Ann. Telecommun. (2017) 72:577–587
DOI 10.1007/s12243-017-0582-7

Preserving patients' privacy in health scenarios through a multicontext-aware system

Alberto Huertas Celdrán[1] · Manuel Gil Pérez[1] · Félix J. García Clemente[2] · Gregorio Martínez Pérez[1]

Received: 12 January 2017 / Accepted: 14 May 2017 / Published online: 23 June 2017

Abstract The Big Data age is characterized by the explosive increase of data managed by electronic systems. Healthcare Information Management systems are aware of this situation having to adapt services and procedures. This, along with the fact that the proliferation of mobile devices and communications has also promoted the use of context-aware services ubiquitously accessible, means that protecting the privacy of the patients' information is an even greater challenge. To address this issue, a mechanism that allows patients to manage and control their private information is required. We propose the preservation of patients' privacy in a health scenario through a multicontext-aware system called h-MAS (health-related multicontext-aware system). h-MAS is a privacy-preserving and context-aware solution for health scenarios with the aim of managing the privacy of the users' information in both intra- and inter-context scenarios. In a health scenario, h-MAS suggests a pool of privacy policies to users, who are aware of the health context in which they are located. Users can update the policies according to their interests. These policies protect the privacy of the users' health records, locations, as well as context-aware information being accessed by third parties without their consent. The information on patients and the health context is managed through semantic web techniques, which provide a common infrastructure that makes it possible to represent, process, and share information between independent systems more easily.

Keywords Context-awareness · Location · eHealth · Privacy-preserving · Policy

1 Introduction

Historically, Healthcare Information Management systems [1] have generated large volumes of data related to Electronic Health Record (EHR) [2]. These massive quantities of data, known as *Big Data*, have influenced critical changes in the patient information management processes. Adding to this fact that current mobile communications have led to the emergence of new ubiquitously accessible services, the management of the patients' location and context-aware information is an even greater challenge.

In this sense, high-level healthcare applications can be further developed by integrating mobile device telecommunication functions with the users' context [3]. Context is a concept that combines the information about the environment where users are, their location, their identities, the identity of nearby people and objects, and any changes in the previous terms [4]. These context-aware applications can be useful and helpful in managing the patients' information, with concern for patients' privacy and how personal information, location, and context information are revealed. An example of these services could be a hospital context, which has a service to share medical information (e.g., the EHR

✉ Alberto Huertas Celdrán
alberto.huertas@um.es

[1] Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, 30071 Murcia, Spain

[2] Departamento de Ingeniería y Tecnología de Computadores, University of Murcia, 30071 Murcia, Spain

of a patient) between patients and doctors that protects the privacy of the patients' information.

1.1 Motivation

Preserving the health information taking into account the context in which patients are located is an open challenge. We can find in the literature a depth survey of eHealth systems oriented to cloud computing that analyzes a large number of solutions by considering different topics [5]. Additionally, a recent work is proposed in [6], where current security and privacy challenges are pointed out from different perspectives oriented to many scenarios. Data privacy is a fundamental issue of modern information systems. In this sense, in [7], they presented a survey of text mining and privacy-preserving techniques. Focusing on non-cryptographic approaches, several solutions have been proposed in order to preserve and exchange health information in a privacy-preserving way [8–10]. These solutions protect the health information without considering the location of users neither their contexts. In this sense, several privacy-preserving and context-aware solutions have been proposed taking into account the location of users in order to protect the personal and contextual information [11–13]. However, these solutions are not oriented to eHealth environments and they do not consider the protection of medical information [14], or they do not manage the mobility of users between different contexts [15]. The main characteristics of the presented solutions are illustrated in Table 1.

We believe that patients of context-aware and health-oriented systems should be able to manage dynamically the privacy of their medical records, personal information, locations, and information related to the environment or context in which they are located (intra-context scenario). This is an even more complex process when users move between several contexts, and there is an exchange of information between them (inter-context scenario). Following the previous example, when the patient leaves the hospital, he goes to the pharmacy in order to buy the prescribed medicines. This implies a change of context and the preservation of information privacy when the pharmacy service accesses the prescribed medicines (information belonging to the hospital context) is mandatory. This raises new challenging questions such as the way that patients should protect their information, what information could be exchanged between different contexts, and who should manage the inter-contextual information.

1.2 Contribution

In addressing the above issues and covering the aspects depicted in Table 1, the main contribution of this paper is a system called h-MAS (health-related multicontext-aware system). h-MAS is a solution-oriented toward health contexts, that enables the secure exchange of information, so allowing users not to have to manage the protection of their sensitive information. Specifically, h-MAS is an important evolution of MASTERY (Multicontext-Aware System That prEserves the useRs' privacY) proposed by [14], but oriented toward the management of the users' privacy in health scenarios by using policies that are intra- and inter-context. These policies protect the users' information by incorporating their consent to reveal their personal information. To this end, h-MAS suggests several sets of privacy-preserving and context-aware policies, called *profiles*, to users. These profiles are created by the administrator of each context. Administrators are trusted entities that know what kind of information is shaped within their contexts and, thus, what part of that information should be protected. Once users receive the profiles, they choose the most suitable profile according to their interests. After that, and in case users want to control their information, they will be able to update the selected profile by adding, deleting, or modifying some of the policies that shape it. To that end, we have designed a mobile application that allows users to manage the privacy of their information in a friendly fashion. Intra- and inter-context policies form the privacy profiles that allow users to protect their location, personal information, activities they

Table 1 Comparison of different privacy-preserving systems

	[8]	[9]	[10]	[11]	[12]	[13]	[15]	[14]
Health privacy-oriented	√	√	√				√	
Context-awareness				√	√	√		√
Intra-context privacy	√	√	√	√	√	√	√	√
Preserve users' location				√	√	√		√
Preserve users' identity		√	√		√	√	√	√
Preserve users' context	√	√	√		√	√	√	√
Policies defined by users	√	√			√	√	√	√
Policies set by the system						√		√
Multicontext solutions							√	√
Inter-context privacy							√	√

are doing at any given time, and information oriented to the context in which they are located. Finally, the complete definition of the information managed by h-MAS and the designed architecture to manage this information are provided in [16].

