COMPUTERS AND INFORMATICS
2757-8259 2023, Volume 3 Issue 1
Review Article

Identity management standards: A literature review

Athanasios Kiourtis*
Department of Digital Systems, University of Piraeus, Piraeus, Greece, kiourtis@unipi.gr
Thanassis Giannetsos
Digital Security and Trusted Computing, Ubitech Ltd, Athens, Greece, agiannetsos@ubitech.eu
Sofia-Anna Menesidou
Digital Security and Trusted Computing, Ubitech Ltd, Athens, Greece, smenesidou@ubitech.eu
Argyro Mavrogiorgou
Department of Digital Systems, University of Piraeus, Piraeus, Greece, margy@unipi.gr
Chrysostomos Symvoulidis
Department of Digital Systems, University of Piraeus, Piraeus, Greece, simvoul@unipi.gr
Alessio Graziani
Engineering Ingegneria Informatica, SpA - R&D laboratory, Rome, Italy, Alessio.Graziani@eng.it
Spyridon Kleftakis
Department of Digital Systems, University of Piraeus, Piraeus, Greece, spiroskleft@unipi.gr
Konstantinos Mavrogiorgos
Department of Digital Systems, University of Piraeus, Piraeus, Greece, komav@unipi.gr
Nikolaos Zafeiropoulos
Department of Digital Systems, University of Piraeus, Piraeus, Greece, nikolaszaf@unipi.gr
Christos-Alexandros Gkolias
Department of Digital Systems, University of Piraeus, Piraeus, Greece, cgkolias95@gmail.com
Dimosthenis Kyriazis
Department of Digital Systems, University of Piraeus, Piraeus, Greece, dimos@unipi.gr

Submitted: 23.02.2023
Accepted: 19.03.2023
Published: 30.06.2023

** Corresponding Author*

Abstract:

Electronic identification (eID) and Identity Management (IDM) in the context of information systems is considered of crucial importance for citizen data safety, since it can authorize the proper stakeholders to access sensitive data. The plethora of information systems' users and devices, the need for increased data confidentiality and integrity, as well as the requirement for proper data exchange considering short-range and long-range distance data exchange protocols and networks, increases the overall necessity for proper IDM mechanisms and techniques. Nevertheless, it needs to be identified that IDM mechanisms are not only security tools that improve technical skill sets, but the leaders towards opportunities that emerge. This manuscript provides an overview of state-of-the-art IDM standards and regulations towards interoperable eID, namely SAML, WS-Federation, OAuth, OpenID, FIDO, and Mobile Connect, including their latest versions. It considers different architectural components and scenarios, covering aspects of multiple domains, with the ability to be exploited across several networking and communication systems.

Keywords: *Electronic Identification, Identity Management, OAuth, SAML, WS-Federation*

Cite this paper as: Kiourtis, A., Giannetsos, T., Menesidou, S.A., Mavrogiorgou, A., Symvoulidis, C., Graziani, A., Kleftakis, S., Mavrogiorgos, K., Zafeiropoulos, N., Gkolias, C.A., & Kyriazis, D., Title of the article, *Computers and Informatics*, 2023, *3*(1), 35-46.

1. INTRODUCTION

Electronic identification (eID) within information systems can be considered as the cornerstone of citizens' safety. Improvements in eID processes and systems is considered as a crucial challenge worldwide, and especially for the states in Europe aiming to improve interactions and relationships among Citizens and Governments (G2C), Consumers and Businesses (B2C), and Employees and Businesses (B2E) [1]. Especially in healthcare, although the past years have been highly disruptive due to the COVID19 pandemic, the long-term trend in several countries has reflected significant annual increases in healthcare spending [2]. The impact that an eID could have in making such spending more efficient, more convenient, and more secure is growing exponentially. Various policies and regulations are being provided to make sure that signatures in electronic form and eIDs within the healthcare ecosystem provide a legal standing which is equal to signatures which are handwritten. Electronic IDentification, Authentication, and trust Services (eIDAS) and National Institute of Standards and Technology-Digital Signature Standard (NIST-DSS) for the European Union (EU) and United States of America (USA) respectively are examples of such regulations [3].

Proper Identity Management (IDM) is considered crucial for todays' organizations [4], since it can help to protect against user credentials which have been compromised, as well as it can also help against passwords which are easily cracked that are considered as network entry points for hackers. IDM in general can enhance data security, it can facilitate within the overall regulatory compliance, it can reduce human errors, it can provide more effective access to specific resources, it can increase data confidentiality, while it can also help towards managing access rights across browsers and devices. Especially in healthcare with a plethora of users, devices, and the need for increased data confidentiality and integrity, proper IDM mechanisms and techniques are considered of vital importance [5]. Since health-related information needs to be exchanged on top of data exchange protocols and accessed by specific users, implementing IDM in the facilities of healthcare can facilitate healthcare professionals and citizens/patients to have an identity of single view, while minimizing errors created by humans, decreasing costs, and improving data compliance and overall security. Consequently, healthcare organizations need authentication beyond the current state-of-the-art (e.g., simple login screen). Monitoring, auditing, and enforcing security policies is another advantage considering modern authentication. It needs to be identified that IDM is not only security tools that improve the technical sets of skills, but the way towards the healthcare opportunities that arise and emerge. This manuscript provides an overview of state-of-the-art IDM standards and regulations towards eIDs of high interoperability, considering different architectural components (e.g., data's domain and confidentiality requirements) and scenarios, along with the usage of short/long-range distance data exchange protocols [6].

