eIDAS Public Digital Identity Systems: Beyond Online Authentication to Support Urban Security

Francesco Buccafurri, Gianluca Lax(✉), Serena Nicolazzo, and Antonino Nocera

DIIES, University Mediterranea of Reggio Calabria, Via Graziella, Località Feo di Vito, 89122 Reggio Calabria, Italy
lax@unirc.it

Abstract. The European regulation eIDAS introduces in EU States interoperable public digital identity systems whose native application is secure authentication on online services. In this paper, we try to offer an enhanced view of the potential benefits that such systems can have in our physical environments. Indeed, cities have seen a dramatic increase in the number of violent acts and crimes. The possibility of monitoring people access to physical critical places is certainly an important issue because this gives the possibility to deny the access to dangerous people, to find the offender of a crime, and, in general, to track suspicions activities. In this paper, we show how to exploit an eIDAS-compliant public digital identity system to meet the above requirements, thus offering a concrete solution with high level of interoperability.

Keywords: Urban security · Public digital identity · eIDAS · SPID · Critical environments · Physical access control

1 Introduction

The problem of identity management [1] is related to many applications, among which physical access control of people and identity auditing and monitoring, are particularly important in the context of urban security [2–4]. Consider a physical place where the access of individuals is controlled, for example a museum or an airport. In the case of a museum, we need that only people with a valid ticket can access: however, it should be useful to log their identities in order to enable accountability activities. In contrast, the access to an airport gate should be granted to users with a valid ticket, only after having verified their identity does not belong to some black list.

Recently, Regulation (EU) No 910/2014 eIDAS (electronic IDentification Authentication and Signature) [5] has been issued with the objective of removing existing barriers to the cross-border use of electronic identification means used in the Member States for authentication. As this Regulation does not aim to intervene with regard to electronic identity management systems and related

A. Longo et al. (Eds.): IISSC 2017/CN4IoT 2017, LNICST 189, pp. 58–65, 2018.
https://doi.org/10.1007/978-3-319-67636-4_7

infrastructures established in Member States, each Member State can design its own secure electronic identification and authentication system, which will be accepted in all EU countries if is complaint with eIDAS: For example, the Public Digital Identity System (SPID) [6] is the Italian identity management system complaint with eIDAS.

The Italian system SPID is an open system thanks to which public and private entities, provided that they are accredited by the Agency for Digital Italy, can offer services of electronic identification for citizens and businesses. The providers of such services have to ensure a suitable procedure for the initial identification and have to implement the authentication of citizens to service providers, which are public or private organizations, provided that they adhere to SPID. SPID is based on the technical specifications widely accepted in Europe and already adopted by experimental projects as Stork and Stork2 (Secure Identity Across Borders Linked) [7,8]. Italy has also already notified the Commission the institution of SPID. Thus, according to eIDAS, since July 2016, SPID is recognized and accepted by all other EU Member States.

In this paper, we try to offer an enhanced view of the potential benefits that such systems can have in our physical environments. In particular, we propose a system to monitor people access to physical places exploiting an eIDAS-compliant public digital identity system. To be concrete, we contextualize our proposal in the Italian framework, thus exploiting the system SPID. Our system has the scope of identifying users and is able to decide whether granting them the access to a monitored area, also logging such accesses. The topic here studied is an emerging research challenge which is attracting a great deal of attention (e.g., [9–15]). The main contribution of our proposal with respect to the state of the art relies on the fact that our solution is based on the use of an authentication tool (i.e., SPID in our solution instantiation), which is simple to use, considered secure, accepted in all EU countries, and expected to be used by the most part of the population in the next years. Consequently, our solution can be considered cheap, effective, and secure w.r.t. the state of the art.

In the next section, we describe how SPID is exploited for users identification. The architecture and protocol of the system are presented in Sect. 3. Finally, we draw final discussion and conclusion in Sect. 4.

2 The SPID Framework

In this section, we present the Public Digital Identity System (SPID) framework [6] and the technical details necessary to understand our proposal. SPID is a SAML-based [16] open system allowing public and private accredited entities to offer services of electronic identification for citizens and businesses. SPID enables users to make use of digital identity managers to allow the immediate verification of their identity for suppliers of services.