In summary, we propose a novel solution that covers the whole aspects presented in Table 1. This comparative table shows the main differences between the existing solutions. In this sense, our proposal covers the whole set of topics indicated in Table 1, being the only one (to the best of our knowledge) allowing users of health scenarios to protect the privacy of their location, identity, and contextual information without having to define their own privacy profiles. Users or patients of the eHealth context just have to choose between the suggested profiles, the most appropriate for them according to their interest in a given moment. Furthermore, despite our solution is oriented to protect the patients' privacy in health environments, it can be extended to protect and manage the privacy of the users' information in another kind of scenarios. To this end, the administrator of h-MAS should include a new ontology that models the information belonging to the context in which the user is interested. Finally, the administrators of each new context should provide the context-aware profiles composed of the privacy policies with which to protect the sensitive pieces of information.

2 Scenario

The inter-context scenario below illustrates the privacy-related concerns that a user, named Andy, can find with respect to his private information. In Fig. 1, we show this scenario graphically, which is composed of four independent contexts distributed in two countries: *CountryA* with a clinic belonging to the National Health Service (NHS) and a CountryB's Embassy, and *CountryB* with a hospital belonging to the NHS of CountryB. Both contexts share an international Health Insurance Company. The exchange of information between the actors is shown with a (dashed) red line and Andy's movements with a (solid) black line.

Andy is a citizen of CountryA who plans to visit CountryB. Before leaving CountryA, Andy has to request the visa to the Embassy of CountryB (which is located in CountryA), providing some information like the days he will stay in CountryB, the places that he wants to visit, and the purpose of the trip, etc. Once the visa is granted by CountryB, the information of Andy's trip (date, itinerary, purpose, etc.) is stored by CountryB's Embassy.

After obtaining the visa, Andy goes to a clinic of CountryA's NHS context to get the required vaccines for CountryB. The Nurse, before vaccinating Andy, needs to see his Health Record (HR) in order to know if he has allergies or some kind of illness. To this end, the nurse accesses Andy's HR. Here is the first privacy concern, because the HR contains personal information like Andy's Social History and he does not want the Nurse to know it. Finally, since Andy wants to have a health insurance valid in CountryB, he goes to an international Health Insurance company to purchase valid insurance for CountryB.

Some weeks later, when Andy is already visiting CountryB, he has a heavy fever and decides to go to a hospital of CountryB's NHS context for a medical check-up. It is important to note that CountryA's NHS and CountryB's NHS contexts share the structure to model the information, but the content is different. Once Andy is in the hospital,

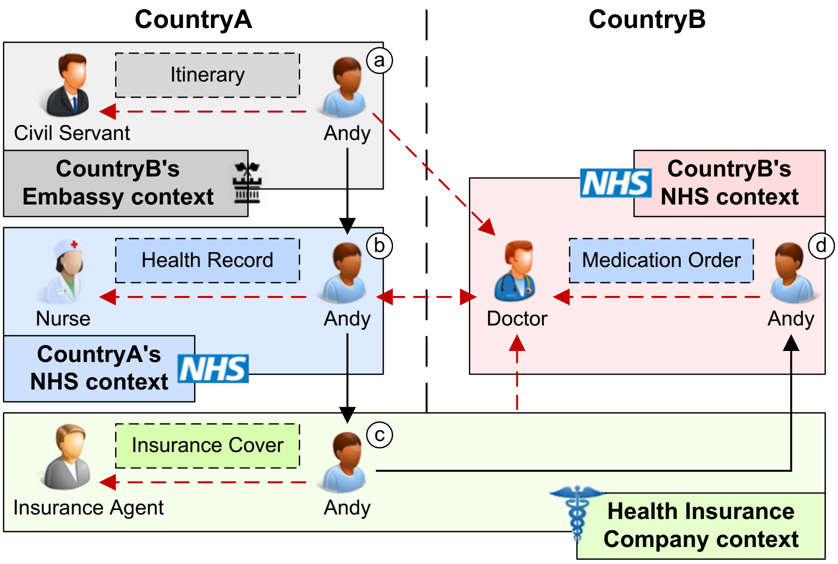


Fig. 1 Scenario with privacy concerns on the information of a given user

the Doctor needs to know if he has a Health Insurance valid for CountryB. The Doctor accesses the information about the Andy's Health Insurance and checks its cover. Here, we have the second privacy concern because the Doctor can see private information about Andy, like Andy's bank account.

Once Andy is in the consulting room, the Doctor wants to know the places Andy has visited during the previous days. The Doctor accesses Andy's Itinerary information, which belongs to CountryB's Embassy. Here, we have the third privacy concern because the Doctor must not access information that belongs to another context. Furthermore, when he accesses the Itinerary, he can see private information such as the cities to be visited by Andy in the next days.

