


Article

A Hybrid Scheme for an Interoperable Identity Federation System Based on Attribute Aggregation Method

Samia EL Haddouti *  and Mohamed Dafir Ech-Cherif EL Kettani

CEDOC ST2I ENSIAS, Mohammed V University of Rabat, 10090 Rabat, Morocco

* Correspondence: samia_elhaddouti@um5.ac.ma

Received: 3 June 2019; Accepted: 24 June 2019; Published: 26 June 2019



Abstract: Several countries have invested in building their identity management systems to equip citizens with infrastructures and tools to benefit from e-services. However, current systems still lack the interoperability requirement, which is the core issue that could lower the wide benefits of having an identity management system. In fact, in the existing systems, the user is allowed to choose only one partial identity from an identity provider (IdP) during a single session with a service provider (SP). However, in some scenarios, an SP needs to retrieve information about user's identities managed by multiple IdPs. The potential method to tackle these shortcomings is attribute aggregation from multiple identity providers. A number of initiatives and projects on attribute aggregation have been explored. Nevertheless, these constructions do not fulfill some identity management requirements. This paper describes a new flexible model that aims to provide the necessary mechanisms to ensure attribute aggregation in order to meet the interoperability challenges of current identity management systems. The proposed scheme is a scalable solution, based on identity federation technologies, that introduces a new IdP called an account linking provider (ALP). The purpose of this ALP is to link together different accounts, holding end users' attributes, whenever more than one source of data is needed to grant access to the requested web resource in a single session. Furthermore, the proposed identity federation system is based on a streamlined, cost-effective, and interoperable architecture, which makes this model suitable for large-scale identity federation environments.

Keywords: attribute aggregation; access control; identity federation; interoperability; privacy; trust relationship

1. Introduction

With the evolution of information and communication technologies (ICT), consumers wait for instant access to information, and need to be connected everywhere and all the time, which inexorably leads to a considerable increase in the risks of cybercrime. In addition, as companies become distributed, access management and the ability to use a trusted online identity to share resources create particular challenges, as the data are available to all stakeholders. As a result, and in order to strengthen digital exchanges, the development of authentication and trust mechanisms has become the current major concern of the digital economy. To overcome these challenges and to address the needs of resource sharing between users of different organizations with a certain level of security and trust, the importance of identity and access management (IAM) becomes even greater and has a large impact on social, business, and government aspects. Thus, several standards, prototypes, and systems have been developed in different sectors to manage the roles and the privileges of the right users in the right context. Identity management systems combine processes, technologies, and strategies to manage digital identities, and specify how they are used by users to access multiple resources through a single

sign-on mechanism with better control of the personal data dissemination [1]. In current identity management systems in general and identity federation in particular, the end users select an identity provider (IdP) that supposedly provides all user's attributes to a service provider (SP) to gain access to protected services. By taking a look at the review of the literature, the existing identity federation approaches assume that the end user can only select one IdP in a given session with a (SP), to provide all the required attributes in order to access the requested resource. While these principles seem to be sufficient for users in a specific context, there are considerable scenarios in which an IdP is not able to disseminate all required data and information to SPs; hence, users need to retrieve their information and attributes from different IdPs by authenticating only once. Therefore, current systems still have limitations and the interoperability requirement continues to be a true challenge. Thus, the need for a cross-border interoperability of identity federation systems is acknowledged and addressed by various research projects. To deal with these issues, the multi-source attribute providers and attribute aggregation [2] may be considered as suitable solutions to overcome challenges related to the interoperability requirement for identity federation systems by gathering required information from multiple sources. Our studies and analysis show that the initiatives that were taken in this direction do not provide adequate models to deal with the main requirements of an identity federation system based on the attribute aggregation method. For this reason, we propose an alternative and a consolidated model that is particularly suitable for the attribute aggregation, while taking into account the satisfaction of as many of identity federation requirements as possible, by giving users the ability to aggregate their attributes and data information in a secure, reliable, and privacy-protected manner. The rest of this paper is structured as follows. After this introduction, Section 2 presents digital identity and identity management concepts. In Section 3, we will give an overview on the identity federation architectures and related standards. Section 4 will be devoted to the study and analysis of the existing models related to attribute aggregation in identity federation. Section 5 introduces and describes our proposed scheme, consisting of an interoperable and flexible model to deal with interoperability challenges. In Section 6, we will detail the operating principle of our model. Next, the implementation of the proposed scheme is described in Section 7. Section 8 analyses how the concept of our approach meets the stated requirements, and discusses the advantages and limitations of our model. Finally, Section 9 serves as a conclusion and discusses future work.

