Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility

Óscar J. Rubio[a,*], Jesús D. Trigo[b,**], Álvaro Alesanco[a], Luis Serrano[b], José García[a]

[a] *eHealthZ Research Group, Communications Networks and Information Technologies for E-health and Quality of experience group (CeNITEQ), Aragón Institute of Engineering Research (University of Zaragoza). Edif. Ada Byron, C/María de Luna 3, 50018 Zaragoza (Spain).*

[b] *Department of Electrical and Electronic Engineering, Public University of Navarre, Campus de Arrosada, 31006 Pamplona, Spain.*

Abstract

The ISO/IEEE 11073 standard for Personal Health Devices (X73PHD) aims to ensure interoperability between Personal Health Devices and aggregators —e.g. health appliances, routers— in ambulatory setups. The Integrating the Healthcare Enterprise (IHE) initiative promotes the coordinated use of different standards in healthcare systems (e.g. Personal/Electronic Health Records, alert managers, Clinical Decision Support Systems) by defining profiles intended for medical use cases. X73PHD provides a robust syntactic model and a comprehensive terminology, but it places limited emphasis on security and on interoperability with IHE-compliant systems and frameworks. However, the implementation of eHealth/mHealth applications in environments such as health and fitness monitoring, independent living and disease management (i.e. the X73PHD domains) increasingly requires features such as secure connections to mobile aggregators —e.g. smartphones, tablets—, the sharing of devices among different users with privacy, and interoperability with certain IHE-compliant healthcare systems. This work proposes a comprehensive IHE-based X73PHD extension consisting of additive layers adapted to different eHealth/mHealth applications, after having analyzed the features of X73PHD (especially its built-in security), IHE profiles related with these applications and other research works. Both the new features proposed for each layer and the procedures to support them have been carefully chosen to minimize the impact on X73PHD, on its architecture (in terms of delays and overhead) and on its framework. Such implications are thoroughly analyzed in this paper. As a result, an extended model of X73PHD is proposed, preserving its essential features while extending them with added value.

Keywords: Authentication, IHE, ISO/IEEE 11073, Privacy, Security

*Phone number: (+34) 976762698, fax number: (+34) 976762111

**Phone number: (+34) 948169264, fax number: (+34) 948169720

Email addresses: orubio@unizar.es (Óscar J. Rubio), jesusdaniel.trigo@unavarra.es (Jesús D. Trigo),

Operators and Notation

Operators	Meaning
[x,y]	Concatenate strings x and y
x=y	x takes the value of y
x==y	Returns the result (true or false) of comparing x and y
x{y}	Cipher or decipher string y using key x
f(x,y)	Execute function f with parameters x and y

Notation	Meaning
X	Entity. It could refer to an agent (A), a manager (M), a user (U), an administrator (Ad) or a manufacturer (Mf)
Ch1	Challenge used by a manager to authenticate an agent
Ch2	Challenge used by an agent to authenticate a manager
h(x)	Hash of string x
MK	Symmetric master key to derive symmetric session keys (S, SA)
S	Symmetric session key for encryption of frames
SA	Symmetric session key for authentication of frames
CEX	Certificate for encryption of entity X
PrEX	Private key for encryption of entity X
PbEX	Public key for encryption of entity X
CSX	Certificate for signature of entity X
PrSX	Private signature key of entity X
PbSX	Public signature verification key for entity X
Fi	Frame in clear text to be exchanged between agent and manager after C&A function
HMAC(Fi,SA)	Message authentication code of frame Fi using key SA
C&A(Fi,S,SA) = [S{Fi}, HMAC(S{Fi},SA)]	Frame i exchanged between an agent and a manager, using session key S for encryption and session key SA for authentication
d	Medical measurement(s)
D	d concatenated with identification or authentication strings
DS(D,PrSX)	Digital signature of frame D performed by entity X
ID(X)	In case of devices, this is the EUI-64. In case of users, this is the PersonID
FP(D,X) = [ID(X),DS(D,PrSX)]	Fingerprint of frame D performed by entity X. It includes the identity (ID) of X and its DS
StAi	Symmetric key i for encryption of data to be stored in an agent
StMi	Symmetric key i for encryption of data to be stored in a manager
RFID-T	Radio Frequency Identification Token
BC	Bar code
SC	Smart Card

1. Introduction

The healthcare model is evolving from hospital-centered care to a user/patient-centered paradigm [1, 2], enabled by the parallel advances in information and communication technologies. Health and fitness monitoring, independent living or remote disease monitoring and follow-up are some examples of innovative user/patient-centered static and mobile health applications [3] within the context of eHealth and mHealth. These applications use personal health devices (PHDs) and/or wearable sensors to gather biomedical measurements of the user in different locations (e.g. at home, in hospital, in daily journeys), which sometimes are accessed only by the user (to consult his/her health status) but often also by healthcare systems (e.g. to trigger alarms at abnormal values) or by some expert in charge of the user's follow-up. Certainly, these applications help to improve the health management of people, and the spread of powerful mobile devices and networks (e.g. 4G) foster their fast deployment [4]. Nonetheless, two important concerns must be addressed before considering eHealth and mHealth as key enablers of healthcare systems. First, achieving the highest possible interoperability level [5] among PHDs and healthcare systems, so that the measurements gathered by the former can be seamlessly integrated in healthcare workflows, making them available for authorized systems and experts anytime. Second, enforcing a continuous protection of the gathered measurements is required to prevent unauthorized accesses, which may result in social and professional damage for the users. There is also a need to address the issues of data forgery, corruption and loss, which may cause misdiagnosis, poor treatments or erroneous research outcomes.

Regarding the syntactic and (to some extent) semantic interoperability among PHDs (e.g. pulse oximeters, blood pressure monitors, weighing scales) and aggregator devices, a robust technical solution is addressed within the ISO/IEEE 11073 (X73PHD) family of standards [6], which define the landscape of transport-independent eHealth/mHealth applications and specify data exchange, data representation, and terminology for communication. Additionally, the Integrating the Healthcare Enterprise (IHE) [7] initiative promotes a model for pragmatic interoperability among healthcare systems by developing technical guidelines (IHE profiles) that coordinate the use of well established standards —e.g. DICOM [8] for medical imaging and HL7 [9] for medical messaging. Moreover, IHE defines the Rosetta Terminology Mapping profile, which enables the interpretation of X73PHD terminology —and thus, measurements acquired by X73PHD-compliant devices— in IHE systems, such as Personal and Electronic Health Records (PHR, EHR), alarm systems or Clinical Decision Support Systems (CDSS). Although setting up a X73PHD-IHE framework

alesanco@unizar.es (Álvaro Alesanco), lserrano@unavarra.es (Luis Serrano), jogarmo@unizar.es (José García)

sharing a common terminology is already feasible, it would lack continuity in security and privacy —given that X73PHD is very limited in this respect— and it would also lack specifications about the IHE profiles —apart from Rosetta— required to implement different eHealth/mHealth applications. As a first approach, one could envision that different existing security measures could be applied to each individual X73PHD framework; however, implementing security directly within the standard — thereby becoming an integral part of it — would greatly facilitate the deployment of secure frameworks in an efficient and homogeneous manner.

Therefore, the enhancement of X73PHD through the most appropriate IHE profiles is the main goal of this paper. The proposed solution is a flexible structure that provides features tailored to the needs of each eHealth/mHealth application —e.g. the identification of users to enable the sharing of PHDs and/or aggregators with privacy, the protection of the communications or the compliance with the IHE profiles implemented by EHRs and CDSS. The rest of this paper is organized as follows. Section 2 describes the materials of this research, which include an overview of X73PHD and IHE and of related works; and Section 3 the methods developed, which include a risk assessment of the X73PHD architecture and the proposal of an IHE-based security extension of this protocol. Section 4 depicts in detail the implications of the suggested proposal on the X73PHD models and on certain IHE profiles. In addition, it discusses the security of the X73PHD extension and evaluates its impact on its architecture —evaluated by means of a study of overhead and delays— and on its surrounding framework. Finally, the main conclusions from this research are drawn in Section 5.

2. Materials

This section introduces an overview of X73PHD and IHE, and works related with the topic of this research.

2.1. X73PHD and IHE overview

The ISO/IEEE 11073 is a set of standards aimed at providing interoperability between PHDs (referred to as "agents" in the X73PHD context) and aggregator devices, usually called "managers" (e.g. smartphones, personal computers, personal health appliances, maybe smart TVs). The full description of the standard can be found in the documents published by IEEE, but some overviews have already been published [10, 11]. Along with the definition and evolution of the family of standards, a variety of successful implementations — in several devices and platforms — have been reported [12, 13, 14]. In a X73PHD architecture (see

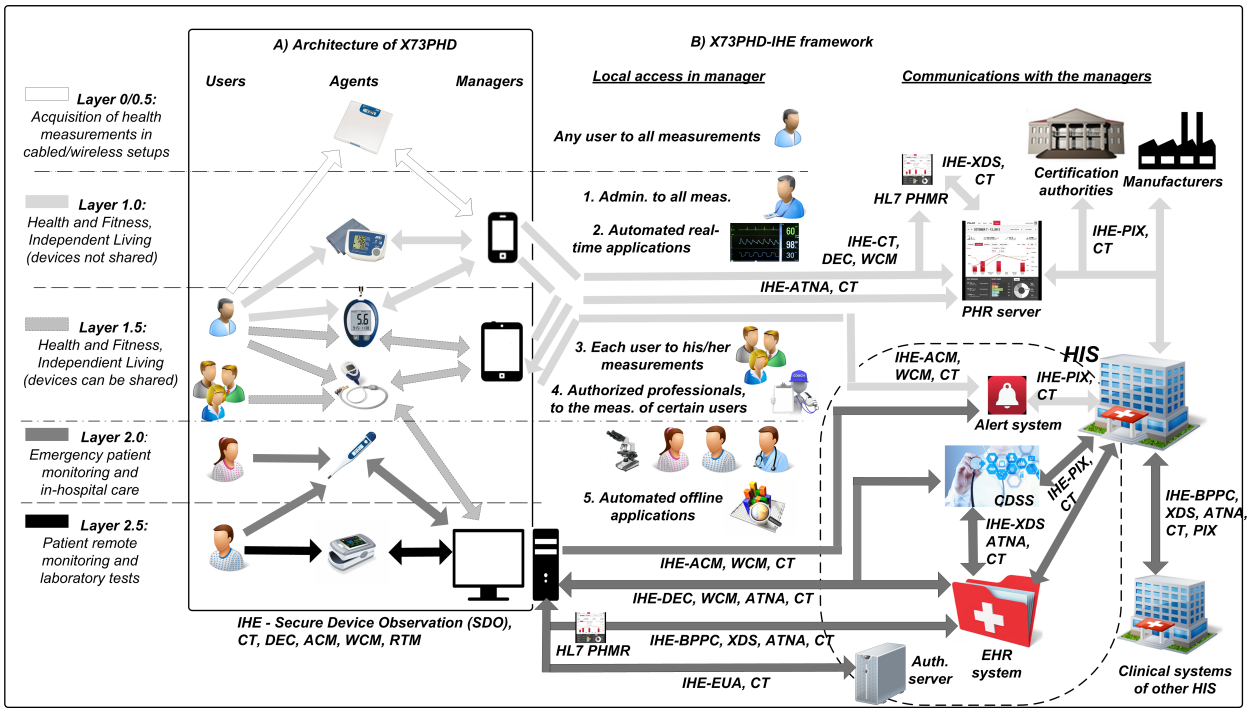

Figure 1: A) Example of a X73PHD-compliant healthcare architecture, B) proposal for a secure X73PHD-IHE framework based on additive layers intended for different eHealth and mHealth applications.