One week ago, Andy stayed in a city with a high risk of getting an infection. Therefore, the Doctor wants to know Andy's HR, which contains his immunization and Medication Orders. Here is the fourth privacy concern, as the Doctor accesses information that contains private data about Andy and his doctors.

When the medical check-up finishes, the Doctor generates a new Medication Order for Andy with the prescribed medicine. Once Andy comes back to CountryA, if he visits a hospital or clinic of CountryA's NHS context and the staff accesses the medication order given in CountryB's NHS context, there will be at fifth privacy concern.

In order to address the concerns introduced during this section, it is necessary to provide some management mechanisms with which to protect the users' information.

3 Preserving users' privacy

Privacy policies should allow users to manage when, where, how, and to whom their private information can be revealed. h-MAS provides users with a group of context-aware and privacy-preserving policies called *profiles*. These profiles are specific to the context in which users are located, aimed to protect the privacy of their personal information. Furthermore, the profile selected by the user can be modified by adding, modifying, or deleting its policies according to his/her interests. The policies that are part of the profiles managed by h-MAS are composed of the following elements:

$$\boxed{\text{Type} \wedge \text{Maker} \wedge \text{Target} \wedge \text{Requester} \wedge [\text{What, Where, When, How}] \rightarrow \text{Result}}$$

h-MAS classify the policies into two groups: intra- and inter-context. The *intra-context policies* are in charge of protecting the information in a given context, while the *inter-context policies* protect the information between different contexts. As an example of these policies, considering again the scenario of Section 2. Both groups of policies are, in turn, composed of two different policies. First, the *disclosure policies* are in charge of indicating what information of users can be shared. Second, the *reveal policies* with which users can decide where, when, and how their information can be shared.

3.1 The intra-context policies

The *intra-disclosure policies* indicate *what* information the *target* wants to share with a given *requester*. The only restriction of the intra-disclosure policies is that the *maker*, *requester*, and *what* fields must belong to the same context. It is important to note that intra-disclosure policies do not indicate where, when, or how the information is revealed. Following the scenario of Section 2, we need an intra-disclosure policy to solve the first privacy concern. The NHS Administrator of CountryA needs to indicate that patients (role in an NHS context) could disclose their EHR to any Nurse, where the latter is another role in CountryA's NHS context. Disclosing the EHR allows the Nurse to know Andy's allergies or medication orders without revealing Andy's social history. An example of this intra-disclosure policy is given by:

$$\boxed{\begin{array}{l} \mathit{Id}: \textbf{ClinicIntraD} \wedge \mathit{Type}: \textbf{IntraDisclosure} \wedge \mathit{Maker}: \textbf{CountryANHSAdmin} \wedge \mathit{Target}: \textbf{Patient} \wedge \mathit{Requester}: \textbf{Nurse} \wedge \\ \mathit{What}: \textbf{EHR} \rightarrow \mathit{Result}: \textbf{Disclosure} \end{array}}$$

On the other hand, the *intra-reveal policies* indicate *where*, *when*, and *how* the target's information can be shared. This kind of intra-reveal policy is related to the previous intra-disclosure one through the target and requester elements. In this sense, this policy activates the disclosure policies when users are in certain places or contexts. Following the scenario of Section 2, in order to activate the policy previously defined (ClinicIntraD), an intra-reveal policy is necessary. Specifically, the Administrator of CountryA's NHS context allows the Nurse to access the information defined by the intra-disclosure policy ClinicIntraD, defined earlier when the Patient is in the Consulting Room of the clinic. This policy is defined below.

Id : **ClinicIntraR** ∧ *Type* : **IntraReveal** ∧ *Maker* : **CountryANHSAdmin** ∧ *Target* : **Patient** ∧ *Requester* : **Nurse** ∧ *Where* : **ConsultingRoom** → *Result* : **Reveal**

3.2 The inter-context policies

The *inter-disclosure policies* are aimed at preserving the exchange of information between different contexts. When a user of a given context wants to access information belonging to another context, it is necessary for the information's context owner to leave it accessible to be exchanged. In these policies, the *maker* must belong to the context of the information and the *what* field must containinformation about the maker's context. In the scenario of Section 2, we detected an information exchange between different contexts: the Doctor accessing the Insurance Cover, Itinerary, and EHR of Andy. Therefore, in order to solve the second concern on privacy, the next policy indicates that Andy discloses the Cover of his Health Insurance to the staff of the hospital belonging to CountryB's NHS context. In this policy, the Insurance Agent is in charge of deciding who can access this information with an inter-disclosure policy.

Id : **InsuranceInterD** ∧ *Type*: **InterDisclosure**[Hospital] ∧ *Maker* : **InsuranceAgent** ∧ *Target* : **Andy** ∧ *Requester* : **HospitalStaff** ∧ *What* : **InsuranceCover** → *Result* : **Disclosure**

Regarding the third privacy concern, the Civil Servant defines the inter-disclosure policyshown below indicating that Andy discloses his Itinerary to the staff of the hospital belonging to CountryB's NHS context.

Id : **EmbassyInterD** ∧ *Type* : **InterDisclosure**[Hospital] ∧ *Maker* : **CivilServant** ∧ *Target* : **Andy** ∧ *Requester* : **HospitalStaff** ∧ *What* : **Itinerary** → *Result* : **Disclosure**

In order to solve the fourth privacy concern of Section 2, the Nurse defines the inter-disclosure policy shown below. In this policy, the Nurse discloses Andy's EHR. Since Andy did not reveal his PHR (Personal Health Record) to the staff of the clinic belonging to CountryA's NHS context, the Nurse cannot disclose this information to another context.

