Assurance, Consent and Access Control for Privacy-Aware OIDC Deployments

Gianluca Sassetti[1,2(✉)], Amir Sharif[1(✉)], Giada Sciarretta[1(✉)], Roberto Carbone[1(✉)], and Silvio Ranise[1,2(✉)]

[1] Fondazione Bruno Kessler, Trento, Italy
{asharif,g.sciarretta,carbone,gsassetti,ranise}@fbk.eu
[2] University of Trento, Trento, Italy

Abstract. The large amount of personal data that is shared in the digital age has proportionally increased the risks of user privacy violations. The same privacy risks are reflected in OpenID Connect, which is one of the most widespread protocols used for identity management to access both private and public administration services. Since personal data is collected and shared via OpenID Connect, appropriate technologies to protect user privacy should be adopted as suggested by data protection guidelines and regulations (e.g., the General Data Protection Regulation). Unfortunately, it is difficult to make the privacy-enhancing technology suggestions in such documents actionable and available to IT professionals who are required to configure them within their OpenID Connect deployments. To overcome this problem, we present a practical approach to improving user privacy in OpenID Connect-based solutions by identifying a set of privacy-preserving features extracted from the available OpenID Connect specifications. We conduct a privacy compliance analysis on popular private and governmental OpenID Providers to determine how widely these privacy best practices are used in the wild. The findings indicate that different OpenID Providers grant varying levels of assurance and address different aspects of privacy, failing to provide full support for data protection principles.

Keywords: OpenID Connect · Digital Identity · Privacy · GDPR

1 Introduction

Online privacy has become increasingly important because of the growing number of digital transactions that require processing personal data. Multi-party applications [55] are a common configuration in which service providers trust identity providers to authenticate users and then make access decisions based on the authentication information provided. Such information includes personal data comprising name, email, address and more. This requires the deployment of appropriate controls to support the privacy of users.

One of the most widely used identity management solutions in multi-party applications is OpenID Connect (OIDC) [53], which is implemented for services supported by both private organizations and public administrations [6,54].

Published by Springer Nature Switzerland AG 2023
V. Atluri and A. L. Ferrara (Eds.): DBSec 2023, LNCS 13942, pp. 203–222, 2023.
https://doi.org/10.1007/978-3-031-37586-6_13

Notable examples of the former are financial and banking applications, while national and international digital identity infrastructures are the most important instances of the latter and are used to allow citizens to access a wide range of online services of the public administration. In both cases, large volumes of highly sensitive personal data are processed and exchanged among identity and service providers, and the disclosure or unauthorized modification of this data may have serious consequences for end users, clients and citizens. As a result, it is crucial to guarantee that OIDC deployments are privacy-preserving and comply with data protection laws, such as the European General Data Protection Regulation (GDPR) [12].

Unfortunately, it is unclear what the current state of the art is for OIDC deployments with respect to the degree of privacy they offer. The problem is twofold. First, there is a lack of a coherent set of Best Current Practices (BCPs) to help in configuring and implementing privacy-aware OIDC deployments. Instead, considerations and suggestions to use data protection mechanisms are scattered in several official OIDC specifications or are emerging as de facto standards while being adopted by a large number of OIDC Providers (OP). The second issue is a lack of privacy compliance analysis for private and public sector OPs to determine how much they use the privacy-enhancing features available in various OIDC specifications.

To address these issues, our work takes a pragmatic approach and considers compliance with existing data protection regulations by using the GDPR principles to characterize the notion of privacy and proposes: (i) a well-defined set of BCPs derived from OIDC specifications and current practices adopted by OPs; (ii) a study of the adoption of the identified set of BCPs in current OIDC deployments used by both private and public online services; this allows us to understand the level of privacy and assurance offered by OPs. The BCPs can serve as a reference for developers to deploy privacy-preserving OPs. Furthermore, they can be used in services that analyze the degree of assurance that various OPs grant. As a matter of fact, this work can provide the main building block to automate the process of detecting BCPs adoption, paving the way for a large-scale analysis of OPs.

Paper Structure. Section 2 presents some notions needed to understand this work. Section 3 details some relevant previous work that deals with privacy issues in OIDC. In Sect. 4, we provide the list of features analyzed for this work alongside our recommended privacy BCPs to provide privacy-preserving OPs' implementations. We present our privacy BCP compliance analysis results for popular private and eIDAS OPs in Sect. 5 and discuss some interesting observations in Sect. 6.

2 Background

We characterize privacy w.r.t. five goals extracted from the GDPR [12] (Sect. 2.1) and provide a concise description of OAuth and OIDC (Sect. 2.2).

2.1 Privacy Principles

We take a pragmatic approach to decomposing privacy with respect to the privacy goals identified in the GDPR [12]. From Article 5 of the GDPR, we recall the following principles, by focusing on those aspects that are more relevant to the privacy of OIDC deployments.

Data Minimization: the parties involved in data exchanges should use and share only the minimum amount of user data necessary for their functions;

Confidentiality: personal data shall be protected from unauthorized, unlawful disclosure. Here we focus on the aspects of confidentiality related to the controlled disclosure of personal information.

Data Accuracy: data shall be exact and correct; the party collecting the data should have a minimum degree of confidence in the correctness of the data;

Transparency: the party collecting data shall clearly state the purpose of the data acquisition and allow the user to opt-in to the processing of their data. Also, the parties with which personal data will be shared need to be communicated to the user.

We also define one more privacy principle which is not explicitly included in Art. 5 of the GDPR, but can be directly derived from it:

Unlinkability: the user should not be identifiable and traceable across different platforms, without giving explicit consent. User data should be stored and shared in a way that would not allow other parties to identify the user and link their actions to a single account, thus granting a minimum level of anonymity. Unlinkability should hold even when colluding parties unlawfully share data.

These privacy principles are the ones that can be supported by OIDC implementations. Principles such as accountability, storage limitation, and lawfulness, which are also defined in the GDPR, are outside the scope of this work. OIDC does neither specify how parties store and keep data nor the data processing policies that are put in place. Although confidentiality is a broad concept, that needs to be ensured at different levels of the implementation stack, we work under the assumption that other security mechanisms [48] have been put in place and consider only the mechanisms to access and disclose user data.