Figure 1-A) users can take their biomedical measurements with any agent(s), each agent can associate to only one manager at a time, each manager can associate to several agents simultaneously (to aggregate their measurements) and there must be an administrator in charge of managing agents and managers. In a home environment any user can play the role of administrator. Among the ISO/IEEE 11073 family, it is worth highlighting the 11073-20601^{TM}-2014 Optimized Exchange Protocol. This defines a reference model based on an object-oriented paradigm that guarantees extensibility and reusability by defining three different models [10, 11]: Domain Information model (DIM), which characterizes information as a set of objects; service model, which provides primitives (e.g. Set, Get, Action, Event Reporting) that are sent between the agent and the manager to exchange data defined in the DIM; and communication model, which defines the dynamic behavior for each connection by means of a finite state machine (FSM).

Complementarily, there are several agent specializations (ISO/IEEE 11073-104zz). When the collection of standards is being referenced, the term ISO/IEEE 11073-104zz is used where zz could be any number in the range from 01 to 99, inclusive. The agent specializations have been grouped in the domains of Disease Management ($zz \in [00, 39]$) —e.g. glucose meters—, Health and Fitness ($zz \in [40, 69]$) —e.g. cardiovascular fitness monitors— and Independent Living ($zz \in [70, 99]$) —e.g. medication monitors. It is worth noting

that while Health, Fitness and Independent Living applications are mainly intended for user self-control of his/her health condition —which can be based on maintaining a PHR and a supervision by means of an alarm system—, Disease Management applications usually require some degree of medical supervision —which can be based on the connection to an EHR, CDSS and/or alarm system. Therefore, these applications demand integration capabilities and security requirements. X73PHD does not address the former and, regarding the latter, only a few aspects can be considered as security-related features:

- User identification: The conditional attribute PersonID may be used to differentiate persons. As a conditional attribute, agents may not support this feature. This attribute is vendor-dependent and is modeled as a 16-bit unsigned integer. In any case, the process of mapping this ID to a specific person is outside the scope of the standard.

- Device identification and authentication: In X73PHD, managers are not identified. Agents include the mandatory attributes System-ID, which is an IEEE EUI-64, and System-Model, which contains the manufacturer's name and the manufacturer's specific model information. Neither of these, however, is used by X73PHD to complete a mutual agent-manager authentication. They are only used to discern different agents in a manager and, eventually, to speed up the configuration process of known agents. Nonetheless, the underlying transport technology may implement its own procedure for secure device pairing.

- Time coordination: In X73PHD, agents shall implement a way of reporting the time when measurements were taken if the measurements delivered by the agent are not "freshly acquired". Timestamps are mandatory when the measurements come from the temporary storage of the agent —the PM-store.

- Encryption: X73PHD does not define any encryption mechanism. However, data may travel encrypted if such a feature is implemented by the lower layer transport technology.

Furthermore, a healthcare framework (see Figure 1-B) commonly includes manufacturers of agents and/or managers; certification authorities; and Health Information Systems (HIS) with components such as PHRs, EHRs, CDSS or alarm systems. IHE is a non-profit organization engaged in improving the way such systems share information. As a result of its activity, IHE has defined several integration profiles that would solve most of the security issues of X73PHD and that would improve interoperability with different healthcare systems:

- *Rosetta Terminology Mapping (RTM).* This defines a vendor-neutral harmonized mapping for patient

care device observations based on ISO/IEEE 11073-10101 nomenclature terms and Unified Code for Units of Measure (UCUM), to facilitate the syntactic —and to some extent semantic— interoperability between devices and systems.

- *Consistent Time (CT).* This provides the means to guarantee that the system clocks —also time stamps and authentication logs— of the devices in a network are synchronized.

- *Device Enterprise Communications (DEC).* This profile —dependent on CT— enables consistent communication between a Patient Care Device and other systems, such as CDSS or EHRs. This communication may include physiological data (e.g. heart rate, patient weight), point-of-care laboratory tests (e.g. home blood glucose tests), continuous data (e.g. electrocardiograms (ECGs)) —but without addressing real-time operation—, patient information and contextual data. The current profile does not address issues of privacy, security and confidentiality associated with cross-enterprise communication of personal measurements. However, it strongly recommends the implementation of IHE compliant transactions for automated acquisition of patient ID credentials —e.g. by means of bar codes (BC) or radio frequency identification tokens (RFID-T)— since this is considered a key process in medical device communication and reporting for reducing errors, increasing user safety and enhancing device and drug effectiveness.

- *Alert Communication Management (ACM).* This profile —an extension of DEC— permits a Patient Care Device to send the notification of an alert to a portable device. This alert may be a physiological alarm (e.g. heart rate out of the safe range for a patient) for a caregiver, a technical alert (e.g. ECG leads off the patient) or advisories not related with an alarm.

- *Waveform Content Module (WCM).* This profile —optional for DEC and ACM— provides the semantics and the data structure (based on the IEEE 11073 Domain Information Model) to enable the transmission of waveforms acquired by Patient Care Devices (e.g. electrocardiograms) to the IHE actors involved in the DEC and ACM profiles. These waveforms can be provided as bounded waveforms, snapshots associated with a diagnostic encounter or with an alarm event; or as continuous waveforms to be used for remote real-time monitoring.

- *Audit Trail and Node Authentication (ATNA).* This profile —dependent on CT— enforces personal health information integrity, confidentiality and user accountability by implementing local user authentication in the nodes of the health IT infrastructure (e.g. based on username and password, biometrics,

smart cards or magnetic cards), connection authentication between communicating nodes and audit trails

- *Cross-Enterprise Document Sharing (XDS).* This profile —dependent on ATNA and CT— provides standard-based means for managing the sharing of documents between any healthcare organization.
- *Enterprise User Authentication (EUA).* This profile —dependent on CT— enables centralized user authentication management —compliant with ATNA— and provides users with reliable and fast single sign-on, which can be based on passwords, tokens, smart-cards and biometrics.
- *Patient Identifier Cross Referencing (PIX).* This profile —dependent on CT— provides interoperability when cross-referencing patients among different systems.
- *Basic Patient Privacy Consents (BPPC).* This profile —a supplement of XDS— permits patient privacy consent(s) to be recorded so that patients can selectively control the access to their healthcare information, and defines a mechanism to enforce this policy.

2.2. Related publications

To the best of our knowledge, four publications address to differing extents the enhancement of X73PHD security. [15, 16] implement and discuss modified agent-manager association procedures, based on mutual challenge-response authentication —a certificate-based authentication method cannot be implemented since the agent has no direct means to check the validity of a certificate. The former uses the RSA2048 algorithm to perform digital signatures —to timestamped challenges—, which introduces high overheads, and implements the USB Personal Healthcare Device Class for secure transmission. The latter derives a biometric key from the user fingerprint, obtaining an insufficient 80% success rate. The third approach, [17], focuses on low-powered PHDs. It proposes either including the sending date and time in the initial association frame of X73PHD and encrypting it partially —to hinder replay attacks and obtain certain privacy—, or encrypting the whole message and attaching an authentication code —for integrity control. Nonetheless, several forms of attack could still thrive —e.g. user impersonation or device hacking. The fourth approach, [18], handles both agent-manager authentication and encryption by means of a complex architecture, relying on either Device Profile Web Services —for hospitalary and domiciliary setups— or the Bluetooth Health Device Profile —for high-mobility scenarios. This proposal includes global IDs for medical devices, the involvement of authorities beyond the manager, the administration of many cryptographic keys and the attachment of timestamps to verify their validity. However, it does not analyze the implications of this proposal on the

X73PHD models and on its framework, and it lacks details for an implementation based on the proposal. Moreover, none of these four works is grounded on a thorough risk assessment of X73PHD or consider coordinating this standard with certain IHE profiles (see Section 2.1), which would increase the usefulness of PHDs within the healthcare ecosystem. On the other hand, [19] addresses the latter issue, but without proposing any specific security enhancement for the X73PHD and presenting a unique solution that limits the communications of X73PHD-compliant devices to PHR systems only.

3. Methods

This section describes the methods developed in this research, comprising an assessment of the risks of the X73PHD architecture (Section 3.1), a cost-effective layered structure to provide support to the X73PHD domains and cope with the security and integration needs of different eHealth and mHealth applications (Section 3.2), a proposal of appropriate IHE profiles to implement each layer (Section 3.3), its translation into detailed modifications of the X73PHD models and its framework (Section 3.4) and a study of optimal algorithms to implement the cryptographic functions that would enhance the security of X73PHD (Section 3.5).

3.1. Risk assessment

The X73PHD architecture, illustrated in Figure 1-A, involves several entities that need to cooperate in order to acquire and transmit the biomedical measurements of the user. Although the transport technologies used to communicate between agent and manager may implement security, there is uncertainty about the actual identities of the user, agent and manager. This extends to a lack of reliability about the provenance and integrity of commands and data transmitted along this framework. Various threats may cause loss, corruption or theft of the measurements, thus endangering the health and the privacy of the user. To address these issues, the hot spots in X73PHD architectures based on the current version of the standard —which may optionally implement means to identify the user and/or rely on secure transport technologies— shall first be analyzed. The following potential risks have been compiled from a couple of reference publications on the matter; [20] covers the topic of security in e-governance whereas [21] specifically deals with the eHealth scenario.

- Users: If the agent does not support the personID attribute, it is hard or impossible to differentiate the measurements of different users. When this attribute is supported, simple methods to distinguish users (e.g. a push button, a keyboard) do not authenticate them. Even if some user authentication method is

implemented, an attacker may try to impersonate users by using open sessions or stolen credentials —e.g. shoulder surfing users' passwords, stealing the user access token, faking the biometric recognition of the victim. If the purpose is causing denial-of-service (DoS), introducing wrong passwords several times might be enough. Finally, those measurements of the user acquired outside the hospital and not digitally signed may later be repudiated by medical entities.

- Agents: A counterfeit/hacked medical device may forward the gathered measurements and/or the user identity credentials to an unauthorized manager. Besides, if the agent stores the measurements provisionally (e.g. in the case that the connection with the manager is temporarily unavailable), an attacker may attempt to establish a local access to retrieve them —from the disk or from the RAM memory. A third possible misconduct, which may affect the user follow-up, is to reprogram the device to deliver fake measurements when using it. Finally, in setups with several agents and managers (e.g. hospitals), an agent may wrongly send the measurements of a user to a manager that was not intended to receive them.

- Agent-manager communication: This is especially sensitive in the case of wireless technologies because of the easy access to the physical medium, which brings several opportunities to attackers. First, they may attempt to inject their own commands in the agent-manager communication and eavesdrop the exchanged frames to obtain measurements. If the communication relies on a secure transport technology, frames are encrypted and authenticated. Cracking the keys used for encryption, authentication or signature usually requires a very significant effort, but less so when the keys are too short, used over long periods of time or for several purposes (e.g. encryption and signature). In the absence of counters or timestamps, attackers may perform replay attacks to inject encrypted frames that have been eavesdropped and it is known that correspond to certain commands. Another possibility is to perform a man-in-the-middle attack: the attacker associates with the agent and manager, even negotiating encryption with each one, to inject commands and obtain measurements without restrictions. On the other hand, injection of noise can be used to disturb the communications and cause DoS.