Id : **ClinicInterD** ∧ *Type* : **InterDisclosure**[Hospital] ∧ *Maker* : **Nurse** ∧ *Target* : **Andy** ∧ *Requester* : **HospitalStaff** ∧ *What* : **EHR** → *Result* : **Disclosure**

Finally, the fifth privacy concern of Section 2 is solved by the next policy, which discloses Andy's Medication Order given by the Doctor of the Hospital context to the NHS Staff of CountryA.

Id : **HospitalInterD** ∧ *Type* : **InterDisclosure**[CountryANHS] ∧ *Maker* : **Doctor** ∧ *Target* : **Andy** ∧ *Requester* : **NHSStaff** ∧ *What* : **MedicationOrder** → *Result* : **Disclosure**

On the other hand, the inter-reveal policies are similar to the intra-reveal policies, although the former are totally oriented to operate between contexts. These inter-reveal policies indicate *where*, *when*, and *how* the information (previously established by the inter-disclosure policies) is revealed.

In the scenario of Section 2, in order to allow the Doctor to access the Cover of Andy's Health Insurance, the Administrator of CountryB's NHS context needs to define an inter-reveal policy. This policy will reveal the Cover of the Foreign Patient (Andy) to the Doctor.

Id : **1HospitalInterR** ∧ *Type* : **InterReveal**[HealthInsuranceCompany] ∧ *Maker* : **CountryBNHSAdmin** ∧ *Target* : **ForeignPatient** ∧ *Requester* : **Doctor** ∧ *Where* : **ConsultingRoom** → *Result* : **Reveal**

Following the scenario of Section 2, in order to allow the Doctor to access Andy's itinerary, we need the inter-reveal policy that reveals the information allowed by the policy EmbassyInterD. This policy defines that when a Foreign Patient (like Andy) is in the hospital of CountryB's NHS, his/her Itinerary is revealed to the Doctor. Although this policy only defines information about CountryB's NHS context, the information to be revealed belongs to CountryB's Embassy context.

Id : **2HospitalInterR** ∧ *Type* : **InterReveal**[CountryBEmbassy] ∧ *Maker* : **CountryBNHSAdmin** ∧ *Target* : **ForeignPatient** ∧ *Requester* : **Doctor** ∧ *Where* : **Hospital** → *Result* : **Reveal**

To reveal the information allowed by the policy ClinicInterD, CountryB's NHS Administrator needs to define a new inter-reveal policy in which he/she allows access to the EHR of the Foreign Patient when he/she is in the Consulting Room. This policy just reveals the information allowed by the context to which the information (policy identifier ClinicInterD defined in CountryA's NHS context) belongs.

Id : **3HospitalInterR** ∧ *Type* : **InterReveal**[CountryANHS] ∧ *Maker* : **CountryBNHSAdmin** ∧ *Target* : **ForeignPatient** ∧ *Requester* : **Doctor** ∧ *Where* : **ConsultingRoom** → *Result* : **Reveal**

Finally, if Andy comes back to CountryA and the NHS accesses the information of Andy's Medical Order, CountryA's NHS context has to define a new inter-reveal policy.

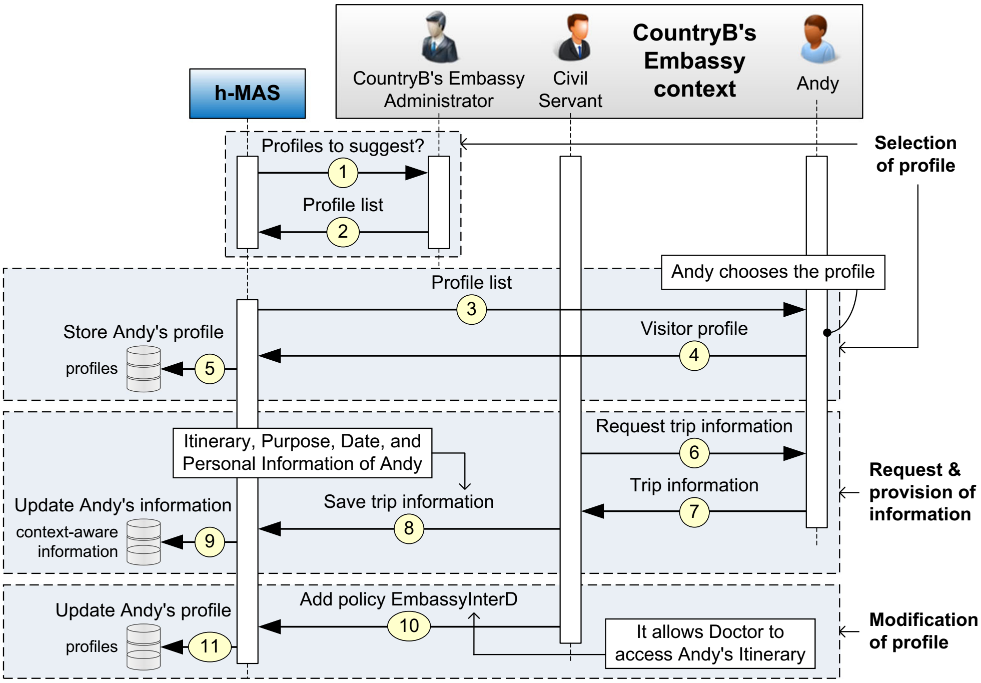
4 Management of the users' information privacy by h-MAS

