# Protocoles d'échange de clés pour des systèmes de surveillance à base de radio-étiquettes

Wiem Tounsi, Joaquin Garcia Alfaro, Nora Cuppens-Boulahia, Frédéric Cuppens

# Protocoles d'échange de clés pour des systèmes de surveillance à base de radio-étiquettes

Wiem Tounsi*
Joaquin Garcia-Alfaro*
Nora Cuppens-Boulahia*
Frédéric Cuppens*

**Abstract:** Dans cet article, nous nous intéressons à la protection des communications entre les composants d'un système de surveillance médicale à domicile. Nous examinons particulièrement le problème d'échange de clés secrètes entre des entités hétérogènes d'un réseau comptant en plus des capteurs actifs, un nombre de capteurs passifs RFID (*Radio Frequency IDentification*) de type EPC (*Electronic Product Code*). L'analyse des différentes approches existantes dans la littérature nous révèle une approche assez robuste pour répondre au contexte de cette étude. Elle se base sur la technique du masque jetable. Dans cette analyse, nous tenons compte des critères liés à la nature du secret partagé et aux coûts des calculs tolérés dans un environnement hétérogène. Nous tenons compte aussi des mesures en qualité d'asymétrie et d'intermittence dans des échanges faisant intervenir des capteurs passifs.

**Keywords:** Sécurité des réseaux, RFID, EPC, Protocoles de cryptographie, Surveillance.

## 1 Introduction

Au cours de ces dernières années, des progrès substantiels ont été réalisés dans le domaine médical pour intégrer la technologie RFID (*Radio Frequency IDentification*) dans les systèmes de soins et de surveillance à distance [14, 18]. Pour éviter toute fuite d'information en relation avec la vie privée des patients, authentifier les composants du système à travers des schémas cryptographiques appropriés tels que l'échange de secrets partagés devient un besoin crucial [4]. Pour intégrer des protocoles d'échange de clés robustes, il est question de les vérifier dans un environnement hétérogène et de trouver un compromis entre la sécurité du système et les contraintes des composants déployés. Nous analysons dans le présent article des protocoles qui se basent sur des approches de référence appliquées aux composants passifs d'un réseau.

Dans un premier temps, nous motivons le besoin de sécuriser les données médicales et exprimons le contexte d'application des protocoles d'échange de clés (Section 2). Ensuite, nous examinons pour chaque protocole son adéquation avec le domaine d'application et le type de capteur auquel nous nous intéressons (Section 3). Enfin, nous tirons la conclusion de cette étude et considérons quelques perspectives (Section 4).

* TELECOM-Bretagne, 02, rue de la Châtaigneraie, 35576 Cesson Sévigné - France

## 2 Motivation et contexte

Les services de surveillance médicale à distance connaissent une demande croissante provenant généralement des patients souffrant de maladies chroniques [2] et particulièrement des personnes âgées vu leurs contraintes de déplacements fréquents [6]. Ces services reposent sur les nouvelles technologies pour surveiller les activités des patients sans imposer à ces derniers de quitter leurs foyers ou d'être accompagnés en permanence. Mais aussi, ces services tendent à considérer les moyens de communications usuels chez les patients pour ne pas leurs imposer des coûts supplémentaires. Nous pouvons imaginer des radio-étiquettes collées aux vêtements et médicaments des patients répondant aux interrogations des lecteurs associés. L'agrégation des données d'identification des radio-étiquettes permettrait aux exploitants des services de santé d'en déduire des informations pertinentes, telles que la chute d'un patient âgé, l'oubli ou la prise erronée d'un médicament.

Au delà des besoins de surveillance, un besoin de protection de l'information privée est considéré. Si les technologies sans fil sont connues par leur vulnérabilité à l'espionnage et aux attaques de type usurpation d'identité, l'utilisation des capteurs de type RFID qui répondent aux interrogations des lecteurs sans préavis, augmente la probabilité d'occurrence de ces menaces [11]. Ainsi, un travail supplémentaire adapté à ce type de composants doit être apporté afin de réduire le risque de violation de la confidentialité [20].

C'est à partir de ces besoins que découle le contexte de notre scénario d'application. Ce scénario s'applique sur un système de surveillance médicale à domicile qui utilise des capteurs hétérogènes : des capteurs actifs pour initier les communications en émettant de l'énergie utile et réaliser des calculs complexes et des capteurs passifs limités en terme de capacité de calcul, de stockage, de mémoire, et d'énergie, pour répondre à une requête d'identification en se servant de l'énergie envoyée par les capteurs actifs.