- Manager(s): A counterfeit/illegitimate manager may attempt to associate to one or several agents to obtain both measurements that they store and measurements that they will acquire in future sessions. Besides, a legitimate manager temporarily storing measurements may also be a target of hacking attacks (e.g. code injection) to corrupt those data, or to steal the data via local access —from the disk or from the RAM memory. Finally, it must be guaranteed that the access to the acquired measurements

is limited to authorized users (e.g. the physicians that supervise a patient) and systems.

3.2. Additive, layered structure

The eHealth and mHealth applications for which X73PHD is currently intended to provide support —grouped in the domains of Health and Fitness, Independent Living and Disease Management— require different levels of security and interoperability with healthcare systems (see Section 2.1). Furthermore, in a real-world market, users expect to have a choice ranging from cheap devices (intended only for basic home monitoring) to increasingly more expensive devices (those which include more dynamic and secure uses). An additive, layered approach is thus a reasonable and cost-effective manner of providing varying enhanced security and interoperability levels for different mHealth applications in a gradual manner. The following bottom-up layered structure would provide a specific solution for the applications of the different domains —and its associated X73PHD agent specializations, see Section 2.1— within a general policy.

- Layers 0.x — intended for simple applications (e.g. basic monitoring) not requiring integration with PHRs, EHRs, alert managers or CDSS —and thus with low security demands.
  - Layer 0 — to be used when taking health measurements in cabled setups.
  - Layer 0.5 — to be used when taking health measurements in wireless setups.
- Layers 1.x — intended for applications which may require integration with PHR systems and alert managers (typically belonging to the domains of Health, Fitness and Independent Living) — and thus with medium-high security demands.
  - Layer 1.0 — to be used when users own their personal devices/equipment.
  - Layer 1.5 — to be used when users share the devices/equipment.
- Layers 2.x — intended for applications which may require integration with EHR systems, alert managers or CDSS (typically belonging to the Disease Management domain) —and thus with high-very high security demands.
  - Layer 2.0 — oriented to patient emergency monitoring and in-hospital care.
  - Layer 2.5 — intended for patient remote monitoring, follow-up and laboratory tests.

It is worth noting that the security measures and interoperability capabilities of each layer have been fixed by the authors. The examples of assignation of specific mHealth domains to the Layers, however,

Table 1: IHE profiles to be created (dark gray) and implemented (light gray) for the enhancement of security and interoperability with healthcare systems in X73PHD-compliant frameworks

Layers \ IHE profiles	SDO:								RTM	CT	DEC:	+ RFID-T or BC	+ SC	ACM	WCM	ATNA	XDS	EUA:	PIX	BPPC
	CBA	SRC	SEC	UID	CMA	MV	UDS	SST										RFID-T or SC		
Layer 2.5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Layer 2.0	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Layer 1.5	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓			
Layer 1.0	✓	✓	✓					✓	✓	✓	✓			✓	✓					
Layer 0.5			✓																	
Layer 0.0																				

are illustrative. Any user would be able to buy a higher or lower device, according to their needs or the requirements of the specific domain or scenario.

As depicted in Figure 1-A-B, the implementation of these layers would not conflict with the already-existing interoperability between agents and managers, since a manager would still be able to associate and operate with one or more agents simultaneously. The only restriction added is that the layer established for an application needs to be supported by the user, agent(s) and manager involved in the measurements acquisition session. To give an example, if the user uses an identification method which is valid up to Layer 2.0, the agent is compliant up to Layer 1.5 and the manager is compliant up to Layer 2.5, they can all work together using up to Layer 1.5 —therefore, this setup would not be appropriate for Disease Management applications. It is also worth noting that there would be five different ways of accessing the measurements in the manager. In Layers 1.0+, the administrator —that is the user in Layer 1.0— would be able to access all the measurements any time and the automated online processes (e.g. warnings if some measurement is abnormal) as they reach the manager —after validating and decrypting them. Besides, each user would be able to directly access his/her stored measurements whereas authorized professionals (e.g. trainers, physicians) would be able to access the measurements of certain users for professional use (e.g. training monitoring, follow-up of a patient). Additionally, in Layers 2.0+ automated offline processes (e.g. monthly analysis of measurements) would be able to access protected measurements stored in the manager after it associates with the agent(s) that acquired them.

3.3. IHE profiles in each layer

A proposal for the implementation of the layers depicted in Section 3.2 by means of the IHE profiles introduced in Section 2.1 is summarized in Table 1. The entities of the X73PHD-IHE framework that implement each of these profiles are illustrated in Figure 1 —they are connected by arrows labelled with the profile name. In the first place, it is worth highlighting that there is a need for a new IHE profile, tightly bound to ISO/IEEE 11073-20601 and called Secure Device Observation (SDO), whose main aim

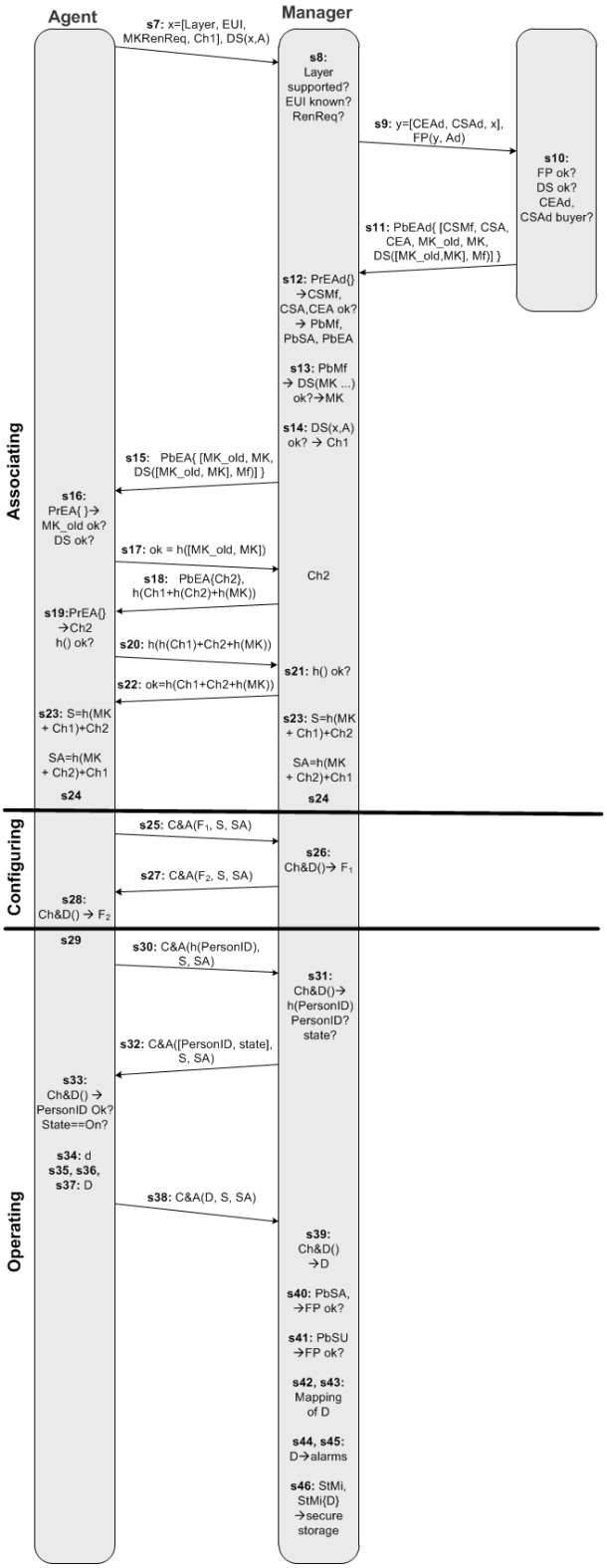

Figure 2: Illustration of a successful first connection between an agent and a manager in Layer 2.5 of the extended X73PHD.

is providing appropriate levels of security in the agent-manager association, configuration and operation to enable the secure acquisition of user measurements (DEC), alerts (ACM) and waveforms (WCM). The security countermeasures defined by SDO, intended to prevent the risks analyzed in Section 3.1, may be divided into challenge-based agent-manager authentication —CBA, enhancing the proposals in [15, 16, 18]— , secure setting and renewal of cryptographic elements (SRC, to hinder key stealing and/or cracking), secure communications (SEC, encrypted and authenticated), user ID capture (UID, to be attached with the user's measurements to prevent its loss), controlled measurements acquisition (CMA, to prevent user impersonation and acquisition of measurements by unauthorized agents and/or managers), measurements verification (MV, to check that they come from a rightful agent), user's digital signature (UDS, to be attached with the user's measurements to prevent their repudiation by medical entities that did not acquired them), and secure standard storage (SST, to hinder the stealing of measurements or their corruption by means of local access).

Regarding already-defined IHE profiles, Layers 1.0+ implement RTM, CT, DEC, ACM and WCM mandatorily since they are essential for supporting the communication of online measurements —in a comprehensive format— and alarms sent from the manager to healthcare systems (and/or to a PHR stored in the manager, based on HL7 PHMR). Layers 1.5+ also add the use of RFID-T or BC (in the agent) to capture the personID of the user whose measurements are to be acquired, ATNA and XDS so that both online and offline measurements (coordinated by DEC/WCM instead of by XDS in the former case) can be transferred with security to healthcare systems. In addition to this, Layers 2.0+ implement three profiles related with the medical context, PIX to enable patient cross-referencing (e.g. in case a user has several identifiers), EUA to enable single sign-on authentication —using a RFID-T or a SC— and BPPC to record and apply the consent of the patient to the authorization policies. Finally, Layer 2.5+ includes the use of SC in the agent, so that these devices can attach digital signatures of the user to his/her measurements, preventing their repudiation when they are acquired out of the hospital.

3.4. Suggested modifications in the X73PHD-IHE framework

This section depicts in greater detail the extended X73PHD-IHE framework and also the role of the entities involved in the implementation of the IHE profiles included in the different layers —see Section 3.3. Focusing first on the enhancement of the X73PHD architecture, the series of steps proposed to carry out this task —by including compliance with the SDO, DEC, ACM, WCM and RTM profiles— are defined in Table 2, and related with the layer(s) that implement it and with the corresponding IHE profile(s). Furthermore, an example with the steps of the first connection between an agent and a manager in Layer 2.5 is included in Figure 2. Regarding the peripheral processes that integrate the X73PHD-IHE framework, the manufacturing

and initial configuration of the devices are addressed in Table 2, and the local consultation of measurements and the forwarding to the appropriate healthcare systems —according to the illustration in Figure 1— are guaranteed through the implementation of the IHE profiles listed in Section 2.1 in the manner described below.