This section shows how h-MAS protects the privacy of the users' information using the scenario of Section 5. Figure 2 depicts the four different groups of messages exchanged by the actors of our solution when Andy is in CountryB's Embassy to get the visa to travel to that country. Firstly, Andy uses his smartphone with the h-MAS application shown in Section 2 to protect his information. In this sense, h-MAS detects him in accordance with the information provided by the embassy's location infrastructure. Then, the first and second groups of messages are oriented to protect the privacy of Andy's information by using profiles. In this sense, h-MAS offers Andy several context-aware profiles, such as Visitor or Citizen (step 3 in Fig. 2). These profiles are suggested by CountryB's Embassy Administrator to h-MAS (steps 1 and 2), and h-MAS is in charge of suggesting them to Andy. Once Andy receives the list of available on his mobile device, he chooses the most appropriate for him, the Visitor profile (step 4), and h-MAS stores and activates the profile to CountryB's Embassy context (step 5). When Andy is before the Civil Servant, the third block of messages is oriented to request and provide Andy's personal information by considering his profiles and consent. To this end, The civil servant asks Andy for the trip information (purpose, itinerary, date, etc.) and h-MAS stores this information (steps from 6 to 9). Finally, the last group of messages shows how the Civil Servant defines the policy EmbassyInterD (presented in Section 3.2) and modifies the Visitor profile to provide the Itinerary information to the Hospital context.

Figure 3 shows the sequence diagram when Andy is in the clinic to get the vaccines, and the Nurse wants to access Andy's EHR. The first group of messages (steps from 1 to 3) shows when h-MAS detects Andy and offers several context-aware profiles, Andy chooses one of them, and h-MAS stores and activates the profile in the context in which Andy is located. After step 3, the second block of information (steps from 4 to 15) shows the messages exchanged to request and provide protected information. Specifically, once Andy is in the consulting room, the Nurse wants to access Andy's EHR to know if he has allergies or illnesses (step 4). The Nurse then uses the NHS application that manages the information available in that context. This application asks h-MAS for Andy's information, and h-MAS checks if Andy's profile allows the Nurse to do it (step 5). To this end, h-MAS has a component, called *Engine*, which is in charge of managing the context-aware information and Andy's personal information and profiles. Specifically, the engine uses the previous information to decide if the Nurse has permission to access the requested information. Since the ClinicIntraD and ClinicIntraR policies of Andy's profile allow the Nurse to access the EHR of Andy, h-MAS asks Andy for confirmation to release his information (step 6); otherwise, the confirmation would not be requested. At this point, Andy receives a request on his mobile device, Andy accepts the request and his information is released to the Nurse (steps 7 and 8). Once Andy is vaccinated, the Nurse wants to modify the EHR of Andy in order to update the information. The Nurse uses again the NHS application to ask h-MAS for access to Andy's EHR (step 9). The h-MAS's Engine manages the required information, infers that the action is allowed (step 10), and asks Andy for confirmation (step 11). Once Andy accepts (step 12), the Nurse updates Andy's EHR with the vaccines (steps 14 and 15).

Finally, the last group of messages is oriented to modify the existing profile. In this sense, since Andy is going to visit CountryB, the Nurse updates the Traveler Patient profile of Andy (steps 16 and 17) with the policy ClinicInterD presented in Section 3.2. This policy allows the hospital of CountryB's NHS context to access Andy's EHR. It is important to note that before updating Andy's Traveler Patient profile, the nurse requested him the authorization to make