The remaining document has the following structure. Section 2 provides an overview of IDM within the healthcare domain, with details about eIDAS. Section 3 discusses the most widely adopted IDM standards, while section 4 includes our concluding remarks, as well as our next steps.

2. IDENTITY MANAGEMENT IN HEALTHCARE

A Digital Identity contains the data and information that is utilized to represent someone in an Information and Communication Technology (ICT) system [7]. This can be a human, a device, a business organization, or a software application. eID gives the suitable authentication means for citizens/patients when requesting healthcare in a state of the EU, keeping safe their rights of access. IDM is the tool or set of tools that entities employ to perform claims management regarding their identities of digital nature. Working on IDM in the healthcare industry involves authenticating not just patients/citizens but also healthcare organizations and experts. Health data of personal type are considered as data of sensitive type, therefore defining and controlling rights is essential to achieving a situation that complies with the legal frameworks of the EU member states [8]. The most known IDM models [9] are (i) the Isolated Model where the provider of the service (SP) and the provider of the identity (IdP) are merge into a unique server, (ii) the Centralized Model that has to do with centralizing the storage of the identity while considering services' separation, and (iii) the Federated Model where the stakeholders involved in the IDM create an agreement on the involved stakeholders which are participating into the overall system, about how they must be referred to, and about the parameters related with the configuration of the participating stakeholders. In addition, there are a number of Identity Federations in the public as well as in the fields of government, research, and education. The STORK [11] and eIDAS [3] are the two hybrid Identity Federations that are most known in the literature, according to [10]. The foundation of identity federations is the development of trust relationships between organizations. By using a singular digital identity that is shared by the entire federation, any user inside it can access the services and the resources of different types of organization. It makes user administration by SPs and credential control by users easier [12].

The eIDAS Regulation [13] on eID and trust services for completing transactions electronically in the European Internal Market was developed as an evolution of both based on the research of the STORK programs. In order to ensure that people and businesses can use their national eIDs to access services of public type across all of Europe with the identical-level legal validity as customary methods being paper-based, the eIDAS Regulation was published in 2014. Transparency and accountability are ensured through eIDAS, which also encourages and makes it easier to use cross-border eID and trust services. The goal is to increase and spread awareness of the usage of eID among EU citizens in their interactions with institutions and the commercial sector. According to eIDAS, citizens are defined as all people and businesses who use their national eID to access online services from any EU member state with validated cost/time benefits, usability, and overall security [14]. By the use of Nodes and Connectors, eIDAS eID streamlines the output of the several separate national eID schemes. The corresponding national input is conditioned and mapped to an interoperable transport form using the eIDAS Node in Country-A, the eIDAS Security Assertion Markup Language (SAML) assertion. Similar assertions may be obtained by an SP via an eIDAS Connector in Country-B during an authentication request [15]. Citizens, European states, node or point of connection operators, attribute suppliers and IdPs that supply knowledge about eIDs and that validate the identities of the users, and SPs that offer services with access authentication via eID make up the majority of an average eID ecosystem [16]. To sum up, eID in eHealth takes into account patient and citizen safety as well as security against unauthorized exposure of medical information, although being acknowledged as a challenging endeavor [17][18].

3. IDENTITY MANAGEMENT IN HEALTHCARE

IDM and authentication standards generally fall into two categories: de facto) standards and de jure standards. A timeline of these standards which can support both wireless short-range and long-range distance data exchange, is depicted in Fig. 1.

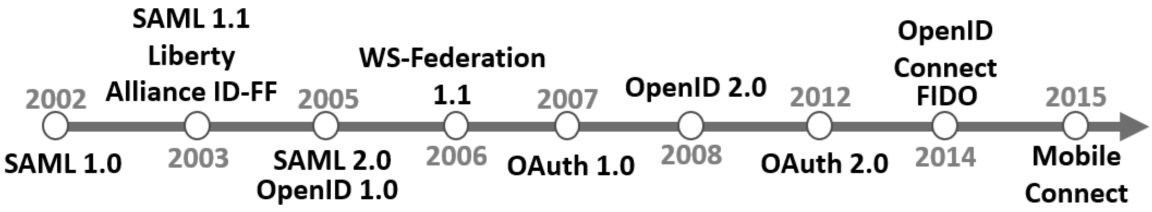


Figure 1. Identity and Authentication standards timeline

3.1. Security Assertion Mark-up Language (SAML)

SAML [19] is categorized as a standard of open nature with an XML basis, built to exchange data related with authentication and authorization among stakeholders, and specifically between an IdP and a SP. This security information is translated as portable SAML assertions that can be trusted by services and applications functioning across the security sector. The standard of OASIS SAML specifies the exact syntax and regulations in order to create, request, use, and communicate the aforementioned assertions. Assertions, Protocols, Bindings, and Profiles make up the bulk of the standard. SAML is among the most significant web-based federated identification standards, which is supported by SaaS companies that want to accept credentials from big business clients. The foundation of it is directing a user's browser to a website on the web that is maintained by their home organization, similar to other identity standards in the federated category. Since this site is considered trustworthy, the home organization provides new data and knowledge about the specific requestor to the original site. In accordance with this standard, IdPs transmit identity data to SPs using digitally signed XML documents.

