A Warning on Software Interoperability in e-Health

Gianluca Lax

***Abstract*—Software interoperability refers to how a software system can be used with other software systems. One of the most relevant challenges in 2017 to reach software interoperability in e-health is to develop a standardized way of identifying patients. The recent Regulation (EU) N. 910/2014, eIDAS for short, enables secure mutual identification between citizens and public authorities, and this is achieved by a cooperative approach defined by the eIDAS Interoperability Architecture. In this paper, we analyze this software architecture and show that it may results in a privacy problem, if the identification procedure regards a health service. Moreover, a solution to this problem is proposed, which is based on a modification of the protocol defined by the eIDAS Interoperability Architecture to reach the goal of the anonymity of the service requested by the patient.**

***Index Terms*—Interoperability, privacy, e-health, eIDAS.**

I. Introduction

With the term software interoperability, we refer to the ease with which a software system can be used with other software systems. More formally, software interoperability can be defined as the ability of two or more systems or components or web services (software modules) to exchange information and to use information that has been exchanged. We have many examples of software interoperability, such us a web server and a browser that are able to work together because use the same protocols, or Web Services that are used to share data or to provide each other with some functionality.

A very important and recent challenge in software interoperability is improving healthcare interoperability, which is a top priority for providers, policymakers, and patients in 2017 [1]. Public and private sectors are working across the industry to facilitate seamless health data exchange between a multitude of health IT systems to coordinate care across various health settings nationwide. Years of health-care interoperability initiatives, health data exchange frameworks, and health IT standards have yielded considerable improvements in proliferating efficient information exchange. However, several challenges still bar stakeholders from achieving true interoperability for optimal care delivery and improved patient health outcomes [2].

Five challenges have been identified to reach interoperability in e-health, which are:

1) Developing a standardized way of identifying patients
2) Enforcing health IT interoperability standards across care settings facilities
3) Enforcing industry-wide interoperability measurement standards
4) Coordinating stakeholders across the industry
5) Ending information blocking and data sharing impediments.

As for as the first challenge (i.e., identifying patients), it is worth noting that the European Union (EU) has recently issued a recent regulation strongly related to this aspect, the regulation named eIDAS (electronic IDentification, Authentication and trust Services). It concerns the standards for electronic identification and trust services for electronic transactions to be used in the European Single Market. The aim of this regulation is to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

Concerning electronic identification, this Regulation enforces mutual recognition between Member States: When an electronic identification and authentication is required to access a service provided by a public sector body online in one Member State, the electronic identification means issued in another Member State should be recognized in the first Member State for the purposes of cross-border authentication for that service. The fragmentation of the market intended as the existence of different rules applying to service providers of Member States is one of the drawbacks that is overcome thanks to the adoption of this common regulatory system. This Regulation is applied from 1 July 2016, meaning that from this date a citizen of a Member State can access a service supplied by a service provider placed in another Member State by exploiting the same credential used with her/his national identity provider. This is achieved by a cooperative approach defined in the eIDAS Interoperability Architecture [3], which contains the technical specifications of the system architecture, the message format, attribute profile, cryptographic requirements, and so on. This is surely an important step for improving software interoperability in e-health, because patients are identified by a unique access credential (typically, user name and password).

In this paper, we study this topic and observe that the current implementation of the eIDAS interoperability architecture may results in a privacy problem, if the identification procedure regards a health service.

For example, consider the case of a citizen who is reserving a medical treatment in a Dialysis Center and uses an identification scheme compliant with eIDAS. Thanks to eIDAS, the citizen can use her/his digital identity to be identified by the Dialysis Center (without the need of doing a registration). However, the eIDAS protocol enforces that the

Manuscript received March 20, 2019; revised July 28, 2019.
Gianluca Lax is with University Mediterranea of Reggio Calabria, Reggio Calabria, Italy (e-mail: lax@unirc.it).

doi: 10.18178/ijmlc.2019.9.5.850

identity provider is aware about the identity of the service provider (i.e., the Dialysis Center): clearly, this can be enough to breach privacy because the identity provider can guess the disease of the citizen.

```xml
<samlp:AuthnRequest Version="2.0" ID="_XXX-XXX" IssueInstant="2018-01-01T12:00:00.000Z"
        Destination="https://www.example.com/profile/SAML2/Redirect/SSO"
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml:Issuer>http://www.example.org</saml:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
                        <Reference URI="#_XXX-XXX">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                                <DigestValue>XXX...</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>XXX...</SignatureValue>
                <KeyInfo>
                        <X509Data>
                                <X509Certificate>XXX...</X509Certificate>
                        </X509Data>
                </KeyInfo>
        </Signature>
        <samlp:NameIDPolicy AllowCreate="true" />
</samlp:AuthnRequest>
```

Fig. 1. An example of SAML message.