Unlinkability is a pragmatic transposition of purpose limitation, for which data shall be collected and processed only for its explicit and legitimate purpose, as stated in Art. 5 par. 1 lit. b of the GDPR. Any unauthorized party that is able to identify the user extracts an additional quantity of data from the user's activity. Thus, it violates the principles of confidentiality and transparency, as the user has not acknowledged and agreed to the use of their data. Given that this scenario is particularly relevant for OIDC, we have included unlinkability as a privacy principle. For ease of reference, we report in Table 1, a summary of the five privacy principles introduced here.

2.2 OAuth and OIDC

We present here an introduction to OAuth and OIDC that is not meant to be exhaustive. Rather, its aim is to illustrate the main concepts and elements of the protocol, with a focus on the features that will be discussed in the following. OAuth is an authorization framework with which an application, called Relying Party (RP), can be granted access to user resources by first asking for consent from the user. OIDC is an identity protocol that adds authentication to the OAuth framework. Authentication is possible by distributing user-identifying data called claims.

OIDC flows start with an authorization request sent by the RP to the OP. Authorization requests include various parameters, but most importantly the `scope` parameter, with which the user's resources are requested. The RP's accesses are limited to the resources listed in `scope`, and thus the parameter is pivotal to enable access control. The list of parameters supported by the authorization request depends on the OP. Distinct OPs may choose to refer to different OIDC specifications and add new parameters. However, all OPs implement a set of mandatory parameters, amongst which `scope`. The OP prompts the user to sign in after processing the authorization request. The user is then directed to an authorization, or consent, page. The authorization page informs the user of what `scope` has been requested and allows the user to consent to share their resources (it is the main way to ensure transparency). Once the user consent has been granted, the OP sends an authorization code back to obtain an Identity (ID) Token and Access Token. The ID Token is a security data structure consisting of a unique user identifier, user claims, and authentication context data. The Access Token can be used to access the user resources and obtain claims on the authenticated user.

3 Related Work

In the past, the security of OAuth and OIDC protocols has been widely studied, both theoretically and practically. The research has been mostly focused on concrete attacks to the protocols [38,40,41], and a number of solutions and mitigations have been proposed to tackle their vulnerabilities [37,46,59]. Despite that, little effort has been put into studying how OPs protect user privacy by integrating privacy-by-design principles within their implementations. In the following, we summarize some of the available works in the literature that deal with privacy issues of OIDC protocol.

Fett et al., proposed a privacy-preserving Single-Sign-On (SSO) system for the web called "SPRESSO" [39] that decouples the direct communication between RP and OP by using a forwarder agent at the user's side with the aim to avoid user linkability by the OP at various RPs. Asghar et al. in [33] introduced a privacy-preserving solution that is a modified version of the cryptographic construction presented in Oblivion [34]. Their solution decouples the interaction between the OP and RP by separating the credential issuance by the OP from its usage by the user at RP. Navas and Beltrán provide a comprehensive

threat model for the OIDC in [51] that highlights the following privacy threats: lack of control over required personal data, personal data leakage, user profiling, and location tracking. The authors also proposed mitigations that include encryption to minimize the risk of personal data leakage and using flow-specific user identifiers to avoid user profiling. In 2020, Apple introduced its SSO solution based on OIDC called "Sign In with Apple" [28] that uses randomized (per RP) identifiers in place of a user email address to avoid user linkability across RPs. Zhang et al. proposed a privacy-preserving system based on OIDC called "EL PASSO" [58] that implements anonymous credentials to enable selective disclosure and avoid user linkability. Hammann et al. [44] and Li et al. [45] proposed solutions to address the problem of user linkability by decoupling the interaction between the OP and RP in obtaining and using credentials. Most recently, Morkonda et al. described a browser extension called "SSOPrivateEye" [50] that provides a privacy comparison where users have multiple choices of OPs to login into an RP. Exploiting this information, users can choose the one that shares less amount of personal data with RPs. This solution provides some privacy insights only for Google, Facebook, and Apple as OPs.

Most of the aforementioned research works demand either major changes to the OIDC protocol or the installation of a browser plugin within the user's device to partially increase the user's privacy. Indeed, none of them provide some easy-to-implement privacy-preserving features by leveraging the features already available in OIDC [47,49,53]. Furthermore, no study has assessed the privacy of solutions that are provided by eIDAS solutions. Given that, our work can be used to complement and enhance plug-in-based solutions by providing more informative data, e.g. privacy principles satisfied by each OP that make the users more aware of the privacy level of the OP. In addition, our research work can be integrated into a stand-alone tool to automate the procedure of privacy compliance analysis. A good candidate for a stand-alone tool can be illustrated by extending our already developed tool for security analysis of OIDC deployments called "Micro-ID Gym" [35].

4 OIDC Privacy Best Current Practices

We have selected three OIDC specifications taken from the official list published by the OpenID Foundation [43]: OIDC core, OIDC for Identity Assurance and OIDC iGov profile [47,49,53]. Besides OIDC Core, which introduces the protocol, the other specifications seek to increase the baseline privacy and assurance of OIDC. With OIDC for Identity Assurance, OPs can issue trustworthy user claims by providing evidence of a verification process. The iGov profile introduces assurance requirements suitable for public, governmental identity services. The other available specifications have not been considered because they are outside the scope of this paper. Either they introduce features to support use cases that are not covered in OIDC Core, such as native applications or wireless network operators, or they do not include privacy considerations.

We have extracted a set of features whose deployment supports our recommended privacy BCPs. A first group (OIDC features) has been extracted from the selected OIDC specifications, whereas a second group (non-OIDC features) is not specified in OIDC standards, but is commonly implemented by OPs. Each feature contributes to one or more of the privacy principles introduced in Sect. 2.1, and can be easily implemented by OPs without making any change to the OIDC protocol. We have not considered non-OIDC features that cover aspects of privacy that are not already within the scope of OIDC, such as policies for data storage, data integrity, and handling breaches.

The analysis has been conducted by surveying the implementation of our BCPs in two groups of OPs: one developed by private companies, from here on called private OPs, and one of eIDAS OPs, developed for European public infrastructures. The analyses carried out on the two groups of OPs use the same set of features, yet they yield different results.