Three roles are specified by SAML: the principal (a user, for example), the IdP, and the SP. The user asks the SP for a specific service in the first use case that SAML addresses. The SP asks the IdP for and receives an authentication assertion. The SP may decide to execute the service for the connected principal based on the premises of this assertion and make an access control decision. In SAML, an IdP can offer SAML assertions to several SPs. In a similar way, a SP may trust and rely on assertions from several different IdPs. A SAML assertion is an XML statement, provided by an IdP about a person (subject) for a recipient (relying party (RP)) usually a website (SP). SAML specifies the way that both assertions and protocol messages are structured, being utilized for transferring this knowledge: (i) SAML assertions include statements for a principal that it claimed to be true from an asserting party. The assertion skeleton is specified by the XML Schema of the SAML assertion, and (ii) messages of the SAML protocol are utilized to create SAML responses and their corresponding requests. The messages' content and skeleton are specified by the XML Schema of the SAML-defined protocol. Additional profiles of SAML are specified for a specific business use case. Profiles usually specify barriers on the SAML assertions' contents, bindings, and protocols to resolve the business-related scenarios with high degrees of interoperability. There also exist attribute profiles, that specify the way to exchange attribute information via assertions through aligning with multiple environments. Fig. 2 depicts the relationships among the basic SAML concepts.

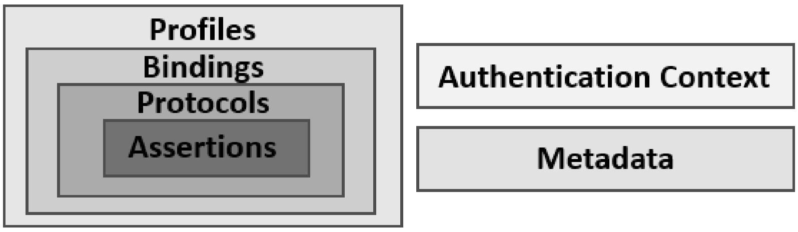


Figure 2. Basic SAML concepts

For a SAML environment, two extra SAML concepts—Metadata and Authentication Context—are crucial. While an Authentication Context is utilized in a statement of authentication of an assertion to convey details related with the overall authentication strength and type that someone provided during the authentication, Metadata specifies the means for disseminating details regarding configuration among SAML parties.

3.2. Web Services (WS)-Federation

WS-Federation is a specification of Identity Federation, specifying techniques that allow multiple realms of security to send knowledge and data on identity attributes, authentication, and identities [20]. WS-Trust, WS-SecurityPolicy, and WS-Security offer a state-of-the-art federation model between IdPs and RPs. The latter specify techniques for assertions' (claims) codification regarding someone who requests (requestor) in the form of tokens of security that can be utilized for protecting and authorizing requests from web services along with specific policies. WS-Federation enhances it through specifying the way that models of the claim transformation inherent in exchanges of security tokens are able to provide more trustworthy relationships of enhanced services' federation. This offers use cases of high value where accessing to resources being managed in a single realm can be offered to security experts whose attributes and identities are considered in external realms. It contains the ability for attribute retrieval, identity brokering, and discovery, claims related with authorization and authentication among federation stakeholders, and guarding these claims' privacy across the boundaries of organizations. A federation is considered as an overall list of realms (security domains) with specific sharing resources' relationships in a secure manner. A provider of the resource in a single realm can authorize access to the managed resource according to claims regarding a principal (e.g., identity attributes) which are being asserted by an IdP in a different realm. The federation's establishment value is to make easier the utilization of attributes related with security principal across boundaries of trust to install a context of federation for that specific principal. A RP is able to utilize this to give or deny a resource access of specific type. When that a federation needs to be established when IdPs and Resource Providers function in external realms, it needs agreement among them on the claims and demands agreement on techniques for transferring these claims via networks which are not protected.

3.3. OAuth 2.0

OAuth [21] is an authorization standard and a collection of established authorization processes that are regarded to be delegated, giving a user the power to authorize access to private resources that are combined and tied to their identity. A specification on issuing access tokens is found in OAuth 2.0 [21]. Without sharing passwords or private identification information, this is accomplished. Table 1 provides a description of OAuth 2.0 (Fig. 3).

