POLITECNICO DI TORINO
Repository ISTITUZIONALE

Providing Login and Wi-Fi Access Services With the eIDAS Network: A Practical Approach

Original
Providing Login and Wi-Fi Access Services With the eIDAS Network: A Practical Approach / Berbecaru, Diana Gratiela; Lioy, Antonio; Cameroni, Cesare. - In: IEEE ACCESS. - ISSN 2169-3536. - ELETTRONICO. - 8:(2020), pp. 126186-126200. [10.1109/ACCESS.2020.3007998]

Availability:
This version is available at: 11583/2840618 since: 2021-06-03T16:06:15Z

Publisher:
Institute of Electrical and Electronics Engineers Computer Society

Published
DOI:10.1109/ACCESS.2020.3007998

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

24 April 2024

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 14, 2020, accepted June 4, 2020, date of publication July 8, 2020, date of current version July 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007998

Providing Login and Wi-Fi Access Services With the eIDAS Network: A Practical Approach

DIANA GRATIELA BERBECARU, (Member, IEEE), ANTONIO LIOY, (Member, IEEE), AND CESARE CAMERONI

Dipartimento di Automatica e Informatica, Politecnico di Torino, 10129 Torino, Italy

Corresponding author: Diana Gratiela Berbecaru (diana.berbecaru@polito.it)

This work was supported by the Framework of the eID for Universities (eID4U) Project, Co-Funded by the European Union's Connecting Europe Facility, Call for Proposals Connecting Europe Facility (CEF) Telecom Call 2017 (Proposal Code 2017-EU-IA-0051), under Grant INEA/CEF/ICT/A2017/1433625.

ABSTRACT The digital identity (or electronic identity) of a person is about being able to prove upon authentication who one is on the Internet, with a certain level of assurance, such as by means of some attributes obtained from a trustworthy Identity Provider. In Europe, the eIDAS Network allows the citizens to authenticate securely with their national credentials and to provide such personal attributes when getting access to Service Providers in a different European country. Although the eIDAS Network is more and more known, its integration with real operational services is still at an initial phase. This paper presents two eIDAS-enabled services, *Login with eIDAS* and *Wi-Fi access with eIDAS*, that we have designed, implemented, deployed, and validated at the Politecnico di Torino in Italy. The validation study involved several undergraduate students, who have run the above services with their authentication credentials and platforms and with minimal indications on their usage. The results indicate that the services were beneficial. Several advantages exist both for the users and for the Service Providers, such as resistance to some security attacks and the possibility to adopt the service without prior user registration (*e.g.* for short meetings, or in public places). However, some students expressed doubts about exploiting their national eID for Wi-Fi access, mainly in connection with usability and privacy issues. We discuss also these concerns, along with advantages and disadvantages of the proposed services.

INDEX TERMS Cross-border authentication, eIDAS regulation, electronic identification, login service, wi-fi access service.

I. INTRODUCTION

The possibility to prove the identity of a person is a primary requirement in online services handling highly sensitive or critical data. Nevertheless, even in less critical services, like Wi-Fi access, secure user authentication solutions are needed to avoid scenarios where the attackers impersonate a valid user (by exploiting weak authentication credentials) and then perform more complex security attacks.

To get access to public or private services, several countries across Europe have developed various solutions to allow citizens to use their digital or electronic identity (eID). In the first place, an authentication credential, like for example a cryptographic smart card, is given to the citizen to be used for authentication and identification purposes. Such cards are considered highly secure and typically contain some personal data and the cryptographic material (a digital certificate and the corresponding private key) to be used for the authentication procedure. This approach has been used so far in several countries like Italy, France, Germany, Austria, Spain, and Portugal. In Europe, in 2020, it is foreseen that citizens will hold more than 250 million eID (smart) cards, which captures half of the total population of 500 million citizens [1]. However, smart-cards pose various problems, from difficult technical integration into applications to complex usage by a citizen with basic technological knowledge. So various alternative user-friendly solutions have appeared for network authentication and identification. For example, the authentication credential could be a reusable password assigned to a citizen in a secure way, to be used alone or in conjunction with a one-time password generated or obtained via a personal device, such as a mobile phone.

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Yan.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

A. EIDAS BASIS

Over time, several European Union (EU) Member State (MS) countries developed specific solutions or protocols to exploit the digital identities at national level, such as the SPID protocol in Italy (further described in Section III-A). On the other hand, several EU-funded projects, such as the STORK [2], FutureID [3], and eID@Cloud [4] ones investigated how the various digital identity systems of different countries can be interconnected and deployed in a unified infrastructure. The STORK project defined and implemented an eID interoperability framework as well as its exploitation in some real use cases, like safe chat or academic student registration. In particular, STORK addressed the legal impact and the recognition of eIDs, it defined a so-called ''STORK person identifier'', and it addressed some privacy issues on the (personal) data transfer through the framework.

The eIDAS (**e**lectronic **ID**entification, **A**uthentication, and trust **S**ervices) Regulation 910/2014 for electronic transactions in the internal market, which put the basis for the legal recognition of eIDs across the EU, exploited the STORK findings and results. Moreover, the software for the eIDAS-Nodes has also inherited parts of the STORK code. Currently, the European Commission (EC), through its Connecting Europe Facility (CEF) programme, and in particular via the CEF eID Building Block is performing several activities to support eIDAS implementation and adoption. In practice, CEF offers a set of eID services composed of the technical specifications, the software, the testing services and the supporting services. In particular, CEF maintains the eIDAS specification [5], it periodically updates and distributes the reference code for the eIDAS-Nodes [6] composing the eIDAS Network, and it performs the validation of the eIDAS-Nodes in the various MS countries. Moreover, it provides information on the current state-of-play of eID in Europe such as the eIDAS-Node implementation status per country [7], or the overview of the eID schemes per country [8]. The Innovation and Networks Executive Agency (INEA) of the EC promotes and funds various projects under the CEF Telecom calls (eIdentification & eSignature) to facilitate the integration of public and private service providers with the eIDAS Network.

Throughout this paper, we call *notified authentication credential* (*NotifiedAuthC*) one provided by an IdP (Identity Provider) implementing a notified eID scheme in an EU country. Such credentials are typically different from the ones that commercial companies or organizations issue to their registered users for access to specific business services.

In many countries, dedicated government agencies perform citizen identification and issue the *NotifiedAuthC* to them. In other countries, also private entities (such as banks or telecom operators) can perform this task. For example, this is the case of Italy where commercial IdPs exist, such as InfoCert SpA or Poste Italiane, provide *NotifiedAuthC* to the Italian citizens. Since some identification procedures and authentication methods are more secure than others, the concept of ''level of assurance'' (LoA) has appeared. In brief, LoA classifies electronic credentials into three levels depending on their security, robustness, and issuance process [1]. Currently, three assurance levels exist in eIDAS: Low, Substantial, and High. They are based on the ISO-29115 [9] standard and the Quality of Authentication Assurance (QAA) concept defined in the STORK project [10]. Countries individually map the characteristics of their eID schemes to the eIDAS LoA levels, for example as documented in [11] and [12].

B. MOTIVATION

Even though several works [13] describe the eIDAS Network, the protocol, and its evolution, its integration with real services usable by the citizens is still an open task. Some previous works addressed the connection of generic FIWARE-based OAuth 2.0 services to the eIDAS infrastructure [14], or the registration of Erasmus students at visiting universities [15]. In general, as stated in [16], ''current and future problem in integrating identity management systems is the myriad of service providers that are not willing (and/or not capable) to implement large modifications in their systems''. The solutions addressing this problem should be technically sound, scalable, economically viable, convenient for human users, and should recognize inter-organizational aspects.

This paper describes the design and implementation of two services integrated with the eIDAS Network, namely *Login with eIDAS* and *Wi-Fi access with eIDAS*. In principle, these services have to securely authenticate and identify a user before granting access to the service. Additionally, they might require a restricted set of personal attributes, *e.g.* name and surname, and they might need additional specific attributes for authorization purposes. For example, a possible authorization policy could state that Wi-Fi access is granted only to persons fulfilling special requirements, such as the ones participating in a specific meeting or event.

Implementing an eIDAS-enabled Login service is not trivial, primarily because there is no unique and persistent identifier for every single person across the EU. Unique citizen identifiers typically exist in many countries, but: 1) often, they are not persistent, that is for the same person, they might change over time; 2) they might not be transferred abroad, due to national privacy legislation;) they should not be shared among different Service Providers (SPs) to avoid user profiling, which implies that possibly other identifiers need to be derived from the national one; 4) in some countries, they might not be defined at all. A unique identifier could be considered a mean of potential mass-surveillance and a hit to privacy, so other forms of identification might be used [17].

On the other hand, also implementing an eIDAS-enabled Wi-Fi access service is not straightforward. Many SP captive portals nowadays use dedicated hardware, *e.g.* a Wireless LAN Controller (WLC), and the SP directly registers the users on its backend, typically with a username and password. So, an additional dedicated application, invoked by the WLC, is required to communicate with the eIDAS Network for user authentication and to transform the retrieved data into a registered user recognized by the WLC. Moreover,

since the portal denies all traffic until a user is properly authenticated and authorized, the SP has to configure additional information before the authentication process can take place. The SP cannot deny all traffic to unauthenticated users but it must permit communication with the components of the national eID schemes and the intermediate network elements.

C. CONTRIBUTIONS

In summary, the main contributions of this paper are the following ones.

(1). The design and implementation of a Login service allowing user authentication with national eIDs via the eIDAS Network. We discuss the lack of a unique identifier (persistent) for every citizen across the EU, and we propose a solution addressing the user identification by exploiting the natural person identifiers. To build this service, we have integrated and transformed data managed by different parties, *i.e.* the Student Service Office, the eIDAS-Node, and the IdPs. In this way, other SPs may understand how to connect to the eIDAS Network.

(2). The design and implementation of a Wi-Fi access service, in which the users exploit their national eIDs and the eIDAS Network to obtain Wi-Fi access. This service may extend the standard Wi-Fi access already available in academic institutions, to support non academic users too. More in general, it may be helpful where the SP wants to provide Wi-Fi access via citizen's national eID without prior user registration. Finally, the service might be adopted in high-security environments where the Wi-Fi access with username and password is considered insecure, so the user would be required to use a strong credential, such as that of eIDAS level Substantial and High.