Beside detecting the risk of information leakage related to the use of the eIDAS authentication procedure, in this paper, we propose a solution by modifying the protocol defined by the eIDAS Interoperability Architecture to reach the goal of the anonymity of the service used by the patient.

The paper is organized as follows. In the next section, we survey the related work of the recent literature. In Section III, we provide the background need to understand the proposal, which is SAML and eIDAS. In Section IV, we present an overview of our solution, whereas in Section V, we describe the technical aspects related to our proposal. In Section VI, we discuss some aspects related to the security of our approach. Finally, in Section VII, we draw our conclusions.

II. Related Work

In this section, we survey the literature related to eIDAS and the problem of privacy in e-health, in order to highlight the importance of the addressed topic.

Using a content analysis of health department sites undertaken each year from 2000 to 2005, the authors of [4] investigated several dimensions of accessibility and privacy, such as readability levels, disability access, non-English accessibility, and the presence of privacy and security statements. They argued that although progress has been made at improving the accessibility and confidentiality of health department electronic resources, there remains much work to be done to ensure quality access for all Americans in the area of public e health.

Electronic health records (EHR) improve communication between health care providers, thus leading to better quality of patients' treatment and reduced costs. To reduce health data misuse, [5] proposes the system PIPE (pseudonymization of information for privacy in e-health), which provides a solution for implementing secure EHR architectures.

The definition set out in the Health Insurance Portability and Accountability Act (HIPPA) highlights that the confidential section of the electronic medical record needs to be protected and a mechanism to protect the patient's privacy is needed during electronic medical record exchange and sharing. The privacy protection mechanism can be categorized into four types, namely anonymity, pseudonymity, unlinkability, and unobservability. The authors of [6] tried to improve the unlinkability mechanism between patient and electronic medical record through cloud computing. According to this approach, the electronic medical record system in a hospital can be integrated, to facilitate the exchange and sharing of electronic medical records, and to provide smaller hospitals or clinics that have fewer resources with adequate electronic medical record storage space.

The study presented in [7] shows that both security and privacy aspects play an important role for acceptance and usage of medical assistive technologies. By a two-step empirical approach based on survey, users' requirements for the use of medical technologies were collected and evaluated in [8] to study the perceived importance of data security and privacy problems. Outcomes showed that both security and privacy aspects play an important role in the successful adoption of medical assistive technologies in the home environment. In particular, analysis of data with respect to gender, health-status and age (young, middle-aged and old users) revealed that females and healthy adults require, and insist on, the highest security and privacy standards compared with males and the ailing elderly.

In [9], a framework for authentication and authorization in e-health services is proposed. It aims to build the architecture for authentication and authorization within an e-health service system in order to build a secure and privacy protection e-health service system and protect medical records of patients in terms of information privacy. Differently from our approach, this proposal does not support digital identity management systems like eIDAS.

The authors of [10] propose a model-driven application-level encryption solution to protect the privacy and confidentiality of health data. In this approach, domain experts specify sensitive data which are to be protected by encryption in the application's domain model, whereas security experts specify the cryptographic parameters used for the encryption in a security configuration. Both specifications support different granularities of data to be encrypted and appropriate security levels.

The proposal described in [11] aims to put the security of the eIDAS transaction system on formal grounds. To this end, they propose a security model which ensures that a transaction system, satisfying the requirements in the model, provides strong authenticity properties of transactions. The model basically guarantees that both parties, card holder and service provider, can have confidence that they agree on the same transaction with the intended partner in a certain session. Their security model contrasts replay attacks or cloning of transactions across executions, in such a way that the secure transaction system remains immune against such attacks.