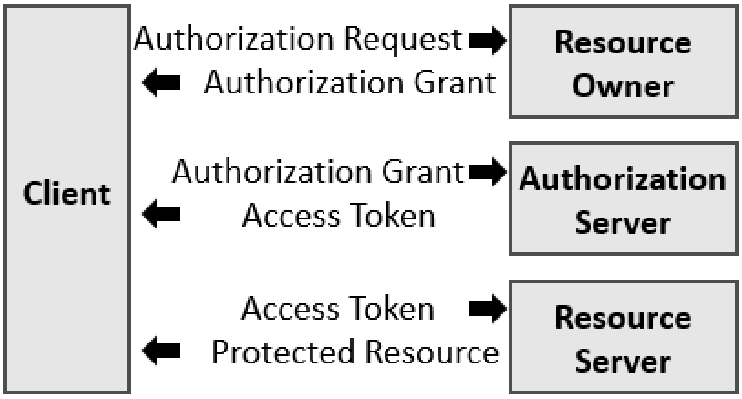
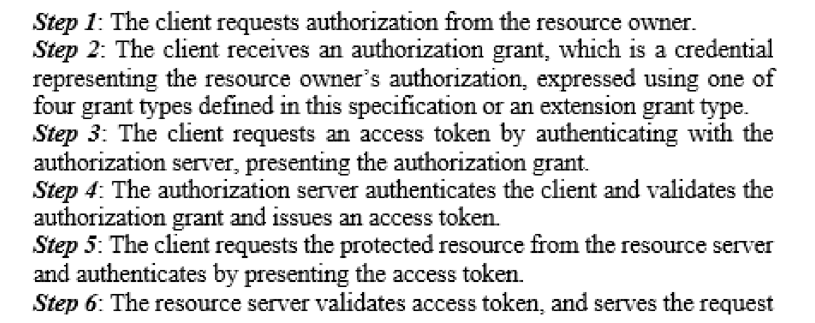


Figure 3. OAuth2 high-level flow

Table 1. OAuth 2 Pseudocode

OAuth 2.0 Algorithm



```
Step 1: The client requests authorization from the resource owner.
Step 2: The client receives an authorization grant, which is a credential representing the resource owner's authorization, expressed using one of four grant types defined in this specification or an extension grant type.
Step 3: The client requests an access token by authenticating with the authorization server, presenting the authorization grant.
Step 4: The authorization server authenticates the client and validates the authorization grant and issues an access token.
Step 5: The client requests the protected resource from the resource server and authenticates by presenting the access token.
Step 6: The resource server validates access token, and serves the request
```

An access token which is long-lasting is provided by the protocol, being able to be utilized by entities that demand continuous user resources' access. Many social networks and software programs continue to actively use OAuth and its newer version OAuth 2.0. In order to make someone allow access to resources, it uses REST Application Programming Interfaces (APIs) and JavaScript Object Notation (JSON) as the data format. By using grant types of a custom type and token types, OAuth 2.0 can be improved. Below is a list of the profiles created using the fundamental framework:

(i) SAML 2.0 Bearer Assertion Profile, which allows for the exchange of SAML assertions when using tokens of access,
(ii) User Managed Access Profile, which provides the owners of the resource to establish a variety of access policies for resources that are being safeguarded in one place;
(iii) Chain Grant Type Profile, which provides a service to utilize the token of access that has been gathered; Token Revocation Profile to cancel an access token,

Token Introspection Profile to enable clients to ask for metadata about the access token, and Dynamic Client Registration Profile to enable client registration with an authorization server and gather client identity.

3.4. OpenID and OpenID Connect (OIDC)

The nonprofit OpenID Foundation actively promotes the authentication standard known as OpenID [22]. It allows users to open an account using an IdP that complies with the standard (i.e., OpenID Provider). A user must use an OpenID IdP to create an account with OpenID (e.g., Google). To avoid managing several sets of credentials, the user will utilize that account to log in to any webpage that supports and trusts OpenID authentication. OpenID authentication requires server A to perform authentication for user U, yet U's details are sent to server B, which is trusted by server A. After confirming that U is who is expected to be there, Server B informs Client A that "this is the expected U". By eliminating the need to remember several websites' login information, OpenID allows users to entrust their OpenID IdP with sensitive information. OpenID, however, lost favor because users were forced to rely on an impersonal system for identification [23]. Table 2 and Fig. 4 show the OIDC flow.