D. ORGANISATION

The paper is organized as follows. Related works are presented in Sec. II. The eIDAS Network, protocol, and attributes as well as the main aspects of the SPID system in Italy are briefly discussed in Sec. III. The detailed design and implementation of the Login with eIDAS and Wi-Fi access with eIDAS services are described in Sec. IV and Sec. V. Sec. VI describes service validation made by a set of users we have involved in testing our scenarios. Finally conclusions appear in Sec. VII.

II. RELATED WORK

A. INTEGRATION OF EIDAS NETWORK WITH OTHER PRE-EXISTENT SYSTEMS

Identities, in general, can be assigned to individuals, legal entities (companies, partnerships), but also to assets (*e.g.* cars, buildings), or software processes. However, digital identities are mostly associated with individuals, that is with natural or legal persons. The identities and the attributes about them, their efficient collection and processing, are gaining increasing interest not only to build more efficient public administration solutions but also in building smart cities or even for Internet of Things [18]. Some solutions, like the blockchain-based identity proposed in [19], collect several attributes and securely transmit them to other systems components for verification and to create a digital identity.

In eIDAS, no single unified solution exists for combining the basic identification attributes for a person (*e.g.* her name, surname, and date of birth) with other attributes about that person (*e.g.* her citizenship, academic title, or her role in an organization). While the personal attributes are typically retrieved from the national eID card or from an IdP, the additional attributes might be retrieved from other entities. Nevertheless, real services typically need many of them, for example citizenship is mandatory for voting, while the academic title is needed to apply for jobs or for course registration.

Two different directions exist to merge user authentication through eIDAS and user attributes management. In the first approach, existing platforms or frameworks handling different personal attributes, like academic title or healthcare data, add support for eIDAS authentication. For example, the HEALTHeID project [20] integrated eIDAS authentication into OpenNCP [21], a framework used to retrieve cross-border healthcare attributes. Another example is MyAcademicID, which aims to enable eIDAS authentication into the eduGAIN framework [22]. In this kind of solution, the main objective is to allow eIDAS authentication to access the existing services and then to combine the basic attributes retrieved through eIDAS with other personal data, already available in the platform. The attribute aggregation requires to securely link the data obtained through eIDAS to other data stored in the framework or retrieved through an alternative protocol. Since currently there is no unique person identifier valid globally, but rather each country, organization, or framework defined its own user identifier, the attribute aggregation is not automatic and normally requires some user involvement.

In the second approach, the eIDAS-Nodes are enhanced to support new (sector-specific) attributes. Moreover, they retrieve attributes both from the IdPs and from other potential additional entities, the Attributes Providers (APs), by extending the specific interface of the eIDAS-Node. The eID4U project [23] exploited this approach. The main advantage, in this case, is that the eIDAS-Node strongly orchestrates the citizen authentication through eIDAS and the attribute retrieval and aggregation. The main disadvantage is that the eIDAS services either need to be built from scratch, or they need to be adapted to the local systems and formats in place at the SPs and APs. Moreover, changes in attributes formats might trigger changes in the eIDAS-Nodes, or at least in its *Specific* part. This implies delays in updating the eIDAS-Nodes and deploying them into production (if the operators of the eIDAS-Nodes authorize such transition), and the necessity to perform interoperability tests.

B. LOGIN AND WI-FI ACCESS SERVICES: EXISTING SOLUTIONS AND INTEGRATION WITH EIDAS

The Login and Wi-Fi access services are frequent, well-known services, and several solutions exist for their implementation.

Eduroam [24] is a world-wide international roaming service providing network access to people in research and education organizations (like teachers, researchers, and students) when they are visiting other institutions. In some countries, the service is also available in other places like libraries, museums, railway stations, and airports. Eduroam authentication is provided by the user's home institution and it is based on IEEE 802.1x and a hierarchy of RADIUS servers [25], which typically consists of three levels: organizational, national, and global. When the local RADIUS server can't authenticate the guest user because she is not among the local users, the user's credentials are forwarded to the home institution RADIUS server passing through the national level Eduroam RADIUS server and, if needed, the top level Eduroam RADIUS server. In this way, users don't need new credentials to access the network of the visited institution, but on the other hand it is not possible to use stronger authentication credentials other than username and password.

Although widely deployed and used, Eduroam presents some drawbacks, such as single point of failure and privacy leakage. If one of the RADIUS servers in the hierarchy is down, this impacts the overall service. Identity theft vulnerabilities and MITM (Man-in-the-Middle) attacks in Eduroam have been investigated in [26], along with some possible countermeasures. Other authors [27] proposed to enhance Eduroam security via a new trust hierarchy based on RADIUS/TLS [28], while Liu and Goto [29] proposed a scheme aimed to improve Eduroam stability and performance.

Some blockchain-based solutions for Wi-Fi access exist too. Trustroam [30] proposes a blockchain-based distributed authentication scheme for cross-domain Wi-Fi access, which prevents the single point of failure and privacy leakage. An authentication method exploiting Bitcoin 2.0 for a more secure Wi-Fi access has been proposed too [31].

Authors in [32] proposed a method for dynamic firewall reconfiguration based on data (meta-attributes and user attributes) retrieved through the STORK infrastructure. Additionally, they discussed an important aspect to be considered in the services exploiting federated identity management infrastructures for network access: the SP needs to apply some authorization decisions *before* the user authentication is complete. In practice, the SP has to whitelist access to some endpoints for permitting users to reach their IdPs. The same authors extended this concept into a general one, named authorize-then-authenticate, and proposed some possible implementations [33]. The whitelisting feature is required also in the Wi-Fi access service proposed here.

III. AUTHENTICATION THROUGH EIDAS AND SPID

The eIDAS Network is composed of several national nodes, called eIDAS-Nodes, and it supports two models, proxy and middleware. In the proxy model, an EU MS runs the eIDAS-Node, which is composed of two logical elements: an eIDAS-Proxy-Service (in short, eIDAS Proxy) and one (or more) eIDAS-Connector(s) (in short eIDAS Connector), as shown in Fig. 1. Note that the specification distinguishes among the *Sending MS* and the *Receiving MS*. The Sending MS is the one whose eID scheme is used in the authentication process, and thus it sends the authentication responses to the Receiving MS. The Receiving MS is the one where the SP (also called Relying Party, RP) requests authentication of a person before providing a service. Note that in this paper we consider only natural persons, while eIDAS also covers legal persons, or a natural person representing a legal one.

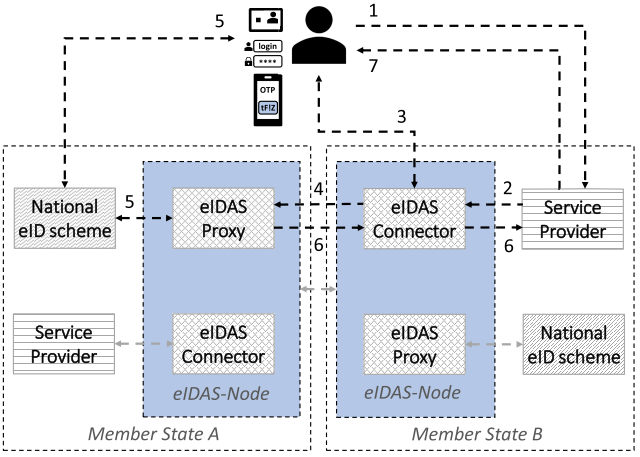

FIGURE 1. High level view of eIDAS architecture (proxy model).

The middleware model, adopted basically by Germany, does not require the Sending MS to run an eIDAS Proxy but it demands other Receiving MS to operate a *Middleware* software. This element implements an eIDAS-Middleware-Service, which is provided by the Sending MS [34]. In the proxy model, the national eIDAS Proxy connects to the national accredited IdPs implementing a (notified) electronic identity scheme under eIDAS to provide cross-border authentication. Moreover, the eIDAS Connector is connected with the SPs requesting cross-border authentication to persons that access their services. The eIDAS-Nodes communicate via a dedicated eIDAS protocol [5], which is based on the SAML 2.0 Web Browser SSO Profile [35] to transfer authentication data and eIDAS attributes. Each eIDAS-Node shares (eIDAS) SAML metadata with the other eIDAS-Nodes through a specific mechanism.

The communication between IdPs and SPs with the national eIDAS-Node is specific to each country. For example, if the eIDAS-Node and the national SPs and IdPs communicate via the SAML protocol, then they share national SAML metadata.

As shown in Fig. 1, when a person tries to access an eIDAS-enabled service (step 1), cross-border authentication is delegated from the SP to its national eIDAS Connector (step 2). Next, the citizen selects the country in which she will authenticate (step 3) and subsequently the eIDAS authentication request is forwarded to the eIDAS Proxy of the citizen's country (step 4). The eIDAS authentication request is handled by the eIDAS Proxy according to the MS specific approach. Typically, a new authentication request is constructed by the eIDAS Proxy and is sent through the user's browser to the national IdP implementing the national eID scheme, where the citizen is asked to authenticate with a national eID (step 5). For example in Italy, the eIDAS authentication request is converted into a SPID authentication request. Upon successful citizen authentication, the eIDAS authentication response, which contains also the requested (personal) attributes, is returned through the eIDAS Network back to the requesting SP (step 6). Finally, the SP grants/denies access to the service based on the authentication response received (step 7). User consent is typically asked twice: in step 3 to inform the user of the attributes that will be requested, and in step 6 before transferring their values to the other eIDAS Node. Each eIDAS-Node is composed of a *Specific* part and a *Generic* part (common to all the eIDAS-Nodes). The functional modules have been redesigned over time, so for example the version 2.x of the eIDAS code proposes a more flexible approach in the Specific part.

According to the specification, only a restricted set of natural person attributes may pass through the eIDAS-Nodes [36]. Four of them are mandatory, in the sense that the national eID scheme must always return their values to the eIDAS Proxy: FamilyName, FirstName, DateOfBirth, and PersonIdentifier. This set of mandatory attributes is named eIDAS Minimum Data Set (MDS). Other attributes like BirthName, CurrentAddress, PlaceOfBirth, and Gender are optional: they may be requested but the national eID scheme might not return their values to the eIDAS Proxy.

