Potential Impacts in Citizens' Privacy of using Federated Identity Management to Offer e-Government Services

Jorge Navas and Marta Beltrán
Department of Computing, ETSII, Universidad Rey Juan Carlos, Madrid, Spain

Keywords: e-Government, Federated Identity Management (FIM), Mobile Connect, OpenID Connect, Privacy, SAML, Threat Modelling.

Abstract: The ability to verify citizens' identity and to authenticate and to authorize them when accessing to e-Government services (such as on-line voting, licence renewal or tax payment) is crucial for the digital transformation of public administrations. Governments need identity management mechanisms valid across different services, platforms, devices, technologies and even physical borders. Federated Identity Management (FIM) can help in ensuring secure identity management, in improving citizens' experience and in increasing services' accessibility. But this comes with a price since relying on Identity Providers, whether public or private, poses new privacy threats that has to be faced. This paper presents a threat model of the most promising and extended FIM specifications, OpenID Connect and Mobile Connect, when used as federated identity management solutions for e-Government services. A set of three improvements is proposed to avoid these threats or to mitigate their impacts, taking into account both, specification and implementation aspects. Furthermore, guidelines and recommendations in order to improve future versions of the specifications and/or their implementations are provided for developers, providers and policy makers.

1 INTRODUCTION

e-Government is the use of information and communication technologies to enable and to improve the delivery of public services to citizens, employees, businesses and agencies. As the adoption of e-Government increases, Identification, Authentication, Authorization and Accounting (IAAA) is becoming one of its main challenges and opportunities. Proposed solutions must be secure, robust, scalable, compliant with regulations and laws, technically feasible, economically acceptable, socially inclusive and easy to use for citizens. At the same time, the issue of privacy is central, because public administrators must play a key role in protecting the privacy of citizens when accessing to their services. Citizens very likely will reveal their real identity (and associated attributes) when accessing e-Government services, just the opposite that they may do, using fictitious identities, pseudonyms or anonymous modes for example, when browsing web pages or accessing social networks.

In these e-Government scenarios federated and token-based mechanisms already proposed and standardized in web and cloud contexts such as SAML (OASIS, 2005), OAuth (IETF, 2012), OpenID Connect (OIDF, 2014) and/or Mobile Connect (GSMA, 2015) are being adopted. These mechanisms allow citizens as end users (EU) to access different e-Government resources, applications and services through a single Identity Provider (IdP), avoiding the need of having an account (with its related password) for each resource, application or service. Resources, application and services are the relying parties (RP) in these schemes, relying on IdPs to support authentication and/or authorization decisions and to store accounting information.

To the best of our knowledge there are not previous works devoted to analyse privacy threats posed by the use of these federated identity management mechanisms in e-Government scenarios. This threat modelling would be a valuable source of information to propose specific improvements which can be made to specifications such as OpenID Connect or Mobile Connect or to their specific implementations when trying to improve the privacy levels of IAAA within e-Government scenarios beyond the traditional web. These are the main contributions of this paper (1) The selection of a threat model of OpenID Connect/Mobile Connect suitable for sce-

Navas, J. and Beltrán, M.
Potential Impacts in Citizens' Privacy of using Federated Identity Management to Offer e-Government Services.
DOI: 10.5220/0007797703500355
In *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019)*, pages 350-355
ISBN: 978-989-758-378-0

narios when these specifications are used for Federated Identity Management in e-Government scenarios (2) The proposal of three improvements regarding specification and implementation aspects, capable of avoiding and/or mitigating these threats (3) The validation and discussion of these contributions using real use cases.

The rest of this paper is organized as follows. Section 2 presents background of Federated Identity Management in e-Government, after that Section 3 motivates our research contributions and introduces the considered threat model for e-Government scenarios, focusing on privacy threats. Section 4 proposes different mitigations and countermeasures focused on improving privacy levels when using Federated Identity Management in e-Government contexts and discusses validation results obtained within a controlled lab replicating real scenarios. Finally, Section 6 summarizes the main conclusions of this work, discussing obtained results and giving some recommendations.