4.1 Privacy-Supporting Features

We propose a set of privacy-supporting features for OIDC deployments, whose adoption constitutes our suggested BCPs. They are depicted in Fig. 1, together with their connection to the privacy goals of Sect. 2.1, also summarized in Table 1, and the sources from which they were extracted. Table 2 provides a short description of the aforementioned features. Below, we discuss them according to the fact that they are parameters in the authorization request, supported subject identifiers, or non-OIDC features (recall the description in Sect. 2.2).

We first discuss the features in the authorization request.

`scope`: Through this parameter, the RP can request access to user-owned resources. Scopes are identifiers for sets of resources or permissions, and thus they are used for access control. The parameter supports data minimization, as all user resources are requested through it. Although it is used in AC policies, the parameter does not directly support confidentiality because it can only be used to specify resources. `scope` was introduced in OIDC Core [53], and is a mandatory parameter in authorization requests; it has to contain the value `openid`. As an example of usage, an RP can include `scope=openid profile email address` in the authorization request. Later on, the RP can obtain the data related to the user's profile, email and address by querying the UserInfo endpoint.

`claims`: Through this parameter, the RP can request specific claims to be returned in the ID Token or from the UserInfo endpoint after successful user authentication. If the parameter is missing, the OP will provide a default set of claims. `claims` can be used to request only the necessary resources, thus limiting the sharing of user data. The parameter is included in OIDC Core [53] and is defined as mandatory in the iGov profile [49] because of its importance for data minimization.

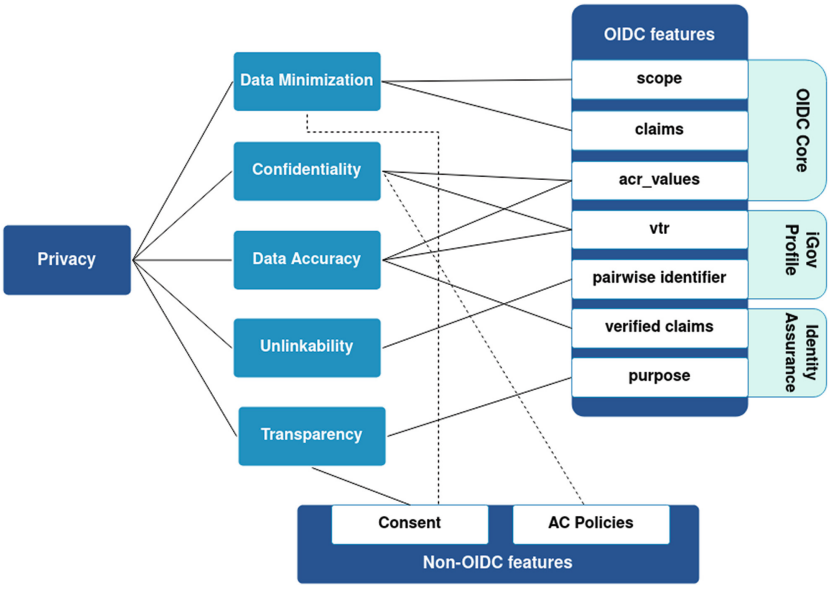

Fig. 1. Summary of our BCPs and their connection to privacy principles

`purpose`: This is a subfield of the `claims` parameter that was introduced in OIDC for Identity Assurance [47]. With it, the RP can specify a reason for requesting the claim. Purposes are displayed to the user on the consent page. If the OP does not implement `claims` it cannot implement `purpose`.
The responsibility of making the consent transparent usually falls on the OP alone. The OP would normally add to the consent page a list of the scopes and claims that have been requested, along with a short description for each. The implementation of the `purpose` parameter creates a new way for RPs to specify their purpose, thus directly contributing to transparency.

`verified_claims`: This is a new parameter introduced in OIDC for Identity Assurance [47] that allows requesting a set of verified user claims. On the OP side, user claims are associated with a verification method and a trust framework which they refer to. An example of such a framework is eIDAS, or a national eID scheme. The verification process usually happens upon registering the user's claims, e.g., via an electronic identity card. After successful authorization, user claims are returned alongside metadata containing evidence of the verification process. A higher level of assurance is guaranteed for the requested claims that are returned in the ID Token. By providing trusted information, the parameter contributes to data accuracy.

`acr_values`: This parameter allows the RP to request strong authentication methods. It defines a set of scalar values representing the minimum levels of identity proofing asserted during authentication. Depending on the value that the RP requests, the OP enforces different authentication methods. For instance, the first level is usually associated with a simple username and password login. Other levels may require Multi-Factor Authentication instead.

Table 1. Summary of the privacy principles

Principle	Description
Data Minimization	Use and collect only the minimum amount of data
Confidentiality	Grant access only to authorized parties
Data Accuracy	Information provided has to be correct
Unlinkability	User accounts cannot be traced across services
Transparency	Clearly state the purpose for collecting and processing user data

Table 2. Summary of privacy-supporting features

Feature	Description	Source
`scope`	Request user resources	Core [53]
`claims`	Request specific user claims	Core, iGov [49,53]
`purpose`	State the purpose of a claim request	Id. Assurance [47]
`verified_claims`	Request specific user claims along with evidence of the verification process	Id. Assurance [47]
`acr_values`	Request stronger authentication	Core, iGov [49,53]
`vtr`	Request stronger authentication, define the authentication context	iGov [49]
`pairwise`	User cannot be identified with the subject type	Core, iGov [49,53]
Consent	Transparent, informative consent page, implementation of selective disclosure	Common practices
AC Policies	Controlled disclosure of user data	Common practices

`acr_values` allows to increase the authentication requirements; therefore, it contributes to privacy by providing greater data accuracy and confidentiality.

`vtr`: Vectors of Trust (also VoT) is a parameter introduced in the iGov profile [49] that has the same purpose as `acr_values`. It allows requesting a minimum identity proofing level. `vtr` is a vector of scalar values, each of which defines a certain aspect of the authentication context. It is, therefore, more precise and flexible than `acr_values` [52]. It provides data accuracy and confidentiality.