Are these attributes enough to build real services? In some cases, they are not sufficient and new ones need to be defined and supported in the eIDAS-Nodes. For example, in [15] new attributes needed to register the students in a visiting university have been enabled on the eIDAS-Nodes. In the services discussed here, we encountered two situations.

In case of Login with eIDAS, the eIDAS MDS attributes are rather inadequate. The Login service needs a persistent unique identifier for any citizen across the EU, widely recognized and used in different domains, or at least in a specific sector (*e.g.* academia). Unfortunately such an identifier does not exist in eIDAS, for several good reasons discussed above. Even the eIDAS attribute named PersonIdentifier is not unique for one person and it might change in time so it is not directly usable for the Login service.

In case of Wi-Fi access with eIDAS, the attributes in the eIDAS MDS are too many and sensitive. Thus, the users might deny user consent for their retrieval or may ask for supplemental guarantees with respect to the processing and storage of their personal data on the SP side.

A. AUTHENTICATION THROUGH SPID IN ITALY

The Public Digital Identity System (in Italian, SPID - Sistema Pubblico di Identità Digitale) [37] is a federated identity system allowing Italian citizens to access public administration SPs by using SPID credentials issued by the SPID IdPs. Currently, support for SPID is mandatory in public services, *e.g.* to access Italian university portals or the services offered by ministries and governmental agencies. As mentioned in [38], SPID is a public identity system which permits public and private entities to act as IdP, provided that they are accredited by the Agency for Digital Italy (AgID). The SPID IdPs have to ensure a suitable procedure for the initial identification of citizens, and have to provide authentication credentials called *SPID credentials* of different levels of security.

On the other hand, since SPID is mandatory for public services, all public administrations must allow citizens to access their online services via SPID credentials. Private service providers can also join SPID by following a specific technical and administrative procedure [39]. SPID IdPs and SPs interact with AgID, which has a central role in creating the circle of trust between them, and in maintaining and distributing accurate information about them through a dedicated ''SPID Registry'' [40].

Examples of Italian SPs that have added support for SPID authentication are Agenzia delle Entrate (Fiscal Agency in Italy), or INPS (Istituto Nazionale per la Previdenza Sociale), the entity in charge with social and retirement procedures. They allow citizens to use their SPID credentials for tax declarations or to handle maternity leave, emergencies, or retirement procedures. Currently, there are 4283 public administration SPs and 7 private sector SPs, and 9 IdPs have issued nearly 7 million SPID credentials [41].

SPID users can authenticate by using three different levels of security, called Level of Assurance (LoA):

- one-factor authentication, for example username and password. It corresponds to the Low security level, called *SpidL1*, which was mapped to eIDAS Low LoA.
- two-factor authentication, for example username, password, and one-time password (OTP). It corresponds to the Intermediate security level, called *SpidL2*, which was mapped to eIDAS Substantial LoA.
- two-factor authentication and secure device, for example username, password, and public-key authentication based on a smartcard. It corresponds to High security level, called *SpidL3*, which was mapped to eIDAS High LoA.

The SPID protocol [40] exploits the SAML 2.0 Web Browser SSO Profile to exchange authentication messages between SPs and IdPs. These entities share their own SAML metadata through the AgID-maintained SPID Registry [42]. Each SP defines in its own SAML metadata one or more sets of requested attributes, and each set is identified by a numeric

index. When the SP sends the authentication request (by using the HTTP Redirect binding or the HTTP POST binding), it refers to the attribute set by specifying its index number. After user authentication and user consent to attributes transfer, the IdP answers with an authentication response by using the HTTP POST binding. SPID SAML messages are signed, but the attributes values are not encrypted.

B. THE ROLES OF IDP PROXY AND SP PROXY IN CONNECTING SPID TO EIDAS

SPID defines a series of user attributes including spidCode, name, familyName, dateOfBirth, placeOfBirth, address, gender, that need to be mapped onto the eIDAS attributes. To adapt the eIDAS Network to the SPID system, the FICEP (First Italian Cross-border eIDAS Proxy Service) project defined two additional modules, namely the SP Proxy and the IdP Proxy. The SP Proxy translates the messages between the SPID SPs and the Italian eIDAS Connector, while the IdP Proxy translates the messages between the SPID IdPs and the Italian eIDAS Proxy Service, as shown in Fig. 2. Thus, the SPID SPs communicate with the eIDAS Connector via the SP Proxy, while other SPs may communicate directly with the eIDAS Connector by exploiting the eIDAS protocol. The mapping between the SPID attributes and the eIDAS ones is shown in Table 1. Since an Italian citizen may have multiple SPID credentials provided by different IdPs, the spidCode is different depending on which IdP the person has used for authentication. Consequently, the citizens exploiting SPID for eIDAS authentication may have several different eIDAS PersonIdentifiers.

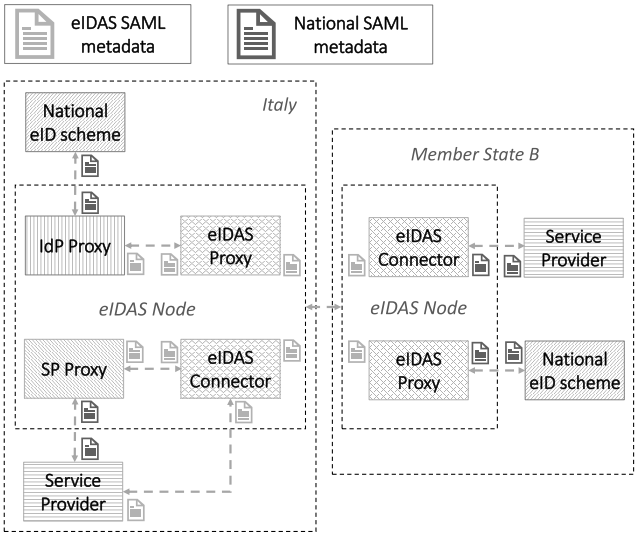

FIGURE 2. Italian eIDAS-Node architecture.

IV. LOGIN WITH EIDAS SERVICE

The Login service is a fundamental security service provided by our university. Once a user is logged into the university portal, she can perform many operations and she can get access to various academic and personal data. For example, a teacher can view and modify some data in his profile, he can enter exam dates and test results, he can manage the teaching material and the homeworks for the students. On the other hand, the students can access the course materials for the enrolled courses, they can book for a test, and they can view the test results. So, it is important that the service is always operational. Moreover, strong and correct user identification is vital: the case where a person may access someone else's data due to wrong identification must never happen.

TABLE 1. Mapping between SPID and eIDAS attributes. (*) <fullCvaddress> tag is not allowed anymore since eIDAS v.2.2 [43].

SPID attribute		eIDAS attribute	
Name	**Example**	**Name**	**Example**
spidCode	INFC0001M-R456	PersonIdentifier	IT/ES/INFC0001-MR456
name	Mario	FirstName	Mario
familyName	Rossi	FamilyName	Rossi
dateOfBirth	1999-09-13	DateOfBirth	1999-09-13
placeOfBirth	Torino	PlaceOfBirth	Torino
address	Via Verdi 1, 10100, Torino (TO), Italia	CurrentAddress	<fullCvaddress> Via Verdi 1, 10100, Torino (TO), Italia </fullCvaddress> (*)
gender	M	Gender	Male

Currently, students and academic staff of the Politecnico di Torino (Polito) can login into the university portal by using any of three methods:

- ($\mathcal{M}1$) username and password;
- ($\mathcal{M}2$) public-key authentication (based on soft or hard X.509 certificate);
- ($\mathcal{M}3$) authentication with SPID.

We analyse now the requirements of the *Login with eIDAS* service, and we detail the adopted solution.

A. ANALYSIS OF THE LOGIN WITH EIDAS SERVICE

The idea in this service is to correctly identify a person of any EU MS country registered at our university, based on a set of attributes retrieved through the eIDAS Network and the registration data stored in the university database. We assume first that the person (*e.g.* student, professor, researcher) is registered in the Polito database with the following data, named $D_{\text{registration}}$:

- name
- surname
- date of birth
- place of birth (country, in case of foreign person)
- gender

Additionally, the university database typically contains other personal information, such as Italian fiscal code, citizenship, current and temporary address, passport (or identity card) number.

When a user exploits the eIDAS Network to login, the data retrieved through the framework is composed of the mandatory attributes in the eIDAS MDS: FamilyName, FirstName,

DateOfBirth, and PersonIdentifier. We call the above data set $D_{\text{eIDASbasic}}$. Additionally, $D_{\text{eIDASbasic}}$ could contain also BirthName, CurrentAddress, PlaceOfBirth and Gender but since these attributes are optional, their values could be missing. If the eIDAS-Node is enhanced with new (sector-specific) attributes, then other additional (personal) data might be retrieved through the eIDAS Network, *e.g.* a passport number or a health card id number. However, we can assume that this additional data is optional, and consequently, the eIDAS Network might not return the corresponding values.

Since the (eIDAS) PersonIdentifier is not stored by default in the university database, then one possible solution to perform a login with eIDAS could consist in comparing the tuple (name, surname, date of birth) in $D_{\text{registration}}$ with the (FamilyName, FirstName, DateOfBirth) in $D_{\text{eIDASbasic}}$. If a match is found, then the user is given access to the university portal. Unfortunately, the above (apparently simple) operation is subject to two potential problems: transliteration and homonyms.

1) TRANSLITERATION

Generally speaking, transliteration is the process of transferring a word from the alphabet of one language to another. In our scenario, transliteration can generate problems because small differences may occur in one person's name when she is registered in the university database with respect to her identity registered in the national IdP. Nowadays, the person's names may appear with several name variants either across different languages or even within the same one. Quite often, such situations occur for the names containing accents, or for persons who have more than one birth name. For example, [44] points to 50 articles in English published on the 14th April 2005 where four different orthographies for the same person occurred: Rafik Hariri, Rafik al-Hariri, Rafiq Hariri, and Rafiq al-Hariri.