Besides users to identify, the stakeholders of SPID are Identity Providers, which create and manage SPID identities and Service Providers, public or private organizations providing a service to authorized users. Moreover, we have

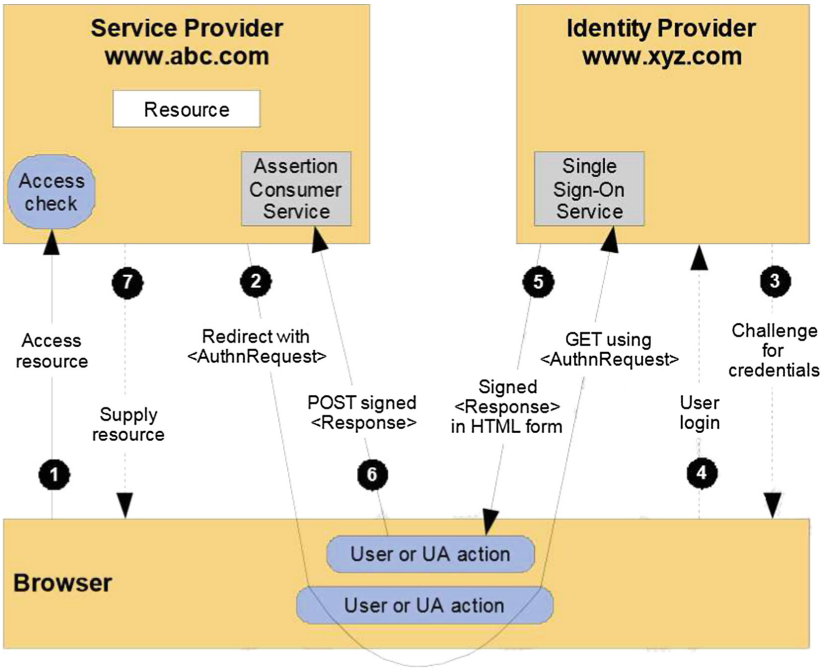

Fig. 1. Authentication by SPID.

a Trusted Third Party (TTP), which guarantees the standard levels of security required by SPID and certifies the involved entities (in Italy, it is "The Agency for Digital Italy").

To obtain a SPID identity, a user must be registered to one Identity Provider, which is responsible of the verification of the user identity before issuing the SPID ID and the security credentials.

A SPID user who needs to access a service sends a request to the Service Provider that gives this service (this is typically done by a Web browser). Then, the Service Provider replies with an `Authentication Request` to be forwarded to the Identity Provider managing the SPID identity of the user.

When the Identity Provider receives such an `Authentication Request`, verifies that it is valid and performs a challenge-response authentication with the user. In case of successful user authentication, the Identity Provider prepares the `Assertion`, a message containing the statement of user authentication for the Service Provider.

Now, Identity Provider returns to the user the message `Response` containing the `Assertion`, which is forwarded to the Service Provider (typically via HTTP POST Binding).

All the steps carried out in a SPID-based authentication are represented in Fig. 1.

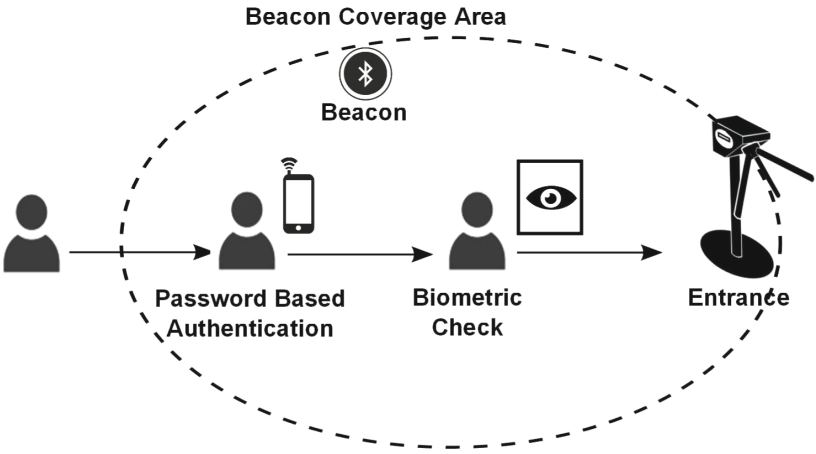

Fig. 2. The physical infrastructure underlying our approach.

Concerning the authentication, SPID supports three different levels: L1 based on only password, L2 using both password and one time password (it is sent to the user by a channel different from the browser), and L3 requiring the use of a smart card in addition to password.

In our proposal, we include a level L4, in which both password and biometric information[1] are exploited.

The SPID identification level to be used depends on the context and the security needs: for example, in case only accountability of user accesses is required (as for a museum), level L1 could be sufficient; in case the access to a zone should be granted to only selected users (as for an airport), then the use of L4 is required.

3 System Architecture and Implementation

In this section, we describe the architecture of our system and provide some details about the technologies and hardware used.

Without lost of generality, we refer to an airport as application scenario, in which the entrance to a secured zone (e.g., the gates area), has to be granted only to authorized users. Figure 2 sketches a representation of the physical infrastructure considered in our approach.