In [12], the authors propose a modification of SPID to allow user authentication by preserving the anonymity of the identity provider which grants the authentication credentials. This approach solves a problem different from the one we address. Moreover, it is not compliant with the eIDAS regulation.

E-Health clouds are gaining increasing popularity by facilitating the storage and sharing of big data in healthcare. However, such an adoption also brings a series of challenges, especially, how to ensure the security and privacy of highly sensitive health data. In [13], a three-factor authentication combining password, smart card and biometrics is proposed. It resists various existing attacks, such as impersonation attack in the registration phase, offline password guessing attack in the login and password change phase, and is able to provide user revocation. The drawback of this solution is that, differently from our proposal, it does not support single-sign-one.

Recently, [14] identified sociodemographic factors affecting privacy surrounding health data and explored the impact of health privacy capital on the use of health-related digital technologies and related perceptions. Health privacy capital was analyzed relative to demographic, social-contextual, and medical condition variables. Findings confirmed three key facets of health privacy capital-awareness of privacy: attitude toward the importance of privacy and data sharing, confidence in the ability to maintain privacy showed positive relationships between privacy capital and engagement, and outcomes related to health-related digital technology. On the other hand, this analysis found that the development of health privacy capital is susceptible to sociodemographic disparities. For instance, a higher level of education was related to all three dimensions of health privacy capital. Interactions between education and health privacy confidence were also significant in both dimensions of health outcomes, indicating that the positive impact of health privacy confidence is moderated by the lower level of education. This analysis shows the importance of the privacy in e-Health, thus motivating our proposal in this context. Finally, we observe that a preliminary and very short description (two pages) of this study appeared in [15].

III. SAML AND EIDAS

In this section, we introduce SAML and eIDAS, which are two topics which our proposal is strongly based on. We start by SAML.

SAML (Security Assertion Markup Language) is an open standard for handling authentication and authorization between an identity provider and a service provider. It is based on XML, which is the markup language used to exchange security assertions. The service provider exploits the identity provider to authenticate a user by means of an authentication assertion. On the basis of this assertion, the service provider decides whether to supply the user with some service. SAML defines the structure of the messages exchanged by the two actors without taking into account the method of authentication (which could be based on username and password, or one-time-password, or multi-factor authentication, or any other authentication form). In Fig. 1, an example of a SAML message used for authentication is shown (note that the structure of this message will be used in Section V).

SAML is widely used and referred by eIDAS, which is the second key topic we present in this section.

The Regulation (EU) N. 910/2014 [16] on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014 enables secure and seamless electronic interactions between businesses, citizens and public authorities. One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate and to ensure that secure electronic identification and authentication is possible for access to cross-border online services offered by Member States. Specifically, this Regulation allows people and businesses of the EU to use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available. It does not intervene with regard to electronic identity management systems and related infrastructures established in Member States, but provides Member States with the technical specifications to develop their own eIDAS-compliant implementation of eIDs.

The eIDAS Interoperability Architecture [3] specifies the components necessary to achieve interoperability among the eID schemes notified by Member States according to the eIDAS Regulation. The stakeholders considered in the specifications are:

1) The citizen/person to be identified/authenticated.
2) The relying party, which requires authenticity and integrity of the citizen identification data. Observe that this entity is called service provider in SAML.
3) The components of the eIDAS network used to fulfill the requirements of the relying party and the citizen.

Moreover, [3] defines also the following terms (the same terminology will be used in this paper):

- MS: State covered by the eIDAS regulation, i.e. a Member State of the European Union and/or the European Economic Area.
- Sending MS: the MS whose eID scheme is used in the authentication process, and sending authenticated ID data to the receiving MS.
- Receiving MS: the MS where the relying party requesting an authentication of a person is established.
- eIDAS-Node: an operational entity involved in cross-border authentication of persons. A Node can have two different roles:

a) eIDAS-Connector: an eIDAS-Node requesting a cross-border authentication.
b) eIDAS-Service: an eIDAS-Node providing cross-border authentication. (For the sake of presentation, we do not introduce here the possibility that the eIDAS Service can be based on proxy or implemented as middleware.)

The process used by a relying party to authenticate a person by the eID of the Sending MS can be summarized by the following steps.