Fig. 2 Sequence diagram of h-MAS in CountryB's Embassy context



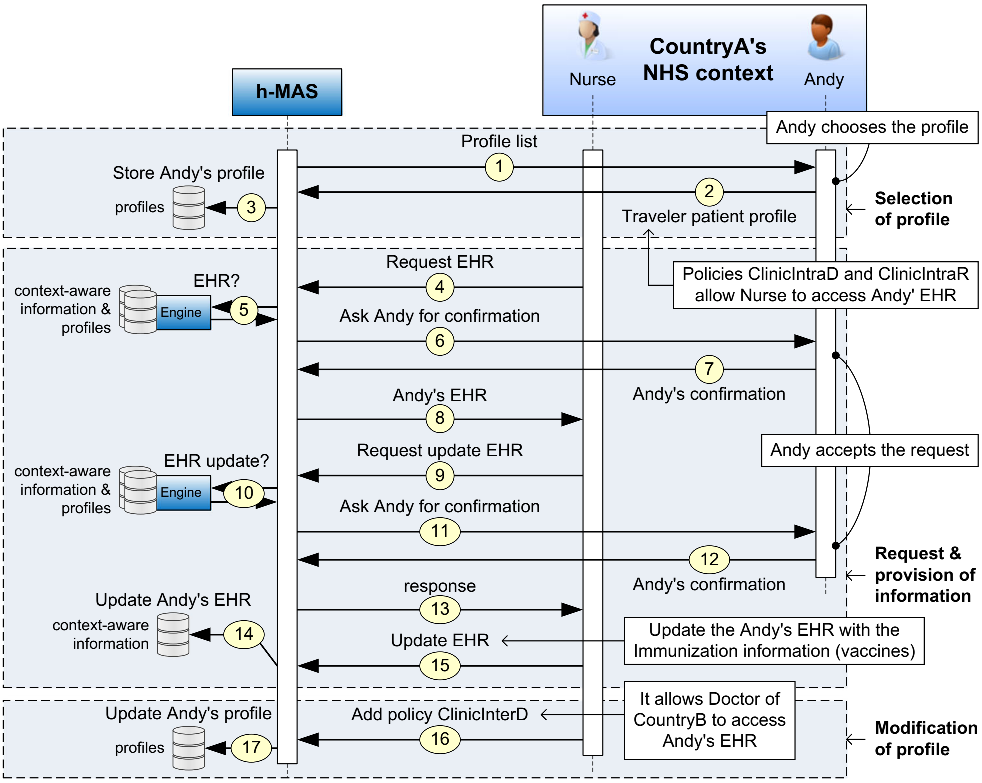


Fig. 3 Sequence diagram of h-MAS in CountryA's NHS context

it. This process has not been included in Fig. 3 because it is similar to the previous confirmation processes and it would increase the diagram's complexity.

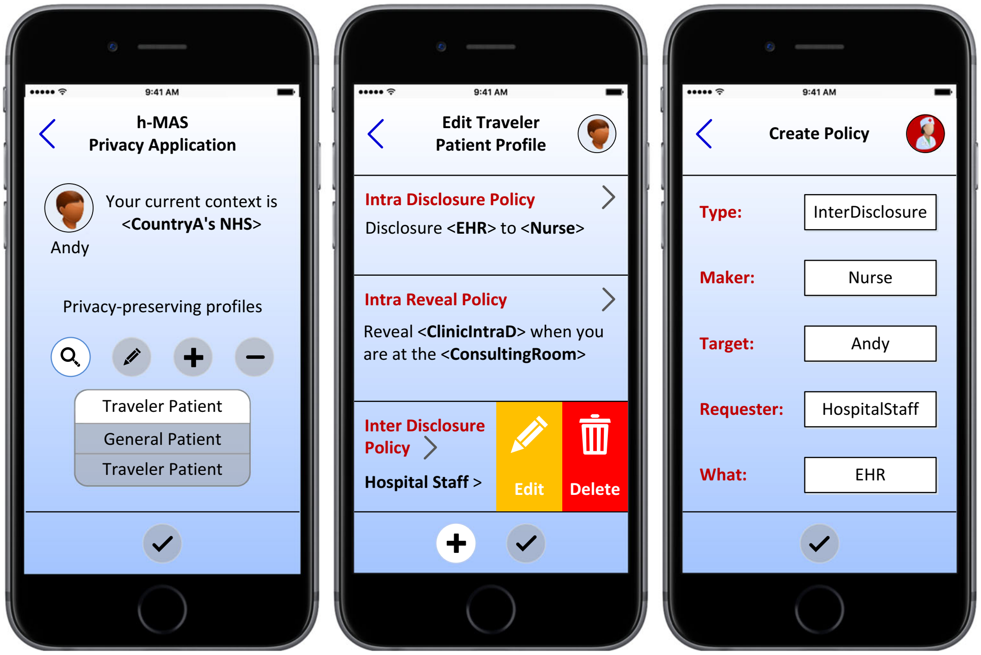
Before leaving CountryA, Andy changes context again when he goes to the international Health Insurance Company, in order to take out Health Insurance valid in CountryB. When he is at the insurance company, h-MAS provides him with several profiles and he selects the most appropriate. Once Andy decides his insurance, he pays for it and the Insurance Agent stores the information using h-MAS. Finally, the Insurance Agent defines and stores in h-MAS the InsuranceInterD policy (explained in Section 3.2). This policy provides the information about the cover of Andy's Health Insurance to CountryB's NHS context. The steps of the process explained in this paragraph are similar to the ones of Fig. 3, but changing the context, actors, information, and policies. When Andy is in CountryB's NHS context, the sequence diagram of h-MAS is similar to the previous ones.

Finally, it is worth noting that to ensure the h-MAS's usability, users just interact with the system to choose the preferred profiles and to consent to the release of their information. In that sense, next section shows how users make it.

5 How users manage their profiles

Although an initial set of profiles is defined by administrators, h-MAS allows users to manage the privacy of their information, modifying the suggested profiles through a *Privacy application* with which users can create, delete, and modify their profiles and policies. Thus, the usability of the approach proposed can be achieved.

Figure 4 shows how users can select a given privacy-preserving profile to protect his/her sensitive information, edit an already defined profile, or create a determined policy by using the *Privacy application* of the h-MAS architecture. Specifically, Fig. 4a shows how Andy's context is discovered and how he can choose the most suitable profile for him in that context. In this example, Andy chooses the Traveler Patient profile that is available in CountryA's NHS context. Furthermore, by using the *Privacy application*, Andy can edit the suggested profiles, create, or delete new profiles. Figure 4b depicts how Andy can edit his *Traveler Patient* profile adding or deleting policies. Finally, Fig. 4c shows how users can create a new policy for a given profile. Specifically, this figure depicts how the Nurse of Andy modifies the Traveler Patient profile of Andy with the ClinicInterD policy presented in Section 3.2.