2. Digital Identity and Identity Management

With the evolution of technologies associated with the increase of web services and online transactions, user expectations have become more complex regarding service quality, access speed, and mobility facilities. Moreover, to secure and control the access to each service, SPs have to restrict the access to authenticated and authorized users, by assigning digital identities with a handling of their lifecycle.

2.1. Digital Identity

A digital identity is at the core of the authenticity of social interactions and the integrity of business processes. Kim Cameron defines identity as “digital identity refers to the aspect of digital technology that is concerned with the mediation of people's experience of their own identity and the identity of other people and things” [3]. A digital identity can be also defined as a set of information and characteristics, called identifiers or attributes, identifying an entity in a specific transaction context. That entity may be a person, organization, application, or device. In the context of a digital service, a digital identity of an entity is always unique, which makes individuals different from one another. However, an entity may have several identities in one or different domains of application. Through a set of attributes such as date of birth, gender, phone number, account number, and so on, a particular person can be safely distinguished within an identity context [4].

2.2. Mobile Digital Identity

Owing to the rise of mobile networks and mobile devices, the use of mobile identity has become increasingly more common, and is a vital element for modern Information Technology (IT) services within the broader digital mobile ecosystem. Mobile identity is an extension of the digital identity concept. It may be divided into three modes [5,6]:

- Device-to-device identity: a mobile identity is used to attest the authority of a particular user in order to grant access to services and resources while using different devices;
- Location-to-location identity: this means that a mobile identity is used to certify the individual authority while moving between different locations;
- Context-to-context identity: in this case, the access to resources is granted to individuals according to different societal roles and depending on the context and the application domain.

2.3. Interaction between Identity Elements

The digital identity is a key component of the digital world and the base of all businesses on the Internet [7]. In fact, providing identity has become a routine part of modern daily life for both consumers and professional users by a credit card transaction we use to buy something, an email address to register for a product, a social security number we add to an application form, and so on. Each of these examples makes up our digital identities. An entity may have one or several identities in an administrative domain. For instance, an individual can be recognized as a director in the context of his company and as a client in the context of his bank. Each identity can be referenced by one or more than one identifier related to specific attributes [8]. The type of credential used during the authentication process depends on the business security requirements. Figure 1 displays the interaction between entities, domains, and identifiers.

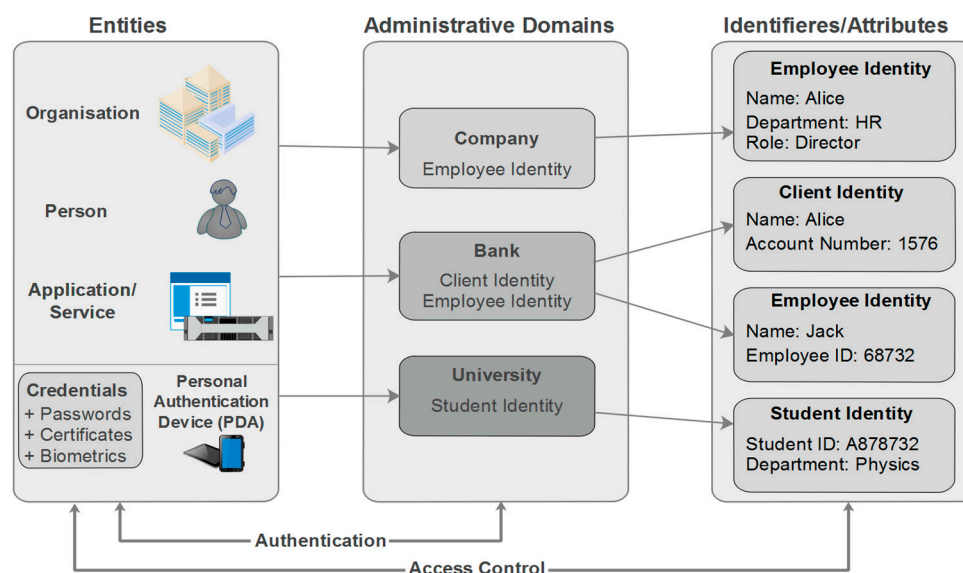


Figure 1. Relationship among entities, identities, and domains.