Consequently, in our case, there is a high probability that for some persons their name or surname registered in the university database (stored in $D_{\text{registration}}$) could differ in part from the ones retrieved through the eIDAS Network (stored in $D_{\text{eIDASbasic}}$).

2) HOMONYMS

Another problem concerns the probability to encounter two persons with the same attributes (name, surname, date of birth). These are the so-called homonyms. If we consider an additional attribute (like place of birth), fewer homonyms could occur, but they still may appear in practice [45]. For example, in our town, the office in charge of the web portal of Turin municipality encountered 8 persons with the same name, surname, date of birth, and place of birth.

To distinguish between homonyms, the persons must have distinct identification numbers, correctly stored and processed. For example, in Italy, even if two persons have the same name, surname, date of birth, gender, and place of birth, their Italian fiscal code is different. Note that every person living or studying (even temporarily) in Italy has an Italian fiscal code assigned by the Agenzia delle Entrate.

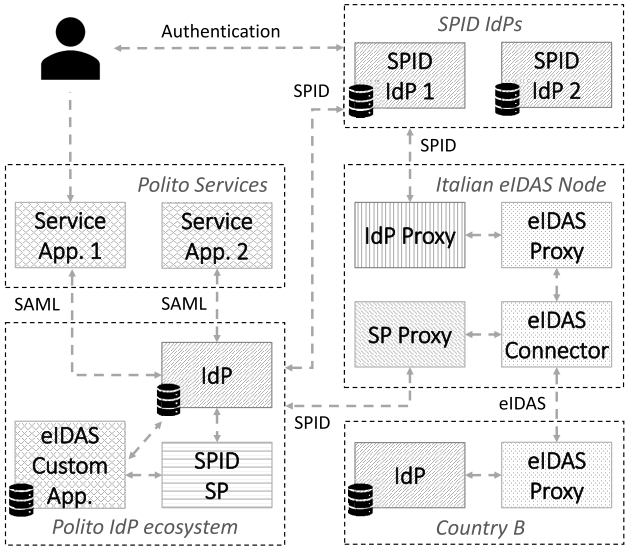

FIGURE 3. Polito service infrastructure with connection to eIDAS Network.

B. DESIGN OF LOGIN WITH EIDAS SERVICE

The service is composed of two phases: registration and authentication.

1) EIDAS PERSONIDENTIFIER REGISTRATION PHASE

In this phase, the person who has an account into the university database performs first the login operation with one of the mentioned methods, *e.g.* username and password, hard or soft X.509 certificate, SPID credential. Then, the person performs authentication through eIDAS to associate his current eIDAS PersonIdentifier with his profile. The person may have more than one eIDAS PersonIdentifiers. However, he will register in his profile the one he will use to perform the login with eIDAS. The functionality of this phase, along with all the components involved in its execution, is shown in Fig. 4.

2) AUTHENTICATION WITH EIDAS AND LOGIN PHASE

In this phase, the person authenticates through the eIDAS Network, and the eIDAS PersonIdentifier is obtained in the authentication response. This value is confronted with the eIDAS PersonIdentifier registered in the previous phase, and the internal components of the Polito IdP ecosystem further process it to correctly identify the person and to provide access to his area. The functional workflow for this phase is shown in Fig. 5.

Before detailing the phases above, we explain briefly the interconnection of several elements involved in providing services at our university. The Polito services are federated with a central identity ecosystem (Fig. 3), which exploits the Shibboleth open-source software [46] and the SAML protocol for the Single Sign-On feature. The Polito identity

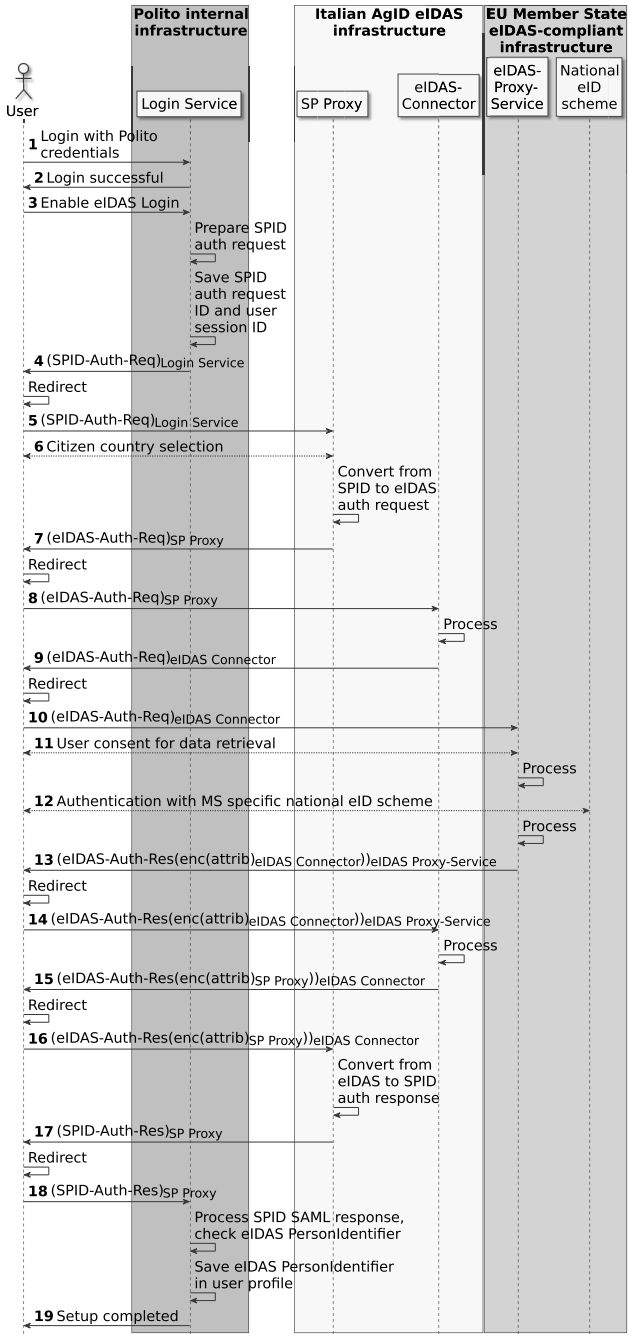

FIGURE 4. Sequence diagram for *eIDAS PersonIdentifier registration* phase. Notation: $enc(X)_Y$ means data X is encrypted by using X.509 certificate of Y, $(Auth)_Z$ means data *Auth* is digitally signed by Z.

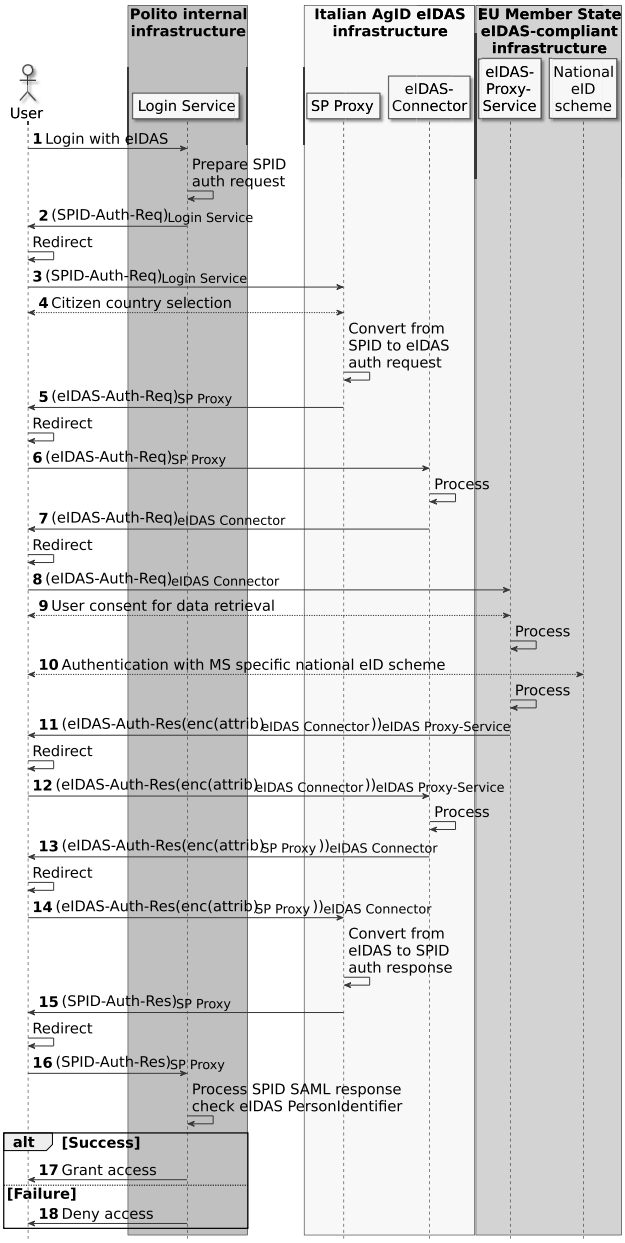

FIGURE 5. Sequence diagram for *Login with eIDAS* phase. Notation: $enc(X)_Y$ means data X is encrypted by using X.509 certificate of Y, $(Auth)_Z$ means data *Auth* is digitally signed by Z.

ecosystem exploits a central database of registered users, and the Italian fiscal code is the primary key for handling information about a user. To allow authentication via SPID, the Polito identity ecosystem contains the SPID SP (SPID Service Provider) component, which is in charge of the communication and trust established with the SPID IdPs. When a person authenticates via the SPID system, the authentication response returned to the SPID SP contains the Italian fiscal code. This value is further passed to the Polito IdP where it is processed internally to allow access of the person to her area.

To integrate eIDAS authentication into the services, the Polito identity ecosystem was further extended with an additional eIDAS Custom App, which communicates with both the Polito IdP and the SPID SP. Since our system administrators preferred not to modify either the IdP logic or the central database itself, this application (and the related database) was developed. Alternatively, authors in [14] have adopted an approach which requires the modification of the registered user data with eIDAS identification information. In their work, the FIWARE Keyrock Identity Provider storing profiles of the registered users has been extended with a so-called "eidas profile" containing the eIDAS PersonIdentifier, in addition to the user information containing other

data, *e.g.* UUID in Keyrock, displayName, email, password. In the Polito case, the eIDAS Custom App handles the association of the eIDAS PersonIdentifier(s) with other useful information (including the Italian fiscal code).

