A Privacy-Preserving User Authentication Mechanism for Smart City Mobile Apps

Maria Papaioannou
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
m.papaioannou@av.it.pt

José C Ribeiro
Instituto de Telecomunicações
Aveiro, Portugal
jcarlosvgr@av.it.pt

Valdemar Monteiro
Instituto de Telecomunicações
Aveiro, Portugal
vmonteiro@av.it.pt

Victor Sucasas
Technology Innovation Institute
Abu Dhabi, UAE
victor.sucasas@tii.ae

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
gimantas@av.it.pt

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Computing, Engineering and Science, University of South Wales
Pontypridd, UK
jonathan@av.it.pt

***Abstract*— In the dawn of the 5G era, the advances in mobile communications have created a suitable environment for the emergence of a wide spectrum of Smart City mobile applications that will play a significant role towards the improvement of citizens' life quality in the upcoming years. It is expected that Smart City mobile applications will allow citizens to access numerous and diverse services, provided by third-party Service Providers, through their mobile devices (e.g., smartphones). However, in order for the emerging Smart City mobile applications to gain the trust of all involved stakeholders and reach their full potential in the 5G market, many security and privacy concerns should be addressed in advance. Towards this direction, this paper proposes a privacy-preserving user authentication mechanism, developed in the context of the Mobilizador5G project, in order to: (a) provide mobile users with efficient and effective means to authenticate towards Service Providers, while preventing user identification and tracking; (b) allow anonymity revocation in case of user misbehavior; (c) avoid multiple user profiles creation on the Service Provider side; and (d) enable easy integration in current mobile application implementations.**

Keywords—5G, privacy-preservation, user authentication, smart city applications

I. INTRODUCTION

5G communication networks and beyond seek to provide, over the same infrastructure, differentiated services to different society sectors (vertical ecosystems), answering to the multiple requirements set by ITU-T in IMT-2020 [1]. Furthermore, 5G networks intend to interconnect, by a common core network, several networks. This infrastructure will support a strong programmability, resorting to virtualization technologies, like SDN and NFV. In this context, with standardization of 5G networks being promoted in the coming years by organizations like 3GPP, the opportunity arises for the development of novel applications that will increase the quality of citizen´s life in the future Smart Cities. However, many privacy concerns should be addressed before novel Smart City applications gain the trust of all involved stakeholders and reach their full potential in the 5G market.

Therefore, in this paper, a privacy-preserving user authentication mechanism, developed in the context of the Mobilizador5G project [2], is presented. The main focus of the Mobilizador5G project was the design, implementation, integration and validation of a new set of mechanisms for 5G-enabled services, gathering efforts from different technology companies in the telecommunications segment, addressing both B2B and B2C models.

Previous research efforts have already provided a number of efficient mechanisms for conditional privacy using pseudonym systems. In general, these mechanisms are either based on Group Signature (GS) [3], [4], or Public Key Infrastructure (PKI) [5], [6] schemes. Nevertheless, these mechanisms do not enable unlimited pseudonym self-generation in the users´ side so as to allow users to make use of different apps simultaneously, while preventing their participation in the same app under distinct pseudonyms, which is known as Sybil attack. Finally, the proposed privacy-preserving authentication mechanism will also prevent malicious users from creating multiple profiles for a specific mobile application at the Service Provider side.

In particular, the proposed mechanism is based on IBC, enabling unlinkable-yet-accountable pseudonymity [7]–[10] and its main objectives are the following: (1) to provide mobile users with effective and efficient means to authenticate