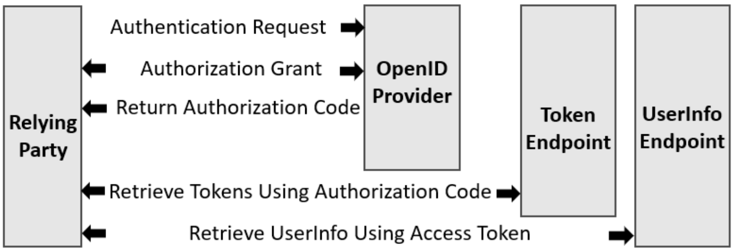
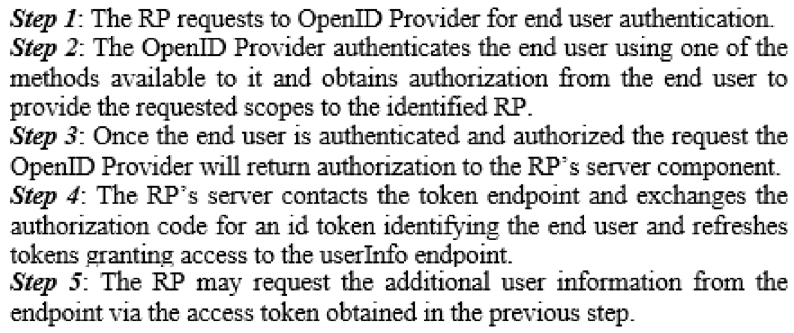

Relying Party
Authentication Request
Authorization Grant
Return Authorization Code
OpenID Provider
Token Endpoint
UserInfo Endpoint
Retrieve Tokens Using Authorization Code
Retrieve UserInfo Using Access Token

Figure 4. OpenID high-level authorization flow

Table 2. OpenID Pseudocode

OpenID Algorithm



```
Step 1: The RP requests to OpenID Provider for end user authentication.
Step 2: The OpenID Provider authenticates the end user using one of the methods available to it and obtains authorization from the end user to provide the requested scopes to the identified RP.
Step 3: Once the end user is authenticated and authorized the request the OpenID Provider will return authorization to the RP's server component.
Step 4: The RP's server contacts the token endpoint and exchanges the authorization code for an id token identifying the end user and refreshes tokens granting access to the userInfo endpoint.
Step 5: The RP may request the additional user information from the endpoint via the access token obtained in the previous step.
```

The most recent version of OpenID is OIDC [22], which merges the characteristics of OAuth 2.0, OpenID Attribute Exchange 1.0, and OpenID 2.0 into one standard. It offers the ability to an application to utilize authority to make sure about the identity of the final user, to retrieve the profile information of the final user, and gather limited access to the information of the end user. OIDC implements a pillar of authentication considering OAuth 2.0 protocol and uses REST/JSON for its messages. It is an OAuth 2.0 "profile" tailored for authentication and release of attributes. It provides to all the different types of users, to approve the user's identity according to the authentication which has been provided by a server built for authorization, also being able to demand and gather knowledge regarding authenticated sessions. The scope variables defined in OAuth 2.0 are used by OIDC Clients to establish the access characteristics that are required in the form of Access Tokens. The scopes that are provided to Access Tokens specify the resources that will be made available when they are utilized for accessing OAuth 2.0 endpoints (which are protected). OIDC and SAML are very similar. An id token, a JSON Web Token in signed form with very identical information, is the equivalent of the SAML assertion. Three roles are listed in the OIDC specification: I the final user or entity needing identity verification; (ii) the RP, or entity seeking to confirm the final user's identity; and (iii) the OIDC provider, being in charge of registering the OpenID URL and is able to confirm and approve the identity of the final user.

3.5. Fast Identity Online (FIDO) Universal Authentication Framework (UAF)

The FIDO UAF [24] framework for authentication, offers websites and online services, the ability to manage security characteristics which are of native type of computing devices of final users for performing authentication of strong type, in a transparent way, reducing the problems associated with remembering and creating multiple credentials. FIDO UAF supports a password-less behavior. In detail, the entity possesses a device with an installed FIDO UAF stack. The entities are able to sing up their device to the available service, which is online, through choosing an authentication way of local type (e.g., fingerprint, face detection, PIN password). The FIDO UAF protocol provides the means to the service to select the techniques being visualized to the user. By the time that the user is registered, he/she has to repeat the action for local authentication whenever there is a need to authenticate to that specific service. The FIDO UAF Architecture is constructed in that way to obey the targets of FIDO and yield the benefits of the ecosystem which is preferred. Fig. 5 depicts this architectural flow.