2 E-GOVERNMENT AND FEDERATED IDENTITY MANAGEMENT

In 2008 New Zealand launched the e-Government Interoperability Framework (Mckenzie et al., 2008) relying on a federated identity management solution, SAML. The United Kingdom, Austria, Canada, Hong-Kong, Denmark, Malta, Switzerland, the Netherlands or Italy, to mention only some examples, followed the same direction a bit later (Baldoni, 2012). In this context the European regulation on electronic IDentification, Authentication and trust Services, or eIDAS, was born in July of 2014 (European Parlament, 2014). It is an initiative designed to provide a regulatory environment that promotes the use of electronic identification (eID) schemes within the European Union. Countries that are part of this Union must accept those eIDAS digital identities that meet the regulation working within an identity federation. The eIDAS technical specification is based on SAML 2.0 and there is a specific implementation profile of SAML focused on interoperability aspects in order to enable e-Government applications (Kantara Initiative, 2010).

Federated identity management specifications have significantly evolved since then and all these governments have progressively adopted or at least, tried to adopt, new standards and specifications such as OpenID Connect or Mobile Connect (GSMA, 2018), (Chausson, 2015), (Future Trust Services, 2017). The main advantage of these new schemes is two-fold. On one hand, unlike SAML or OAuth, they are able to solve authentication and authorization with only one flow (through the use of two tokens, and ID token and Access token). On the other hand, many citizens are already enrolled at Identity Providers supporting these specifications, being Facebook, Google, Twitter and MNOs the most extended providers. This enables the evolution from government-issued eIDs to third parties-issued eIDs. For example, Estonian mobile-ID (e-Estonia, 2018) allows citizens to use a special SIM card (which must be requested to the mobile phone operator) in order to use their mobile phone as a form of secure digital identity. BankID (Finansiell ID-Teknik BID AB, 2019), supported in Norway, Sweden and Finland, enables the use of bank-issued eIDs to access to e-Government services.

All these solutions, with their specificities, have certain aspects in common regardless the underlying FIM specification or the kind of IdP. Perhaps the most important is that, a citizen, in order to use any Identity Provider (public or private, i.e. governmental or third-party), needs to register or to enrol first. This usually requires to provide some Personally Identifiable Information (PII) such as full name, email address, telephone number, etc. At the enrolling moment it is also required to provide a citizen ID, passport number, Unique Tax Number or National Insurance Number, something that the government is able to check or to verify against existing data in order to know who is the real person behind the eID.

3 MOTIVATION

When evaluating the use of OpenID Connect to solve citizens IAAA, a government has two options: to deploy its own infrastructure as Identity Provider relying on any of the available frameworks, both open source or proprietary certified OpenID Provider Servers and Services (OIDF, 2018), or to rely on an external provider such as Facebook, Google, an MNO etc. In either case, as it has been mentioned before, the citizen needs an account at the IdP with its associated authenticators (at least a password)

Governments have shown a great interest in introducing OpenID Connect and Mobile Connect as an alternative to SAML for eID due to their aforementioned advantages, but they hesitate whether to evolve in this direction because they are younger specifications less tested than the mature SAML. Figure 1 shows the login page of the Spanish Official State Gazette (BOE). Citizens are able to perform this login with a local account or using their Twitter, Facebook

Figure 1: Login page of the Spanish Official State Gazette.

Figure 2: Login page when using France Connect.

or Google accounts, i.e. using one of these third parties as Identity Provider with OpenID Connect. Figure 2 shows the login page when using France Connect to consume any e-Government service in France. In this case, five different identity providers can be used: one of them is governmental (the French tax agency) and the rest are private (a postal service company, two assurance companies and Orange, when relying on Mobile Connect).

In these two cases different concerns arise. Citizens lose control over their PII at Twitter, Facebook, Google, La Poste, Orange, etc. (at the selected IdP) and at the government website (the BOE or any other, the RP in this scenario), citizens are not able to know if this PII is shared with third parties or how this sharing is performed, PII can be leaked from the IdP or the RP infrastructures as well as from the citizen's devices (since HTTPS is used, we assume that communication channels are properly protected within the different performed flows), both, the IdP and the RP have the ability to track citizens activity at the accessed resource, application or service and to gather information about their specific interests and finally, both, the IdP and the RP are able to track citizens locations over time through different techniques and mechanisms.

All these threats may lead to different kinds of impacts such as exclusion, loss of autonomy and/or liberty, stigmatization, power imbalance, economic loss or even, physical harm. As a result, citizens will likely lose trust on their government, being reluctant to engage in further e-Government initiatives due to their bad experience about how sensitive data is collected, used, secured, transmitted, shared, etc.