C. IMPLEMENTATION DETAILS

1) EIDAS (PERSON) IDENTIFIER REGISTRATION PHASE

The workflow for this phase is described further below and is shown in Fig. 4.

The user accesses the university portal, where she founds a dedicated *Login* button. Once pressed, the user is redirected to the university IdP, which is implemented with a Shibboleth IdP component. The user can select one of the local authentication methods, *e.g.* username and password, X.509 certificate, or SPID (step 1). If authentication with one of these credentials is successful, the user gets redirected to his profile area, where he will find an *eIDAS* button (step 2). By pressing it, the control passes to the Login service, which involves the eIDAS Custom App and the SPID SP to handle the eIDAS authentication. The SPID SP performs several operations such as saving the user session id, which contains information about the user authenticated by the university IdP. In Shibboleth, the session layer in the IdP tracks information associated with a subject across multiple transactions separated significantly in time. Then, the SPID SP constructs a SPID authentication request (*SPID-Auth-Req*) that is sent through the user's browser to the SP Proxy, where the user can choose the country where he wants to be authenticated (steps 3-5). On the SP Proxy interface, the user selects his country where he will authenticate with a notified authentication credential (step 6). The SP Proxy translates the authentication request from the SPID format to the eIDAS format (step 7), and the user browser is redirected along with the eIDAS authentication request (*eIDAS-Auth-Req*) to the Italian eIDAS Connector (step 8). Next, the *eIDAS-Auth-Req* is sent through the eIDAS Network and an eIDAS authentication response (*eIDAS-Auth-Res*) is received back by the eIDAS Connector as described in Sec. III (steps 9-15). The *eIDAS-Auth-Res* is sent to the SP Proxy (step 16), which translates it into the SPID format (*SPID-Auth-Res*), and sends it to the Login service through the user browser (steps 17-18). When it's received, the Login Service extracts the *inResponseTo* field from the SPID SAML response and uses it to retrieve the previously saved user session id. Next, it saves the eIDAS PersonIdentifier in the user profile corresponding to the retrieved user session id. Since the user profile also contains the Italian fiscal code, the eIDAS PersonIdentifier is associated with it. Once this setup phase is completed, the user is able to access his profile area on the university portal by authenticating through eIDAS (step 19).

2) LOGIN WITH EIDAS PHASE

The sequence diagram for this phase is shown in Fig. 5, and is detailed further below.

The user clicks on "Login with eIDAS" on the dedicated Login area of the Polito website (step 1). The Login Service starts a SPID authentication, *i.e.* it generates a *SPID-Auth-Req*, which is sent to the SP Proxy where the user selects his country (steps 2-4). The SP Proxy translates the authentication request from SPID format to eIDAS format and redirects the user browser to the Italian eIDAS Connector along with the *eIDAS-Auth-Req* (steps 5-6). Next, the usual eIDAS steps of the eIDAS protocol are executed as described in Section III (steps 7-13). Once the SP Proxy receives the *eIDAS-Auth-Res* (step 14), it translates it to SPID format. Thus, the SP Proxy prepares the *SPID-Auth-Res* and sends it back through the user browser to the Login service (steps 15-16). Finally, the Login Service extracts from the *SPID-Auth-Res* the value of the spidCode attribute, which contains an eIDAS PersonIdentifier value and checks it against the eIDAS PersonIdentifier value stored in the Polito user profile. If a match is found, then the access is granted to the restricted user area (step 17), otherwise, the access is denied (step 18). Some screenshots illustrating the performed steps for an Italian citizen are shown in Fig. 6.

D. DISCUSSION

The Student Service Office may exploit the Login with eIDAS service in several ways. For example, if a person forgets his password (that often happens after summer vacations), he might run a password recovery procedure involving "Login with eIDAS" to allow him to set up a new password. Normally, the password reset procedure involves either an interaction with a person in the user support or requires registration to a dedicated service for password reset via SMS. With eIDAS, these procedures could be avoided.

Moreover, the Student Service Office may select services that can be accessed only upon authentication with more secure LoA levels, *e.g.* Substantial or High. So, in this case, the students and teachers can exploit their national eIDs to easily get access to such services. For example, Wi-Fi access is a typical service provided upon authentication with username and password. If an attacker manages to guess or intercept a password used to get access to Wi-Fi, then he can impersonate a legitimate user and perform advanced (insider) attacks with the stolen identity. By requiring a Substantial LoA for network access, the users will employ a stronger authentication methods In this way, password sniffing and guessing attacks can be mitigated, and this is an advantage for the company (*e.g.* university) and for the legitimate users.

V. WI-FI ACCESS WITH EIDAS SERVICE

A. ANALYSIS OF WI-FI ACCESS INTEGRATED WITH EIDAS NETWORK

The goal in this service is to provide Wi-Fi access to Internet at Politecnico di Torino to EU citizens by leveraging the eIDAS Network, citizen's notified authentication credentials, and the Wi-Fi infrastructure already in place. Currently, Polito provides Wi-Fi access either to the persons

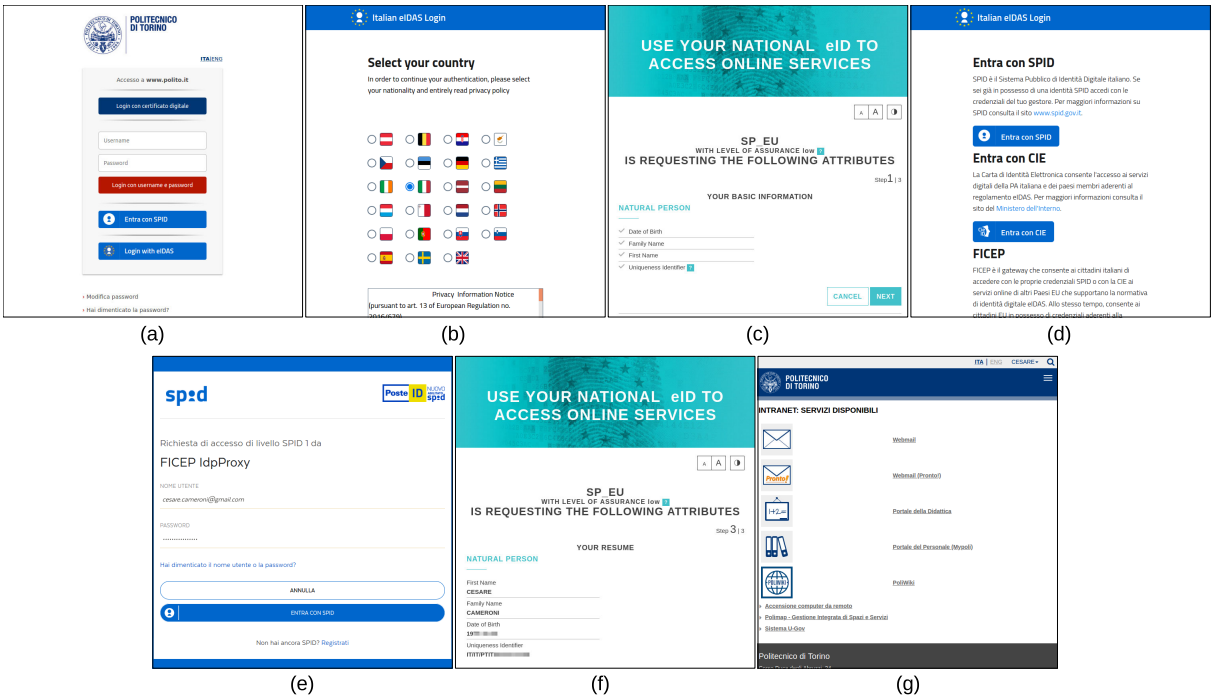

FIGURE 6. **Some screenshots of the user browser in *Login with eIDAS* phase. (a) Initial page with dedicated button. (b) Selection of citizen country on SP Proxy. (c) User consent page for attributes requested. (d) Selection of authentication method, SPID/national card (in Italy). (e) Authentication with a SPID credential. (f) User consent for valued attributes. (g) Access granted to the restricted area on web portal.**

(students/academic staff) registered at our university, or to the visiting persons working in academic domain (through eduroam). By exploiting our proposed service, other EU citizens visiting our university will be able to gain Wi-Fi access by using their *NotifiedAuthC*. Such persons can belong to various organizations, companies, or private entities that temporarily visit our campus (*e.g.* for a meeting, a conference, or an exhibition) but they cannot access Wi-Fi either because they are neither academic personnel (so they cannot use eduroam) nor registered at our university.

We have addressed several challenges in designing this service.

Challenge 1: SAML-enabled captive portal or dedicated networking hardware (HW)? Originally, we considered several SAML-enabled captive portal implementations, since the eIDAS Network itself is based on SAML. Possible software tools that can be used for this purpose are Zeroshell [47], PacketFence [48], and NoDogSplash [49]. We have tested Zeroshell, as described briefly in [33], but we encountered several technical issues in interconnecting it with the eIDAS Node. We have found incompatibilities between the cryptographic requirements of the eIDAS Connector and the cryptographic algorithms used by Zeroshell. Additionally, the SAML metadata of Zeroshell is not published (*i.e.* available at an URL), so the eIDAS Connector needs to configure it statically instead of downloading it at run time. Due to these limitations, Zeroshell is partly incompatible with the eIDAS-Node and should be modified in part. As a consequence, we have adopted the second choice.

Challenge 2: Whitelisting. The dedicated networking HW (*i.e.* the WLC) needs to support whitelisting, so an Access Control List (ACL) needs to be configured and updated continuously. As described in Sec. V-C, the discovery of the URLs to be whitelisted can pose problems (independently of the HW used), while the ACL may have a limited size. First of all, at least one ACL entry needs to be created for each eIDAS Proxy in the other MS countries. Next, depending on how many IdPs need to be configured for each MS country, it might not be possible to add an ACL entry for each of them due to the limited ACL size. However, this depends also on which WLC software version is employed.