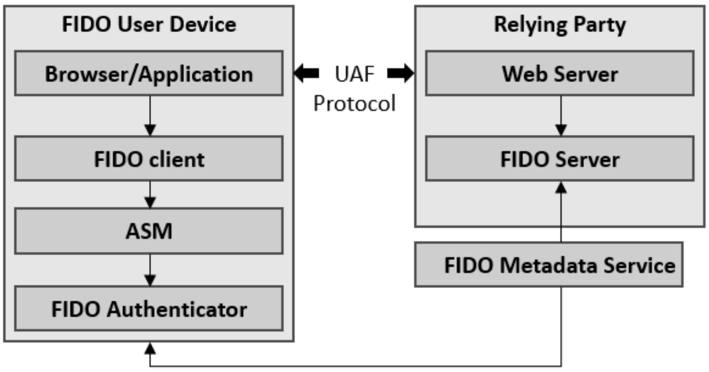


Figure 5. FIDO UAF high-level architecture

In order to connect with the Server of the FIDO UAF, a client of FIDO UAF must I interact with certain FIDO UAF authenticators via the Abstraction layer of the FIDO UAF Authenticator through the FIDO UAF Authenticator's API, and (ii) interact with a device's agent by using specific interfaces. A FIDO UAF Server constructs and builds the FIDO UAF protocol server side and has the responsibility to (i) interact with the RP web server to exchange the protocol messages of the FIDO UAF to a FIDO UAF Client through an agent of the device, (ii) validate attestations of FIDO UAF authentication on top of the metadata that configure the authenticator to make sure that only authenticators of trusted type are signed up for use, (iii) manipulate the FIDO UAF Authenticators that are registered to users' accounts at the RP, and (iv) evaluate the responses related with the transaction and authentication of users, to check their validity. A FIDO UAF Authenticator can be considered as an entity of secure type, assigned to FIDO user devices, able to generate keys related with a RP. This has the ability to be utilized for the FIDO UAF authentication.

3.6. FIDO Universal 2nd Factor (U2F) Authentication

U2F [25] is a standard for authentication that enhances and makes simpler the 2-factor authentication (2FA) via specialized devices, following an equal security technology that can be discovered in smart cards. The FIDO U2F protocol [25] gives the ability to RPs to provide a cryptographic 2nd factor option of strong type for the security of the end user. Consequently, the dependence of the RPs on specific credentials is minimized. Final users possess a U2F device that functions with any RP that is being supported by the protocol. Hence, the user can utilize a single device of "keychain" type, being offered security of more convenient type. FIDO U2F gives the ability to online services to increase the overall password systems' security by offering additionally a big 2nd factor to user sign-in, while the user can log in with his/her credentials as in the previous cases. This can also give the ability to the user to provide a 2nd factor device whenever the user wants to. During authentication, the final user must present the 2nd factor by just pushing a USB attached button or utilizing an NFC or Bluetooth device. The end users can utilize their FIDO U2F device in all services of online type that are able to offer web browser support of the protocol. The user can also utilize the same device among different sites, and as a result it can serve as the keychain of the user with a plethora of virtual-type keys to multiple websites provisioned from a single device. Utilizing the open U2F standard, any origin can use any browser supporting U2F to communicate with any U2F compliant device for authentication. Fig. 6 depicts this U2F flow.

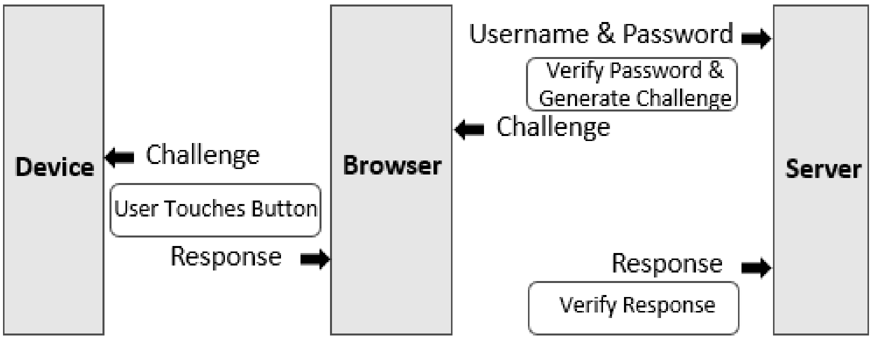


Figure 6. U2F high-level flow

The User hits Register during the U2F Registration procedure, and the RP sends the request with the appid + challenge. After receiving the request, the Device creates a pair of Kpriv/Kpub and a key handle for each RP for each user upon successful checking of the existence of the user, (ii) the Client confirms the appid before providing the request, (iii) the check of the user's presence is performed by selecting the U2F keys when they begin to blink, (v) The device's key handle and the response's digital signature are produced by the attestation private key, (vi) the RP stores the Kpub and the key handle for the user and, upon receiving the answer, verifies its signature using the attestation public key, which is located on the FIDO Metadata server.

The user enters the first factor after clicking Login during the U2F authentication process. The second factor enters the picture at that point. (ii) The RP provides the Challenge/Key handle for the user attempting to sign into the client. (iii) The application of the client verifies the id of the application and provides it to the device. (iv) In order to prevent a replay attack after a successful user presence check, the device determines the Kpriv by examining the key and performs a counter increase. (v) The device gives back the reply signed by KPriv, and (vi) The RP checks the counter, origin, and challenge as well as the response signature through KPub as the 2nd factor.

3.7. FIDO Web Authentication API (WebAuthN)

WebAuthN [26] specifies an API designed and implemented for systems and platforms enabling FIDO Authentication support. It is a technique allowing users to log in into systems without requiring any password or username credentials. The main goal is to enhance the experience of the user and create a user authentication mechanism being robust. The WebAuthN standard also outlines a number of elements that can be expanded, such as the inclusion of novel attestation forms and protocol extensions that define their processing guidelines. For the purpose of confirming user identities, FIDO uses the pre-existing specifications U2F, FIDO, and UAF. To log in, the user must provide password information and as a 2nd mechanism of authentication the user must provide his/her biometrics or other similar mechanisms. The FIDO WebAuthN flow is described in Fig. 7 and Table 3.