### *Caractéristiques de l'environnement*

EPCglobal a définit un standard pour les radio-étiquettes RFID de type EPC (*Electronic Product Code*) appelé UHF Class 1 Gen 2 [10]. Ce standard représente les capteurs passifs proposés pour le scénario de cette étude. Dans la suite, nous désignons par Gen 2, les capteurs de ce standard. Le choix de Gen 2 est retenu pour plusieurs raisons. Premièrement, la petite taille des radio-étiquettes permet de les intégrer discrètement sur des objets quotidiens. Deuxièmement, le faible coût de ces composants passifs permet aux services de la santé de les utiliser suivant la nécessité des patients. Troisièmement, l'indépendance d'une source d'énergie caractérise la longue durée de vie des radio-étiquettes passives. Enfin, en ce qui concerne l'organisation EPCglobal, elle définit une plateforme globale quant à l'utilisation de ses standards.

Le modèle d'adversaire à contrer est une autre alternative à considérer dans le scénario d'application. Le but étant de garder secrète l'information demandée auprès de la radio-étiquette, il est question de limiter l'écoute illégale de l'information. L'écoute permet par exemple à un attaquant de localiser la personne malade portant la radio-étiquette, de reconnaître le type de médicament qu'elle utilise et par conséquent, de savoir la maladie par laquelle elle est portée. Dans ce scénario, on se trouve devant un modèle d'adversaire spécifique. En raison de la distance entre le lecteur, la radio-étiquette et l'adversaire, ce dernier aura une difficulté à suivre tous les échanges possibles entre les composants du réseau [3]. Les canaux d'émission (lecteur-étiquette) et de réception (étiquette-lecteur) dans la communication faisant intervenir Gen 2 sont différents. Cette constatation limite l'accès de l'adversaire à un seul sens, celui du lecteur-étiquette étant donné l'intensité du champs de ce canal. D'ailleurs, EPCglobal a définit la distance de l'adversaire par rapport au réseau, pour appliquer son standard.

La solution clé pour protéger l'échange des données dans la communication est la cryptographie. À cause des contraintes matérielles imposées par les capteurs passifs Gen 2, il n'est plus possible d'utiliser la cryptographie traditionnelle pour authentifier les composants du système. Un recours aux protocoles de type *low-overhead* est alors la méthode retenue. Dans cette optique, un bref aperçu des solutions existantes peut être vu dans les références suivantes [5, 8, 12].

Suite à l'examen des approches d'authentification considérant la présence des composants passifs dans les systèmes de surveillance, nous avons analysé et résumé sous forme de protocoles d'échange de clés les approches qui rappellent le contexte de notre scénario [21]. Dans la suite, nous discutons la pertinence de ces protocoles à répondre aux critères établis en présence des capteurs de type Gen 2.

# 3 Analyse des protocoles et discussion

## 3.1 Critères d'analyse

Pour analyser les protocoles d'échange de secrets, il est question de vérifier leur adaptation à un contexte de composants hétérogènes. Ainsi, nous vérifions la source du secret à échanger et le coût des calculs engendrés par l'échange. Nous vérifions aussi des critères liés à la nature des communications en présence des capteurs passifs, à savoir l'asymétrie et l'intermittence des communications [3]. L'asymétrie des communications est due à l'utilisation des radio-étiquettes RFID sans batteries, amorcées uniquement par l'énergie recueillie à partir du lecteur. Quant à l'intermittence, elle est due aux échanges interrompus entre la radio-étiquette et le lecteur. Par conséquent, les protocoles appliqués à ce type de composants doivent gérer les interruptions et garder des échanges synchrones.

## 3.2 Analyse des Protocoles

Plusieurs approches dans la littérature se basent sur les valeurs SEV (*Secure Environmental Value*) [19, 22]. Ces valeurs sont utilisées comme secret dans l'établissement des clés d'échange afin d'authentifier les composants d'un système de communication. Les valeurs SEV, quand elles sont appliquées dans un contexte médical, se basent sur des informations biométriques. Ainsi, les dispositifs impliqués dans le processus d'établissement de clé symétrique se mettent d'accord sur une valeur commune déduite du corps du patient (exemple, la variation de la fréquence cardiaque [1]). Parmi ces différentes approches utilisant les valeurs SEV, nous dérivons un premier protocole de synthèse [21]. Ce protocole utilise une fonction de hachage réalisée au niveau de la radio-étiquette et du lecteur. Malgré sa robustesse de calcul et son respect des contraintes d'asymétrie et d'intermittence dans la communication, ce protocole ne présente pas une solution applicable au scénario de cette étude et ceci pour deux raisons, à savoir, la nature du secret et les coûts de calcul. D'abord, il n'est pas possible d'utiliser des valeurs biométriques comme secret à échanger en raison de la diversité des intervenants pouvant être étiquetés. Par exemple, il n'est pas possible à priori de générer une valeur de type SEV à partir d'un objet portant la radio-étiquette. D'autant plus que l'utilisation des valeurs biométriques reste un sujet de préoccupation d'un point de vue juridique dans certain pays, en raison de la possibilité de violer avec cette information la vie privée des patients [15]. Ensuite, les fonctions de hachage, utilisées dans cette approche présentent une contrainte considérable car, suivant plusieurs études [11, 16], ces fonctions ne sont pas recommandées pour être implémentées sur des radio-étiquettes RFID de type Gen 2.