In our solution, we assume that:

1. The SPID identity of authorized users is available to the system;

[1] The currently standardized biometrics used for this type of identification system are facial recognition, fingerprint recognition, and iris recognition. Biometric identification is adopted in many countries: for example, in USA, beginning on April 1, 2016, the electronic passport contains relevant biometric information [17].

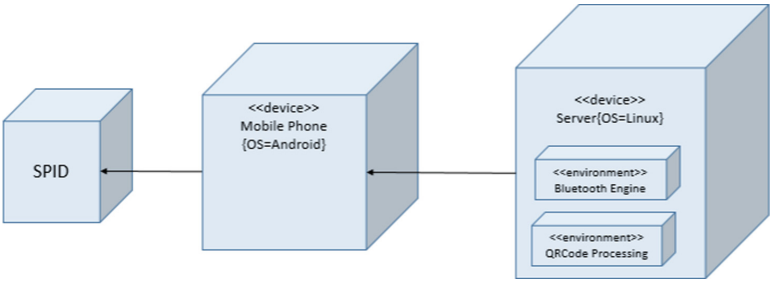

Fig. 3. The deployment diagram of our system.

2. Users are equipped with a smart portable device (for example, a smartphone or a tablet);
3. The device of users can connect to the Identity Provider site.

Our solution integrates the SPID service to authorize the accesses to secured areas. To describe the approach in a very synthetic way, we can say that the authorization procedure starts when a user approaches the entrance of a secured zone, such as an airport turnstile. Here, an access point of the system is placed and the user is prompted to perform the SPID authentication via his personal device. The result of this procedure is used by the system to decide if the user is authorized to access the secured area, depending on his SPID identity.

The system implementing our proposal, whose deployment diagram is illustrated in Fig. 3, is composed of two main subsystems:

- User Interface Subsystem (`UI`, for short), which implements all the features to allow the user interaction with the system. It is a single module implemented through an application running on the mobile device of the user.
- Physical-Service Provider Subsystem (`PSP`, for short), which performs all verifications to monitor the entrance to secured zone. It consists of three main modules, namely: PreAuth Module, IDScanner Module, and Processing Module.

The first module involved in the protocol is the PreAuth Module, which inquiries users devices approaching the secured zone entrances to initiate the SPID authentication. It is implemented by using `Bluetooth beacons` placed on airport turnstiles to initialize the communication with `UI` subsystem. The design choice of using `Bluetooth beacons` is due to the extremely simple integration in existing infrastructures. Indeed, this kind of device belongs to a class of low energy bluetooth hardware transmitters [18,19], often battery powered, able to broadcast messages and perform basic interactions with smart devices in close proximity. Typically, `Bluetooth beacons` are used to issue location-based actions on devices and have been already adopted in environments where check-in is needed.

In proximity of the monitored zone, the user device receives via Bluetooth the authentication request from the PreAuth Module and is prompted to execute

Algorithm 1. Workflow of our approach

Notation U: user entering a secured zone
Notation UI: user interface on mobile device
Notation PM: PreAuth Module on Bluetooth Beacon
Notation IDM: IDScanner Module on QR Code Scanner
Notation $ProsM$: Processing Module on Central Server
1: U approaches a monitored entrance
2: PM inquiries UI to initiate the SPID authentication
3: UI generates a QR Code for this Authentication Request
4: U inserts his credential for SPID authentication via UI
5: U approaches the entrance and shows the QR Code to IDM
6: U performs biometric authentication
7: IDM verifies the assertion and forwards it to $ProsM$
8: $ProsM$ grants/denies access

the SPID authentication, which is executed by connecting to the site of the Identity Provider of the user. Moreover, this module randomly generates a QR Code [20], which is associated with this `Authentication Request` and shown on the mobile device of the user.

As for authentication, we assume that L4 authentication is required (this is typical for an airport): thus, both password and biometric information are exploited in two different steps. In this first step, user is required to insert the password.

Observe that because this first step may require more time, it can starts when the user is quite distant from the access point (depending on the Beacon coverage area).

When the user arrives in the access point, the second step of the authentication is done: the user shows the QR Code to the IDScanner Module.

This module is a smart 2D bar code scanner placed right in the turnstile: because QR Code scanning requires high proximity, this solution is particularly suitable in our scenario to avoid de-synchronization between user physical access and identity verification.

In this step, the biometric authentication is performed and the result of this authentication, which contains the `Assertion`, is returned to the Processing Module. This module is deployed in a central server and receives all the access requests coming from the different PreAuth Module. It enforces access policies by driving the opening of turnstiles: in our example, it verifies that this SPID identity is of an authorized user.

The algorithm describing the whole approach is reported in Algorithm 1.