Challenge 3: SPID interface or eIDAS interface? Since the WLC can be configured with an external application to handle authentication, it is possible to develop a Wi-Fi access eIDAS application with a SPID interface towards the Italian SP Proxy, as we did for the Login with eIDAS service. Alternatively, the Wi-Fi access with eIDAS application could communicate directly with the eIDAS Connector via the eIDAS protocol. We have adopted the second choice, although an Italian SP that already provides Wi-Fi access via SPID to the Italian citizens might prefer the first solution to allow also foreign citizens to gain Wi-Fi access through eIDAS (via SPID interface). Examples of some public entities that exploit SPID-aware captive portals in public places are the SPIDwifi-UniTO [50] in place at the University of Torino (Italy) or the free Wi-Fi of the City of Turin [51].

B. IMPLEMENTATION DETAILS

Together with the network team at our university, we have installed dedicated network equipment, which is identical to the one used in production to provide the Wi-Fi access service in the university area. The testbed environment illustrated

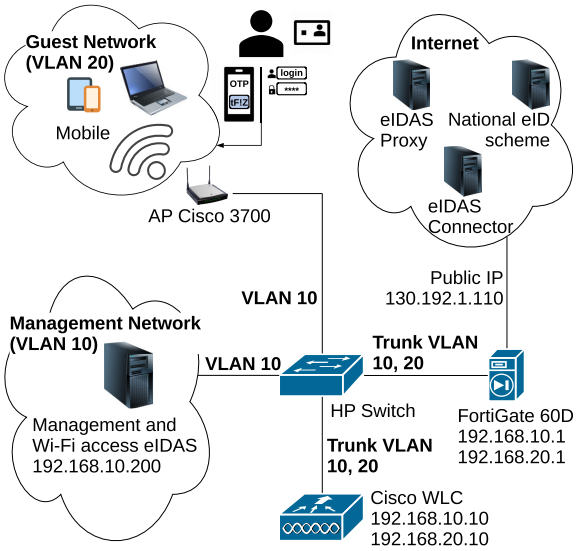

FIGURE 7. Testbed environment for Wi-Fi access through eIDAS Network.

TABLE 2. Configuration of network interfaces (on Fortigate firewall).

Name	Addresses	Type
management	192.168.10.1/24	VLAN
wifi_clients	192.168.20.1/24	VLAN
wan1	130.192.1.110	Physical

TABLE 3. Firewall policies configuration (on FortiGate firewall).

ID	From interface	To interface	Source	Dest.	Action
1	management	wan1	any	any	allow
2	management	wifi_clients	any	any	allow
3	wifi_clients	wan1	any	any	allow
4	wan1	management	eIDAS Connector	wifi-auth Server	allow
5	any	any	any	any	deny

TABLE 4. NAT Rule configuration (on FortiGate firewall).

Name	Public address	Internal address
wifi-auth server	130.192.1.110:443	192.168.10.200:443

in Fig. 7, is composed of several networking components, which have been properly connected and configured as described further below:

a) an Access Point Cisco 3700. This component has been configured with a new SSID named "eIDAS".

b) a Cisco 2500 Series Wireless LAN Controller (WLC). This component is a central element in our testbed and communicates with all the other ones. Its configuration was modified to allow external authentication through the Wi-Fi access with eIDAS application. The WLC internal database can hold at most 2048 guest client accounts. More accounts, if needed, can be created on an external RADIUS server [52]. In this WLC model, the number of simultaneously active guest client sessions is limited to 1000, but other Cisco WLC models can go up to 64,000 [53].

c) a FortiGate 60D firewall. This component controls the communications between the inside (private) network and the Internet. Thus, we have configured several firewall policies to control the connections in three stages: (i) before the authentication took place; (ii) during the authentication with eIDAS; (iii) after the authentication with eIDAS has been completed.

Besides, we have installed a dedicated server connected to the Cisco WLC, which runs the *Wi-Fi access eIDAS application*. We developed this application by exploiting the eIDAS demo-SP application, which is part of the official eIDAS source code v1.4.4 [6]. Such application already supports the eIDAS protocol, including eIDAS messages generation and validation, SAML metadata downloading validation and processing, and citizen country selection.

For the TLS communication with the user agent, we obtained an X.509 certificate from Let's Encrypt [54] and configured it into the Wi-Fi access eIDAS application. For the same application, we generated three more X.509 certificates allowing it to communicate via eIDAS protocol with the eIDAS Connector, and we've configured them into the dedicated keystore [55]. In particular, one certificate for validation of the digital signature on the SAML metadata of the Wi-Fi access eIDAS application, one for validation of the digitally signed SAML messages sent to the eIDAS Connector, and one needed for the decryption of the received SAML attributes values.

Subsequently, we have modified the application in several parts, such as to generate temporary guest accounts upon successful eIDAS authentication. Such accounts are subsequently configured (over a secure SSH channel) in the Cisco WLC device. The username of a temporary guest account is composed of the eIDAS PersonIdentifier (for user traceability) plus a pseudo-random string to avoid username conflicts among multiple sessions of the same user. The password, instead, is a pseudo-random string. The lifetime of the temporary guest account can be configured in the Wi-Fi access eIDAS application, and, once expired, the network access is denied to the user. Moreover, we have used the additional PC in the testbed also for configuring the network elements. When needed, to set up and update their configuration, we have used the management applications to connect to the Cisco WLC and the firewall. Additional details on the configuration of the network components in the testbed environment, as well as our ad-hoc Wi-Fi access eIDAS application may be found in [56].

The sequence diagram describing the eIDAS-enabled Wi-Fi access authentication flow is illustrated in Fig. 8, and is described below.

On a device (*e.g.* a PC or a mobile phone with Wi-Fi connectivity), the person chooses first the "eIDAS" SSID configured on the Access Point. At this step, in a web browser, the user can try to access via HTTP a web page at his choice, and the Cisco WLC intercepts the request (step 1). Note

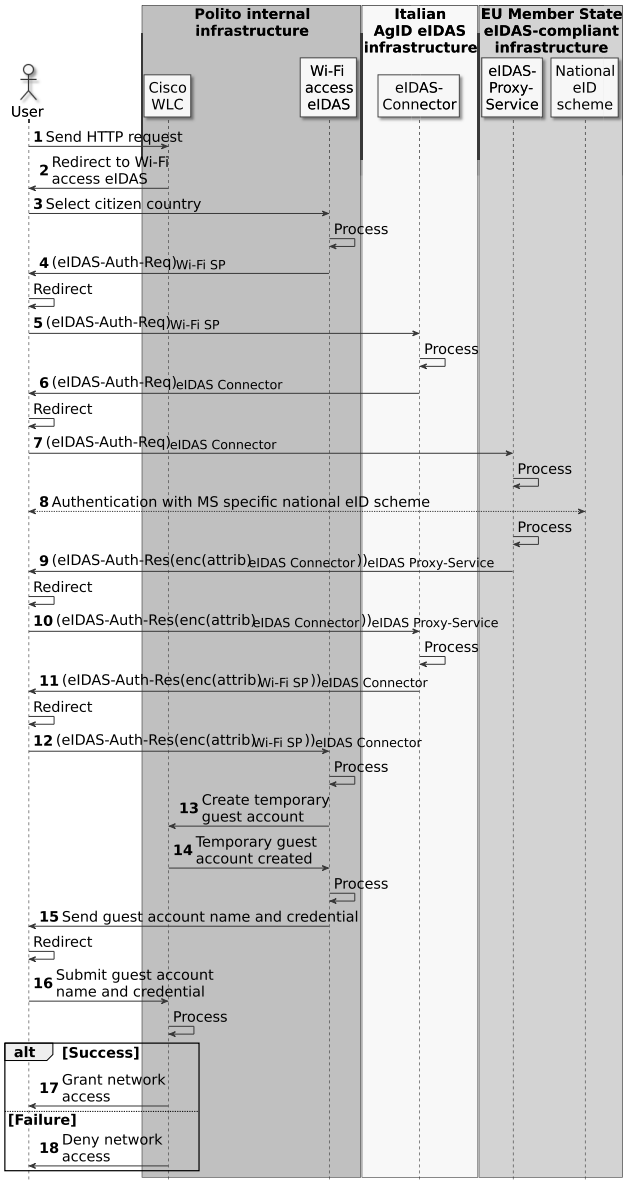

FIGURE 8. Sequence diagram for Wi-Fi access with eIDAS. Notation: $enc(X)_Y$ means data X is encrypted by using X.509 certificate of Y, $(Auth)_Z$ means data $Auth$ is digitally signed by Z.

that the Cisco WLC cannot capture web browser's requests over HTTPS, so a failed connection would occur. Some browsers automatically use HTTPS even when the user wants to use HTTP. In this case, other alternatives exist, *e.g.* many operating systems and web browsers nowadays provide an ''Open network login page'' button so that when clicked, they automatically open a default HTTP connection, which can be further intercepted by the captive portal.

Next, the Cisco WLC redirects the user browser to the Wi-Fi access eIDAS application, where the user selects the citizen country code (steps 2-3). By clicking on a dedicated ''Login with eIDAS'' button, an *eIDAS-Auth-Req* is generated and is sent through the user browser to the Italian eIDAS Connector (steps 4-5). The steps 6-11 contain the eIDAS messages generation and processing as described in Sec. III. When the eIDAS Connector sends back the *eIDAS-Auth-Res* to the Wi-Fi access with eIDAS application (step 12), a temporary user with a random password is created based on the eIDAS PersonIdentifier (step 13). Next, the application connects over an SSH channel to the Cisco WLC to create a temporary guest user account with the above credentials, along with certain parameters, such as the temporary account's lifetime (step 14). Subsequently, the Wi-Fi access eIDAS application sends the temporary guest account name and password via the user browser to the Cisco WLC (steps 15-16). Finally, if a match is found among the temporary guest accounts created, then Cisco WLC grants Internet access to the user's device (step 17), otherwise the network access is denied (step 18).