2.4. Authentication Methods

To access services and entitlements, identity proofing and authentication are required. Without identity validation, people may face exclusion from economic and social life by denying them access to services and rights. The models and mechanisms by which an entity can be authenticated differ widely across countries, industries, and contexts. Generally speaking, users are constantly finding stronger authentication using claims based on the following:

- What you know (e.g., password, personal identification number (PIN)): this form of authentication is still the most widely used for online applications by means of a user name (user ID) and password [9]. However, using passwords as an authentication mechanism is far from adequate for providing a high security level [10];
- What you have (e.g., certificate, token, and smart card): to meet the security requirements and to achieve strong authentication, a possession-based authentication scheme has been developed to basically check the user's credentials validity. This technique is based on the generation of tokens using the login credentials of the users. The latter will be allowed to access protected resources, on a specific time period, without using their credentials repeatedly. Given that the tokens expire within a set time limit, users will be asked to authenticate themselves once more. Thus, this method increases the security and helps users stay safer online. However, possession of a valid token does not prove ownership as it may have been stolen. Thus, possession-based authentication is useless in uncontrolled environments [11].
- What you are (e.g., biometrics): this refers to recognition of a person based on human physiological or behavioral characteristics. Among these characteristics are the following: face, fingerprint, hand geometry, iris, retinal, signature, and voice [12]. This solution avoids risks associated with other authentication methods. It cannot be stolen, forgotten, or borrowed. However, despite the benefits of biometrics, some security issues still must be addressed. In fact, biometrics systems are not always accurate, and there are privacy concerns as they may collect more information than what is needed to grant the access. In addition, there are several attack points in biometrics systems [13].

In some situations, identity validation requires more than one authentication form to add an extra protection layer and to increase the security aspects. This authentication approach is called "multi-factor authentication (MFA)" [14].

2.5. Access Control Models

Many access control approaches have been devised to establish effective and secure access to protected applications and services within information systems, by defining the roles to assign to users and resources. The identity based access control (IBAC) model was historically the first type of access control. This model is based on the use of a matrix with access control lists (ACLs). The entitlements are assigned directly to users' accounts and any access not explicitly authorized is prohibited [15]. The IBAC model is the simplest one when the number of users according to the resources to be protected is very small. However, the complexity of ACLs increases according to the number of identities and the number of resources, because it is necessary to exhaustively list the authorizations for each combination. Therefore, the authorization management becomes more complex. To tackle the limitations of the IBAC model, the National Institute of Standards and Technology (NIST) has elaborated on the role-based access control model (RBAC), in which the entitlements are assigned to the roles [16]. The registration of a new user only needs to assign him the necessary roles to carry out his mission instead of granting him all the underlying authorizations, so that the management of entitlements becomes more simplified. Nevertheless, the implementation of the RBAC model within an organization requires the establishment of a role engineering policy, which is not an easy task. This model is particularly adopted by organizations whose definition of trades and missions is fixed and knows little evolution. With the emergence of the service oriented architecture (SOA) [17], the attribute based access control (ABAC) model was constructed to reduce the complexities of previous models. This model controls the access to resources by defining a policy for one or more attributes that identities are likely to possess [18]. Thus, access control management becomes easier with a dynamic access to protected data based on a user's attributes instead of ACLs. In order to enable ABAC implementations, the access control markup language (XACML) [19] has been developed by the Advancing Open Standards for the Information Society (OASIS). Given that the ultimate goal of identity management and identity federation systems is to share information in a secure manner and

to ensure the collaboration within and across domains with a simplified administration, the process to manage the access to a variety of content and services within an identity federation environment is typically based on the ABAC model [20].