In (Navas and Beltrán, 2019) a complete and generic threat model of OpenID Connect/Mobile Connect is provided, taking into account all security and privacy aspects and considering both, specification and implementation issues. From this model, the set of privacy threats affecting e-Government services considered in this work is:

1. Lack of control over required PII.
2. Lack of transparency in the sharing of PII.
3. PII leakage.
4. Citizen profiling.
5. Location tracking.

4 PROTECTING CITIZENS FROM IDENTIFIED THREATS

In this section we propose a set of specific mitigations, countermeasures and remediation options capable of avoiding or mitigating impacts of threats identified in the previous section, acting on aspects of both, specification and implementation of OpenID Connect (OIDF, 2014).

4.1 Encryption of PII

PII must be hashed and encrypted by citizens before sharing it with identity providers. This measure provides control over the data stored at IdPs, protecting confidentiality and integrity. Therefore, when an end user is registering with an IdP she has to hash and to encrypt with a private key her sensitive PII (email, telephone number, picture, address, credit card numbers, social security numbers, etc.), not essential for IdPs operation. This procedure must be performed by some kind of agent running on end users' side (a browser plugin, an app: some component at the User Agent). This plugin or app can rely on cryptographic software primitives or on some kind of trusted hardware (following the FIDO Alliance standards or relying on Trusted Platform Modules) to guarantee isolation from other applications running on the same device and better protect the private key. These aspects may be out of the scope of the new specification, the essential recommendation here is to use cryptographic mechanisms regardless of how they are implemented.

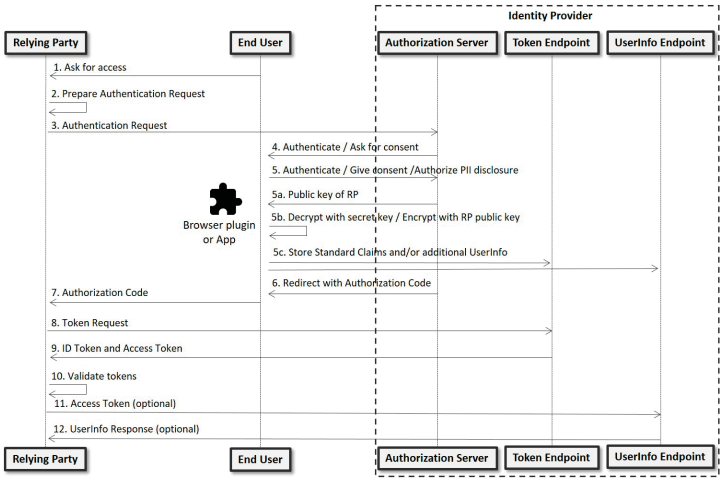

Figure 3: Authorization Code Flow with encrypted PII.

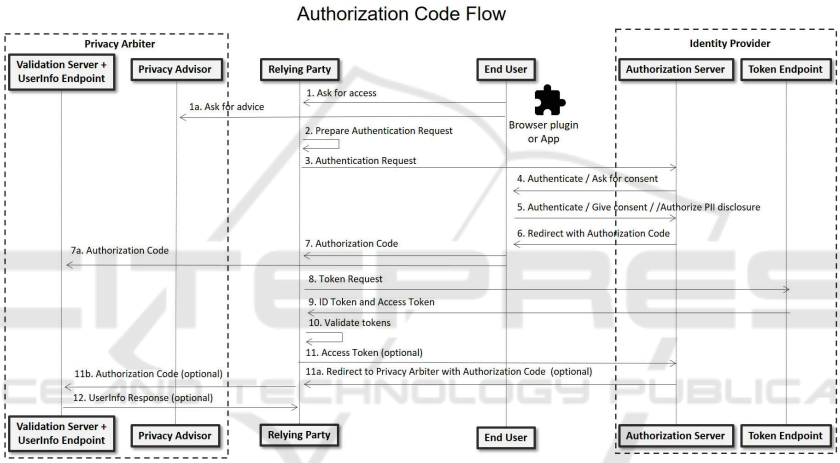

Figure 4: Authorization Code Flow with Privacy Arbiter.