Your current context is <CountryA's NHS>

Disclosure <EHR> to <Nurse>

Reveal <ClinicIntraD> when you are at the <ConsultingRoom>

Type: InterDisclosure

Maker: Nurse

Target: Andy

Requester: HospitalStaff

What: EHR

Fig. 4 How a user can choose a given profile and how its policies can be created or edited with a mobile application: **a** Andy chooses Traveler Patient to protect his information in the NHS context; **b** Andy edits the Traveler Patient profile to modify the third policy; **c** Andy's Nurse generates an Inter Disclosure Policy to control the Andy's EHR

6 Results

In previous sections, we have seen how our solution is able to protect the patients' information in health scenarios. In this section, we are going to demonstrate the viability of deploying our proposal in a real scenario. In this sense, the time needed to load and infer information (reasoning time) as well as the time required by users to receive the requested information *query time* are two of the most important metrics to know the throughput of systems based on semantic web [17]. In this sense, two experiments are presented in this section to measure how the computing *time of reasoning* and the *time of query* are in inter-context scenarios considering different amounts of individuals composing the scenarios.

As experimental setting, the tests were carried out in a dedicated PC with an Intel Core i7-3770 3.40 GHz, 16 GB of RAM, and an Ubuntu 14.04 LTS as operative system. The results shown below were obtained by executing the tests 100 times and computing their arithmetic mean. In our experiment, the information about users and contexts is shaped with ontologies defined in OWL 2 (Web Ontology Language) [18]. On the other hand, the policies that are part of the users' privacy profiles are expressed in SWRL (Semantic Web Rule Language) [19]. In order to decide what information is revealed, where, when, how, and to whom, h-MAS uses the Pellet reasoner [20]. This reasoner receives the ontological models generated by the Jena API [21] and applies the SPARQL queries [22] to obtain the requested information.

In order to ascertain the reasoning time in inter-context scenarios and its scalability, we have conducted an experiment in the health scenario presented in Section 2, with different levels of complexity. The complexity depends on the number of individuals present in the ontologies and the number of semantic rules forming the policies. For this experiment and in order to create as realistic a scenario as possible, we have obtained the percentages of the individuals considered in the health environment from *The World Bank* [23]. In more detail, we have based the percentages on the official number of patients, doctors, and nurses per population in different countries of the world. For instance,

Table 2 Individuals and statements per population

Population	0	1	2	3	4
Individuals	30,000	60,000	90,000	120,000	150,000
Patients	3000	6000	9000	12,000	15,000
Statements	247,140	494,280	741,420	988,560	1,235,700

Patient is 10% of the individuals; Space 75%; context-aware elements, such as HealthRecord, HealthInsurance, or Trip, 10%; and others, such as NHSStaff or NHSService, 5%. In order to conduct the experiment, we started with 30,000 individuals, which were increased by 30,000 in each step. Table 2 shows the relationships between the individuals and the statements generated by the reasoner, which indicates the complexity of our ontologies.

We used the previous populations in order to check the *reasoning time* in inter-context scenarios, where the information is shaped in different ontologies and it is necessary to combine two ontologies. Figure 5 depicts how the reasoning time (y-axis) in inter-context scenarios varies depending on the populations of two ontologies (x-axis).

The previous experiment demonstrated that when our solution combines ontologies in inter-context scenarios, the reasoning time is less than the sum of the reasoning time of the individual ontologies. This is because the ontologies share individuals and properties, so the number of statements is not the sum of the individual ontologies' statements. It is important to notice that although the reasoning time is measured in seconds, users do not have to wait for this time in order to receive the requested information. This time is just needed in the process of checking the consistency of the ontology, which must be performed when the h-MAS ontology is updated. It is important to consider that other important question, like the intra-context reasoning times, has already been analyzed with positive results in [13].

On the other hand, to evaluate the time needed by users to receive the requested information, we measured the *query time* when a user asks for information about another user. This was shown in Section 4 when the Civil Servant or the Nurse wants to access Andy's information. Figure 6 shows that the response time (y-axis) for queries is mainly influenced by the population (x-axis). This is because there are more statements in the ontologies. Furthermore, policies do not have a great impact on the query time, as policies are related to patients and they are the 10% of the individuals contained in each population.

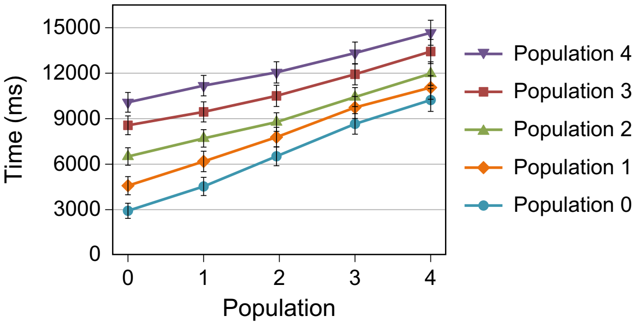


Fig. 5 Reasoning time combining ontologies from different contexts (inter-context) with different populations

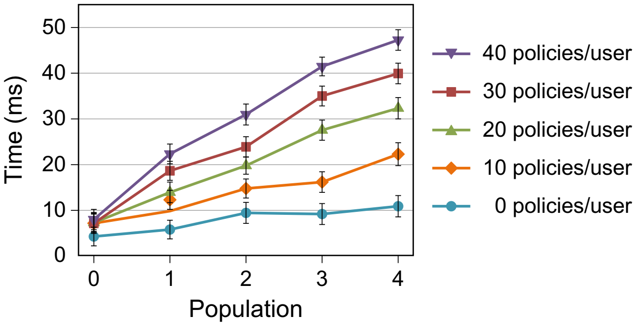


Fig. 6 Query time variation for different populations and profiles

In this section, we have demonstrated that policies forming profiles do not have a significant impact on the performance of h-MAS. Furthermore, it can be efficiently used to protect the privacy of user's information with no scalability problem.