2.6. Identity Management

Today's increasingly digital world is bogged down by different systems, applications, and resources. As result of these evolutions, users need quick and easy access to different platforms wherever they are located. Meeting these demands across a variety of applications and services requires the creation of user accounts into different platforms. However, it is not easy to spend all the time handling and administering large numbers of different user accounts in different services and the partial identities associated with them. In addition, the bad usability of identities often leads to a decrease in security and the demise of privacy. To overcome the above challenges, identity management comes into play. It refers to the process of representing, using, and maintaining digital identities in computer networks [21]. In other words, identity management aims to establish environments, rules, and procedures to handle the user's identity life cycle while reducing the effort, time, and cost associated with the typical administration process. The main components of an identity management system are as follows [22]:

- End user: person wants to access a resource;
- Digital Identity: a set of attributes and credentials;
- Identity provider (IdP): an organization that issues and manages identities of users;
- Service provider (SP): an organization offering services to end users or other organizations. It also known as a relying party;
- Personal authentication device (PAD): a personal device holding identifiers and credentials.

In mobile environments, identity management handles mechanisms to follow the user's identity from device to device, location to location, and context to context.

3. Identity Federation: Architectures and Related Standards

The identity federation is a specific technology of the identity management system. It is built upon the basis of trust relationships between two or more administrative domains to share applications and services. This approach is designed to mitigate the lack of an effective trust management mechanism that may arise in the other identity management approaches. The identity federation systems can be built according to different architectures [23].

3.1. Full Mesh Federation

The full mesh federation architecture is the approach most adopted by identity federations in the academic sector. The REFEDS survey 2016 [24] showed an interest from NREN (National Research and Education Networks) federations around the world—including InCommon in the United States, SurfNET in the Netherlands, and SWAMID in the Sweden, among others—in building this architecture. In a full mesh federation topology, IdPs and SPs connect to each other without any central component [25]. They take charge of all required configurations including attributes release, discovery service (DS), and trust relationships. In fact, the federation metadata file includes all SPs and IdPs, and each federation member has a copy of this file. The DS may be operated centrally, typically by the federation operator, or locally on the SPs' side. The model becomes more expensive and difficult to maintain with the increase of trust relationships between multiples parties. Thus, slightly increased efforts are required from the federation members. The most popular technical solution used in such a topology is Shibboleth software [26], developed by Internet2. Figure 2 illustrates the full mesh federation topology.

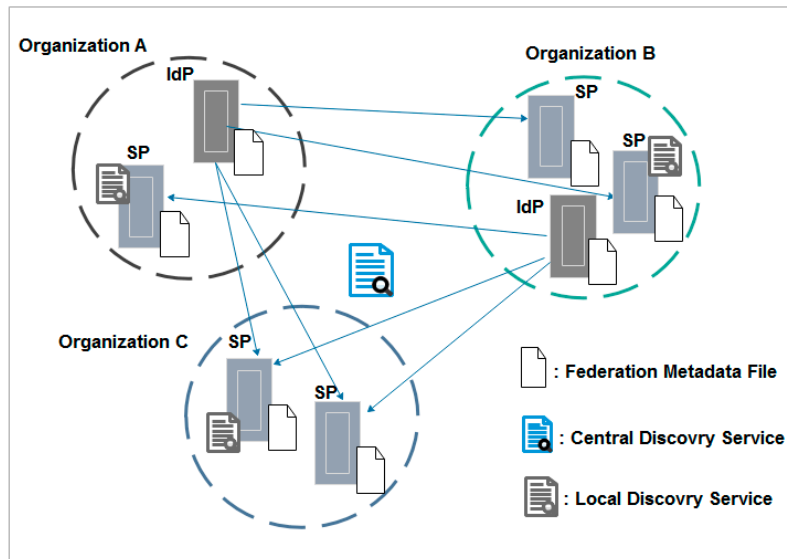


Figure 2. Full mesh federation topology. IdP—identity provider; SP—service provider.