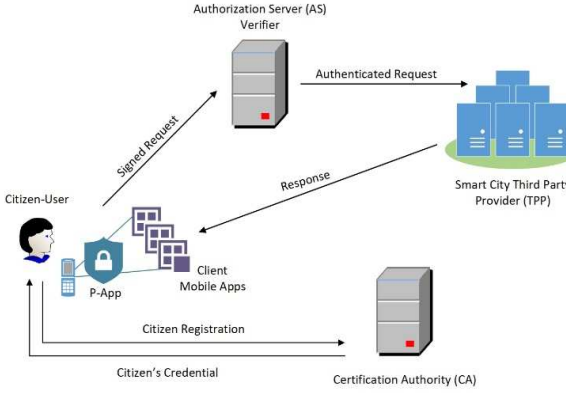

Figure 1. Proposed System Model Architecture

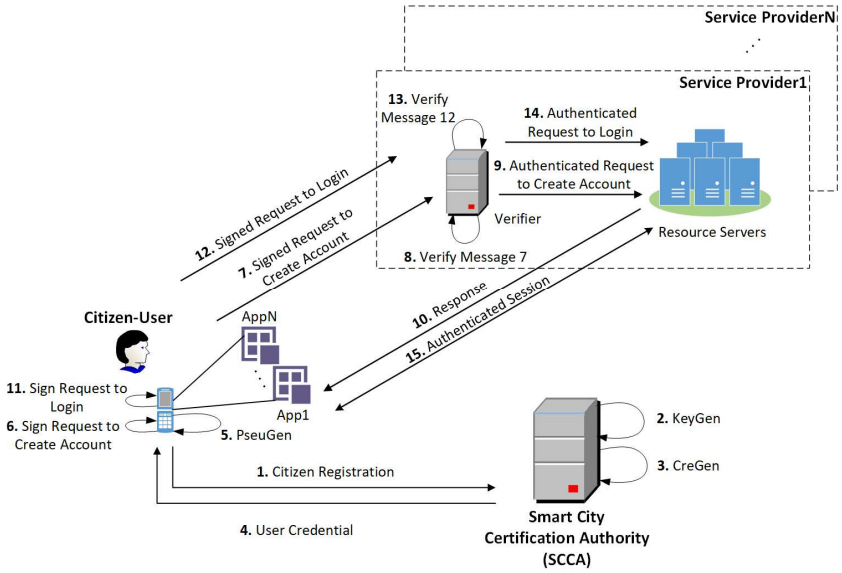

Figure 2. Proposed Privacy-Preserving User Authentication Protocol (PPUAP) for Smart City Apps

towards Service Providers, while preventing user identification and tracking; (2) to allow anonymity revocation in case of user misbehavior; (3) to avoid multiple user profiles creation on the Service Provider side; and (4) to enable easy integration in current mobile application implementations. In addition, the proposed mechanism is resilient to attack scenarios that involve dishonest and selfish mobile users.

Following the Introduction, the proposed system model architecture of the proposed privacy-preserving user authentication mechanism is presented in Section II, while the detailed description of the proposed mechanism is given in Section III. Furthermore, implementation details of the proposed mechanism, as well as DEMO setup details and validation results are provided in Section IV. Finally, Section V concludes the paper.

II. System Model

Our proposed system model architecture is composed by the following entities, also depicted in Fig. 1.:

- **The Certification Authority (CA)** is considered as an honest entity enabling privacy-preserving user authentication. It is in charge of: (i) storing user's real IDs, and (2) triggering the anonymity revocation process given user's pseudonym when needed. The CA is responsible for issuing legitimate credentials for users (afterwards their registration). The CA oversees the distribution of a revocation list with all the revoked pseudonyms in the other entities.
- **The Verifier** is an Authentication Server in the side of Smart City. The Verifier provides efficient mechanisms to enable users to authenticate and authorize mobile applications installed in their mobile device to access to remote services. It is in charge to authenticate the signed requests sent by the user and forward them to a service provider.
- **The Smart City Third Party Provider (TPP)** is considered an honest-but-curious entity, receives the authenticated requests from The Verifier and provides personalized and ubiquitous services to the users. It is in charge of identify the outliers and malicious users and report them to the CA in order to trigger the revocation process. For each application provided by TPP, it enables a specific application index, hence users can participate to certain application using their unique pseudonym of such index value.
- **The citizen** - user is subscribed to one or several services and owned an account to one or several applications. The user registers to the CA and the CA issues its valid credentials. The user is able then to self-generate unlimited pseudonyms and sign requests. The user can self-generate a new pseudonym per each application by using the unique index value of such application. In the user's mobile device, it is installed the application
- **Privacy App (P-App)** performs the cryptographic operations of the proposed privacy-preserving mechanism. It also stores the required information for the efficient operation of the proposed protocol that is considered the non-sensitive information. Therefore, the disclosure of such information would not give any advantage to a malicious actor to jeopardize user's privacy.

III. Proposed Privacy-Preserving User Authentication Mechanism for Smart City Apps

The main objective of the proposed protocol is twofold: a) to ensure that a user creates only one account for each application and thus preventing malicious users from creating multiple accounts to the same application, and b) to guarantee that different user's accounts for different applications will not be linkable.