We now describe the features related to subject identifiers. The `subject_type` defines how to generate the `sub` field, or subject identifier, a mandatory parameter of the ID Token that uniquely identifies the user. `subject_type` can have two values: `public` and `pairwise`, both defined in OIDC Core [53]. With `public` all the RPs under the same OP receive the same identifier for a fixed user. Instead, with `pairwise`, the same user will have a different identifier for each RP. The purpose of `pairwise` is to minimize the risk of linkability between RPs. The implementation of `pairwise` identifiers for unlinkability has been questioned in the past [44,45]. As amatter of fact, `pairwise` identifiers grant unlinkability only if `sub` is the only identifying information contained in the ID Token. If data such as email or name is returned by the OP, RPs can easily identify and trace the

user just by sharing the ID Token. There are available solutions in the wild that tackle this problem. However, except for the use of pseudonymization, the other solutions (e.g., Blind broker architecture [36] or Zero-Knowdlege Proofs [44]) demand either major changes to the OPs or to the OIDC protocol. Despite that, the iGov profile [49] stresses the importance of `pairwise` identifiers and makes their implementation mandatory. We stand by this privacy guideline because `pairwise` identifiers are a necessary step to grant unlinkability.

Finally, we explain the non-OIDC features that are commonly implemented by OPs.

Consent page: We check for the presence of a descriptive consent page, where the data collected is transparently communicated. Moreover, we check for the implementation of selective disclosure, a feature of consent pages that allows the user to select which resources, among those requested, to grant access to. Selective disclosure helps make the user aware of which personal data is being processed while contributing to transparency and data minimization.

Access Control (AC) Policies for sensitive scopes: This feature includes any kind of policy for accessing high-risk or sensitive resources (e.g., users' health records, biometric data). Through said policies, RPs may have their access restricted or limited in case they request sensitive resources through `scope` or `claims`. An example of said policies would be to initiate multi-factor authentication when sensitive resources are requested. Another option would be to restrict access to some scopes only to a subset of specifically authorized RPs. In general, we take into consideration any policy that enforces access control on requested resources.

Access control policies are ouside the scope of OIDC. We investigate them as they impact the security of user data and confidentiality. Despite being a security mechanism, the feature falls under our definition of confidentiality. We consider the AC policies that are enforced on requested scopes, and that concern the access and disclosure of user data.

OIDC for Identity Assurance and iGov profile [47,49] make up for the lack of privacy considerations in OIDC Core [53] by addressing data minimization, accuracy, confidentiality, transparency and unlinkability. Each specification contributes to different aspects of privacy, with some overlaps. Our BCPs connect the contributions of each specification, thus providing a complete and well-rounded set of recommendations. Moreover, the privacy principles, as well as the BCPs that enforce them, are interlinked. The risks deriving from the violation of any privacy principle impact negatively all the others. We argue that our BCPs should be implemented altogether to minimize the overall risk to privacy and grant the highest degree of assurance to users.

4.2 BCPs for Assurance, Consent and Access Control

In digital identity management, assurance is the ability to trust that an electronic credential belongs to the user. Higher assurance levels allow for regulated

scenarios like government, finance, and healthcare. Privacy goals vary by use case, and Fig. 1 helps determine the necessary features to achieve the desired privacy posture of OPs. We observe that tuning the level of assurance can be seen as a prerequisite for establishing a suitably strong trust relationship between an OP and RPs deployed in a certain use case scenario. In other words, Fig. 1 can be considered a high-level map to orient designers in the adoption of privacy features capable of yielding the right level of assurance and trustworthiness for the ecosystem (comprising OPs and RPs) supporting a certain use case scenario. Needless to say, we are assuming that other security measures, such as those extensively discussed in various OIDC specification documents, are put in place as an obvious and much-needed complement to the BCPs described in Fig. 1. As a final remark, we observe that—despite not being included in the OIDC standard—the Consent and Access Control features seem to be crucial in providing adequate support for assurance and trustworthiness as they support the controlled sharing of personal data among OPs and RPs, thereby helping to achieve three of the five privacy goals in Sect. 2.1 (namely Data Minimization, Confidentiality and Transparency) and comply with the GDPR.

5 BCPs in the Wild

We now want to understand how well OIDC deployments support privacy-preserving features. We do this by checking whether the privacy BCPs identified in Sect. 4.1 are implemented by a significant set of OPs. We decompose our evaluation w.r.t. private and eIDAS OPs and the identified privacy principles. We now explain how the OPs were selected and how we performed the analysis. Our findings are summarized in Fig. 2 and Table 3.

We have analyzed 14 private and 13 eIDAS OPs. The private OPs have been selected from the lists of OIDC-certified providers available at [42], and based on their popularity according to their Alexa rank. Only the OPs that have a developer console accessible without a subscription have been considered for this study.[1]

The 13 eIDAS OPs[2] that have been selected are European-notified and pre-notified solutions of EU Member States. They have been taken from the list of (pre-)notified eIDAS solutions available at the EU Commission official website [56]. Since the eIDAS regulation is not binding as for the choice of technologies, OPs implement mainly either SAML 2.0 or OIDC [27,53]. From the list, we have selected only those OPs that already implement OIDC or are in the process of implementing OIDC within their solutions.

Our analysis relies on the official documentation provided by OPs. Whenever possible, we have tested each feature of each OP either through publicly available

[1] Despite Alexa rank ending its service in May 2022, we have used the data available as of April 2022, which we considered reasonably updated.

[2] NHS Login is not currently an eIDAS solution due to international political developments, but was developed as such. We have included it since it complies with the specification.

demos, by deploying the OP server locally, or by creating test applications on their platforms and interfacing with their API. In total, we have tested all private OPs and 12 eIDAS OPs.