- *CT*: The manager shall connect, as time client, to a NTP/SNTP server to obtain the current time.
- *DEC and WCM*: The manager shall act as the Device Observation Reporter, which forwards the acquired measurements to Device Observation Consumers, such as PHR, EHR or CDSS, by means of a subscription mechanism that enables their filtering by means of Device Observation Filtering actors.
- *ACM and WCM*: The manager shall act as the Alert Reporter —whose alerts may have their origin in the agent— communicating with an Alert Manager which notifies Alert Communicator(s) such as the smartphone of the administrator —e.g. for advisories regarding security issues—, or nurses and next of kin —for physiological and technical alarms.
- *ATNA*: The manager and the healthcare systems (e.g. PHR, EHR, CDSS, alert system) shall implement a secure node, so that they can authenticate users and authorize them to consult stored measurements. The events of acquisition of measurements —as they reach the manager, PHR, EHR, CDSS or alert system— and access of users to them are recorded in an audit repository to which these entities connect to.
- *XDS and BPPC*: When the manager stores the measurements acquired by agents as documents, it may become a XDS-compliant Document Source for PHR and EHR systems that shall implement a Document Repository for persistent, secure and reliable storage. Both PHR and EHR systems may implement a Document Registry to facilitate easier retrieval of these documents for Document Consumers (e.g. a CDSS). BPPC shall be implemented by XDS actors to implement policies of private access based on user consent, that is to say, a type of access to personal biomedical data that is constrained by the consent of the user.
- *EUA*: The manager shall act as a Client Authentication Agent, which connects to a centralized Kerberos Authentication Server of the HIS to get user authentication —based on either RFID-T or SC— and service tickets, enabling further kerberized secure communications. In addition, a specific system filters any meaningful command that a malicious user may try to introduce as a password through the Authentication Agent.

- *PIX*: The HIS takes the role of Patient Identity Source —providing patient identity feed based on the users demographic data and on his/her personID (e.g. extracted from RFID-T, BC or SC), which is registered as patientID—, and also the role of PIX Manager —in charge of the cross-referencing— and the entities with access to user measurements (e.g. PHRs, EHRs, CDSS, alert systems) shall act as PIX Consumers —for homogeneous referencing.

3.5. Suggested algorithms for the SDO profile

Various alternatives are available for performing the cryptographic functions required by the IHE profile (SDO) proposed to extend the security of ISO/IEEE 11073-20601 —see Table 2. Those showing the best balance between security, complexity, overhead and free availability of the algorithm will be recommended. To assess security we follow the recommendations of the NIST [22] about long term use (> year 2030) and crypto periods (time span during which a key is authorized for use), and give priority to algorithms not usually implemented by the transport technologies. This practice, implementing the same cryptographic functions at different levels with different algorithms, minimizes the risk of attacks based on the vulnerability of some specific algorithm. The time complexity of the candidate algorithms [23] is estimated in cycles per operation (e.g. digital signature) or cycles per byte (e.g. in encryption), which is directly related with energy consumption and with delays, two major issues in BAN/PAN architectures [24]. With respect to space complexity, it is estimated by means of the overheads introduced, regarded as a fixed amount of bytes when calculating security items (challenge, hash, HMAC, DS or FP) and an estimation (half block length) when performing encryption, since the latter case is due to the addition of padding bytes to fit the cipher block length. It is worth noting that the overhead introduced by the algorithms will also have an impact on the energy consumption and delays of the architecture that implements them (due to the transmission of extra bytes) and hence on the demand of more powerful processors to enable real-time transmission. Finally, it is checked whether the algorithm is standard, under any restricting license, and if there are reliable free implementations available. This proposal includes the following:

- Symmetric encryption: Twofish [25], which is a suitable supplement to the Advanced Encryption Standard (AES [22]), usually implemented by secure transport technologies. This algorithm, designed by Bruce Schneier, was in fact one of the five finalists to become the AES [26], together with MARS, RC6 [27], Rijndael (chosen) and Serpent [28]. It can be considered very secure (third most voted after Rjindael and Serpent) and pretty fast (29.4 cycles/B), although slower than Rijndael (28.6 cycles/B) and RC6 (17.3 cycles/B). Regarding overheads, the three produce the same since their block size and

Table 2: Steps for a successful first connection between an agent and a manager in the extended X73PHD

Step	Layer(s	Entity	Action(s)	IHE profile(s)
State: processes of device(s) manufacturing and initial configuration (related to X73PHD framework)				
1	1.5+	Mf	Providing the agent with a BC reader and a passive RFID sensor, and each user with a BC or RFID-T —e.g. as bracelets, as personal cards.	SDO, DEC, ACM
	2.0+		Providing the manager with a RFID sensor and a SC reader	EUA
	2.5		Providing the agent with a port that enables the attachment of a SC reader with its corresponding keypad.	SDO, DEC, ACM
2	1.0+	Mf	Generating, signing and holding the CEA and CSA certs of the agent. These contain the agent's EUI-64, and respectively, its public encryption key, PbEA, or its public signature verification key, PbSA. CEA and CSA are stored in a public repository and their paired private keys, PrEA and PrSA, are stored inside the agent.	SDO:SEC
3	1.0+	Mf	Repeating the actions of step 2 in the manager —if off-the-shelf— with CEM (only in Layers 2.0+) and CSM.	SDO:SEC
		Ad	Repeating the actions of step 2 in the manager —if not off-the-shelf— with CEM (only in Layers 2.0+) and CSM.	
4	1.0+	Ad	Installing the admin's CEAd and CSAd certs, bundled with their password-protected private key, in the manager.	SDO:SEC
5	1.0+	Ad	Based on the consent of the users, implementing a XACML-based policy setting which users (e.g. trainers, physicians) can access the measurements of others (e.g. clients, patients) after authentication (with password in Layer 1.0, with RFID-T/SC in Layers 1.5+).	EUA, ATNA, BPPC, SDO:SST
	1.5+		Configuring the manager to establish the RFID-T/BC of the users from which it is allowed to receive measurements.	SDO:CMA
	2.5+		Storing a copy of the public encryption cert (CEU) of the users from which it is allowed to receive measurements.	SDO:CMA
6	0.5+	Ad	Pairing/associating agent and manager with authentication (e.g. PIN, passkey, NFC) if the chosen transport technology supports it.	SDO:SEC
State: associating with authentication process (related to X73PHD standard)				
7	1.0+	A	Negotiating a security layer and launching its EUI (the manager may have requested it) together with a fresh challenge, Ch1. Signing this frame, x, with PrSA —to enable further verification— and sending it to the manager.	SDO:CBA
8	1.0+	M, A	The manager receives the frame and checks whether the security layer is supported. If it is not supported, the agent will attempt to establish an association with lower security requirements in s24. If the proposed security is supported, the manager consults its association table to check if there has been previous association to that EUI. If so, the manager knows MK and goes to step 14 —unless if frame x contains a request to renew some key or cert.	SDO:CBA
9	1.0+	M	Sending a frame to the agent's manufacturer, including the administrator's certificates CEAd, CSAd and x (from s7), concatenated with the admin's fingerprint. To obtain the fingerprint, the admin is required to manually introduce the password of his/her private signature key, PrSAd.	SDO:SRC
10	1.0+	Mf	Verifying the fingerprint of y and the signature of x, and also that CSAd corresponds to the buyer of that agent.	SDO:SRC
11	1.0+	Mf	Sending its certificate CSMf, the agent's certificates CSA and CEA and MK signed by the manufacturer. If x (from s7) contained a renewal request —which happens with a periodicity of 1-3 years—, both the old and the new key/cert requested will be attached and digitally signed. This entire frame is encrypted with the corresponding admin's public encryption key, PbEAd.	SDO:SRC
12	1.0+	M	Decrypting the frame by using PrEAd. Then, verifying the certs by means of CRL or OCSP. If they are not valid, rejecting the connection —by means of a frame in s24— and instructing the admin to contact the agent's manufacturer. Otherwise, PbMf, PbSA and PbEA are obtained.	SDO:SRC, ACM
13	1.0+	M	Using PbMf to verify DS(MK,Mf), both decrypted in the previous step. If it is valid, obtaining MK.	SDO:CBA-SRC
14	1.0+	M	Using PbSA to verify the signature of frame x (from step 7). If it is valid, obtaining the challenge Ch1 and generating its own fresh challenge, Ch2.	SDO:CBA
15	1.0+	M	If x (from s7) contained a renewal request —which happens with a periodicity of 1-3 years—, sending to the agent both the old and the new key/cert requested and its digital signature —by the manufacturer—, all encrypted with its public encryption key, PbEA.	SDO:SRC
16	1.0+	A	Decrypting the frame with its private decryption key, PrEA. Next, checking that the signature of the frame is valid and that the old cert/key is correct.	SDO:SRC
17	1.0+	A	Accepting or rejecting the update of the key/cert (based on the previous step) by means of a frame sent to the manager. Destroying the old key/cert in case of acceptance and sending a warning message to the admin otherwise.	SDO:SRC, ACM
18	1.0+	M	Sending an authentication frame, composed of PbEA{Ch2} and h(Ch1 + h(Ch2) + h(MK)), to the agent.	SDO:CBA
19	1.0+	A	Decrypting Ch2 by using PrEA. Using it, Ch1 and MK to check that the received h(Ch1+h(Ch2)+h(MK)) is valid. Authenticating the manager if the verification is successful.	SDO:CBA
20	1.0+	A	Calculating h(h(Ch1)+Ch2+h(MK)) and sending it to the manager.	SDO:CBA
21	1.0+	M	Authenticating the agent if the verification of the frame received is successful.	SDO:CBA
22	1.0+	M	Confirming the authentication to the agent, by sending the frame h(Ch1+Ch2+h(MK)).	SDO:CBA
23	1.0+	A, M	Deriving session keys for encryption, S = h(MK + Ch1) + Ch2, and authentication, SA = h(MK+ Ch2) + Ch1.	SDO:SRC-SEC
24	1.0+	A, M	Aborting the connection if the certs of the agent are not valid (s12) or to negotiating a lower security layer that both agent and manager support (s8). The frames exchanged between agent and manager from here on are encrypted and authenticated.	SDO:CBA-SRC
State: configuring process (related to X73PHD standard)				
25	1.0+	A	Sending the frame Fi, encrypted with S, to establish the further transmission of measurements. This frame is concatenated with a Hash Message Authentication Code, HMAC(S{Fi}, SA), dependent on both the encrypted frame, and on the session key for authentication SA. The resulting frame, [S{Fi}, HMAC(S{Fi}, SA)], is denoted as C&A(Fi, S, SA), named after "Ciphering & Authentication".	SDO:SEC
26	1.0+	M	Using SA to verify the HMAC of Fi. If it is valid, then the manager deciphers the frame with S and interprets it. This process, inverse to that in s25, is denoted as Ch&D(C&A(Fi, S, SA)) named after "Checking HMAC & Deciphering".	SDO:SEC
27	1.0+	M	Sending the frame C&A(Fj, S, SA) to continue with the configuration process.	SDO:SEC
28	1.0+	A	Using SA to verify the HMAC of Fj.	SDO:SEC
			Steps 25-28 may be repeated several times, until all configuration frames have been exchanged.	
State: data measurement and transmission processes (related to X73PHD standard and its framework)				
29	1.5-2.0	U	Swiping his/her RFID-T/BC through the passive sensor of the agent.	SDO:UID, DEC:RFID-T or BC
	2.5		Inserting his/her SC in the slot of the agent and introducing his/her PIN/password.	SDO:UID, DEC:SC
30	2.0+	A	Applying C&A() to a frame Fi = h(PersonID) and sending C&A(Fi, S, SA) in order to find out if the manager knows the user corresponding to h(PersonID).	SDO:CMA
31	1.5+	M	Applying Ch&D() to the received frame and obtaining Fi = h(PersonID).	SDO:CMA
	1.5+		Checking that the admin had configured a PersonID whose hash is precisely the received h(PersonID). Otherwise, requesting the admin to do it now. If he/she does nothing, rejecting the association.	SDO:CMA ACM
	2.5		Checking that the admin had stored the public certificate whose PersonID hash is precisely the received h(PersonID). Otherwise, requesting the admin to do it now. If he/she does nothing, rejecting the association.	SDO:CMA ACM
	1.5+		If the connection has not been rejected, checking the state of the ID credentials of that user (enabled or disabled). If it is disabled, sending a warning message to both the user and the admin.	SDO:CMA ACM
32	1.5+	M	Sending C&A([PersonID, state], S, SA) to the agent.	SDO:CMA
33	1.5+	A	Calculating Ch&D(C&A([PersonID, state], S, SA)). Subsequently, checking that the PersonID of the user identified in the agent matches the PersonID received from the manager. If the state of the credentials is disabled, the acquisition session is not started, go back to step 29	SDO:CMA, ACM
34	0+	U	Taking his/her measurements "d" by means of the agent.	DEC, WCM
	1.5+	A	Logging off the user 10-seconds after he/she takes his/her last measurement.	SDO:CMA
	0+	A	Going back to step 29 to begin a new acquisition session —unless agent and manager were disassociated for some reason.	SDO:CMA
35	1.5-2.0	A	Adding the PersonID, provided by his/her RFID-T or BC, to d. D= [d, PersonID].	SDO:UID, DEC: RFID-T or BC, WCM
	2.5		Adding the user's fingerprint, provided by his/her SC, to d. D= [d, FP(d, U)].	SDO:UID-UDS, DEC:SC, WCM
36	1.0+	A	If it does not know the user (checked in step 31), generating a symmetric key for storage, StAi, calculating and storing StAi{D} and PbEM{StAi} in the PM-Store. Next, wiping properly the variables and buffers storing the plain D and StAi, and going back to step 29.	SDO:SST
37	2.0+	A	Adding its own fingerprint to D, D=[D, FP(D,A)]	SDO:MV, DEC, WCM
38	1.0+	A	Sending C&A(D,S,SA) to the manager.	SDO:SEC, DEC, WCM
39	1.0+	M	Calculating Ch&D(C&A(D,S,SA)).	SDO:SEC, DEC, WCM
40	2.0+	M	Verifying the agent's fingerprint in D with its associated public signature verification key, PbSA. If it is not valid, refusing D.	SDO:MV, DEC, WCM
41	2.5	M	Verifying the user's fingerprint in D, with its associated public signature verification key, PbSU. If it is not valid, refusing D.	SDO:MV, DEC, WCM
42	2.0+	A	If steps s38 or s39 fail, getting notified and storing D in the PM-store, as in step 33 —the data rejected. Instructing the admin to check the certificates CSA and CSU, and rejecting the association.	ACM
43	1.0+	M	Mapping the acquired measurements D for its representation with IHE-harmonized syntax and semantics.	RTM, DEC, WCM
44	1.0+	M	The measurements D are readily available for applications that need to process them online (e.g. real-time displaying).	
45	1.0+	M	Generation of physiological alarms, if the value(s) of D are far out of a healthy range (e.g. systolic blood pressure $\geq$ 180 mmHg, the user did not take several pills of his/her medications), and also technical alarms, if the values of D are inconsistent (e.g. constant zero).	ACM, WCM
46	1.0+	M	Secure standard storage of D:	SDO:SST
			Creation of a symmetric key StMi for encrypting StMi{D} of D.	
			Storage of StMi{D} in a HL7 Personal Healthcare Monitoring Report (PHMR).	
			Wiping properly the variables and buffers storing the plain D and StMi.	
			The securely stored D are available for those users authorized by the XACML policy —implemented in step 5— after an authentication process that will filter any attempt of code injection.	