The generic flow of the proposed privacy-preserving user authentication protocol for smart city apps consists of the following steps, as it is also depicted in Fig. 2:

1. Mobile user (citizen) with identity ***ID*** registers to Smart City CA (SCCA).
2. SCCA generates *(KeyGen algorithm)* the public parameter ***PP*** and the secret key ***SK***.

3. SCCA generates *(CreGen algorithm)* the credential ***cred*** for the user with identity ***ID***. Although the value ***ID*** is not used in the credential generation, the SCCA stores the tuple ***(ID, cred)*** in a registry REG.
4. SCCA sends the ***cred*** to the user over a secure channel and the user stores it secretly.
5. User makes use of the ***cred*** and the application index ***x*** to generate *(PseuGen)* the valid user pseudonym $\boldsymbol{pseu_x}$ for the application with the given index ***x***, (see Fig. 3).
6. User signs *(Sign algorithm)* a request to create a new account, with the pseudonym $\boldsymbol{pseu_x}$ for the application with the given index ***x*** and the user credential ***cred***.
7. User sends the signed request for account creation to Verifier through the application (e.g., App1).
8. Verifier verifies *(Verify algorithm)* the signed request for account creation. It requires the public parameter ***PP***.
9. If the signed request in step 8 passes the verification, then the authenticated request for account creation is forwarded to Smart City Servers (SCSs), and the account is created.
10. An acknowledgement of the account creation is sent back to Verifier.
11. Verifier forwards the acknowledgement of the account creation to the application (e.g., App1).
12. User signs *(Sign algorithm)* a request to login to his/her account, with the pseudonym $\boldsymbol{pseu_x}$ for the application with the given index ***x*** and the user credential ***cred***.
13. User sends the signed request to login to his/her account to Verifier through the application (e.g., App1).
14. Verifier verifies *(Verify algorithm)* the signed request for account login.
15. If the signed request in step 14 passes the verification, then the authenticated request to login is forwarded to SCSs, and the user logs in.
16. An authenticated session between the application (e.g., App1) and the Service Provider (e.g., Service Provider1) is established.

A. *The cryptographic algorithms*

In this subsection, the suite of cryptographic algorithms needed to implement the proposed security system model are presented. In particular, the algorithms are performed by three different entities: a) the Certification Authority (CA); b) the Authorization Server (AS) – Verifier; and c) the Citizen – User.

1) CA algorithms:

- **KeyGen:** The CA takes a security parameter K as input and outputs a set of *public* parameters *PP* and a *secret* key *s*.

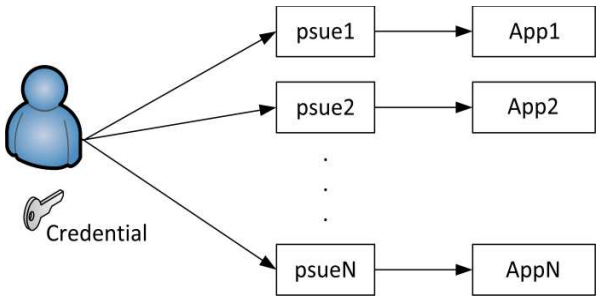

Figure 3. Pseudonym Generation Function.

- **CreGen:** The CA runs this algorithm after user´s registration to generate a credential *cred* for a user with identity *ID*. The CA stores a registry *REG* with the (*ID,cred*). The user secretly stores the credential.

2) User algorithms:

- **PseuGen:** The user takes the credential *cred* and the index of the pseudonym *x* as input. The index is a public value provided by the Smart City TPP. The output of this algorithm is a pseudonym $pseu_x$ and μ'.
- **Sign:** The user runs this algorithm to sign an arbitrary message *M*, with a pseudonym $pseu_x$, for the index *x* and the credential *cred*. The output is the signature σ.

3) Authorization Server (AS) – Verifier:

- **Verify:** This algorithm performs two sub-algorithms, namely RevCheck and SignCheck, whose description is following, and outputs ``valid´´ if and only if both sub-algorithms output ``valid´´. The sub-algorithms are:
  - **RevCheck:** The algorithm returns ``invalid´´ if RL contains the pseudonym *pseu.* Otherwise, it outputs ``valid´´.
  - **SignCheck:** Checks whether the signature σ is correct for the message *M*, with respect to the pseudonym $pseu_x$ for the index *x*.