(a) Per each privacy BCPs (b) Per each privacy goal

Fig. 2. Implementation rate of the privacy-supporting features for private and eIDAS OPs

Table 3. Summary of the supported BCPs for private and eIDAS OPs

	scope	claims	purpose	verified_claims	acr_values	vtr	pairwise	consent	AC policies
Authlete [3]	●	●	●	●	●		●		
ForgeRock [9]	●	●			●		●		●
Connect2id [7]	●	●	●	●	●		●	●	●
Cloudentity [5]	●	●			●		●	●	●
WSO2 [31]	●	●			●			●	●
IBM [14]	●							●	●
Google [13]	●							●	●
Facebook [8]	●						●		●
Yahoo [32]	●								
Amazon [4]	●								●
Microsoft [17]	●						●		●
Ping [24]	●				●		●		●
OKTA [23]	●								●
Auth0 [2]	●				●				●

	scope	claims	purpose	verified_claims	acr_values	vtr	pairwise	consent	AC policies
itsme (BE) [16]	●	●			●		●		
MitID (DN) [18,20]	●	●			●		●		
NemID (DN) [18,20]	●	●			●		●		
FC (FR) [10]	●				●		●		
FC+ (FR) [10,11]	●	●			●		●		
P.S.C. (FR) [25]	●				●		●		
SMART-ID (ES) [29]	●				●				
SPID (IT) [30]	●	●			●		●		
CIE (IT) [30]	●	●			●		●		
ID Austria (AT) [1]	●						●		
ID-Porten(NO) [15]	●	●			●		●		
NHS (UK) [21]	●				●	●			
MojeID (CZ) [19]	●	●			●		●	●	

5.1 Private OPs

Regarding data minimization, `scope` has been implemented by all OPs since it is mandatory for OIDC. Instead, `claims` has been implemented only in 5 out of 14 (35%) cases. The fact that `claims` cannot be used for AC and that it can be replaced by returning a default set of user claims associated with the requested scopes can be the reason for its low implementation rate.

The analysis of confidentiality features yields diverging results. Despite having the same purpose, and the flexibility and precision granted by `vtr`, `acr_values` has been implemented in 7 (50%) OPs, whereas `vtr` in no OP. Moreover, the results for AC policies show that OPs implement a wide range of solutions.

In the wild, each OP adopts its own specific solution to manage RP accesses, which makes it difficult to categorize policies. Nevertheless, during our study, we have found a very significant trend in private OPs. 10 (71%) OPs allow the customization of AC policies, that are also enforced on scopes. There is a clear trend for OPs to deliver AC as part of their service and grant developers a high level of customizability. The purpose of customizing AC policies is to share claims and grant scopes only to a subset of RPs, or only under certain conditions, such as a higher authentication context. Some OPs give the possibility to create AC policies from scratch, while others allow to modify default policies. As part of their service, OPs may allow to change the list of claims that are returned for each scope. Or also to create new scopes and return claims based on the RP or the authentication context.

An example of AC policy customization would be to allow developers to flag scopes with security levels, and then define for each security level a set of authentication requirements. The OP would then match the highest authentication level among the requested scopes before granting access to the resources. Some OPs allow managing users with user groups. When that is the case, AC policies could define different authentication requirements and accessible resources for each user group.

The example above introduces step-up authentication [57]. That is the request for stronger authentication, also through Multi-Factor Authentication, upon accessing protected resources. We have found that all the OPs that implement AC customization allow step-up authentication, which highlights the importance of this feature. Just like in the example above, this feature is often integrated as part of AC customization. This means that developers define which resources start the step-up process. Although, it can also be the case that sensitivity levels cannot be changed by developers and a default set of scopes will always start the step-up flow. This would limit the degree of customization but ensure a baseline security level.

Another viable solution for OPs is to make developers submit their RP for review. In this case, a dedicated team checks the RP activity and purpose. Only once it is deemed conforming to the provider rules, the RP is allowed to access protected scopes and API resources. This solution is often adopted by OPs that allow to quickly create and set up RPs. Thus, developers can easily access basic

functionalities, while sensitive scopes are protected by granting access only to verified RPs. Nevertheless, this solution suffers from a lack of scalability and flexibility and is therefore adopted only in 2 (14%) cases.

For data accuracy, we have already considered the results of `acr_values` and `vtr`. We only add that also `verified_claims` saw little implementation: only in 2 (14%) OPs.

As for unlinkability, `pairwise` identifiers have been implemented in 7 (50%) OPs. In order to find a trend in the implementation of `subject_types`, we have also surveyed the implementation of `public` identifiers. Since `sub` is a mandatory field, the OPs that have not implemented `pairwise` have instead implemented `public` identifiers. Also, 5 (35%) OPs implement both `sub` types. That is usually the case for OPs that want to allow RPs greater flexibility. Interestingly, there are 2 (14%) OPs, Google and Microsoft, that allow only the use of `pairwise`. This should be considered a privacy-preserving design choice.

The features that support transparency have seen little implementation. `purpose` has been implemented only in 2 (14%) OPs, and consent page with selective disclosure capability in 5 (35%) OPs. Despite that, OPs show in the consent pages short descriptions of the requested `claims` and `scope`. In this case, OPs still meet an adequate level of transparency.

5.2 eIDAS OPs

Some of the trends seen in private OPs are confirmed in eIDAS OPs as well. The results differ the most for unlinkability, confidentiality and data accuracy. In general, eIDAS OPs show a tendency to grant higher assurance to both users and RPs and have better privacy-preserving designs.

For data minimization, `claims` has been implemented in 8 out of 13 (61%) cases, which marks a sharp increase in comparison with private OPs.

The results for the features that enforce confidentiality reflect the higher assurance requirements of eIDAS OPs. `acr_values` has been implemented in 12 (92%) cases, almost all OPs, which is a steep increase w.r.t. the implementation rate in private OPs. Despite that, the trend of preferring `acr_values` to `vtr` is confirmed, since the latter was implemented only 1 (7%) time. Unfortunately, we haven't been able to test the AC policies enforced by eIDAS OPs and we have no results in that regard. That is because eIDAS OPs' demos often do not allow for the creation of testing RPs but rather only offer a test flow.

The higher implementation rate of `acr_values` leverages the overall higher support for data accuracy. That being said, another trend of private OPs is confirmed since `verified_claims` was never implemented.