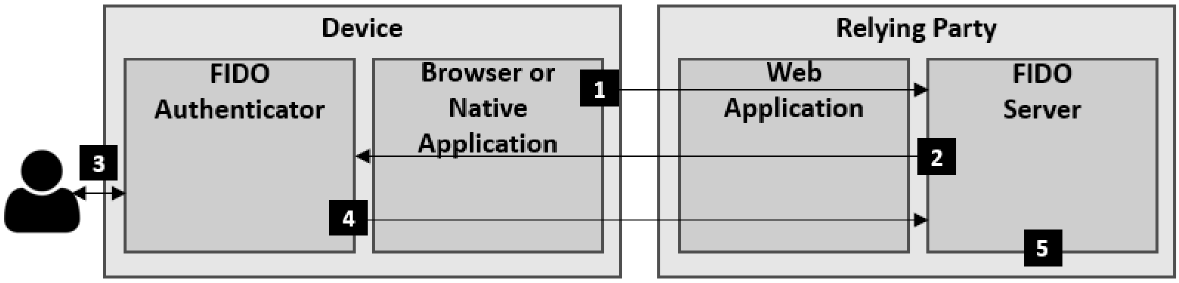
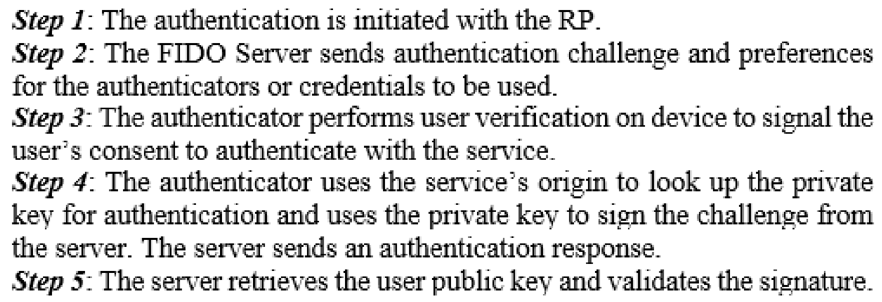


Figure 7. FIDO high-level authentication flow

Table 3. FIDO Pseudocode

FIDO Algorithm
 *Step 1*: The authentication is initiated with the RP. *Step 2*: The FIDO Server sends authentication challenge and preferences for the authenticators or credentials to be used. *Step 3*: The authenticator performs user verification on device to signal the user's consent to authenticate with the service. *Step 4*: The authenticator uses the service's origin to look up the private key for authentication and uses the private key to sign the challenge from the server. The server sends an authentication response. *Step 5*: The server retrieves the user public key and validates the signature.

3.8. Mobile Connect

Mobile Connect [27] is a secure universal identity solution being mobile operator-facilitated. Mobile Connect can be considered as a list of services being mobile-enabled that have the ability to be integrated into a SP's application for supporting services' access to the ones that are offered by the SP. It offers trustworthy user identity and network context information permissioned access, authentication, and authorization for consumers. Every deployment is surrounded by a wide range of technical standards to guarantee that from the perspective of an SP, the Mobile Connect services consumption from each of the Mobile Operators is of a stable type. It makes use of an architecture being distributed so that each Mobile Operator can provide Mobile Connect services to its base. It enables users to securely authenticate using their mobile device with security provided by the SIM card using their Mobile Station Integrated Services Digital Network (MSISDN) for user identification. Mobile Connect has specified two OIDC profiles to handle requests initiated by devices or servers for authentication, permissioned access, or authorization to particular user attributes. For consumers to receive requests on their mobile devices and receive responses, the providing Mobile Operator supports a reliable authenticator. The user's permission to have certain properties validated by the Operator or shared with the SP may be obtained via the Authenticator.

4. CONCLUSIONS

IDM is the security discipline that deals with providing the right entities to use the correct resources when they must, without any interferences, utilizing the wanted devices. It consists of several systems, processes and standards that provide the ability to ICT administrators to assign a single digital identity to each entity, authenticate them, authorize them for specified resources, as well as monitor these entities across their lifecycle. Since organizations should provide secure access for their remote and mobile users, IDM must be among the top priorities. With digital transformation, identities are also provided to Internet of Everything (IoE) devices, Cyber-physical systems, and hybrid ICT [28], thus the IDM becomes more complex. A list of the most adopted IDM standards was provided, covering devices, platforms, and systems built to wirelessly exchange and access data. Next steps include the continuous analysis of IDM standards, to conclude to the most appropriate IDM solutions based on domain-agnostic regulations and policies [29].

Acknowledgment

The research leading to the results presented in this paper has received funding from the European Union's funded Project PolicyCLOUD under grant agreement no 870675, and the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation under the call RESEARCH-CREATE-INNOVATE (project code: BeHEALTHIER-T2EDK-04207).