7 Conclusions

We have proposed a privacy-preserving multicontext-aware solution called h-MAS that protects users' information in health scenarios. h-MAS is an evolution of MASTERY oriented toward health scenarios. It provides several privacy-preserving and context-aware profiles and suggests them to users of the proposed system. These profiles are formed by a pool of privacy policies so as to protect the users' location, personal information, the activities they are doing at any given time, and the information oriented toward the context in which they are located. The users of h-MAS can modify the profiles by adding, deleting, and modifying their policies to control what, where, when, how, and to whom they want to reveal their information.

As further steps in this research, we plan to migrate our architecture to a decentralized environment, by making use of federation mechanisms. We also plan to provide more intelligence to h-MAS in order to offer customized profiles that consider the actions performed by users on previous visits to the context. Finally, we plan to focus our proposal on the Medical Cyber-Physical Systems (MCPS) topic. MCPS is a relevant research topic that combines aspects like eHealth, privacy, context-awareness, network communications, and security. The privacy of patients' sensed information and contextual information are essential aspects of MCPS that our proposal can help to guarantee and manage.

Acknowledgments This work has been supported by a Séneca Foundation grant within the Human Resources Researching Training Program 2014, the European Commission Horizon 2020 Programme under grant agreement number H2020-ICT-2014-2/671672 - SELFNET (*Framework for Self-Organized Network Management in Virtualized and Software Defined Networks*), the Spanish MICINN (project DHARMA, *Dynamic Heterogeneous Threats Risk Management and Assessment*, with code TIN2014-59023-C2-1-R), and the European Commission (FEDER/ERDF).

References

1. Ngai EWT, Poon JKL, Suk FFC, Ng CC (2009) Design of an RFID-based healthcare management system using an information system design theory. Inf Syst Front 11(4):405–417
2. Huang LC, Chu HC, Lien CY, Hsiao CH, Kao T (2009) Privacy preservation and information security protection for patients' portable electronic health records. Comput Biol Med 39(9): 743–750
3. Schilit B, Adams N, Want R (1994) Context-aware computing applications. In: Proceedings of the 1st workshop on mobile computing systems and applications, pp 85–90
4. Abowd GD, Dey AK, Brown PJ, Davies N, Smith M, Steggles P (1999) Towards a better understanding of context and context-awareness. In: Proceedings of the 1st international symposium on handheld and ubiquitous computing, pp 304–307
5. Abbas A, Khan SU (2014) A review on the state-of-the-art privacy-preserving approaches in the e-Health clouds. IEEE J Biomed Health Inform 18(4):1431–1441
6. Gupta BB, Agrawal DP, Yamaguchi S (2016) Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global Publisher, USA
7. Veluru S, Rahulamathavan Y, Gupta BB, Rajarajan M (2015) Privacy preserving text analytics: research challenges and strategies in name analysis. Standards and standardization: concepts, methodologies, tools, and applications, pp 1415–1435
8. Wu R, Ahn GJ, Hu H (2012) Secure sharing of electronic health records in clouds. In: Proceedings of the 8th international conference on collaborative computing: networking, applications and worksharing, pp 711–718
9. Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller G (2011) Aspects of privacy for electronic health records. Int J Med Inform 80(2):26–31
10. Van Gorp P, Comuzzi M (2014) Lifelong personal health data and application software via virtual machines in the cloud. IEEE J Biomed Health Inform 18(1):36–45
11. Myles G, Friday A, Davies N (2003) Preserving privacy in environments with location-based applications. IEEE Pervasive Comput 2(1):56–64
12. Jagtap P, Joshi A, Finin T, Zavala L (2011) Preserving privacy in context-aware systems. In: Proceedings of the 5th IEEE international conference on semantic computing, pp 149–153
13. Huertas Celdrán A, García Clemente FJ, Gil Pérez M, Martínez Pérez G (2014) What private information are you disclosing? A privacy-preserving system supervised by yourself. In: Proceedings of the 6th international symposium on cyberspace safety and security, pp 1221–1228
14. Huertas Celdrán A, García Clemente FJ, Gil Pérez M, Martínez Pérez G (2016) MASTERY: A multicontext-aware system that preserves the users' privacy. In: Proceedings of the 2016 IEEE/IFIP network operations and management symposium, pp 523–528
15. Martino LD, Ni Q, Lin D, Bertino E (2008) Multi-domain and privacy-aware role based access control in eHealth. In: Proceedings of the 2nd international conference on pervasive computing technologies for healthcare, pp 131–134
16. University of Murcia (2016) h-MAS architecture and ontologies. http://dharma.inf.um.es/h-mas. Accessed 2 May 2017
17. Dentler K, Cornet R, Ten Teije A, De Keizer N (2011) Comparison of reasoners for large ontologies in the OWL 2 EL profile. Semant Web 2(2):71–87
18. W3C Recommendation (2012) OWL 2 web ontology language: structural specification and functional-style syntax, 2nd edn
19. W3C Member Submission (2004) SWRL: a semantic web rule language combining OWL and RuleML
20. Sirin E, Parsia B, Cuenca Grau B, Kalyanpur A, Katz Y (2007) Pellet: a practical OWL-DL reasoner. Web Semant Sci Serv Agents World Wide Web 5(2):51–53
21. The Apache Software Foundation (2016) The Apache Jena2 ontology API. http://jena.apache.org/documentation/ontology. Accessed 2 May 2017
22. W3C Recommendation (2008) SPARQL query language for RDF
23. The World Bank (2016) Percentages of medical information around the world. http://data.worldbank.org. Accessed 2 May 2017