As for unlinkability, `pairwise` has been implemented in 11 (84%) cases, compared to 50% of private OPs. Interestingly, we can see a change in the implementation rate of `public` too. `public` has been implemented 6 (46%) times. Although the number of OPs that implement public only, without pairwise, decreased to 2 (14%), compared to 50% of private OPs. At the same time, the number of OPs implementing only `pairwise` has increased to 6 (46%). However, the number of OPs that implement both identifiers stays the same. The results

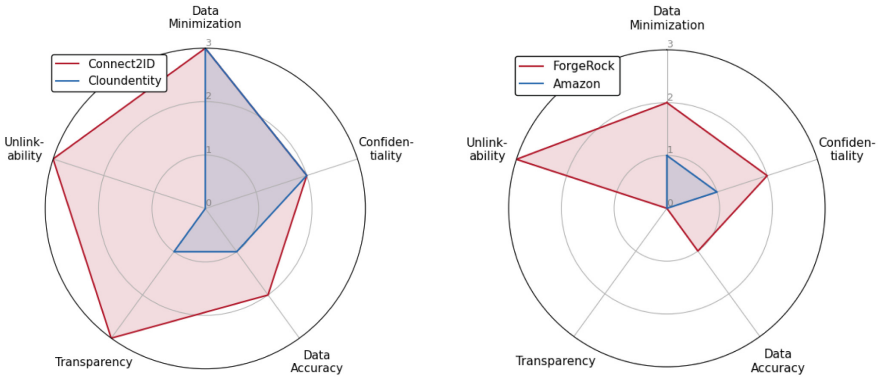

Fig. 3. Comparison of the assurance level of different private OPs

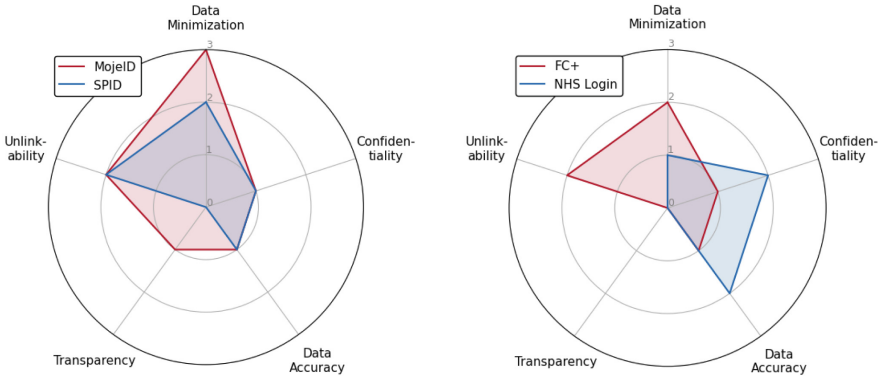

Fig. 4. Comparison of the assurance level of different eIDAS OPs

could derive from the emphasis given to `pairwise` identifiers in the OIDC iGov profile, their relevance for unlinkability, as well as the higher privacy assurance requirements that are fulfilled by eIDAS OPs.

Transparency has been mostly overlooked since `purpose` has never been implemented and consent page with selective disclosure has been in only 1 (7%) OP. Interestingly, while 4 (30%) OPs presented a normal, static consent screen with short `scope` descriptions, 6 (46%) OPs skipped the consent page. So the user, after logging in, would be redirected to the RP with the access code right away. This behaviour can be explained with the following: (*i*) the eIDAS regulation [26] defines the minimum set of user data that can be shared with RPs and that is needed for user accountability; (*ii*) since it is required to share at least the minimum set of data with the RPs to access their services, the user is not left with the choice of sharing the aforementioned data. The user would consent to sharing said set of data upon logging in. We would like to highlight

that this is possible only with eIDAS OPs, private OPs would otherwise violate the principles of transparency and purpose specification.

6 Discussion, Conclusions and Future Work

The results show that 6 out of 14 (42%) private OPs implement half or more of our BCPs, whereas the rate rises to 8 out of 13 (61%) for eIDAS OPs. The difference between the two groups is further highlighted if we consider only the OIDC features. In this case, 6 (42%) private OPs implement at least half of the features, whereas 11 (84%) eIDAS OPs do. We can also see that a subset of OIDC features, namely `purpose`, `verified_claims` and `vtr` were implemented by almost no OPs from both the private and eIDAS groups. Interestingly, a subset of OPs have implemented only the mandatory features that are required to be certified by the OpenID Foundation. The features in question are `scope` and `public` identifiers, without implementing `pairwise`. The results show that 5 (35%) private OPs fall under this category, whereas no eIDAS OP does.

Our study shows a very low adoption rate of the OIDC for Identity Assurance specification, which was implemented only in 2 private OPs, and in no eIDAS OPs. This result could be explained by the novelty of the specification, which was released only recently. Also the requirements of the iGov profile, which are the implementation of `claims, acr_values, vtr` and `pairwise`, were satisfied by no OPs. Although, the reader should mind that a larger group of OPs complies partially with the iGov profile. If we do not take into account `vtr`, which has the lowest support rate overall, 5 (35%) private OPs and 8 (61%) eIDAS OPs comply with the other requirements of the iGov profile. Interestingly, new specifications for public infrastructures have been derived from the iGov profile, such as the Netherlands Gov Assurance Profile [22].

The OPs from both groups have shown to have different priorities for the privacy goals. As shown in Fig. 2(b), data minimization and unlinkability are the most widely supported goals in both groups, with unlinkability having a higher priority in eIDAS OPs. Confidentiality is the third most supported privacy goal for all OPs. Instead, transparency and data accuracy are the least supported privacy goals in both groups.

Moreover, to make clear the importance that the two groups give to different privacy goals, for each goal we have analyzed the number of OPs that implement at least one feature that contributes to that goal. We have found that a minimal level of confidentiality is supported by 13 OPs (92%) in both groups. Without considering the `scope` parameter, which is mandatory, 7 private OPs (50%) and 9 eIDAS OPs (69%) support data minimization. Unlinkability is supported in 6 private OPs (42%) and 12 eIDAS OPs (92%). Data accuracy has a minimum level of support in 7 (50%) private OPs and 12 (92%) eIDAS OPs. Transparency is supported in 6 (42%) private OPs and only in 1 (7%) eIDAS OP.

The previous results for data minimization, unlinkability and transparency are confirmed, although we can see that many eIDAS OPs support at least one feature for confidentiality and data accuracy. We can see that the biggest

differences between the two groups are in their support for data accuracy, transparency and unlinkability. Specifically, eIDAS OPs prioritized the development of features for data accuracy and unlinkability with the aim to enhance the assurance level for users and RPs, whereas private OPs developed transparency-enhancing features more often. We would like to clarify that the lack of support for transparency derives from two main reasons: the low implementation rate of OIDC for Identity Assurance and the possibility for eIDAS OPs to skip the consent page (Sect. 5.2). That does not mean no compliance with the GDPR requirements for transparency and purpose specification.