4) Specific CA operations for conditional privacy:

Additionally, the CA performs the following operations in order to enable conditional privacy. In this way, the CA can trigger user´s anonymity and block selfish and misbehaving users to access the provided services. Therefore, the CA creates a Revocation List (RL) including some or all pseudonyms of the revoked users and transmits is to the AS-Verifier.

- **GenPseuList**(*REG,* $\{x_1, \ldots, x_n\}$): The algorithms generates the pseudonym list *PseuL* with all valid pseudonyms of registered users and index values $\{x_1, \ldots, x_n\}$ of *n* registered services provided by Smart City TPP.
- **Open**(*pseu*)**:** If and only if the pseudonym *pseu* is part of a valid signature, then the algorithm returns the *ID* of the user owning the pseudonym *pseu*.
- **Revoke**(*pseu,* $\{x_1, \ldots, x_n\}$)**:** It revokes the user owning the pseudonym *pseu* by including in the *RL* the user´s pseudonyms with indexes $\{x_1, \ldots, x_n\}$.

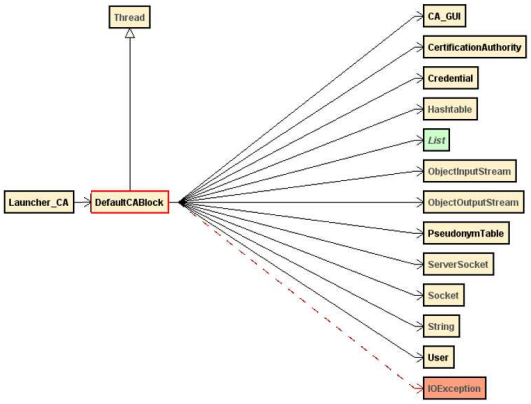

Figure 4. CA Server.

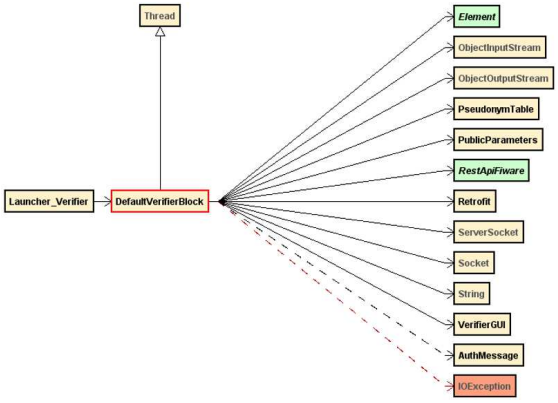

Figure 5. Verifier Server.

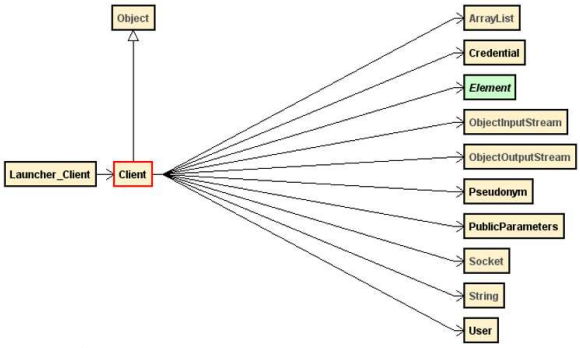

Figure 6. Client.

IV. Implementation of the Proposed Privacy-Preserving User Authentication Mechanism

The implementation testbed is constituted by a smartphone, where the P-App and a given smart city app run, and three distributed servers (i.e., the CA, the Verifier and the Smart City server) deployed in OpenStack platform [11].

A. Class Diagrams

Implementation details (e.g., classes, attributes, operations, relations among objects) of the CA Server, the Verifier Server and the P-App are provided by the corresponding class diagrams, as shown in Fig. 4, 5 and 6.

