End-to-End Security for Personal Telehealth

Paul KOSTER a,1, Muhammad ASIM a, Milan PETKOVIC a, b

a Philips Research, b TU/e, Eindhoven, The Netherlands

Abstract. Personal telehealth is in rapid development with innovative emerging applications like disease management. With personal telehealth people participate in their own care supported by an open distributed system with health services. This poses new end-to-end security and privacy challenges. In this paper we introduce new end-to-end security requirements and present a design for consent management in the context of the Continua Health Alliance architecture. Thus, we empower patients to control how their health information is shared and used in a personal telehealth eco-system.

Keywords. security, privacy, consent, telehealth

Introduction

Healthcare around the world is facing important challenges through a substantial increase of the average age of the population and an increase of chronic diseases. Personal telehealth systems are expected to take an important role in addressing these issues. They extend healthcare from acute institutional care to outpatient care and home healthcare. Technological developments in this area are followed by standardization, policy and marketing activities of more than 230 companies that joined their efforts within the Continua Health Alliance [1] to ensure interoperability and further develop the personal telehealth market.

Although personal telehealth technologies bring a lot of benefits, they also create new security and privacy challenges. With personal telehealth services, it becomes simpler to collect, store, and search electronic health data, which in turn endangers people’s privacy. Furthermore, mistakes that are made because patient measurements are not available, associated to a wrong patient or modified in an unauthorized way can endanger patient safety. Therefore, technological means that empower patients with control over their health information while preventing security breaches and ensuring information correctness are of utmost importance.

Traditionally, security in healthcare treats protection of sensitive data by considering individual systems and communication. For personal telehealth applications like remote patient monitoring common security means are (role-based) access control and secure communication protocols [2]. However, emerging trends to open, distributed and user-centric telehealth architectures call for a more end-to-end

1 Corresponding Author: Paul Koster, Philips Research, Koninklijke Philips Electronics N.V., High Tech Campus 34, 5656AE, Eindhoven, The Netherlands; E-mail: r.p.koster@philips.com
approach to security. Only an end-to-end approach can provide a consistent level of security and meet patient empowerment expectations.

In this paper, we present new requirements for an end-to-end approach to security for personal telehealth. Moreover, we describe a digital consent management solution. This work represents ideas that have been contributed to and further elaborated in the Continua Health Alliance. This paper is organized as follows. In section 1, we introduce the Continua Health Alliance. Security and privacy requirements are described in section 2. Section 3 focuses on consent management to empower patients and presents a design addressing Continua requirements. Section 4 concludes the paper.

1. Continua Health Alliance

The Continua Health Alliance is an industry alliance formed with the intention to foster the growth of personal telehealth. Its 230+ members recognize the need for alignment and interoperability for applications such as disease management, fitness and aging independently. Continua provides a reference architecture for personal telehealth systems and the Continua guidelines [3], which select and profile standards to realize the interoperability objectives.

Architecture. The Continua architecture is characterized by its interfaces and device classes as illustrated in Figure 1. Medical observation devices measure people’s vital signs such as weight and blood pressure. These devices can be stationary, portable or body-worn, and use USB, Bluetooth or Zigbee to transmit the measurements to an application hosting device (AHD). Measurement communication follows the IEEE 11073 standard.

The AHD acts as an intermediary between observation devices and remote services. The AHD can be a gateway device, PC or smartphone. It uses the WAN interface to forward observations to the remote services such as a disease management organization (DMO). WAN communication makes use of the IHE Patient Care Device transaction standard, which is based on web-services and HL7 2.6 message standards.

A WAN service collects the observation data to provide care, e.g. a DMO employing nurses supported by IT systems to coordinate a patient’s care. If measurements fall outside the expected range then a nurse may prepare a Personal Health Monitoring Report (PHMR) and forward this to care providers e.g. a patient’s family physician. The HRN interface facilitates the exchange of the PHMR documents. HRN services interact with WAN services using IHE XDR (Cross-Enterprise Document Reliable Interchange) and IHE XDM (Cross-Enterprise Document Media
Interchange) standards. HRN services include electronic health record (EHR) systems belonging to care providers or personal health record (PHR) systems.

**Security.** As mentioned in the introduction, for adoption of personal telehealth systems, trust, security and privacy are very important. The same holds for compliance to legislation like EU Directive 95/46 and HIPAA. Continua acknowledges the importance of these issues amongst others through its E2E Security Task Force. The authors actively participate in this task force.

Initial security and privacy issues have been addressed in Continua version 1 guidelines for the PAN and HRN interfaces. Continua version 1.5 guidelines added security features for the WAN and LAN interfaces with e.g. TLS for secure communication and SAML 2.0 tokens for authentication of AHD users, see table 1.

**Table 1.** Security standards in Continua version 1.5

<table>
<thead>
<tr>
<th>Security standard</th>
<th>Security objective</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.0</td>
<td>confidentiality + integrity + authentication</td>
<td>HRN</td>
</tr>
<tr>
<td>IHE XDM (S/MIME)</td>
<td>confidentiality + integrity + authentication</td>
<td>“</td>
</tr>
<tr>
<td>IHE ATNA</td>
<td>auditing</td>
<td>“</td>
</tr>
<tr>
<td>WS-I BSP (TLS 1.0)</td>
<td>confidentiality + integrity + authentication</td>
<td>WAN</td>
</tr>
<tr>
<td>IHE ATNA</td>
<td>auditing</td>
<td>“</td>
</tr>
<tr>
<td>WS-I BSP (WS-Security + SAML 2.0)</td>
<td>entity authentication</td>
<td>“</td>
</tr>
<tr>
<td>Zigbee security</td>
<td>confidentiality + integrity + authentication</td>
<td>LAN</td>
</tr>
<tr>
<td>Bluetooth security</td>
<td>confidentiality + integrity + authentication</td>
<td>PAN</td>
</tr>
</tbody>
</table>

2. **End-to-end security and privacy requirements**

Continua version 1.5 addresses basic security requirements for personal telehealth with a strong focus on point-to-point transport security. However, a telehealth system with such open and distributed nature calls for an end-to-end approach, which follows from the risk analysis for remote patient monitoring performed by ENISA [4]. An end-to-end approach helps service providers to ensure compliance with legislation, empowers patients and eases seamless integration by defining a homogeneous security framework. The next paragraphs sketch end-to-end requirements as identified in Continua.