Furthermore, when the step 5 of Figure 3 takes place, the end user not only performs her authentication or gives her consent, she also decides, explicitly, which attributes of her PII can be revealed to this specific RP. To avoid this kind of decisions to the end user, she could be asked during her registration at the IdP what subset of PII attributes she would like to reveal to all RPs or to all RPs within certain categories (for example, by sector, by domain name, etc.).

If any of these attributes is encrypted at the IdP, the end user decrypts it and encrypts it again with the public key of the RP involved in this specific flow. This public key is provided by the IdP and it must be gathered during the RP registration at the IdP (the JSON Web Key specification is recommended to represent the cryptographic keys (IETF, 2015)). In this way, only the RP, using her private key, will be able to recover this sensitive PII.

4.2 Flow ID

To mitigate threats regarding profiling and tracking, we propose to change the meaning of the *sub* parameter of the ID token, instead of being a unique identifier of the end user at the IdP it should be a unique identifier of a specific IAAA flow. The Flow ID can be generated at the IdP after receiving an Authentication Request from the RP, based on the RP identifier, the end user identifier and a salt. It has to be pointed that IAAA flows do not change, only the meaning of this parameter.

4.3 Privacy Arbiter

The main idea is to have a third-party, different from the Identity Provider, allowing the citizen to know how her attributes are being shared, to have an effective and real-time control over her data deciding

to who, when and how are forwarded, to easily use metrics such as reputation, trust or risk to make decisions, to use pseudonyms, etc. To avoid significant modifications in the current specification of OpenID Connect/Mobile Connect, we propose this mitigation, mainly, as an implementation improvement, extending the IdP standard functionalities with an additional service provider, the Privacy Arbiter or PA (instead of the aforementioned Validation Service, or actually, extending it). This new provider should not have, ever, the aforementioned dual-role (RP and PA at the same time), avoiding therefore the threat of amplification that arises from account compromises, etc.

Figure 4 shows the Authorization Code flow with OpenID Connect when a Privacy Arbiter is used (it can be also used with the Implicit Flow, it is only an example). As in previous mitigations, some kind of agent running on end users' side (a browser plugin, an app: some component at the User Agent) is required. Again, when the step 5 of Figure 4 takes place, the end user not only performs her authentication or gives her consent, she also decides, explicitly, which attributes of her PII can be revealed to the RP when the PII is shared with the RP using the Standard Claims of the ID token. This would be the first modification affecting the current OpenID Connect specification.

The second modification is related to the UserInfo Endpoint, no longer required since the sharing of additional PII with RPs will be performed, if necessary, through the Privacy Arbiter. When the RP presents the Access Token at the IdP, the IdP has to redirect this information request to the Privacy Arbiter specified by the End User during her registration process.

4.4 Validation

All proposed mitigations have been validated and evaluated in a controlled lab reproducing real use cases like those introduced in the Motivation section. The proposed privacy improvements at the IdP infrastructure have been implemented through a proxy (located before the IdP), proposed measures and best practices act as a wrapping improving current solutions without changing core implementations, adding as a new layer additional privacy capabilities.

The development of the plugin/app for the end user and of a complete Privacy Arbiter are out of the scope of this research, in our experiments for validation and evaluation their behaviour has been assessed with very preliminary prototypes executing only their essential functionalities. As a proof of concept, to know how easy or complicated it would be for RPs to adapt to the proposed improvements when working with the most popular IdPs, Facebook and Google, we have extended the Facebook ID PHP SDK (Facebook, 2018) and the Google's OAuth 2.0 APIs in Python (Google, 2018) to implement all the specification modifications and best practices proposed to mitigate privacy threats and it only required a little more than 60 code lines.

It has to be pointed that the costs of incorporating proposed mitigations comes from required changes in current software projects, not from a significant increase in the computational complexity of using OpenID Connect (not in terms or resource - CPU, memory - consumption). This complexity is increased only by using cryptographic mechanisms and in this case all the burden falls on the IdP (Twitter, Facebook or Google) and on the new Privacy Arbiter, therefore, on the agents of the flow in possession of large and powerful resources.

As it can be observed, almost all proposed mitigations imply changes in the OpenID Connect core specification, but the two first trying to add certain aspects that until now has been considered out of its scope (use of encryption for PII, meaning of the *sub* parameter of the ID token). Only the proposal of the Privacy Arbiter can be considered a significant modification to the current specification approach. But we think that it is conveniently justified given the introduced threat model and that our proposal minimizes required modifications in the specification.