1) The relying party sends an authentication request to the eIDAS-Connector responsible for the Sending MS. The eIDAS-Connector can be directly attached to the relying party (Decentralized MS) or operated by a separate entity (Centralized MS). The request contains an identifier of the MS whose eID scheme has to be used for the authentication.
2) The eIDAS-Connector sends a SAML-Request to the eIDAS-Service corresponding to the selected MS. This request must include the name of the relying party. Just the presence of this name results in a breach of privacy, thus motivating our proposal. For example, the knowledge that a user accessed a medical testing facility for an assertion is enough to breach privacy even if the contents of the assertion is kept confidential. It is worth noting that the simple removal of this name from the request would make the scheme unusable because this field is necessary for the response message (see the next steps).
3) The eIDAS-Service performs the authentication of the person according to the selected eID scheme and sends a SAML Response to the requesting eIDAS-Connector containing an encrypted SAML Assertion.
4) The eIDAS-Connector sends the received authenticated person identification data to the requesting relying party.

Clearly, at every step, the integrity and authenticity of a SAML message is checked and if any check fails, the procedure is aborted.

The diagram in Fig. 2 illustrates the main components in an eIDAS solution.

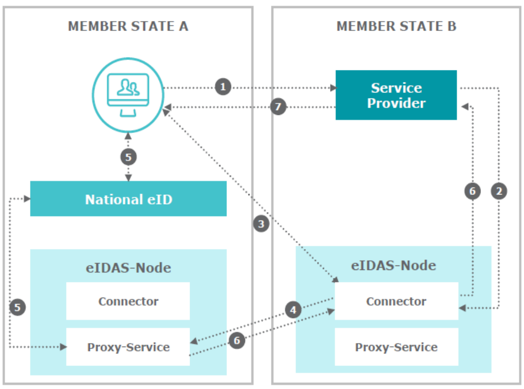

Fig. 2. The main components in an eIDAS solution.

IV. Our Proposal

In this section, we describe our proposal aimed to hide to the identity provider the identity of the relying party that provides the service requested by a citizen. For the sake of presentation, we describe how our technique is applied to a specific scenario, which allows us to refer to a real-life eID scheme: however, it is easy to understand that our approach can be applied to all other cases (i.e., eID schemes), thanks to the interoperability guaranteed by eIDAS. Moreover, we discuss more technical issues related to the implementation in Section V.

The considered scenario is illustrated in Fig. 3 and is composed of the following entities:

- I is an Italian citizen who has organized a holiday in another Member State of the European Union, say RMS (Receiving MS). Unfortunately, I is a patient needing a regular dialysis treatment.
- *RP* is a Dialysis Center located in RMS.
- RP_1, ..., RP_n are n relying parties. In our scenario, we assume that they are located in RMS but, in general, they can be located in any Member State of the European Union.
- S is an Italian eIDAS-Service.
- C is an eIDAS-Connector in RMS.
- I D is the Italian Identity Provider that guarantees the digital identity of I. The electronic identification scheme used in this case is SPID [17], which is the only one allowed in Italy.

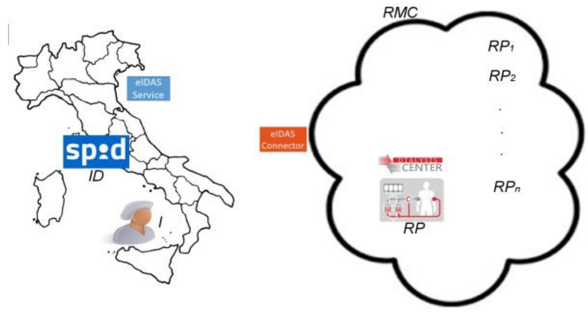

Fig. 3. The considered scenario.

The case we consider in our scenario concerns the need of I to reserve the medical treatments supplied by RP necessary during his holiday. This reservation can be done on-line, provided that the patient is identified by RP. Unfortunately, I have never accessed RP and has not any credential to be identified. Moreover, I and RP belong to two different Member States of the European Community. Thanks to eIDAS, I can use his Italian digital identity to be identified by RP. However, with the standard eIDAS protocol, this identification procedure has the side effect of informing ID that I am accessing a Dialysis Center, which can be enough to breach privacy. This is the problem highlighted in this paper, and a proposal to solve this problem is presented in the following.