key length are equally set to 128 bits. The main advantage of Twofish over RC6 is that the former has not been patented and has a reference implementation in the public domain. Symmetric master keys (MK) will be renewed every year. Symmetric keys for encrypting frames, S, will be renewed every session and symmetric keys for encrypting stored data have a single use. If Twofish were to be compromised in the future, we would recommend Serpent as a replacement.

- Asymmetric encryption: RSA2048 [29] is the algorithm recommended for the exchange of master secrets, which supplements DH/ECDH [30], implemented by most secure transport technologies. RSA and elGamal [31] are the alternatives, the former is preferred for being standard and less similar to DH. Nonetheless, RSA2048 introduces more overheads than ECDH (block length 2048 bits vs 256) and performs more slowly (11.41 Mcycles vs 5.17). Asymmetric encryption keys will be renewed every 1–2 years. If RSA were to be compromised in the future, we would recommend elGamal as a replacement.

- Challenges generation: The standardized SHA-512 [32], which produces longer challenges (512 bits) than other hash functions and ciphers, and thus reduces the possibilities of repetitions. Besides, it does not imply extra overheads since challenges are protected with RSA2048, resulting in 2048 bits regardless of the fact that the initial length is less. Another advantage is its performance (17.7 cycles/B), very close to the fastest cipher (RC6, 17.3 cycles/B). To obtain a challenge, a secret seed stored in the device is concatenated with the current time (at its maximum resolution) and hashed. If SHA-512 were to be compromised in the future, we would recommend Whirlpool [33] as a replacement.

- Hashing: RIPEMD-256 [34], which performs faster (11.1 cycles/B) than other reference functions such as SHA-256 [32] (15.8 cycles/B) or Whirlpool (30.5 cycles/B). RIPEMD-256 and SHA-256 introduce less overhead than Whirlpool [33] (512 bits), fulfilling the recommendation of the NIST (256 bits). Although Tiger operates faster (8.1 cycles/B), its key length (192 bits) is not secure enough. RIPEMD-256 will never be patented and reference implementations can be found in the public domain. If RIPEMD-256 were to be compromised in the future, we would recommend Whirlpool as a replacement.

- HMAC with counter: The standardized Secure Hash Algorithm (SHA)-1 [35] is sufficient to implement these codes, since they do not need to be as secure as regular hashes. Part of the original content, a key SA, is unknown to the attacker, which minimizes the odds of finding collisions. Among the SHA family of standards, SHA-1 is the fastest (11.9 cycles/B) and most compact (160 bits). The counter is a 2-byte number, used to avoid a replay attack by re-sending frames gathered from the current session. SA will be renewed every session.

- Digital signature, fingerprints and certificates: The standardized Elliptic Curve Digital Signature Algorithm (ECDSA) 256 [36], which performs signature-verification slightly faster (3.92-6.56 Mcycles) than the other two algorithms authorized by the NIST, DSA [37] and RSA [29] with 2048-bit key length. DSA was replaced by ECDSA because the latter operates with smaller numbers, and thus it is hard to find implementations of DSA supporting 2048 bits. On the other hand, RSA2048 has a similar overall performance (11.06-0.29 Mcycles), but ECDSA produces a much shorter signature (512 bits vs 2048) with a roughly similar security level. Digital signature keys will be renewed every 1–3 years. If ECDSA were to be compromised in the future, we would recommend DSA as a replacement.

4. Results and Discussion

This section analyzes the implications that the proposals in Section 3 would have for X73PHD (Section 4.1) and for IHE (Section 4.2). In addition, the performance of the X73PHD extension is evaluated by analyzing the countermeasures that each security layer implements against different threats (Section 4.3) and also by measuring the impact that each layer produces on the X73PHD architecture, in terms of overhead and delays, and on its surrounding framework (Section 4.4). Finally, the potential limitations of this proposal are summarized in Section 4.5.

4.1. Implications for X73PHD

The implications that the proposal suggested in Section 3.4 would have for X73PHD can be seen through the modifications involving its service, communication and domain information models. This is mainly illustrated in Table 3 —service model and, eventually, DIM— and Figure 3 —communication model and, incidentally, service model. The four columns on the left in Table 3 show the four modified and four newly-created frames to meet the proposals suggested in Section 3.4. The modified frames and attributes are shown in shaded cells, while the newly created ones appear in unshaded cells. Additionally, an explanation of the frame or attribute can be found in the second to the right column, which is linked to the proposals in Section 3.4. The layers involved in every modification are shown in the far right column. A few of them are required only in Layers 2 and 2.5. Regarding the —MDER [6]— data types of the attributes, those with a fixed numeric value —indicated between brackets— are INT-U16, and the rest of them —hashes, HMACs, FingerPrints, etc.— are OCTET STRING. The types CHOICE and SEQUENCE (concatenation) are used to represent the combination of two or more attributes.

Similarly, a complementary illustration of the implications is provided in Figure 3. The figure shows a conveniently modified FSM of both agents and managers. Thus, it includes the existing states frames and

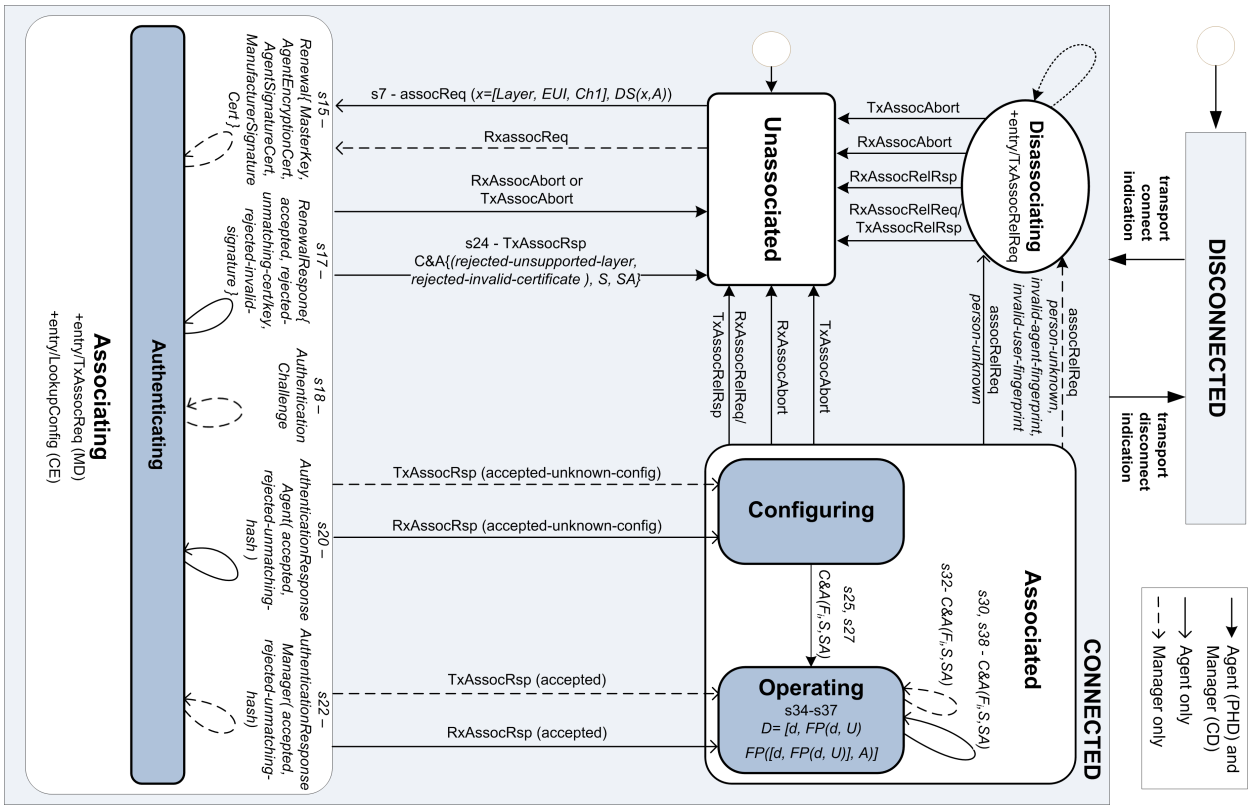

Figure 3: Proposed FSM for both agents and managers, including the state frames and attributes existing in the current approved version of X73PHD, along with the newly suggested sub-state (authenticating sub-state) and the new frames and attributes.