The results presented up to this point show the differences between private and eIDAS OPs. We can safely state that eIDAS OPs provide on average a higher degree of assurance, for both users and RPs. That is understandable, as they are designed to handle sensitive information. To grade the general level of assurance that each OP grants, we have scored each OP for each privacy principle based on the number of features that it supports, according to Fig. 1. The results of some selected OPs are shown in Fig. 3 and 4. We have then included the entire survey in our Drive folder[3]. The results show homogeneity in the assurance level of eIDAS OPs, caused by their similar requirements, and a greater diversity for private OPs, which often do not refer to the same set of requirements. This is true also for the features' implementation, Table 3. We can see that eIDAS OPs adopt a similar set of features, whereas private OPs are more diverse. Moreover, we can differentiate between two groups of private OPs, one of which implements way more features than the other. Instead, we cannot make such a distinction for eIDAS OPs.

The BCPs that we have provided and the extracted features can serve as a reference for developers to deploy privacy-preserving OPs. Furthermore, they can be used in services that analyze the degree of assurance that various OPs grant. As a matter of fact, most of the analyses on OIDC features in this work can be automated. As future work, we are planning on extending the functionalities of a tool to perform security analysis of OIDC deployments called "Micro-Id-Gym" [35]. We will integrate the privacy BCPs into the tool to extend the metrics that are already present and to automatically perform compliance analysis on any OP to provide the level of privacy satisfied by the OP w.r.t. privacy goals. Another possible future route would be to improve existing browser plug-in-based solutions to provide more information, such as the privacy goals satisfied by the OP. Our aim is to assist users in making an informed decision when choosing among different OPs based on the level of assurance and privacy granted.

Acknowledgements. This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU, by "Futuro & Conoscenza S.r.l.", jointly created by the FBK and the Italian National Mint and Printing House (IPZS), Italy and by the project "METAfora: Metodologie e tecnologie di rappresentazione per il metaverso" (CUP code B69J23000190005), proposed by BIT4ID S.r.l.

[3] https://drive.google.com/drive/folders/1SVKA9ti2-0Rt6Lu_bIX2jaWxjsN5cVfP.

References

1. AUSTRIA ID OIDC documentation. https://eid.egiz.gv.at/wp-content/uploads/2021/10/ID-Austria-Technisches-Whitepaper-fuer-Service-Owner-1.pdf. Accessed 28 Nov 2022
2. Auth0 API documentation. https://auth0.com/docs/api/authentication. Accessed 28 Nov 2022
3. Authlete API documentation. https://docs.authlete.com/en/shared/2.2.19. Accessed 28 Nov 2022
4. AWS Cognito OIDC documentation. https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-userpools-server-contract-reference.html. Accessed 28 Nov 2022
5. Cloudentity API documentation. https://cloudentity.com/developers/api/authorization_apis/oauth2/. Accessed 28 Nov 2022
6. Cnil dossier thématique dédié à l'identité numérique. https://www.cnil.fr/sites/default/files/atoms/files/cnil_dossier-thematique_identite-numerique.pdf. Accessed 4 Mar 2023
7. Connect2Id API documentation. https://connect2id.com/products/server/docs/api. Accessed 28 Nov 2022
8. Facebook OIDC documentation. https://developers.facebook.com/docs/facebook-login/guides/advanced/manual-flow/. Accessed 28 Nov 2022
9. ForgeRock API documentation. https://backstage.forgerock.com/docs/am/7.1 . Accessed 28 Nov 2022
10. FranceConnect identity provider documentation. https://partenaires.franceconnect.gouv.fr/fcp/fournisseur-identite. Accessed 28 Nov 2022
11. FranceConnect+ OIDC documentation. https://github.com/france-connect/Documentation-FranceConnect-Plus/blob/main/fs/docs-fs.md. Accessed 28 Nov 2022
12. General data protection regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Accessed 25 Nov 2022
13. Google Identity API documentation. https://developers.google.com/identity/openid-connect/openid-connect. Accessed 25 Nov 2022
14. IBM Oidc documentation. https://www.ibm.com/docs/en/sva/9.0.7?topic=methods-openid-connect-oidc-authentication. Accessed 25 Nov 2022
15. ID-Porten OIDC documentation. https://docs.digdir.no/docs/idporten/oidc/oidc_guide_english. Accessed 25 Nov 2022
16. itsme API documentation. https://belgianmobileid.github.io/slate/login.html. Accessed 25 Nov 2022
17. Microsoft OIDC documentation. https://connect2id.com/products/server/docs/api. Accessed 25 Nov 2022
18. MitID and NemID service provider documentation. https://broker.signaturgruppen.dk/application/files/7415/8763/0084/Nets_MitID_Broker_Technical_reference_v._0.9.5.pdf. Accessed 25 Nov 2022
19. MojeID OIDC documentation. https://www.mojeid.cz/documentation/html/ImplementacePodporyMojeid/OpenidConnect/index.html. Accessed 25 Nov 2022
20. NemID identity provider documentation. https://broker.signaturgruppen.dk/application/files/6616/5166/7106/Nets_eID_Broker_Identity_Providers_v.1.2.6.pdf. Accessed 25 Nov 2022
21. NHS Login OIDC OIDC documentation. https://developer.nhs.uk/library/systems/eis/. Accessed 25 Nov 2022