In the countermeasure we propose to solve this problem, the identification procedure is modified in the following way (we will remark the steps which remain the same as in eIDAS).

1) When I visit the RP's web site and clicks the login button to start the eIDAS identification procedure, the authentication request is not directly sent to the eIDAS-Connector responsible for it (as done in the standard protocol). Instead, RP:

a) generates a non-negative integer *h* (hops); some considerations about the use of h are presented in Section

VI;

b) generates a pair of asymmetric keys K_p (public) and K_s (secret);
c) selects a relying party RP_i among $RP_1, ..., RP_n$;
d) creates a new authentication request AR containing also h and K_p, which is sent to RP_i;

2) When RP_i receives AR, it checks the value h. If $h > 0$, then RP_i;

a) decreases h by 1;
b) selects a relying party RP_j among $RP_1, ..., RP_n$;
c) forwards the received authentication request AR to RP_j (observe that the requests contain the updated value of h). Moreover, RP_j processes the received request in the same way as done by RP_i.

Otherwise, if h=0, then RP_i sends the authentication request to the eIDAS-Connector responsible for it and includes itself as relying party. In this way, this RP will be seen as the relying party requiring the user identification, thus hiding the identity of the actual relying party providing the service to I. Moreover, in this step, each involved relying party stores the information about the relying party from which the request has been received and the value of h and K_p, which are associated with the identifier of the authentication request. This association is stored by a map M using the identifier of the authentication request as key.

1) The eIDAS-Connector acts exactly as expected by the eIDAS protocol (see Step 2 of Section III).
2) As in Step 3 of Section III, the eIDAS-Service performs the authentication of C by forwarding the request to ID. Then, ID identifies C and sends a SAML Response to the requesting eIDAS-Connector containing an encrypted SAML Assertion. Moreover, the personal identification data of I are encrypted by K_p.
3) As in Step 4 of Section III, the eIDAS-Connector sends the received authenticated person identification data to the relying party from which the request was received.
4) Now, this relying party:

a) verifies the integrity and authenticity of the response message (i.e., that it comes from I D and it has not been modified) by exploiting its digital signature (this is a standard feature provided by eIDAIS);
b) verifies that the response message uses K_p to encrypt the person identification data (by using its map M);
c) selects the relying party RP_k from which the corresponding authentication request come from (again, by using M);
d) forwards the response message to RP_k. Clearly, when the response reaches the initial relying party that actually started the identification process (i.e., RP), the message forwarding is stopped.

5) Finally, RP receives the response message and:

a) Again verifies the integrity and authenticity of the response message;
b) uses K_s to decrypt the person identification data;
c) handles the reservation request done by the patient I according to its policy (this is clearly out of the scope of this paper).

The result of this procedure is that the identity provider is not aware about the service requested by the citizen, because the authentication request comes from a relying party different from the one actually requiring the patient identification. Moreover, all the relying parties involved in this request (by the forwarding mechanism) cannot know the person identification data because they are encrypted by an asymmetric key pair generated by the Dialysis Center (i.e., RP).

In the next section, we present more technical issues related to the implementation of our protocol, whereas we discuss its effectiveness against malicious behaviors in Section VI.

V. Implementation

We start our discussion about the technical issues related to the implementation from the communication between the nodes of the network. First, we observe that, as required by eIDAS, all communications are performed via the citizen's browser and protected by Transport Layer Security (TLS) [18], version 1.1 or higher.

The cipher suite used by TLS defines the key exchange algorithm, the subsequently used symmetric encryption and integrity check algorithms: In order to guarantee perfect forward secrecy, the allowed mechanism of key agreement and authentication must be DHE_RSA using AES-128 for encryption and SHA-256 for integrity check. Clearly, more secure cipher suites can be also used: for example, key exchange algorithms which use elliptic-curve cryptography such as ECDHE_RSA, or encryption based on AES-256, or digest computed by SHA-384. However, if elliptic-curve cryptography is used, then the key length must be at least 224 bits.