Table 3: Generic structures (lightly shaded cells), modified (shaded cells) and newly created (unshaded cells) frames and attributes in the extended X73PHD

Frame	Sub-Frame (level 1)	Sub-Frame (level 2)	Sub-Frame (level 3)	Additional information	Security Layers
AarqApdu	PhdAssociationInformation	ProtocolVersion	protocol-version4(3)	This bit shall be set if the extended version of 11073-20601 is supported.	0+
		option list	RegCertDataList	It is recommended adding auth-body-IHE(3) to the AuthBody compliance list.	0+
		Layer		This indicates the layer of the extended version of 11073-20601.	0+
			zero(0)		0+
			zero-and-a-half(1)		0+
			one(2)		0+
			one-and-a-half(3)		0+
			two(4)		0+
			two-and-a-half(5)		0+
		RenewalRequest		Request to renew z, the master key and/or certain certificates, {MK, CEA, CSA, CSMf}.	1+
			MasterKey(0)		1+
			AgentEncryptionCert(1)		1+
			AgentSignatureCert(2)		1+
			ManufacturerSignatureCert(3)		1+
		Challenge 1		This is the agent-to-manager challenge, Ch1.	1+
	DigitalSignature			Signature by the agent, DS(PhdAssociationInformation, PrSA).	1+
RerqApdu				This is a manager-to-agent frame, encrypted with the public encr. key of the agent, PbEA.	1+
	Renewal{MasterKey, AgentEncryptionCert, AgentSignatureCert, ManufacturerSignatureCert}			[z_old, z]. Purpose: updating an old key/certificate with a new one.	1+
	DigitalSignature			Signature by the manufacturer, DS(Renewal{...}, PrSMf).	1+
RereApdu				This is an agent-to-manager frame.	1+
	ResultRenewal{MasterKey, AgentEncryptionCert, AgentSignatureCert, ManufacturerSignatureCert}		accepted	h([z_old, z]). Purpose: to approve the update of a key/cert.	1+
			rejected-unmatching-{key/cert}	h([z, z_old]). Purpose: to reject the update of a key/cert, z, because the value of the current key/cert in RerqApdu, z_old, was not correct.	1+
			rejected-invalid-signature	h([z, z_old, z_old]). Purpose: to reject the update of the key/cert because the signature in RerqApdu was invalid.	1+
AucApdu	AuthenticationChallenge			This is a manager-to-agent frame. It contains the manager-to-agent protected challenge, PbEA{Ch2}, concatenated with h(Ch1+h(Ch2)+h(MK)). Purpose: to allow the agent verify that the manager knows MK.	1+
AurApdu				This could be both an agent-to-manager and a manager-to-agent frame.	1+
	AuthenticationResponseAgent			This is an agent-to-manager frame, based on hashes to hinder its manipulation.	1+
			accepted	h(h(Ch1)+Ch2+h(MK)). Purpose: to verify positively AucApdu.	1+
			rejected-unmatching-hash	h(h(Ch1)+h(Ch2)+h(MK)). Purpose: to indicate that AucApdu does not match the value calculated by the agent.	1+
	AuthenticationResponseManager			This is a manager-to-agent frame, based on hashes to hinder its manipulation.	1+
			accepted	h(Ch2+1+h(MK)). Purpose: to verify AuthenticationResponseAgent positively.	1+
			rejected-unmatching-hash	h(Ch2+2+h(MK)). Purpose: to indicate that AuthenticationResponseAgent does not match the value calculated by the manager.	1+
AareApdu	AssociateResult			Encrypted with session key S if Layer requires so.	1+
			rejected-unsupported-layer(9)		1+
			rejected-invalid-certificate(10)		1+
	HMAC			HMAC(AssociateResult, SA). Purpose: to authenticate AssociateResult.	1+
RlrqApdu	ReleaseRequestReason			ReleaseRequestReason travels encrypted with session key S if Layer requires so.	1+
			person-unknown(3)	This could be both an agent-to-manager and a manager-to-agent frame. Purpose: it is sent by the manager when it does not know the person to whom the data pertain, and by the agent when it checks that the manager does not know that person.	2+
			invalid-agent-fingerprint(4)	This is a manager-to-agent frame. Purpose: to indicate that the agent's fingerprint is invalid.	2+
			invalid-user-fingerprint(5)	This is a manager-to-agent frame. Purpose: to indicate that the the user's fingerprint is invalid.	2.5
	HMAC			HMAC(ReleaseRequestReason, SA).	1+
PrstApdu	DataApdu			DataApdu travels encrypted with session key S if Layer requires so.	1+
		Message	personID	If Layer $\leq$1.0, this is the PersonID as defined in 11073-20601^{TM}-2014 (16b). If 1.5 $\leq$ Layer $\leq$ 2.0, then PersonID takes the same value as the EUI-64 RFID-T/BC (64b). If Layer == 2.5, then PersonID is the Subject Unique Identifier of the X.509 CU (64b).	1+
			knownPerson	This is the hash of PersonID in agent-to-manager frames and PersonID otherwise.	2+
		FingerPrint		This is necessary if measurement data are present inside the frame.	2+
	Counter and HMAC			HMAC(DataApdu, SA).	1+

attributes, along with the newly suggested sub-state (authenticating), and the new frames and attributes. The links between the new frames and the steps (noted as sX and suggested in Table 2) are also shown in Figure 3. To differentiate existing and newly proposed states, frames and attributes, the latter are written in italics.

The creation of additional DIM attributes supporting the new security features could be useful for better modeling of PHDs. However, this is not imperative because not all transmitted information is modeled in the DIM. For example, within the PhdAssociationInformation frame, there is the ProtocolVersion information which is used to communicate acceptable X73PHD versions. ProtocolVersion is not modeled in the DIM, even though it provides information of what the agent is. The newly proposed Layer provides comparable information and therefore, according to the DIM definition it could be incorporated to the DIM but not necessarily. Similarly, in the PhdAssociationInformation frame, the RenewalRequest —defining requests to update some important keys or certificates— and the Challenge 1 could be added to the DIM if a new, security-enhanced version of the standard were to be created, but not compulsorily.

4.2. Implications for IHE and its profiles

The main implication is the suggestion of SDO (see Sections 3.3-3.5), a new IHE profile which would belong to the PCD domain and which would enable a standardized and secure communication in the first segment of DEC (alone or combined with WCM) —from the PCD to the Device Observation Reporter— and ACM (alone or combined with WCM) profiles —from the Alarm Source to the Alarm Aggregator—, which are currently not detailed. The hypothetical integration of SDO in IHE would imply the addition of new advisories in ACM, related with security issues —e.g. invalid certificate, unauthorized user trying to take his/her measurements— and would open up the possibility of recommending the use of the enhanced —SDO-compliant— version of ISO/IEEE 11073 in implementations of DEC, ACM and WCM.

4.3. Security analysis

The security analysis is depicted in detail in Table 4. Columns 1–2 summarize the risk assessment of the X73PHD architecture —as described in Section 3.1— and columns 3–4 the measures against those threats depending on the layer implemented —based on the proposal described in Sections 3.4-3.5. Table 4 shows that the preexisting Layer 0 implements no security and that the preexisting Layer 0.5 puts emphasis only on the secure pairing of devices (which on the other hand might be counterfeits or have been hacked) and on secure wireless communications between them. Layers 1.0+ add security measures to both agent and manager to detect counterfeiting, to impede hacking and undue local access to measurements, and new

countermeasures for private and authenticated communications. Layers 1.5+ include the possibility that several users share agents and managers with privacy, by means of secure identification/authentication with BC/RFID tokens or smart-cards, passwords, automatized user log-off, remote activation/deactivation of identification credentials and checking that the user is known by the manager before he/she takes his/her measurements. In addition, these layers also implement audit trails of measurements acquisition, transmission (e.g. to EHR systems) and access to guarantee data traceability and user accountability. Layers 2.0+ add mandatory timestamps and fingerprints in the measurements for a strengthened verification in the manager. Finally, Layer 2.5 improves the identification of users in the agent (by requiring a smartcard and a password), and includes the digital signature of the user in his/her measurements to prevent their repudiation.

The chosen algorithms, their key sizes and crypto periods are considered secure until 2030, regardless of the layer. Furthermore, the key management policy (described in Section 3.4) is oriented towards Perfect Forward Secrecy. This implies that in the unlikely case that a session key is cracked, the damage is confined to that session and the attacker will only be able to read those frames (if he/she discovers S) or to authenticate forged frames (if he/she discovers SA). To minimize the likelihood that the master key is discovered, it is used only to derive session keys that protect the transmission of frames. But even if at some point an attacker discovers MK and some session keys, frames exchanged in previous sessions will be safe since session keys are derived from MK and another random secret, Ch2, which is protected by the public key of the agent. Finally, the measurements from an acquisition session are protected with symmetric keys of single use protected with asymmetric cryptography.