5 CONCLUSION

When considering to offer a new e-Government service, public administrations must analyse what form of eID is most secure, robust, scalable, compliant with regulations and laws, technically feasible, economically acceptable, socially inclusive and easy to use for citizens within the specific considered context. Nowadays, an additional value is that electronic identities can be used for cross-border transactions. It is very likely that the result of this analysis will lead to the deployment of a FIM based on OpenID Connect or Mobile Connect. If this is the case, the IdP can be controlled by the own government or it can be a third-party such as Facebook, Google, Twitter, an MNO, an assurance company or a bank. Governments should ensure that citizens without third party-issued electronic identities are not excluded from e-Government services, citizens cannot be forced to enrol with a private company. All threats identified in our threat model must be thoroughly considered before making this decision.

Finally, proposed mitigations and measures should be deployed. We have checked that the en-

cryption of PII and the use of the Privacy Arbiter returns citizens the control over required PII, significantly improves the transparency in the sharing of PII and makes very complicated the leakage of PII. The use of the Flow ID, on the other hand, hinders citizens profiling and location tracking.

Ideally, future versions of specifications will include these or other similar. Or new e-Government profiles of current specifications will be proposed considering privacy aspects and not only interoperability aspects as it has happened so far. But this is not the scenario yet, so governments and/or third-parties should follow the generic specifications (OpenID Connect, Mobile Connect) and add the proposed privacy improvements afterwards. Whatever the chosen option (government-issued or third party-issued IDs, set of implemented improvements, etc.), the principle of data minimization must be always applied, gathering only the PII required by the FIM scheme to work. Identities must be revocable when necessary at the request of any of the agents the IAAA scheme (in the event of compromise, for example). We also wish to note that the use of biometric data should be avoided unless absolutely necessary, because in the event of a compromise, biometric data cannot be revoked.

ACKNOWLEDGEMENTS

This research has been partially supported by the Government of Spain (RTC-2017-6253-1) and by the Ericsson-URJC Chair ("Data Science applied to 5G").

REFERENCES

Baldoni, R. (2012). Federated identity management systems in e-government: the case of Italy. *Electronic Government, An International Journal*, 9:64–84.

Chausson, C. (2015). France Connect: an ID federation system to simplify administrative processes. https://joinup.ec.europa.eu/document/france-connect-id-federation-system-simplify-administrative-processes.

e-Estonia (2018). Mobile-ID. https://e-estonia.com/solutions/e-identity/mobile-id.

European Parlament (2014). Regulation (EU) no 910/2014 of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN.

Facebook (2018). Facebook login. https://developers.facebook.com/docs/facebook-login/.

Finansiell ID-Teknik BID AB (2019). Bankid. https://www.bankid.com/en/.

Future Trust Services (2017). Overview of eID services. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b52e19d7&appId=PPGMS.

Google (2018). Google identity platform. https://github.com/googleapis/google-api-python-client.

GSMA (2015). Mobile Connect. https://github.com/GSMA-OneAPI/Mobile-Connect.

GSMA (2018). Mobile Connect for cross-border digital services lessons learned from the eIDAS pilot. https://www.gsma.com/identity/wp-content/uploads/2018/02/MC-for-cross-border-digital-services_eIDAS_Feb2018-FINAL-web.pdf.

IETF (2012). The OAuth 2.0 authorization framework. http://tools.ietf.org/html/rfc6749.

IETF (2015). JSON web key (JWK). https://tools.ietf.org/html/rfc7517.

Kantara Initiative (2010). eGovernment implementation profile of SAML v2.0 (version 2.0bis). https://kantarainitiative.github.io/SAMLprofiles/eGovImplProfile.html.

Mckenzie, R., Crompton, M., and Wallis, C. (2008). Use cases for identity management in e-government. *IEEE Security & Privacy*, 6:51–57.

Navas, J. and Beltrán, M. (2019). Understanding and mitigating OpenID connect threats. *Computers & Security*, 84:1–16.

OASIS (2005). SAML v2.0 standard. https://wiki.oasis-open.org/security/FrontPage.

OIDF (2014). OpenID Connect 1.0. http://openid.net/connect/.

OIDF (2018). Certified OpenID Connect implementations. https://openid.net/developers/certified/.