Au lieu d'utiliser les valeurs biométriques, nous proposons d'utiliser les séquences provenant des générateurs pseudo aléatoires PRNG (*Pseudo Random Number Generators*) inhérents aux technologies RFID. Ce type de solutions peut-être intégré dans les circuits des radio-étiquettes Gen 2 depuis la ratification du standard associé [10]. De plus, des études ont montré que la complexité de la mise en œuvre de tels générateurs est équivalente à celles des fonctions de hachage à sens unique ou des fonctions de chiffrage équivalentes [17]. Ces dernières raisons font que cette solution résolve le problème de la génération des secrets tout en préservant la robustesse des fonctions de hachage utilisées auparavant. Le protocole que nous citons dans ce paragraphe est un exemple d'une approche utilisant les générateurs PRNG pour définir les secrets à partager [21]. Ce protocole dérive de l'approche de Karthikeyan et Nesterenko [13] traitant le principe des secrets pré-distribués. La sécurité de ce protocole réside dans la difficulté de récupérer les opérandes utilisées pour synchroniser les secrets partagés en considérant, à priori, que l'adversaire est contraint à suivre tous les échanges entre le lecteur et la radio-étiquette [3]. Malgré sa satisfaction des critères du contexte hétérogène (exemple, la nature du secret, le coût des calculs raisonnable et l'asymétrie des communications), ce protocole présente des failles dans la gestion de l'intermittence des communications. Dans ce sens, Chien et al. [7] montrent que si un lecteur intrus injecte des informations arbitraires ou précédemment écoutées à la radio-étiquette, d'une part cela désynchronise les secrets échangés mais d'autre part, peut donner la possibilité à l'intrus de tracer et de relire des données partagées entre les composants légitimes.

Pour traiter le risque de désynchronisation pendant le processus d'échange de clés, nous avons dirigé cette étude vers des solutions traitant toujours des valeurs pré-distribuées et des générateurs PRNG mais avec une approche pro-active basée sur la technique de masque jetable (ou *One Time Pad*). La solution d'authentification des composants proposée par Dolev et al. [9] est un exemple rapporté à cette approche. Le protocole de gestion des clés synthétisé de la solution de Dolev et al. [21] se base sur les sessions de communication répétées pour actualiser de manière pro-active un ensemble de secrets partagés. Le principe est d'utiliser à chaque session un nouveau masque jetable choisi au hasard par le lecteur et de le protéger en lui combinant une séquence aléatoirement générée. La synchronisation de cette génération est faite à partir d'une fonction et d'une valeur communes convenues dès le départ entre les composants. Le présent protocole garantit que même dans le cas où un adversaire malveillant est à l'écoute des échanges effectués sur plusieurs sessions, le rafraîchissement des secrets entre le lecteur et la radio-étiquette demeure sécurisé. Actuellement, ce protocole satisfait les exigences du contexte de notre étude.

# 4 Conclusion et perspectives

Nous avons examiné des approches de pointe dans le but d'établir des clés secrètes entre les composants d'un réseau sans fil basé sur des capteurs de capacités différentes. Le contexte du travail étant la surveillance des patients à distance dans un environnement hétérogène moyennant des radio-étiquettes Gen 2, nous avons discuté la possibilité de chaque approche d'utiliser des secrets supportables par tous les composants de l'environnement mais aussi, leurs possibilité de considérer les capacités de calcul et les critères d'échange relatifs à ce type de RFID. L'approche utilisant le masque jetable s'avère la plus intéressante dans le contexte défini. Elle fera le sujet de nos prochains travaux d'implémentation en considérant de plus prés les capacités du modèle d'adversaire dont les pouvoirs sont limités aux caractéristiques des canaux de communication spécifiées par le standard Gen 2.

**Remerciements** — Les auteurs remercient gracieusement le support financier reçu de l'Institut TELECOM grâce à son programme *Future et Rupture*.