4 Conclusion

In this paper, we designed and implemented a system based on SPID to monitor physical access of individuals to controlled areas. The exploitation of our proposal gives two main advantages with respect to a standard management of accesses (i.e., when a human operator is in charge of verifying user's identity): the first advantage is to speed up this process, the second one is to make user's identification more robust to human errors.

Moreover, filtering mechanisms can be enabled (e.g., only adults may access), or the use of attribute providers can be involved to remove the need of showing an electronic ticket (the ticket is associated with the identity).

Concerning pervasiveness, we observe that, even though our implementation makes use of SPID, our approach supports any identity management system complaint with eIDAS. This is an important aspect because there are many cases in which individuals may have heterogeneous nationalities.

As for accountability, it is easily obtained by suitably storing all information need (for example, besides the identity, also the timestamp of the access).

The last observation is related to the technologies that can be exploited. In our example, we showed the use of Beacon and QR Code. However, they can be replaced by other similar technologies, such as Wi-Fi or NFC, or by long-range UHF RFID systems.

References

1. Buccafurri, F., Lax, G., Nocera, A., Ursino, D.: Discovering missing me edges across social networks. Inform. Sci. **319**, 18–37 (2015)
2. Jara, A.J., Genoud, D., Bocchi, Y.: Big data in smart cities: from poisson to human dynamics. In: 2014 28th International Conference on Advanced Information Networking and Applications Workshops, AINA 2014 Workshops, Victoria, BC, Canada, 13–16 May 2014, pp. 785–790 (2014)
3. Anttiroiko, A., Valkama, P., Bailey, S.J.: Smart cities in the new service economy: building platforms for smart services. AI Soc. **29**(3), 323–334 (2014)
4. Buccafurri, F., Lax, G., Nicolazzo, S., Nocera, A.: Comparing twitter and facebook user behavior: privacy and other aspects. Comput. Hum. Behav. **52**, 87–95 (2015)
5. European Union: Regulation EU No 910/2014 of the European Parliament and of the Council, 23 July 2014. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014R0910&from=EN
6. European Union: Regulation EU No 910/2014 of the European Parliament and of the Council, 23 July 2014. http://ec.europa.eu/growth/tools-databases/tris/en/index.cfm/search/?trisaction=search.detail&year=2014&num=295&dLang=EN
7. Leitold, H.: Challenges of eID interoperability: the STORK project. In: Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R., Zhang, G. (eds.) Privacy and Identity 2010. IFIP AICT, vol. 352, pp. 144–150. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20769-3_12
8. Cuijpers, C., Schroers, J.: eidas as guideline for the development of a pan European eid framework in futureid. In: Open Identity Summit 2014. vol. 237, pp. 23–38. Gesellschaft für Informatik (2014)
9. Edwards, A., Hughes, G., Lord, N.: Urban security in Europe: translating a concept in public criminology. Europ. J. Criminol. **10**(3), 260–283 (2013)
10. Zhang, R., Shi, J., Zhang, Y., Zhang, C.: Verifiable privacy-preserving aggregation in people-centric urban sensing systems. IEEE J. Sel. Areas Commun. **31**(9), 268–278 (2013)
11. Krontiris, I., Freiling, F.C., Dimitriou, T.: Location privacy in urban sensing networks: research challenges and directions (security and privacy in emerging wireless networks). IEEE Wirel. Commun. **17**(5) (2010)

12. Niu, B., Zhu, X., Chi, H., Li, H.: Privacy and authentication protocol for mobile RFID systems. Wireless Pers. Commun. **77**(3), 1713–1731 (2014)
13. Forget, A., Chiasson, S., Biddle, R.: Towards supporting a diverse ecosystem of authentication schemes. In: Symposium on Usable Privacy and Security (Soups) (2014)
14. Doss, R., Sundaresan, S., Zhou, W.: A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems. Ad Hoc Netw. **11**(1), 383–396 (2013)
15. Habibi, M.H., Aref, M.R.: Security and privacy analysis of song-mitchell RFID authentication protocol. Wireless Pers. Commun. **69**(4), 1583–1596 (2013)
16. Wikipedia: Security Assertion Markup Language – Wikipedia, The Free Encyclopedia (2016). https://en.wikipedia.org/w/index.php?title=Security_Assertion_Markup_Language&oldid=747644307
17. Security, H.J.H.: Visa Waiver Program Improvement and Terrorist Travel Prevention (2016). https://www.congress.gov/bill/114th-congress/house-bill/158/text
18. Miller, B.A., Bisdikian, C.: Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communication. Prentice Hall PTR, New Jersey (2001)
19. Bluetooth, S.: Bluetooth Specification (2017). https://www.bluetooth.com/specifications/bluetooth-core-specification
20. Soon, T.J.: Qr code. Synth. J. **2008**, 59–78 (2008)