C. DISCUSSION AND OPEN ISSUES

The usage of automatically-generated temporary guest accounts on the WLC allows us to mitigate some common attacks against username and password-based authentication:

- The automatically generated password can have length and complexity of choice, protecting the user from a dictionary attack.
- There is no password reuse problem since the pseudo-random password is not shared among different accounts of the same user.
- Usually, in a Wi-Fi access scenario multiple sessions of the same user are allowed to permit the usage of several devices at the same time (*e.g.* a laptop and a smartphone). However, this implies that if an attacker discovers a password, he can use it at the same time as the legitimate user. In our proposed solution, each temporary guest account can have only one active session. The user can still access the network using several devices at the same time, but each user device is associated with a different temporary guest account.
- Temporary guest accounts have a limited lifetime which can be configured by the administrator, so compromised passwords can be used for a limited time interval.

From the privacy point of view, the usage of eIDAS authentication protects against user tracking done by IdPs. In Eduroam for example, the connection between the IdP and the SP discloses to the IdP details about the SP the user is authenticating for and the location. By exploiting the eIDAS Network, the IdP only connects to the eIDAS-Proxy-Service, so the user's location is not disclosed.

To allow the user to reach the IdP's authentication endpoint or other endpoints of his national eID scheme, we had to whitelist them in the ACL of the WLC. In particular, we have whitelisted the IP addresses of the following entities, although it is possible to configure also their DNS names: (a) the Wi-Fi access eIDAS service, (b) the (Italian) eIDAS Connector, (c) the (Italian) eIDAS Proxy, (d) the IdP Proxy, (e) the national IdPs' authentication endpoints, such as of

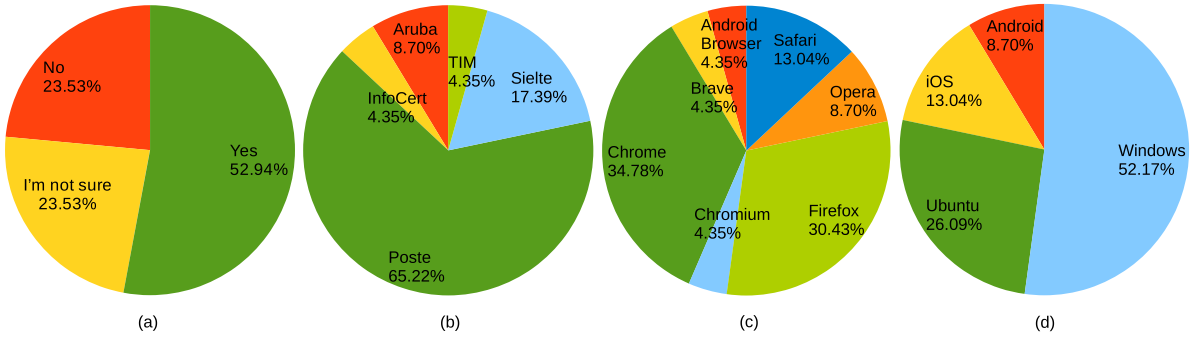

FIGURE 9. Services validation by users employing different SPID IdPs (b), various web browsers (c) and operating systems (d), and user perception on services use (a).

InfoCert SpA or Poste Italiane, (f) the eIDAS Proxies in the other MS countries, and (g) the authentication endpoints of the national eID schemes in other MS countries (when known).

Thus, two critical points still remain and need to be mitigated with alternative methods:

- Discovery of the authentication endpoints. For some national eID schemes in the other MS countries, it might be difficult to discover the actual authentication endpoints. Since this information is not rendered public in the eIDAS Network, we can only assume that it is obtained through an out of band channel or by using some other mechanisms.
- Whitelisting of the authentication endpoints. As said, the number of entries in the Cisco WLC's ACL is limited. By configuring the IP addresses, the ACL can hold at most 64 entries. Thus, at most 32 entity endpoints can be configured because each entity requires one ACL rule for the input traffic and one for the output traffic. By configuring the DNS names, the limitation is 20 names. However, this limitation depends on the software version run in the Cisco WLC component, which is 8.2.1.166.0 in our case.

VI. USE CASES VALIDATION

To validate the implemented services, we organized several test sessions in which we involved overall 23 people, mainly students but also teaching staff of Politecnico di Torino. Each test session took about thirty minutes and included experiments with both Login with eIDAS and Wi-Fi access with eIDAS. In the tests, the participants used their SPID credentials issued by different IdPs, like InfoCert, Poste, or Aruba. Moreover, they exploited their Wi-Fi enabled devices, and the web browsers they typically employed, like Firefox, Chromium, or Safari. Most of them used personal computers running Windows or Ubuntu OS, but five participants have also used smartphones. The participants had not to make any particular configuration. When needed, in the Cisco WLC we whitelisted some additional IdP's endpoints, easily discovered through DNS queries. At the end of each session, the participants filled out an online survey about the usefulness and usability of the tested services, and they could add comments to clarify their answers.

The pie chart in Fig. 9 (a) summarises the answers to the question "*I've used my eID to connect to the Wi-Fi network with eIDAS and I think this may help me in various environments and services where network access is required*". Many of the negative and undecided answers were accompanied by comments stating that the Wi-Fi access procedure was slower (due to the intermediate steps through eIDAS) and more complicated than the direct access to the home institution network or the Eduroam access to the visited institution network. Some participants were worried about the disclosure of personal attributes sent through eIDAS Network. Others were annoyed because the user consent request regarding the attributes transfer was asked twice, once on the eIDAS Node, and once on the SPID IdP. Among the positive comments, we encountered the consideration of being able to access the network without having to register or create a new service account first. A participant said "*Logging into wifi with eID is amazing*", another one stated "*Very useful and time-saving*". Another participant instead proposed some improvement regarding the data shown in each step: "*The information-gathering process might be more straightforward, so switches are active by default and the user may choose to unselect them*".

The other three pie charts show more details on the credentials used and the software (browser, operating system) employed. In practice, the tests performed by the participants involved five different SPID IdPs (Fig. 9 (b)), different web browsers (Fig. 9 (c)) and various operating systems both desktop and mobile (Fig. 9 (d)).

VII. CONCLUSION

The eIDAS Network links the various countries' eID systems in a unified framework and allows persons to use, with legal value, their national issued eID in cross-border services across Europe. To create eIDAS-aware services, additional work is required to adapt SP systems and workflows to eIDAS.

We have integrated with the eIDAS Network two services widely used in any university, and in general in most public

entities and companies: the *Login with eIDAS* and *Wi-Fi access with eIDAS*. We described in detail the problems encountered and the possible solutions that may be adopted. In the Login service, the lack of a unique persistent identifier for individuals across the EU requires people to link together a local identifier data (such as the national one, if defined) with the identifier defined in eIDAS. In the Wi-Fi access service, the integration of the eIDAS Network with the captive portal is not trivial, and we proposed a possible solution based on the dedicated network equipment we already have in place at our site.

The implemented services proved feasible and they can be adapted to the existing workflows already in place with minimal effort. From the user perspective, the students involved in the validation of the proposed services perceived them as useful, even when the services are just an add-on to other authentication solutions. The test users have also provided some interesting suggestions regarding the usability of the services. Future work is needed to improve the implementation of whitelisting in the Wi-Fi access with eIDAS service because this could affect the wide-scale deployment and use of the service.

ACKNOWLEDGMENT

The authors thank Muhammad Ali Anjum (former student at Politecnico di Torino) for his work in implementing the Wi-Fi Access Scenario. The authors also thank Antonio Lantieri from the Networking and Data Center Office, Giorgio Santiano and Andrea Garzena from the Student Service Office of Politecnico di Torino, and Paolo Smiraglia from Agenzia per l'Italia Digitale (AgID) for their help in integrating our proposed services with Politecnico di Torino backend and with the official Italian eIDAS-Node, hosted by AgID.

REFERENCES

[1] S. Mouille. *EIDAS Regulation Presentation*. Accessed: Jun. 26, 2020. [Online]. Available: https://www..net/StefaneMouille/eurosmart-presentation-on-the-eidas-regulation-67132056

[2] J. L. Hernandez-Ardieta, J. Heppe, and J. F. Carvajal-Vion, "STORK: The European electronic identity interoperability platform," *IEEE Latin Amer. Trans.*, vol. 8, no. 2, pp. 190–193, Apr. 2010, doi: 10.1109/TLA.2010.5514447.

[3] *FutureID-Shaping the Future of Eletronic Identity*. Accessed: Jun. 26, 2020. [Online]. Available: https://cordis.europa.eu/project/id/318424

[4] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. Garcia-Blas, "Federated identity architecture of the European eID system," *IEEE Access*, vol. 6, pp. 75302–75326, Nov. 2018, doi: 10.1109/ACCESS.2018.2882870.

[5] *eIDAS SAML Message Format Version 1.2*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Message%20Format%20v.1.2%20Final.pdf

[6] *eIDAS-Node Software Releases*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+Integration+Package

[7] *Country Overview of the Status of eIDAS-Node Implementation and eID Use Across Europe*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

[8] *Overview of Pre-Notified and Notified eID Schemes Under eIDAS*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[9] *Information Technology—Security Techniques—Entity Authentication Assurance Framework*, Standard ISO/IEC 29115 2013, Jun. 2020. [Online]. Available: https://www.iso.org/standard/45138.html

[10] B. Hulsebosch, G. Lenzini, and H. Eertink. D2.3-quality authenticator scheme. STORK Project Deliverable. Accessed: Jun. 26, 2020. [Online]. Available: https://www.cs.ru.nl/E.Verheul/SIO2019/D2.3_final.pdf

[11] Federal Office for Information Security. *German eID based on Extended Access Control V2. LoA mapping: Mapping of the characteristics of the German eID scheme to the eIDAS Level of Assurance*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_LoA_Mapping.pdf

[12] Finnish Transport and Communications Agency Traficom, National Cyber Security Centre. *Guidance for the Application of the Levels of Assurance Which Support the eIDAS Regulation*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance.pdf

[13] D. Berbecaru, A. Lioy, and C. Cameroni, "Providing digital identity and academic attributes through European eID infrastructures: Results achieved, limitations, and future steps," *Software: Pract. Exper.*, vol. 49, no. 11, pp. 1643–1662, Nov. 2019, doi: 10.1002/spe.2738.