# Références

[1] S. D. Bao, Y. T. Zhang, and L.F. Shen. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. *27th Annual International Conference of the Engineering in Medicine and Biology Society*, pp. 2455–2458, 2005.

[2] C. Boult, M. Altmann, D.Gilbertson, C. Yu, and RL. Kane. Decreasing disability in the 21st century : the future effects of controlling six fatal and nonfatal conditions. *Am J Public Health*, pp. 86(10) :1388-1393, 1996.

[3] M. Buettner, B. Greenstein, A. Sample, J. Smith, and D. Wetherall. Revisiting Smart Dust with RFID Sensor Networks. *7th ACM Workshop on Hot Topics in Networks (HotNets-VII)*, 2008.

[4] H. J. Chae, D. J. Yeager, J. R. Smith, K. Fu. Maximalist Cryptography and Computation on the WISP UHF RFID Tag. *Conference on RFID Security (RFIDSEC 2007)*, 2007.

[5] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. *IEEE Symposium on Security and Privacy*, pp. 197–215, 2003.

[6] Commission on Behavioral and Social Sciences and Education (CBASSE). Preparing for an Aging World : The Case for Cross-National Research. *National Academy Press -Washington, D.C.*, p. 31, 2001

[7] H. Chien and C. Chen. Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards. *Computers Standards and Interfaces*, 29(2), pp 254-259, 2007.

[8] S. A. Çamtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Transactions on Networking (TON)*, 15(2) :346–358, 2007.

[9] S. Dolev, M. Kopeetsky, and Adi Shamir. RFID Authentication Efficient Proactive Information Security within Computational Security. Tech. rep., Department of Computer Science, Ben-Gurion University, July 2007.

[10] EPCglobal. EPC Radio-frequency identity protocols Class-1 Generation-2. Technical report, http ://www.epcglobalinc.org/standards/, January 2005.

[11] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. Analysis of Threats to the Security of EPC Networks. *6th Annual Communication Networks and Services Research (CNSR) Conference*, IEEE Communications Society, Halifax, Nova Scotia, Canada, May 2008.

[12] J. Garcia-Alfaro, M. Barbeau, and E. Kranakis. Handling Security Threats to the RFID System of EPC Networks. *Security of Self-Organizing Networks : MANET, WSN, WMN, VANET*. Auerbach Publications, Taylor & Francis Group, 2010.

[13] S. Karthikeyan and M. Nesterenko. RFID Security without Extensive Cryptography. *3rd ACM workshop on security of ad hoc and sensor networks (SASN)*, pp. 63–67, New York, 2005.

[14] M. Moh, L. Ho, Z. Walker, T. S. Moh. A Prototype on RFID and Sensor Networks for Elder Health Care. *RFID Handbook : Applications, Technology, Security, and Privacy*, CRC press, pp. 311–328, 2008.

[15] A. Liberatore. Balancing Security and Democracy : the Politics of Biometric Identification in the European Union, European Univerity Institute. *EUI Working Paper RSCAS*, Robert Shuman Centre for Advanced Studies, 2005.

[16] P. Peris-Lopez, J. C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda. LAMED - A PRNG for EPC Class-1 Generation-2 RFID specification. *Journal of Computer Standards & Interfaces*, 2008

[17] P. Peris-Lopez, J. C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda. An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks. *Emerging Directions in Embedded and Ubiquitous Computing*, LNCS, vol. 4809, pp. 781–794, 2007.

[18] M. Philipose, J. R. Smith, B. Jiang, A. Mamishev, S. Roy, K. Sundara-Rajan. Battery-free wireless identification and sensing. *IEEE Pervasive Computing.*, January-March 2005.

[19] C. C. Y. Poon, Y. T. Zhang, and S. D. Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4) :73-81, 2006.

[20] J. J. Shen, L. F. Samson, E.L. Washington, P. Johnson, C. Edwards, and A. Malone. Barriers of HIPAA regulation to implementation of health services research. *Journal of Medical Systems*, 30(1) :65–69, Springer, 2006.

[21] W. Tounsi, J. Garcia-Alfaro, N. Cuppens-Boulahia, and F. Cuppens. Securing the Communications of Home Health Care Systems based on RFID Sensor Networks. *8th Annual Communication Networks and Services Research (CNSR) Conference*, IEEE Communications Society, Montreal, Quebec, Canada, May 2010.

[22] K. K. Venkatasubramanian and S. K. S. Gupta. Security for pervasive health monitoring sensor applications. *4th International Conference on Intelligent Sensing and Information Processing (ICISIP)*, 197–202, 2006.