3.2. Hub-and-Spoke Federation with Distributed Login

The hub-and-spoke federation with distributed login model resolves the complexity of a full mesh federation model, by introducing a central hub or proxy to manage the trust relationships between several parties. All IdPs and SPs are hidden behind this central hub via which all security assertion markup language (SAML) [27] assertions are sent. In other words, each IdP still manages the users’ identities, but it needs only a trust relationship with the central hub. Vice versa, SPs only need metadata of the central hub. The latter acts as an SP for IdPs’ members and as an IdP for SPs’ members. In this architecture, there is only one centralized DS at the hub level [28]. Despite the benefits of this model, which is reflected in the facilitation of the federation metadata, which needs to be updated much less frequently, the central hub is a single point of failure that must be highly available and carefully secured and protected. The central hub is also a single point to intercept attributes because it may control, extend, or transform attributes. Therefore, the model includes privacy and security concerns. Figure 3 gives an overview of the hub-and-spoke federation with distributed login.

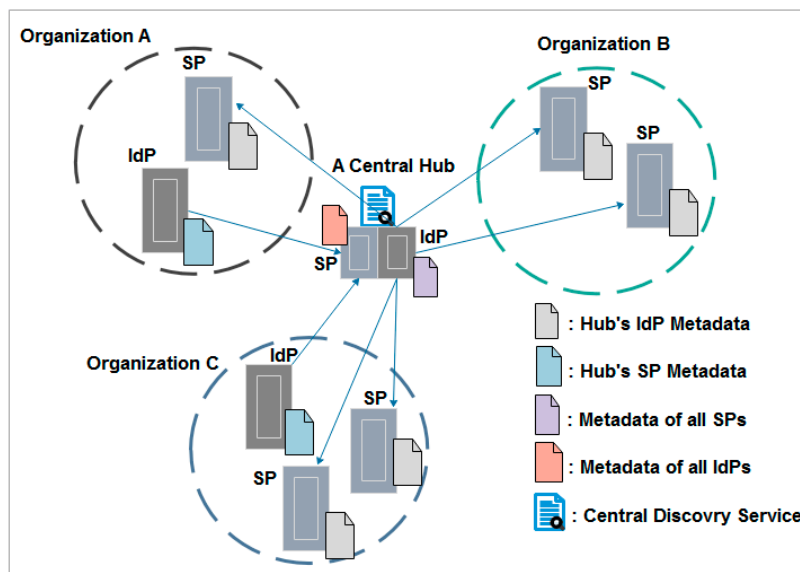


Figure 3. Hub-and-spoke federation with distributed login topology.

3.3. Hub-and-Spoke Federation with Centralized Login

The hub-and-spoke federation with centralized login is used by organizations that do not want to establish their own IdP. In this model, there is only one central IdP that is trusted by all SPs and all local user databases are connected to this IdP, which introduces potential privacy concerns [29].

Figure 4 illustrates the hub-and-spoke federation with centralized login topology.

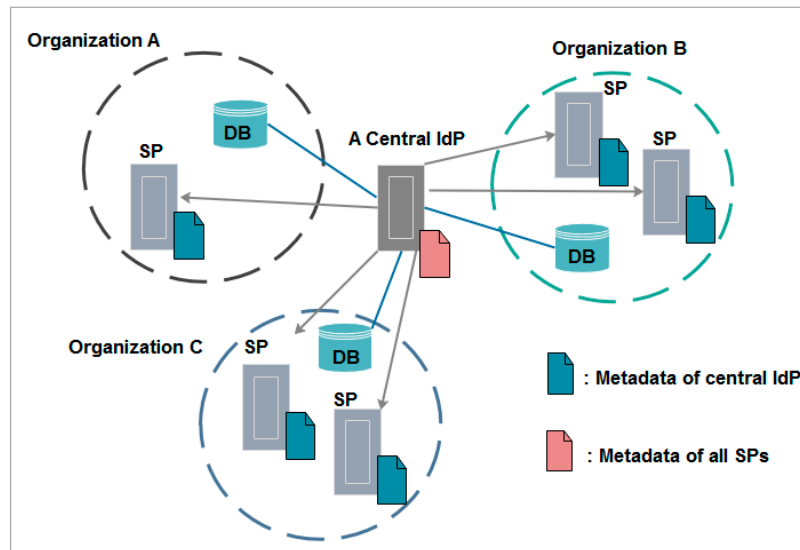


Figure 4. Hub-and-spoke federation with centralized login topology.