In particular:

- *CA Server's class diagram (Fig. 4):*
  The *DefaultCAblock* class implements a thread listening port 6066 and waiting for communication from the Verifier or the P-App. It is initiated by the *"Launcher_CA"* class andconnected with the "*Credential*", "*CertificationAuthority*" and "*PseudonymTable*" classes to generate and provide the credentials to user.
- *Verifier Server's class diagram (Fig. 5):*
  The *"DefaultVerifierblock"* is initiated by the *"Launcher_Verifier"* class and implements a thread, opening a TCP socket and listening port 6065 while waiting for communication with P-App. The Verifier server communicates with the CA server through a TCP socket as a client.
- *P-App's class diagram (Fig. 6):*

  The P-App is initiated by the *"Launcher_Client"* class. It communicates with the CA server to register as a user and request credentials. It uses the *"Pseudonym"* class to generate the pseudonyms with the received credentials. It also connects with the Verifier server for signature verification.

B. DEMO Setup

The DEMO setup consists of the following steps:

1. Start the CA server on the OpenStack platform
2. Install and run the P-App on the smartphone
   a. User registration
   b. User login
3. Start the Verifier server on the OpenStack platform
4. Start the Smart City Server, where the Smart City service runs, on the OpenStack platform
5. Install and run the Smart City app, requesting the Smart City service, on the smartphone
   a. User registration
   b. User login
   c. Session establishment

C. Validation

In the context of the Mobilizador5G project, we implemented and tested four cases of the privacy-preserving user authentication mechanism, as shown in Table I, in order to evaluate whether it functions properly. In all four cases, the implemented mechanism functioned properly.

TABLE I. Tested Cases

Order	*Tested functionalities and Performances*	*Check List*
1	Local implementation	✔
2	Implementation in OpenStack platform	✔
3	Implementation in OpenStack platform, connection to the Smart City service	✔
4	Implementation in OpenStack platform, Android emulator connected to M5G network, connection to the Smart City service	✔

V. Conclusions

The advances in 5G mobile communications have created a suitable environment for the deployment of a wide spectrum

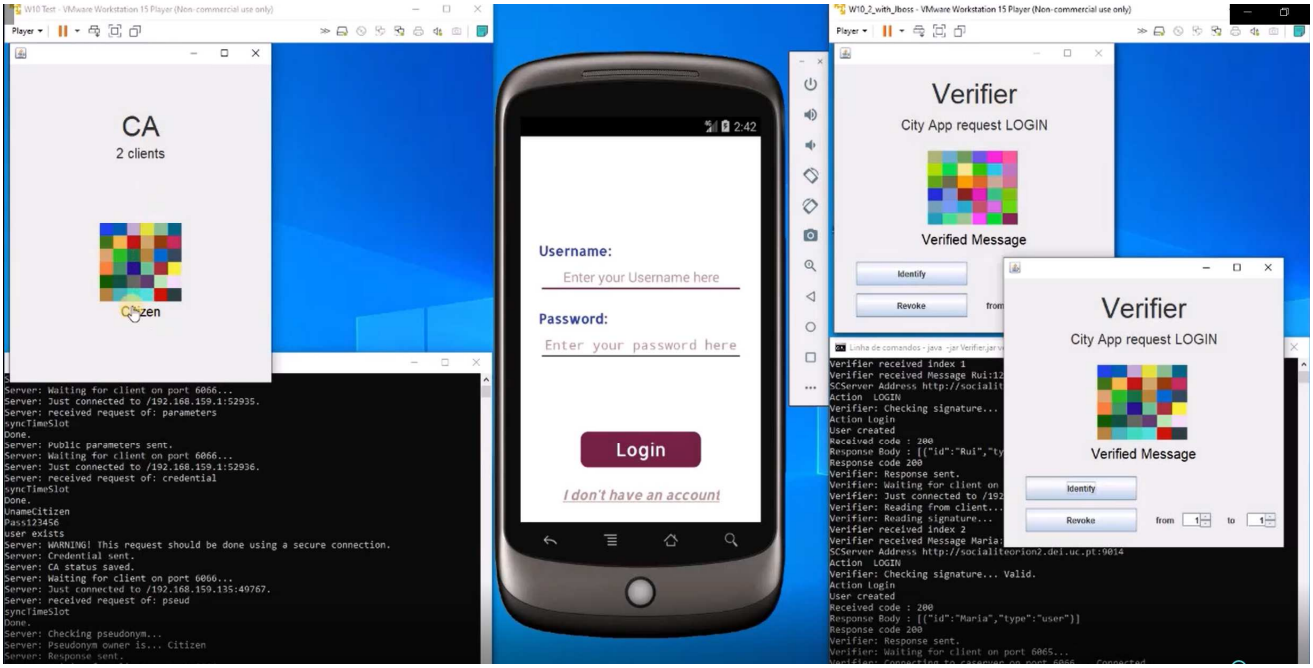

Figure 7. DEMO Setup – Local Implementation with Android Emulator.

of Smart City mobile applications. It is anticipated that Smart City mobile applications will play a key role towards the improvement of citizens' life quality in the upcoming years, allowing them to access numerous and diverse services, provided by third-party Service Providers, through their mobile devices (e.g., smartphones). Nevertheless, many security and privacy concerns should be addressed before novel Smart City applications gain the trust of all involved stakeholders and reach their full potential in the 5G market.