[14] A. Alonso, A. Pozo, J. Choque, G. Bueno, J. Salvachua, L. Diez, J. Marin, and P. L. C. Alonso, "An identity framework for providing access to FIWARE OAuth 2.0-based services according to the eIDAS European regulation," *IEEE Access*, vol. 7, pp. 88435–88449, Jul. 2019, doi: 10.1109/ACCESS.2019.2926556.

[15] D. Berbecaru, A. Lioy, and C. Cameroni, "Electronic identification for universities: Building cross-border services based on the eIDAS infrastructure," *Information*, vol. 10, no. 6, p. 210, Jun. 2019, doi: 10.3390/info10060210.

[16] A. Bazarhanova and K. Smolander, "The review of non-technical assumptions in digital identity architectures," in *Proc. 53rd Hawaii Int. Conf. Syst. Sci.*, Maui, HI, USA, 2020, pp. 6408–6417, doi: 10.24251/HICSS.2020.785.

[17] N. Tsakalakisz, S. Stalla-Bourdillon, and K. O'Hara, "Identity assurance in the U.K.: Technical implementation and legal implications under eIDAS," *J. Web Sci.*, vol. 3, no. 1, pp. 32–46, Dec. 2017, doi: 10.1561/106.00000010.

[18] S. Pal, M. Hitchens, and V. Varadharajan, "Modeling identity for the Internet of Things: Survey, classification and trends," in *Proc. 12th Int. Conf. Sens. Technol. (ICST)*, Limerick, Ireland, Dec. 2018, pp. 45–51, doi: 10.1109/ICSensT.2018.8603595.

[19] K. O. Asamoah, H. Xia, S. Amofa, O. I. Amankona, K. Luo, Q. Xia, J. Gao, X. Du, and M. Guizani, "ZERO-chain: A blockchain based identity for digital city operating system," *IEEE Internet Things J.*, early access, Apr. 8, 2020, doi: 10.1109/JIOT.2020.2986367.

[20] *eHealth Digital Service Infrastructure*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Mission

[21] *OpenNCP Community Home*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/EHNCP/OpenNCP+Community+Home

[22] *MyAcademicID Project*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.myacademic-id.eu/

[23] *eID4U Project*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2017-eu-ia-0051

[24] *Eduroam Project*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.eduroam.org/

[25] C. Rigney, A. Rubens, W. Simpson, and S. Willens, *Remote Authentication Dial in User Service (RADIUS)*, document RFC 2865, Jun. 2000, doi: 10.17487/RFC2865.

[26] S. Brenza, A. Pawlowski, and C. Pöpper, "A practical investigation of identity theft vulnerabilities in Eduroam," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*, New York, NY, USA, 2015, pp. 1–11, doi: 10.1145/2766498.2766512.

[27] K. Wierenga, S. Winter, and T. Wolniewicz, *The Eduroam Architecture for Network Roaming*, document RFC 7593, Sep. 2015, doi: 10.17487/RFC7593.

[28] S. Winter, M. McCauley, S. Venaas, and K. Wierenga, *Transport Layer Security (TLS) Encryption for RADIUS*, document RFC 6614, May 2012, doi: 10.17487/RFC6614.
[29] H. Liu and H. Goto, "Certificate-based, disruption-tolerant authentication system with automatic CA certificate distribution for eduroam," in *Proc. IEEE 38th Int. Comput. Softw. Appl. Conf. Workshops*, Vasteras, Sweden, Jul. 2014, pp. 169–173, doi: 10.1109/COMPSACW.2014.32.
[30] C. Li, Q. Wu, H. Li, and J. Liu, "Trustroam: A novel blockchain-based cross-domain authentication scheme for Wi-Fi access," in *Wireless Algorithms, Systems, and Applications* (Lecture Notes in Computer Science), vol. 11604. Honolulu, HI, USA: Springer, Jun. 2019, pp. 149–161, doi: 10.1007/978-3-030-23597-0_12.
[31] T. Sanda and H. Inaba, "Proposal of new authentication method in Wi-Fi access using bitcoin 2.0," in *Proc. IEEE 5th Global Conf. Consum. Electron.*, Kyoto, Japan, Oct. 2016, pp. 1–5, doi: 10.1109/GCCE.2016.7800479.
[32] D. Berbecaru, A. Lioy, and M. D. Aime, "Exploiting proxy-based federated identity management in wireless roaming access," in *Trust, Privacy and Security in Digital Business* (Lecture Notes in Computer Science), vol. 6863. Toulouse, France: Springer, 2011, pp. 13–23, doi: 10.1007/978-3-642-22890-2_2.
[33] D. Berbecaru, A. Lioy, and C. Cameroni, "Authorize-then-authenticate: Supporting authorization decisions prior to authentication in an electronic identity infrastructure," in *Intelligent Distributed Computing XIII* (Studies in Computational Intelligence), vol. 868. Saint Petersburg, Russia: Springer, 2020, pp. 313–322, doi: 10.1007/978-3-030-32258-8_37.
[34] *eIDAS Interoperability Architecture Version 1.2*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20Interoperability%20Architecture%20v.1.2%20Final.pdf
[35] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, and P. Mishra. (Mar. 2005). Profiles for the OASIS security assertion markup language (SAML) V2.0. OASIS Standard. Accessed: Jun. 26, 2020. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
[36] *eIDAS SAML Attribute profile Version 1.2*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf
[37] *Public Digital Identity System (SPID)*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.spid.gov.it/?lang=en-001
[38] F. Buccafurri, L. Fotia, G. Lax, and R. Mammoliti, "Enhancing pblic digital identity system (SPID) to prevent information leakage," in *Electronic Government and the Information Systems Perspective* (Lecture Notes in Computer Science), vol. 9265. Valencia, Spain: Springer, 2015, pp. 57–70, doi: 10.1007/978-3-319-22389-6_5.
[39] *How to Become a Public or Private Service Provider With SPID, Agency for Digital Italy*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.spid.gov.it/come-diventare-fornitore-di-servizi-pubblici-e-privati-con-spid?lang=en-001
[40] *Regolamento Recante Le Regole Tecniche SPID (in Italian)*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.agid.gov.it/sites/default/files/repository_files/circolari/spid-regole_tecniche_v1.pdf
[41] *SPID Statistics (in Italian)*. Accessed: Jun. 26, 2020. [Online]. Available: https://avanzamentodigitale.italia.it/it/progetto/spid
[42] *SPID Registry (in Italian)*. Accessed: Jun. 26, 2020. [Online]. Available: https://registry.spid.gov.it/
[43] *eIDAS-Node Migration Guide V2.2*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/82773434/eIDAS-Node%20Migration%20Guide%20v2.2.pdf
[44] B. Pouliquen, R. Steinberger, C. Ignat, I. Temnikova, and A. Widiger, "Multilingual person name recognition and transliteration," Maison des Sci. de l'Homme et de la Société, Univ. Poitiers, Poitiers, France, Tech. Rep. HS-2, 2005, doi: 10.4000/corela.1219.
[45] A. Charpentier and B. Coulmont. (2017). *We are not Alone! (At Least, Most of Us). Homonymy in Large Scale Social Groups*. Accessed: Jun. 26, 2020. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01568038/document
[46] *Shibboleth Products*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.shibboleth.net/
[47] *Configure the Captive Portal to Authenticate Users Against an IdP SAML 2.0 Using Shibboleth*. Accessed: Jun. 26, 2020. [Online]. Available: https://zeroshell.org/shibboleth-captive-portal/
[48] *PacketFence Overview*. Accessed: Jun. 26, 2020. [Online]. Available: https://packetfence.org/about.html
[49] *NoDogSplash Overview*. Accessed: Jun. 26, 2020. [Online]. Available: https://nodogsplashdocs.readthedocs.io/en/stable/overview.html
[50] *La rete Spidiwifi-UniTO (in Italian)*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.unito.it/servizi/servizi-line/il-wifi-delluniversita/la-rete-spidwifi-unito
[51] *Free Torino Wi-Fi Access With SPID credentails (in Italian)*. Accessed: Jun. 26, 2020. [Online]. Available: https://servizi.torinofacile.it/wifi/cp/
[52] *Cisco Wireless Controller Configuration Guide, Release 8.10*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/aaa_administration.html
[53] *Cisco Wireless Guest Access FAQ*. Accessed: Jun. 26, 2020. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107458-wga-faq.html#anc2
[54] *Let's Encrypt Certificate Authority*. Accessed: Jun. 26, 2020. [Online]. Available: https://letsencrypt.org/
[55] *eIDAS-Node Installation, Configuration and Integration, Quick Start Guide 1.4.4*. Accessed: Jun. 26, 2020. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/download/attachments/84421967/eIDAS-Node%20Installation%2C%20Configuration%20and%20Integration%20Quick%20Start%20Guide%201.4.4.pdf
[56] M. A. Anjum, "Design and development of WiFi access with eIDAS for cross border authentication," M.S. thesis, DAUIN, Politecnico di Torino, Turin, Italy, Dec. 2019. [Online]. Available: https://webthesis.biblio.polito.it/13122/1/tesi.pdf

DIANA GRATIELA BERBECARU (Member, IEEE) received the M.Sc. degree in computer science from the University of Craiova, Romania, and the Ph.D. degree in computer engineering from the Politecnico di Torino. She is currently a Senior Research Assistant with the Department of Control and Computer Engineering, Politecnico di Torino. She is also a member with the TORSEC Cybersecurity Research Group. Her research interests include X.509 certificate validation, multicast authentication, and electronic identity infrastructures.

ANTONIO LIOY (Member, IEEE) received the M.Sc. degree *(summa cum laude)* in electronic engineering and the Ph.D. degree in computer engineering from the Politecnico di Torino. He is currently a Full Professor with the Politecnico di Torino, where he leads the TORSEC Cybersecurity Research Group. His research interests include network security, policy-based system protection, trusted computing, and electronic identity.

CESARE CAMERONI received the M.Sc. degree in computer engineering from the Politecnico di Torino, in 2010. From 2011 to 2014, he was a Research Assistant with the Department of Control and Computer Engineering, Politecnico di Torino, where he has also been a Research Assistant, since 2018. He is currently a member with the TORSEC Cybersecurity Research Group. His research interests include security and dependability of ICT systems, electronic identities, and federated identity infrastructures.