22. NL Gov Assurance Profile OIDC documentation. https://logius.gitlab.io/oidc/#authorization-endpoint. Accessed 25 Nov 2022
23. OKTA Api documentation. https://developer.okta.com/docs/reference/api/oidc/. Accessed 28 Nov 2022
24. PING Federation SSO documentation. https://docs.pingidentity.com/bundle/pingone/page/gbj1632772285136.html. Accessed 28 Nov 2022
25. Pro Santé Connect OIDC documentation. https://industriels.esante.gouv.fr/produits-services/pro-sante-connect/documentation-technique. Accessed 28 Nov 2022
26. Regulation on electronic identification and trust services for electronic transactions. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN. Accessed 25 Nov 2022
27. Security assertion markup language (saml) v2.0 technical overview. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html. Accessed 4 Mar 2023
28. Sign in with apple. https://developer.apple.com/sign-in-with-apple/. Accessed 23 Dec 2022
29. SMART-ID OIDC documentation. https://e-gov.github.io/TARA-Doku/TechnicalSpecification. Accessed 28 Nov 2022
30. SPID Oidc documentation. https://docs.italia.it/AgID/documenti-in-consultazione/lg-openidconnect-spid-docs/it/bozza/index.html. Accessed 28 Nov 2022
31. WSO2 Identity Server documentation. https://is.docs.wso2.com/en/latest/guides/before-you-start/. Accessed 28 Nov 2022
32. Yahoo OIDC documentation. https://developer.yahoo.com/oauth2/guide/openid_connect/. Accessed 28 Nov 2022
33. Asghar, M.R., Backes, M., Simeonovski, M.: Prima: Privacy-preserving identity and access management at internet-scale. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2018)
34. Simeonovski, M., Bendun, F., Asghar, M.R., Backes, M., Marnau, N., Druschel, P.: Oblivion: mitigating privacy leaks by controlling the discoverability of online information. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) ACNS 2015. LNCS, vol. 9092, pp. 431–453. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-28166-7_21
35. Bisegna, A., Carbone, R., Pellizzari, G., Ranise, S.: Micro-id-gym: a flexible tool for pentesting identity management protocols in the wild and in the laboratory. In: Saracino, A., Mori, P. (eds.) Emerging Technologies for Authorization and Authentication, pp. 71–89. Springer International Publishing, Cham (2020)
36. Boysen, A.: Decentralized, self-sovereign, consortium: the future of digital identity in Canada. Front. Blockchain 11 (2021)
37. Calzavara, S., Focardi, R., Maffei, M., Schneidewind, C., Squarcina, M., Tempesta, M.: WPSE: Fortifying web protocols via Browser-Side security monitoring. In: 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, pp. 1493–1510. USENIX Association, August 2018. https://www.usenix.org/conference/usenixsecurity18/presentation/calzavara
38. Chari, S., Jutla, C., Roy, A.: Universally composable security analysis of oauth v2.0. Cryptology ePrint Archive, Paper 2011/526 (2011). https://eprint.iacr.org/2011/526
39. Fett, D., Küsters, R., Schmitz, G.: Spresso: a secure, privacy-respecting single sign-on system for the web. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1358–1369 (2015)

40. Fett, D., Küsters, R., Schmitz, G.: A comprehensive formal security analysis of oauth 2.0. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. CCS 2016, pp. 1204–1215, New York, NY, USA. Association for Computing Machinery (2016). https://doi.org/10.1145/2976749.2978385, https://doi.org/10.1145/2976749.2978385
41. Fett, D., Küsters, R., Schmitz, G.: The web sso standard openid connect: In-depth formal security analysis and security guidelines. In: 2017 IEEE 30th Computer Security Foundations Symposium (CSF), pp. 189–202. IEEE (2017)
42. Foundation, O.: Certified openid providers, https://openid.net/certification/. Accessed 23 Nov 2022
43. Foundation, O.: List of openid specifications (2023). https://openid.net/developers/specs/. Accessed 6 Mar 2023
44. Hammann, S., Sasse, R., Basin, D.: Privacy-preserving openid connect. In: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. ASIA CCS 2020, New York, NY, USA, pp. 277–289. Association for Computing Machinery (2020). https://doi.org/10.1145/3320269.3384724, https://doi.org/10.1145/3320269.3384724
45. Li, W., Mitchell, C.J.: User access privacy in oauth 2.0 and openid connect. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 664–6732. IEEE (2020)
46. Li, W., Mitchell, C.J., Chen, T.: Oauthguard: protecting user security and privacy with oauth 2.0 and openid connect. In: Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop. SSR 2019, New York, NY, USA, pp. 35–44, Association for Computing Machinery (2019). https://doi.org/10.1145/3338500.3360331, https://doi.org/10.1145/3338500.3360331
47. Lodderstedt, T., Fett, D., Haine, M., Pulido, A., Lehmann, K., Koiwai, K.: Openid connect for identity assurance 1.0. https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html. Accessed 23 Nov 2022
48. Lodderstedt, T., Bradley, J., Labunets, A., Fett, D.: OAuth 2.0 Security Best Current Practice. Internet-Draft draft-ietf-oauth-security-topics-21, Internet Engineering Task Force, September 2022. https://datatracker.ietf.org/doc/draft-ietf-oauth-security-topics/21/. work in Progress
49. Varley, M., Grassi, P.: International government assurance profile (igov) for openid connect 1.0. https://openid.bitbucket.io/iGov/openid-igov-profile-id1.html
50. Morkonda, S.G., Chiasson, S., van Oorschot, P.C.: Ssoprivateeye: timely disclosure of single sign-on privacy design differences. arXiv preprint arXiv:2209.04490 (2022)
51. Navas, J., Beltrán, M.: Understanding and mitigating openid connect threats. Comput. Secur. **84**, 1–16 (2019)
52. Richer, J., Johansson, L.: Vectors of trust. RFC 8485, RFC Editor, October 2018. https://www.rfc-editor.org/info/rfc8485
53. Sakimura, N., Bradley, J., Jones, M., De Medeiros, B., Mortimore, C.: Openid connect core 1.0. The OpenID Foundation, p. S3 (2014)
54. Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F.A., Ranise, S.: The eidas regulation: a survey of technological trends for European electronic identity schemes. Appl. Sci. **12**(24) (2022). https://doi.org/10.3390/app122412679
55. Sudhodanan, A., Carbone, R., Compagna, L., Dolgin, N., Armando, A., Morelli, U.: Large-scale analysis & detection of authentication cross-site request forgeries. In: 2017 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 350–365. IEEE (2017)

56. eID User Community: Overview of pre-notified and notified eid schemes under eidas (2019). https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS . Accessed 23 Nov 2022
57. Wilson, Y., Hingnikar, A.: Solving Identity Management in Modern Applications: Demystifying OAuth 2.0, OpenID connect, and SAML 2.0. Springer, Berkeley (2019). https://doi.org/10.1007/978-1-4842-5095-2
58. Zhang, Z., Król, M., Sonnino, A., Zhang, L., Rivière, E.: El passo: privacy-preserving, asynchronous single sign-on. arXiv preprint arXiv:2002.10289 (2020)
59. Zhou, Y., Evans, D.: SSOScan: automated testing of web applications for single Sign-On vulnerabilities. In: 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, pp. 495–510. USENIX Association, August 2014. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/zhou