4.4. Impact on the X73PHD architecture and on its framework

This is evaluated in Table 5 by means of three reference examples, carefully chosen to cover a broad range of information transmission cases when using X73PHD. They have very different frame sizes —which affects the relative overhead— and may require real-time transmission —which is influenced by delays:

- Case 1: sending a discrete measurement, a weight represented with a frame of 36 bytes.
- Case 2: sending a continuous signal, a 3-lead ECG divided into 1-second blocks, sampled at 200 Hz and represented with 16 bits per sample. That is to say, blocks of 9600 bits. It is worth noting that this is a concrete —although rather common— set of parameters for ambulatory ECGs. Nonetheless, ECGs may range from a few seconds —e.g. 10 seconds in a resting ECG test— to several hours —e.g. in a Holter test. Regardless of their duration, the analysis of the features in the transmission of the

Table 4: Analysis of risks in the architecture of the extended X73PHD according to the layer implemented

Hot spot	Threats	Countermeasures	Layer 0	Layer 0.5	Layer 1.0	Layer 1.5	Layer 2.0	Layer 2.5
USER	User impersonation by credential theft or no request of identification/authentication credentials	Use of physical tokens for user identification/authentication				✓	✓	✓
		Use of an additional password for user identification in the agent						✓
		Use of an additional password for user authentication in the manager					Op.	Op.
		Remote activation/deactivation of identification credentials —used in the agent— and user warnings				✓	✓	✓
	User impersonation by using open sessions	User log-off 10s after taking user measurements				✓	✓	✓
	DoS by wrong user identification in the agent	BC/RFID token requested				✓	✓	✓
		Smartcard requested						✓
	Repudiation of user measurements	Including the PersonID attribute with all the measurements				✓	✓	✓
		Including a digital signature of the user in his/her meas.						✓
		Including a timestamp with meas. from agent's PM-store	✓	✓	✓	✓	✓	✓
		Extending the timestamp to freshly acquired measurement					✓	✓
AGENT	Device counterfeiting	Device certificate, signed by manufacturer, requested			✓	✓	✓	✓
		Authentication by manager			✓	✓	✓	✓
	Device hacking to deliver wrong measurements	Fingerprints in measurements					✓	✓
		Manager verifies fingerprints					✓	✓
	Data theft by local access	Asymmetric encryption of the PM-store: decryption possible only in the manager			✓	✓	✓	✓
		Proper wiping of critical variables/buffers			✓	✓	✓	✓
	Sending measurements to a wrong manager	Checking if the user is known by the manager				✓	✓	✓
AGENT-MANAGER	Injection of commands	Secure transport		✓	Op.	Op.	Op.	Op.
		Frames with HMACs			✓	✓	✓	✓
	Cracking of cryptographic keys	Use of secure algorithms, complementary to those of the secure transport layer			✓	✓	✓	✓
		Key sizes recommended by NIST			✓	✓	✓	✓
		Keys are renewed (and the previous ones are destroyed) before expiration or if they are revoked			✓	✓	✓	✓
		Perfect Forward Secrecy			✓	✓	✓	✓
	Eavesdropping	Secure transport		✓	Op.	Op.	Op.	Op.
		Frames encryption			✓	✓	✓	✓
	Replay attack	Secure transport		✓	Op.	Op.	Op.	Op.
		Fresh challenges			✓	✓	✓	✓
		Counter in frames			✓	✓	✓	✓
	Man in the middle attack	Secure device pairing (PIN, PBC, NFC, etc.)		✓	Op.	Op.	Op.	Op.
		Agent-manager authentication			✓	✓	✓	✓
	DoS by injecting noise	HMACs and retrials			✓	✓	✓	✓
		Report to admin, secure storage of meas. in PM-store			✓	✓	✓	✓
MANAGER	Counterfeiting to associate to a rightful agent	Admin and agent's manufacturer authorization requested to operate as manager.			✓	✓	✓	✓
		If ad-hoc device, cert. requested —signed by its manufacturer					✓	✓
		Authentication by agent			✓	✓	✓	✓
	Hacking to corrupt the measurements	Audit trails of measurements acquisition, transmission and access				✓	✓	✓
	Data theft by local access	Single-use keys and asymmetric encryption of measurements: authenticators required for decryption			✓	✓	✓	✓
		Proper wiping of critical variables/buffers			✓	✓	✓	✓
	Access of authorized users to unintended measurements	Role-based access control: regular users, professionals, admin, automatized online and offline applications				✓	✓	✓
	Injection of malicious codes	Command filtering in the authentication system				✓	✓	✓

Table 5: Absolute and relative overhead and delay of the new and modified frames proposed above

Frame(s)	Entity	Case	Original size (b)	Absolute overhead (b)	Relative overhead	Delay (Mcycles)
s7, s8	A, M	1-3	54	16+64+512+512=1104	20.44	3.92
s14, s18	M	1-3	—	2048+256=2304	—	6.86
s19-s20	A	1-3	—	256	—	11.12
s21-s22	M	1-3	48	256-48=208	4.33	>0.01
s23	A, M	1-3	—	—	—	> 0.01
s25/s27	A/M	1-3	var	≈ 128/2+176=240	var	>0.01
s26/s28	M/A	1-3	—	—	—	>0.01
s30	A	1-3	—	256+176=432	—	>0.01
s31-32	M	1-3	26	128-26+176=278	10.69	>0.01
s33	A	1-3	—	—	—	>0.01
s35-s41, s46 — Layer 2.5 —	A, M	1, 2, 3	x= 288, 9600, 516096	1424, 1456, 1456 — ceil((x+2·(64+512)+64)/128)·128+176-x —	4.94, 0.15, >0.01	22.73, 22.86, 29.95
s35-s40, s46 — Layer 2.0 —	A, M	1, 2, 3	Idem	912, 944, 944 — ceil((x+2·64+512+64)/128)·128+176-x —	3.17, 0.10, >0.01	12.25, 12.38, 19.47
s35, s38, s39, s46 — Layer 1.5 —	A, M	1, 2, 3	Idem	272, 304, 304 — ceil((x+64)/128)·128+176-x —	0.94, 0.03, >0.01	0.89, 1.02, 8.11
s35, s39, s46 — Layer 1.0 —	A, M	1, 2, 3	Idem	272, 176, 176 — ceil(x/128)·128+176-x —	0.94, 0.02, >0.01	0.31, 0.44, 7.53

security-enhanced signals at global scale is the same as per each individual signal block when real-time transmission is guaranteed [38]. Therefore, it is necessary to obtain an estimation of the computational power required to guarantee real-time operation.

- Case 3: sending measurement(s) in a frame whose size is the maximum allowed in X73PHD (63 KBytes). In this case, there is no real-time transmission involved. It consists of one large frame being transmitted in one go. It is worth noting that this is an extreme case.

The proposed extension of the protocol consists of 46 steps, described in Section 3.4. Nonetheless, only 16 of these steps introduce some overhead or delay, which are calculated based on the data given in Section 3.5. The results in Table 5 show that the maximum overhead introduced by one step is 2304 bits. Although this can be considered as high (in relative terms) when the original frame is short (e.g. s7), it is almost negligible when protecting ECG signals or long measurements for transmission (Layers 1.0–2.5, cases 2 and 3). It is also worth noting that the relative overhead grows significantly with the layer when protecting short measurements (Layers 1.0–2.5, case 1), varying from 0.94 in Layer 1 to 4.94 in Layer 2.5. This is mainly due to the addition of the fingerprints of the user (s35) and the agent (s37). Regarding delays, each operation has either a fixed delay (a certain amount of cycles) or a variable delay, which depends on the input data size (e.g. in encryption). The latter is calculated by multiplying the speed of the operation and the data size. Some steps involve two or more sequential operations —e.g. those denoted as C&A()— and in that case

their individual delays will be added. Therefore, the cells in the delay column are calculated by summing the delays produced by all operations involved for each row. It is observed that steps s35-s41 contribute most to the overall delay, which grows notably with each layer implemented. Short measurements and ECG signals (cases 1 and 2) obtain similar results (<1 Mcycle in Layers 1.x, about 12 Mcycles in Layer 2.0, about 23 Mcycles in Layer 2.5), while the same evaluation with the maximum frame size (case 3) obtains approximately 7 extra Mcycles.

One of the most demanding real-time application that can currently be supported by X73PHD is the transmission of ECGs, as in our case 2. Table 5 shows an associated delay of 22.86 Mcycles when implementing Layer 2.5, the most secure and complex, to protect the ECG block and access it. On the other hand, real-time ECG applications usually require that the overall delay, starting when the acquisition of the block begins and finishing when the block can be interpreted, is approximately $\leq 2s$ [38]. Since the block length is 1s, there is 1s (disregarding the transmission delay) to execute 22.86 Mcycles in real-time. Assuming that the transport technology introduces low/moderate overhead and that it is able to transmit the protected ECG block (11056 bits) with a negligible delay, it is enough that the agent and the manager operate at approximately 23 MHz. If the manager features a much faster processor (e.g. >1 GHz), which is very typical in smartphones or tablets, the requirement for the agent can be dropped to 9 MHz. This happens because the selected algorithm, ECDSA, performs the signature (in the agent) with fewer operations than the signature checking (in the manager, which is usually a more powerful device). It is worth noting that, for these estimations, the authors have assumed a throughput of 1 MIPS/MHz (1 million instructions per second per megahertz), which is a reasonable ratio in off-the-shelf 8-bit microcontrollers (e.g. the Atmel ATmega328). We have chosen a simple 8-bit microcontroller as reference for the following reasons: a) an 8-bit microcontroller is powerful enough to run an X73PHD agent [39, 40], b) manufacturers of medical devices look for cost-effective implementations, and c) by choosing an 8-bit architecture for the estimations, we are positioned in a scenario with limited processor capability (considering the current state-of-art), i.e. if the architecture is changed (e.g. a manager running in a mobile phone, which has for example an ARM Cortex micro, which is a much more powerful processor), the processor would have a larger MIPS/MHz throughput, which implies the capability of executing more instructions per clock cycle, and so the situation would be more favorable.

Regarding the impact of the X73PHD extension on its framework, a simple initial setup is required. As detailed in Section 3.4, an administrator installs his/her certificate in the manager (s4) and implements a XACML-based privacy policy setting out which users are authorized to take and/or consult measurements

(s5). He/she may also pair/associate the agent and the manager with the most secure method implemented by the transport technology (s6). In addition to this, certain layers of the enhanced X73PHD —see Table 1— demand items to identify/authenticate users —which requires extra hardware—, the implementation of reliable PHRs in the manager and the implementation of IHE profiles to enable communications with healthcare systems. Nevertheless, the proposed enhancement of X73PHD does not hamper the automatic verification, access and processing of the acquired measurements and it would facilitate its integration with PHRs, EHRs and CDSS, and the triggering of alarms at abnormal values. Furthermore, when an authorized user accesses this data with his/her regular software, additional information about its associated features (layer, validity of timestamps and fingerprints) may be displayed.

With respect to the agent implementation, the authors would suggest a programming language featuring a reduced computational load, such as ANSI C. It is worth noting that the delays presented in Table 5 have been calculated based on the results of [23], a speed benchmark of cryptographic algorithms coded in C++. Nevertheless, the programming language choice for the agent implementation falls directly on the developer (or the manufacturer), who would assume the inherent trade-off between scalability/easiness and computational efficiency. Managers, on the other hand, could be developed using a different programming language —e.g. Java in an Android-based manager. Java has the advantages of being highly portable and abstract but it is —generally speaking— less computationally efficient. However, since managers are, at the same time, more powerful devices, their performance would not be greatly affected.

4.5. Potential limitations and future work

Although the proposal presented herein has several advantages over the regular non-extended standard, there are also some challenging caveats to be considered. In the first place, it is necessary to keep track of the discovery of potential vulnerabilities in the security algorithms implemented, so that the compromised algorithms can be replaced with the second options proposed in Section 3.5 (or by new, more secure algorithms that might be created in the future). Also, users of the system have to be appropriately trained in security practices, e.g. choice of strong passwords, remote activation/deactivation of identification credentials. Additionally, a reference software implementation –which has not been carried out at the moment of writing— would be useful for testing purposes. In fact, a pilot evaluation comprising a variety of potential users (e.g. fitness enthusiasts, elderly people, hospital patients, physicians and systems administrators) would certainly be a reliable source for learning valuable lessons about the possible technical enhancements and potential social issues (e.g. reluctance to use personal authentication means) as well as the benefits of deploying and using this security framework in daily practice. Moreover, it would be mandatory to keep

track of new versions of the standards and norms on which our proposal relies. Should a new version of the X73PHD standard or the IHE profiles be published, this security proposal must be revised to guarantee flawless adaptation to them. Finally, since there is ongoing work towards the inclusion of remote control in X73PHD devices [41], it would be mandatory to review this eventual final document for two main reasons. First, it is necessary to check whether the new remote control feature compromises the security framework proposal. If so, the proposal must be modified to cover the new potential security breaches. Second, the new feature could be used to extend the security framework so that administrators can send security commands to PHDs (e.g. force the device to use 256-bit key size —instead of 128-bit— in symmetric encryption, so that all devices comply with an eventual new recommendation of NIST, without the need for physical access to the device to update it).