Concerning the TLS session, after the parties negotiate the algorithms and the keys to be used, the authentication is done by X.509 certificates [19]. The content of the communication is protected by SAML, which ensures confidentiality, authenticity and integrity of the person identification data, and secure identification of communication end-points: for this purpose, authentication requests and response messages are signed by the sending party.

Authentication requests can be transmitted preferably by HTTP Redirect binding if the message size is short enough to allow this mechanism, in order to reduce message latency; otherwise, HTTP POST binding should be used.

The public key K_p introduced in our approach is included as a self-signed X.509 certificate in the authentication request, by the <ds:X509Data> element of the SAML AuthnRequest: indeed, this element contains one or more identifiers of keys or X.509 certificates.

In Step 2.(c) of Section IV, we have seen that the reference to the current relying party handling the request is updated at each forwarding with the reference to the current relying party handling the request. From the technical point of view, this is obtained by changing the attributes ProviderName and AssertionConsumer ServiceURL, in such a way to hide the actual relying party requiring the identification.

VI. Discussion

In this section, we discuss some important aspects related to our proposal. The first aspect concerns its effectiveness. A reader could observe that the forwarding mechanism allows a relying party to deliberately sabotage the identification procedure by simply stopping to forward the request or the response. This is clearly true. However, we can observe that, the odds of this event are higher with the increasing of the value h (which, we recall, defines the number of forwards of the request before it reaches the eIDAS-Connector). The higher h, the greater are the relying parties involved in the forwarding. In particular, h = 0 avoids the possibility that some relying party can deny the identification: clearly, in this case, no forwarding mechanism is adopted. However, the identity provider cannot guess (or be certain) that h = 0, because this value is chosen by the relying party.

Moreover, a reputation mechanism could be used to reduce trust in relying parties involved in an identification procedure that failed, in such a way that this misbehavior is detected and this relying party is isolated.

Another important aspect to be considered regards personal data. A relying party involved in the forwarding mechanism could change the public key K_p used in the authentication request with a self-generated one, in order to sniff personal identification data from the response. However, this attack is detected when the response comes back, because each relying party checks the integrity of the public key used in the response. Also in this case, a reputation mechanism could be used to contrast this action. It is worth noting that, beside the knowledge of the name of the citizen, the malicious relying party cannot take any other advantage from this attack (because, the relying party should provide the citizen with a service).

As observed above, these malicious actions have the only effect to abort the authentication procedure. However, this is not a critical result: indeed, also in absence of attacks, the authentication procedure can fail for several reasons, such as wrong credentials or connection time-out. The standard response to these events is to run another authentication procedure: as the relying parties (selected for the forwarding procedure) change at each request, the second time that the authentication is run, it is very likely that the malicious relying party is not involved in the forwarding mechanism, so that the procedure can be carried out.

We conclude our analysis by observing that this theme is strongly related to the EU's General Data Protection Regulation, which aimed to harmonize data privacy laws across Europe and protect EU citizen’s privacy. From this point of view, this regulation is a good motivation of our proposal. However, since the request of privacy contrasts with the need of auditing and transparency of service usage, a solution with parameters whose setting allows the tuning between probability of identifying people and their right to privacy is welcome. This is the case of our solution: by setting the parameter h=0, no privacy is provided, and this can be done for very critical services. In contrast, at each increasing by 1 of the value h, a new intermediate party is introduced in the communication, thus increasing privacy. However, auditing and transparency of service usage can be guaranteed by forcing each party to log each operation carried out in the protocol (in particular, the sender and/or receiver of the messages) and to disclose these logs in case of need, in such a way that an authority can recover what happened by collecting and merging logs from the involved parties.

VII. Conclusion

Software interoperability is an important topic, and recently, the eIDAS Interoperability Architecture has been issued to provide European Union citizens with the possibility to use a unique identification credential valid over the whole European Union to access several services. Beside the benefits derived from eIDAS, in this paper, we observed that the current implementation of the eIDAS interoperability architecture may results in a privacy problem, if the identification procedure regards a health service. We showed by a real-life example a case of privacy breach, in which an identity provider can guess the disease of a patient.

Beside detecting the risk of information leakage related to the use of the eIDAS authentication procedure, in this paper, we proposed a solution by modifying the protocol defined by the eIDAS Interoperability Architecture to reach the goal of the anonymity of the health service used by the patient.

