundamentals/authentication-authorization-protocols.html. [Consulté le : 20 avril 2025].

[29] HAUT CONSEIL DE LA SANTÉ PUBLIQUE. Définitions et apports de la télémédecine pour la santé publique. ADSP – Actualité et dossier en santé publique, n°101, décembre 2017. Paris : HCSP. Disponible sur : https ://www.hcsp.f

[30] P. Richard. 5G : un déploiement à haut risque ? Informatique et Numérique. November 2020.