REFERENCES

[1] Lips, S, Tsap, V, Bharosa, N, Krimmer, R, Tammet, T, Draheim, D. Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership: Learning from the Case of Estonia. Information Systems Frontiers 2023; 1-18.

[2] Maltezou, H C, Giannouchos, T V, Pavli, A, Tsonou, P, Dedoukou, X, Tseroni, M, Souliotis, K. Costs associated with COVID-19 in healthcare personnel in Greece: a cost-of-illness analysis. Journal of Hospital Infection 2021; 114: 126-133.

[3] Sharma, A K. A Study on Digital-Signatures with Hash-Functions. Journal of Comp. Sciences & Eng 2019; 7: 604-607.

[4] Liu, Y, He, D, Obaidat, M S, Kumar, N, Khan, M K, Choo, K K R. Blockchain-based identity management systems: A review. Journal of network and computer applications 2020; 166: 102731.

[5] Bouras, M A, Lu, Q, Zhang, F, Wan, Y, Zhang, T, Ning, H. Distributed ledger technology for eHealth identity privacy: state of the art and future perspective. Sensors 2020; 20(2): 483.

[6] Kiourtis, A, Mavrogiorgou, A, Kyriazis, D, Graziani, A, Torelli, F. Improving Health Information Exchange through Wireless Communication Protocols. In: 2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 32-39.

[7] Rannenberg, K. A framework for identity management (ISO/IEC 24760).

[8] Kovac, M. E-health demystified: An e-government showcase. Computer 2014; 47(10): 34-42.

[9] Carretero, J, Izquierdo-Moreno, G, Vasile-Cabezas, M, Garcia-Blas, J. Federated identity architecture of the European eID system. IEEE Access 2018; 6: 75302-75326.

[10] Torroglosa-García, E, Skarmeta-Gomez, A F. Towards Interoperabilty in Identity Federation Systems. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl. 2017; 8(2): 19-43.

[11] Ribeiro, C, Leitold, H, Esposito, S, Mitzam, D. STORK: a real, heterogeneous, large-scale eID management system. International Journal of Information Security 2018; 17: 569-585.

[12] Edris, E K K, Aiash, M, Loo, J K K. The case for federated identity management in 5G communications. In: 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), pp. 120-127.

[13] Trust Services and eID (eIDAS regulation), https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[14] Kennedy, E, Millard, C. Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. Computer Law & Security Review 2016; 32(1): 91-110.

[15] Masi, M, Bittins, S, Cunha, J, Atzeni, A. e-SENS 5.2 eHealth eIDAS eID Pilot: Technical Feasibility Report, 2017.

[16] Pöhn, D, Grabatin, M, Hommel, W. eID and self-sovereign identity usage: an overview. Electronics 2021; 10(22): 2811.

[17] Katehakis, D G, Gonçalves, J, Masi, M, Bittins, S. Interoperability Infrastructure Services to Enable Operational Secure Cross-Border eHealth Services in Europe 2021.

[18] eIDAS-Node National IdP & SP Integration Guide, Version 2.1, 2018.

[19] Sobh, T S. Identity management using SAML for mobile clients and Internet of Things. Journal of High Speed Networks 2019; 25(1): 101-126.

[20] Aldosary, M, Alqahtani, N. A Survey on Federated Identity Management Systems Limitation and Solutions. International Journal of Network Security & Its Applications (IJNSA) 2021; 13.

[21] 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.

[22] Navas, J, Beltrán, M. Understanding and mitigating OpenID Connect threats. Computers & Security 2019; 84: 1-16.

[23] OpenID: The Web's Most Successful Failure, http://www. webmonkey. com/2011/01/openid-the-webs-most-successful-failure.

[24] Hu, K, Zhang, Z. Security analysis of an attractive online authentication standard: FIDO UAF protocol. China Communications 2016; 13(12): 189-198.

[25] Srinivas, S, Balfanz, D, Tiffany, E, Czeskis, A, Alliance, F. Universal 2nd factor (U2F) overview. FIDO Alliance Proposed Standard 2015; 15.

[26] Frymann, N, Gardham, D, Kiefer, F, Lundberg, E, Manulis, M, Nilsson, D. Asynchronous Remote Key Generation: An Analysis of Yubico's Proposal for W3C WebAuthn. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 939-954.

[27] Mobile connects, https://mobileconnect.io/

[28] Mavrogiorgou, A, Kiourtis, A, Kyriazis, D. A Generic Approach for Capturing Reliability in Medical Cyber-Physical Systems. In Artificial Intelligence Applications and Innovations: AIAI 2018 IFIP WG 12.5 International Workshops, SEDSEAL, 5G-PINE, MHDW, and HEALTHIOT, pp. 250-262.

[29] Kyriazis, D, Biran, O, Bouras, T, Brisch, K, Duzha, A, del Hoyo, R., Tsanakas, P. Policycloud: analytics as a service facilitating efficient data-driven public policy management. In Artificial Intelligence Applications and Innovations: 16th IFIP WG 12.5 International Conference, AIAI 2020, pp. 141-150.