Acknowledgment

This work has been partially supported by INdAM – GNCS Project 2019 "Innovative methods for the solution of medical and biological big data".

References

[1] A. Walinjkar and J. Woods, “Fhir tools for healthcare interoperability,” *Biomedical Journal of Scientific and Technical Research*, 2018.

[2] Top 5 challenges to achieving healthcare interoperability. (2019). [Online]. Available: https://ehrintelligence.com/news/top-5-challenges-to-achieving-health care-interoperability

[3] eIDAS - interoperability architecture. (2018). [Online]. Available: https://ec.europa.eu/ cefdigital/wiki/download/attachments/46992719/eidas_interoperabilit y_architecture_v1.00.pdf

[4] D. M. West and E. A. Miller, “The digital divide in public e-health: Barriers to accessibility and privacy in state health department websites,” *Journal of Health Care for the Poor and Underserved*, vol. 17, no. 3, pp. 652–667, 2006.

[5] B. Riedl, V. Grascher, S. Fenz, and T. Neubauer, “Pseudonymization for improving the privacy in e-health applications,” in *Proc. the 41st Annual on System Sciences*, pp. 255–255, 2008.

[6] Z. R. Li, E. C. Chang, K. H. Huang, and F. Lai, “A secure electronic medical record sharing mechanism in the cloud computing platform,” in *Proc. the 15th International Symposium on Consumer Electronics*, pp. 98–103, 2011.

[7] W. Wilkowska and M. Ziefle, “Perception of privacy and security for acceptance of e-health technologies: Exploratory analysis for diverse user groups,” in *Proc. the International Conference on Pervasive Computing Technologies for Healthcare*, 2011, pp. 593–600.

[8] W. Wilkowska and M. Ziefle, “Privacy and data security in e-health: Requirements from the user’s perspective,” *Health Informatics Journal*, vol. 18, no. 3, pp. 191–201, 2012.

[9] S. Han, G. Skinner, V. Potdar, and E. Chang, “A framework of authentication and authorization for e-health services,” in *Proc. the 3rd ACM Workshop on Secure web Services*, pp. 105–106, 2006.

[10] Y. Ding and K. Klein, “Model-driven application-level encryption for the privacy of e-health data,” in *Proc. the Conference on Availability, Reliability, and Security*, 2010.

[11] F. Morgner, P. Bastian, and M. Fischlin, “Securing transactions with the eidas protocols,” in *Proc. the IFIP International Conference on Information Security Theory and Practice*, pp. 3–18, 2016.

[12] F. Buccafurri, L. Fotia, G. Lax, and R. Mammoliti, “Enhancing public digital identity system (SPID) to prevent information leakage,” in *Proc. the International Conference on Electronic Government and the Information Systems Perspective*, pp. 57–70, 2015.

[13] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

[14] Y. J. Park and J. E. Chung, "Health privacy as sociotechnical capital," *Computers in Human Behavior*, vol. 76, pp. 227–236, 2017.

[15] G. Lax, "Privacy-preserving access to e-health systems." in *Proc. the 11th PErvasive Technologies Related to Assistive Environments Conference*, pp. 120–121, 2018.

[16] eIDAS Regulation (Regulation (EU) N°910/2014). [Online]. Available: https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

[17] SPID - Public system for digital identity. (2018). [Online]. Available: https://www.spid.gov.it/

[18] T. Dierks, "The transport layer security (TLS) protocol version 1.2," 2008.

[19] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Rfc 5280: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," *Internet Engineering Task Force (IETF)*, 2008.

Gianluca Lax is an assistant professor of computer science at the University Mediterranea of Reggio Calabria, Italy. In 2005, he received his PhD in computer science from the University of Calabria.

In 2013, he got the habilitation as associate professor of computer science by the Italian National Scientific Qualification Procedure and, in 2018, he got the habilitation as full professor of computer science. His research interests include information security and social network analysis. He is an author of more than 100 papers published in top-level international journals and conference proceedings. He serves as a referee for many international journals and is in the program committee of many conferences. He is also included in the editorial board of several international journals and participates in many funded projects.