**Identity management.** A correct association of health information to patient identities is essential to provide high quality and safe personal telehealth services. However, a person typically has different identifiers at the various systems in a distributed architecture like Continua. These multiple identifiers imply linking and cross-referencing of identities at the AHD, WAN and HRN systems and services. Up to now, service providers often provide a vertically integrated solution and deal with identity management out-of-band. However, larger number of patients, operational cost pressure, less vertical integration, and vendor interoperability ask for standardized in-band identity solutions. This leads to the following requirements: i) measurement uploads should be unambiguously linked to a particular patient, and ii) identity linking should be in-band using interoperable protocols and preferably user-initiated.

**Integrity and data origin authentication.** Health measurements performed by patients require healthcare professionals to place trust in information that patients report. For example, for a blood pressure measurement it is crucial to know that blood pressure of a registered patient is actually measured on his body, that the measurement is taken with a certified device and that it is not modified on the way to healthcare providers. However, end-to-end integrity is not trivial to guarantee as in the Continua architecture health measurements pass through multiple parties and undergo
transformations before a health provider obtains them. Therefore, it is required to i) authenticate data sources including users and devices, and ii) prevent or detect unauthorized data modifications while allowing legitimate transformations. A more detailed description of related requirements and security mechanisms is presented in [5].

**Consent management.** Traditionally, consent has been an important concept in healthcare. Signed paper consent forms are used to grant (opt-in) or withhold (opt-out) consent and enable patients to regulate which care providers have access to their health information. In perspective of user centered care and patient empowerment trends, patients should be in more direct control for distributed applications like personal telehealth. Digital consent addresses this requirement and increases consistency, compliance and efficiency for both patients and care providers. Consequently, high-level end-to-end requirements include that i) patients should be able to define and manage their digital consent and privacy policies in a user-friendly manner, e.g. on a device at home or online, ii) digital consent should propagate together with the patient data, and iii) systems of care providers and services must enforce digital consent.

### 3. Design for consent management in the Continua architecture

Consent management entails the specification, exchange and update of patient’s digital consent preferences. For maximum effect, a patient should indicate his consent and privacy policies as early as possible such that they can travel together with the patient data through the ecosystem. In Continua, the AHD device would be a practical location for a patient to specify his consent. Alternatively, it could be specified at a WAN service by the patient online or taken care of by a nurse on behalf of the patient. Propagation of consent policies over the WAN and HRN interfaces must be enabled to ensure that disease management organizations and care providers use and share patient data in accordance with the patient’s digital consent policy.

The Implementation Guide for HL7 CDA R2 Consent Directive [6] forms the basis for our approach to consent management in Continua. This recently approved draft standard for trial use defines a document format for digital consent and enables the expression of structured patient consent policies. The advantage of this standard lies in the fact that it is based on the CDA R2 standard, which is already used at the Continua HRN interface for the health PMHR document. Similarly, well-defined protocols exist for the exchange of this type of documents through the IHE XD* family of profiles. Figure 2 provides an overview of how these document and document exchange standards realize the consent management interactions at the HRN interface. The WAN interface solution is a subset of the solution for the HRN interface.

Consent at the HRN interface is supported through a basic and a more advanced interaction. In the basic interaction the patient consent document is included in the same transaction as the health PHMR document as shown in Figure 2a. This makes use of the IHE XDR transaction in Continua, which allows inclusion of both documents in the existing submission set.

In the more advanced interaction the patient consent document is retrieved online on demand as depicted in Figure 2b. Such interaction allows for more flexibility as a receiver may obtain consent documents e.g. when it does not have the required consent to perform its intended task. Technically, this variant involves the IHE XDS standard, which provides a superset of the functionality provided by XDR. To enable online retrieval of consent documents, a sender at the HRN interface implements the
Document Repository and Registry actors to host the consent documents. The receiver implements the IHE XDS Document Consumer actor. Optionally, the receiver may query and lookup the appropriate consent document identifiers and their location URLs. Subsequently, the HRN receiver requests the consent document through an XDS retrieve transaction. The receiver may include a token in the request to authenticate to the sender and enable personalization of the consent document. Finally, the sender responds with the requested patient consent document personalized for the recipient.

![Diagram](image)

**Figure 2.** Consent management at the HRN interface

4. Conclusions

Novel use cases in personal telehealth cannot be addressed with point-to-point or transport security alone anymore and a more end-to-end approach to security and privacy is required. The user-centered and open architecture of personal telehealth systems introduce challenging end-to-end security needs in the areas of identity management, integrity, data origin authentication and consent management. This paper presents a design to extend personal telehealth with digital consent. This design is applied to and presented in context of the Continua Health Alliance interoperability architecture. It demonstrates how the application and combination of novel standards from the healthcare domain realizes consent management and thereby empowers users.

References