5. Conclusions

This work has analyzed the built-in security features of the X73PHD standard and its potential extensibility to enhance its levels of security and interoperability with healthcare systems —PHRs, EHRs, alert managers and/or CDSS— according to the needs of its application domains —Disease Management, Health and Fitness and Independent Living. A bottom-up layered-based model has been proposed to adapt to those needs while constraining complexity and expenditure (cost of hardware, delays, overhead). Each layer adds the most suitable IHE profiles to be implemented and translates them into modifications of the X73PHD.

The modification that this extension produces in the three models defining X73PHD can be considered as moderate. No attributes have been added to the DIM; four new frames have been added to the service model, and another four have been extended with new sub-frames (most of them common to all layers); and only one new sub-state, 'Authenticating', has been added in the communication model. Furthermore, the enhanced X73PHD architecture can be considered lightweight since an agent with a simple 9 MHz processor (assuming a throughput of 1 MIPS/MHz) can implement the top layer and transmit a 3-lead ECG in real-time to a manager with a one-core processor at 1 GHz (also assuming the same throughput). With respect to its surrounding framework, an administrator performs an initial configuration of the agent and the manager, the users are required to use tokens for identification/authentication when sharing these devices, and the manager needs to implement several IHE profiles to enable its integration with healthcare systems. Regarding IHE, the newly proposed SDO profile is intended to improve the level of interoperability with X73PHD and to facilitate reliable and secure communications from the PCD to the concentrating gateway in implementations of the DEC, ACM and WCM profiles.

To conclude, it is worth highlighting that the defining features of X73PHD have been maintained and enhanced. The agent can persistently store the acquired measurements with security; the manager can establish associations with different agents at the same time, by negotiating differentiated layers, and it can also communicate with PHRs, EHRs, alert managers and CDSS; the manager is able to access and process all the information without human intervention and also to show authorized users additional information regarding security and interoperability features. Therefore, it can be concluded that this proposal of enhancing the security of X73PHD and its interoperability with IHE may have a positive impact on healthcare delivery solutions based on this standard.

Acknowledgements

This research work was supported in part by the Ministerio de Economía y Competitividad (MINECO) under project TIN-2011-23792/TSI, in part by the Gobierno de Aragón (research group T98), in part by the European Regional Development Fund (ERDF), and in part by the European Social Fund (ESF). The work of J. D. Trigo was supported by the Public University of Navarre under project Res. 637/2014.

References

[1] K. Davis, S. C. Schoenbaum, A.-M. Audet, A 2020 vision of patient-centered primary care, Journal of General Internal Medicine 20 (2005) 953–957.

[2] R. M. Epstein, K. Fiscella, C. S. Lesser, K. C. Stange, Why the nation needs a policy push on patient-centered health care, Health Affairs 29 (2010) 1489–1495.

[3] R. Istepanian, S. Laxminarayan, C. S. Pattichis, M-health, Springer, 2006.

[4] R. Istepanian, N. Philip, X. Wang, S. Laxminarayan, Non-telephone healthcare: the role of 4G and emerging mobile systems for future m-health systems, Studies in health technology and informatics (2004) 465–470.

[5] C. Turnitsa, Extending the levels of conceptual interoperability model, in: Proceedings IEEE summer computer simulation conference, IEEE CS Press.

[6] Health Informatics.Personal Health Devices Communication (x73–PHD), ISO/IEEE 11073 (First edition: 2006). [P11073-00103, Technical report-Overview][11073-10101, Nomenclature] [11073-104zz, Device specializations] [11073-20601^{TM}–2014, Application profile-Optimized Exchange Protocol] [11073–20101, Medical Device Encoding Rules (MDER)], Accessed in October 2014, `http://http://goo.gl/i14L9h`, 2006.

[7] IHE International, Inc., IHE.net Home, Welcome to Integrating the Healthcare Enterprise, 2014.), Accessed in October 2014, `http://ihe.net`, 1998.

[8] Digital Imaging and Communications in Medicine (DICOM), National Electrical Manufacturers Association (NEMA), Accessed in October 2014, `http://goo.gl/BtYbVP`, 1993.

[9] Health Level 7, ANSI standard, Accessed in October 2014, `http://goo.gl/zjATS2`, 2004.

[10] M. Clarke, D. Bogia, K. Hassing, L. Steubesand, T. Chan, D. Ayyagari, Developing a standard for personal health devices based on 11073, in: 29th Annual International Conference of the Engineering in Medicine and Biology Society (EMBS), IEEE, pp. 6174–6176.

[11] J. Escayola, J. Trigo, I. Martínez, M. Martínez-Espronceda, A. Aragüés, D. Sancho, S. Led, L. Serrano, J. García, Overview of the ISO/IEEE 11073 family of standards and their applications to health monitoring, User-Driven Healthcare: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications (2013) 357–381.

[12] I. Martínez, J. Escayola, M. Martínez-Espronceda, P. Muñoz, J. D. Trigo, A. Muñoz, S. Led, L. Serrano, J. García, Seamless integration of ISO/IEEE11073 personal health devices and ISO/EN13606 electronic health records into an end-to-end interoperable solution, Telemedicine and e-Health 16 (2010) 993–1004.

[13] J.-H. Lim, C. Park, S.-J. Park, Home healthcare settop-box for senior chronic care using ISO/IEEE 11073 PHD standard, in: Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE, pp. 216–219.

[14] J. D. Trigo, I. Martínez, A. Alesanco, A. Kollmann, J. Escayola, D. Hayn, G. Schreier, J. García, An integrated healthcare information system for end-to-end standardized exchange and homogeneous management of digital ECG formats, IEEE Transactions on Information Technology in Biomedicine 16 (2012) 518–529.

[15] L. Caranguian, S. Pancho-Festin, L. Sison, Device interoperability and authentication for telemedical appliance based on the ISO/IEEE 11073 personal health device (PHD) standards, in: Engineering in Medicine and Biology Society (EMBC), 2012 Annual International Conference of the IEEE, pp. 1270–1273.

[16] A. Egner, A. Soceanu, F. Moldoveanu, Managing secure authentication for standard mobile medical networks, in: 2012 IEEE Symposium on Computers and Communications (ISCC), IEEE, pp. 390–393.

[17] S. S. Kim, Y. H. Lee, J. M. Kim, D. S. Seo, G. H. Kim, Y. S. Shin, Privacy protection for personal health device communication and healthcare building applications, Journal of Applied Mathematics 2014 (2014).

[18] A. Kliem, M. Hovestadt, O. Kao, Security and communication architecture for networked medical devices in mobility-aware eHealth environments, in: 2012 IEEE First International Conference on Mobile Services (MS), IEEE, pp. 112–114.

[19] P. Urbauer, S. Sauermann, M. Frohner, M. Forjan, B. Pohn, A. Mense, Applicability of IHE/Continua components for PHR systems: Learning from experiences, Computers in Biology and Medicine (2013) –.

[20] A. Roy, S. Karforma, Risk and remedies of e-governance systems, Oriental Journal of Computer Science & Technology (OJCST) 4 (2011) 329–339.

[21] F. Kargl, E. Lawrence, M. Fischer, Y. Y. Lim, Security, privacy and legal issues in pervasive eHealth monitoring systems, in: 7th International Conference on Mobile Business, 2008. ICMB '08, pp. 296–304.

[22] Bluekript, NIST Cryptographic key length recommendations. Accessed in October 2014 `http://goo.gl/BCxRWl`, 2013.

[23] W. Dai, Crypto++ 5.6.0 Benchmark. Accessed in October 2014 `http://goo.gl/XJXbtr`, 2009.

[24] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, V. C. Leung, Body area networks: A survey, Mobile networks and applications 16 (2011) 171–193.

[25] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, The Twofish encryption algorithm: a 128-bit block cipher, John Wiley & Sons, Inc., 1999.

[26] W. Burr, Selecting the Advanced Encryption Standard, IEEE Security and Privacy 1(2) (2003) 43–52.

[27] R. L. Rivest, M. J. Robshaw, Y. L. Yin, RC6 as the AES, in: AES Candidate Conference, pp. 337–342.

[28] R. Anderson, E. Biham, L. Knudsen, Serpent: A proposal for the advanced encryption standard, NIST AES Proposal 174 (1998).

[29] J. Jonsson, B. Kaliski, PKCS 1: RSA Cryptography Standard. Accessed in October 2014, http://goo.gl/13HJ4i, June 2002.

[30] E. Barker, D. Johnson, M. Smid, Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography, NIST Special Publication (2007) 800–56A.

[31] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, in: Advances in Cryptology, Springer, pp. 10–18.

[32] H. Gilbert, H. Handschuh, Security analysis of SHA-256 and sisters, in: Selected areas in cryptography, Springer, pp. 175–193.

[33] P. Barreto, V. Rijmen, The Whirlpool hashing function, in: First open NESSIE Workshop, Leuven, Belgium, volume 13, p. 14.

[34] H. Dobbertin, A. Bosselaers, B. Preneel, RIPEMD-160: A strengthened version of RIPEMD, in: Fast Software Encryption, Springer, pp. 71–82.

[35] D. Eastlake, P. Jones, US secure hash algorithm 1 (SHA1), 2001.

[36] D. Johnson and A. Menezes, and S. Vanstone, Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography, Version 2.0. Accessed in October 2014, http://goo.gl/tXhz2h, May 2009.

[37] D. W. Kravitz, (FIPS PUB 186-2: Digital Signature Standard (DSS). Accessed in October 2014 http://goo.gl/GgSDKe, January 2000.

[38] Ó. J. Rubio, Á. Alesanco, J. García, Secure information embedding into 1D biomedical signals based on SPIHT, Journal of Biomedical Informatics 46 (2013) 653–664.

[39] M. Martínez-Espronceda, I. Martínez, L. Serrano, S. Led, J. D. Trigo, A. Marzo, J. Escayola, J. García, Implementation methodology for interoperable personal health devices with low-voltage low-power constraints, IEEE Transactions on Information Technology in Biomedicine 15 (2011) 398–408.

[40] M. Martínez-Espronceda, J. D. Trigo, S. Led, H. G. Barrón-González, J. Redondo, A. Baquero, L. Serrano, Event-driven, pattern-based methodology for cost-effective development of standardized personal health devices, Computer methods and programs in biomedicine 117 (2014) 168–178.

[41] H. Barrón-González, M. Martínez-Espronceda, J. Trigo, S. Led, L. Serrano, Proposal of a novel remote command and control configuration extension for interoperable Personal Health Devices (PHD) based on ISO/IEEE 11073 standard, in: 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 6312–6315.