Although previous research efforts have already provided a number of efficient mechanisms for conditional privacy using pseudonym systems, these mechanisms are not considered suitable for the emerging Smart City mobile applications. In particular, these mechanisms do not enable unlimited pseudonym self-generation in the users´ side so as to allow users to make use of different apps simultaneously, while preserving users´ privacy and preventing Sybil attacks.

Towards this direction, this paper proposes a privacy-preserving user authentication mechanism, developed in the context of the Mobilizador5G project, in order to: (a) provide mobile users with efficient and effective means to authenticate towards Service Providers, while preventing user identification and tracking; (b) allow anonymity revocation in case of user misbehavior; (c) avoid multiple user profiles creation on the Service Provider side; and (d) enable easy integration in current mobile application implementations.

Our next steps include the integration of the proposed privacy-preserving user authentication mechanism into already developed Smart City mobile applications on smartphones and evaluate its performance.

ACKNOWLEDGMENT *(Heading 5)*

This work is supported by the European Regional Development Fund (FEDER), through the Regional Operational Programme of Lisbon (POR LISBOA 2020) and the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework [Project 5G with Nr. 024539 (POCI-01-0247-FEDER-024539)] and the Moore4Medical project, funded within ECSEL JU in collaboration with the EU H2020 Framework Programme (H2020/2014-2020) under grant agreement H2020-ECSEL-2019-IA-876190, and Fundação para a Ciência e Tecnologia (ECSEL/0006/2019).

REFERENCES

[1] E. Mohyeldin, "Minimum Technical Performance Requirements for IMT-2020 radio interface(s)," ITU-R Workshop on IMT-2020 terrestrial radio interfaces, 2020.

[2] "Mobilizador 5G Project." [Online]. Available: https://5go.pt/en/home/.

[3] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "AnonySense : Privacy-Aware People-Centric Sensing Categories and Subject Descriptors," *Proceeding ACM 6th Int. Conf. Mob. Syst. Appl. Serv.*, pp. 211–224, 2008.

[4] S. Rahaman, L. Cheng, D. D. Yao, H. Li, and J.-M. J. Park, "Provably Secure Anonymous-yet-Accountable Crowdsensing with Scalable Sublinear Revocation," *Proc. Priv. Enhancing Technol.*, vol. 2017, no. 4, pp. 384–403, 2017.

[5] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "SPPEAR : Security & Privacy-Preserving Architecture for Participatory-Sensing Applications," pp. 39–50.

[6] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," *SASN'05 - Proc. 2005 ACM Work. Secur. Ad Hoc Sens. Networks*, vol. 2005, pp. 11–21, 2005.

[7] V. Sucasas, G. Mantas, M. Papaioannou, and J. Rodriguez, "Attribute-based pseudonymity for privacy-preserving authentication in cloud services," *IEEE Trans. Cloud Comput.*, vol. 7161, no. c, 2021.

[8] V. Sucasas, G. Mantas, J. Bastos, F. Damião, and J. Rodriguez, "A Signature Scheme with Unlinkable-yet-Accountable Pseudonymity for Privacy-Preserving Crowdsensing," *IEEE Trans. Mob. Comput.*, vol. 19, no. 4, pp. 752–768, 2020.

[9] V. Sucasas *et al.*, "A privacy-enhanced OAuth 2.0 based protocol for Smart City mobile applications," *Comput. Secur.*, vol. 74, pp. 258–274, 2018.

[10] L. Oliveira, V. Sucasas, G. Mantas, and J. Rodriguez, "Implementation of a pseudonym-based signature scheme with bilinear pairings on Android," in *Proceedings of the 12th EAI International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM 2017)*, 2017, pp. 75–87.

[11] "OpenStack." [Online]. Available: https://www.openstack.org/.