3.4. Liberty Alliance

The Liberty Alliance is a group of more than 200 companies from diverse sectors including technology vendors, consumer-facing companies, educational organizations, and governments. The main objective of this group is to establish standards and guidelines in order to converge towards a business agreement and to implement an identity federation framework. The Liberty Alliance architecture is made up of three main components [30]:

- Identity federation framework (ID-FF): This defines protocols and profiles to enable the identity federation solution. The ID-FF is designed to be used on its own or in conjunction with existing identity management systems using heterogeneous platforms and various network devices. The main functions of the ID-FF protocols are account linkage, simplified single sign-on, simple session management, and real-time discovery and exchange of metadata.
- Web services framework (ID_WSF): This defines web services that can be provided to users in order to support the Liberty Alliance business model. It utilizes the ID-FF for authentication and the federation and privacy mechanisms. ID-WSF offers features including permission-based attribute, identity service discovery, and interaction service.
- Services interface specifications (ID-SIS): This provides interfaces for web services allowing providers to exchange different parts of identity. These services are built on top of Liberty's ID-WSF and comprise registration, contact book, calendar, geo-location, presence, or alerts.

3.5. Web Service Federation (WS-Federation)

The WS-federation is developed by a group of companies. It is a part of the largest web service security framework [31]. The main goal of this standard is to define guidelines and mechanisms to manage security aspects and trust relationships across web services and organizations boundaries. The WS-federation model includes three core elements: the requestor (RQ), which is used to require access to web services; the identity provider (IdP) or security token server (STS), which handles

the authentication process with the transmitting of security tokens with relevant attributes; and the resource provider (RP), which includes one or more web services to provide resources required by the RQ [32].

Figure 5 below shows the interaction between web service (WS)-federation components.

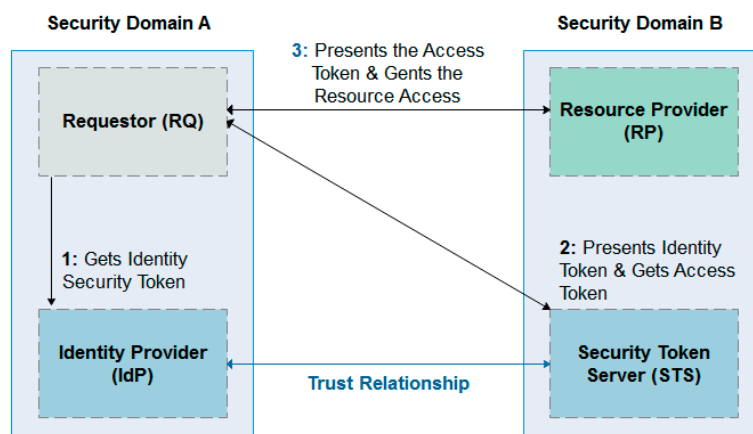


Figure 5. Interaction between web service (WS)-federation components.

4. Attribute Aggregation in Identity Federation

During the typical operation of an identity federation system, the end user contacts an SP and is redirected to the chosen IdP for authentication. If the end user has been authenticated successfully, the SP sends an attribute query to the IdP in order to grant resource access to the authenticated user. The IdP has to send all required attributes to the SP. In this way, the identity federation systems facilitate the access to web resources by avoiding registration and repetitive authentication constraints, while securing the exchanges between all stakeholders. However, despite the advantages of the current identity federation systems, they still suffer from limitations regarding the lack of a standard approach to aggregate attributes from different IdPs, and they cannot solve the interoperability problem perfectly. To deal with this issue, it is necessary to go one step further and work on improving the existing systems. Several models and frameworks have been proposed, each with their own inherent strengths and weaknesses.

4.1. Related Work

Nowadays, there are diverse attribute aggregation models that allow users to collect required attributes from more than one IdP in order to get access to protected resources. Depending on where the attribute aggregation takes place, the existing models can be divided into three categories: aggregation at the client level, aggregation at IdP level, and aggregation at SP level.

In the work of [33], the authors provide a comparative analysis of some existing attribute aggregation models and discuss several aspects of attribute aggregation in a general manner.

Chadwick et al. [34] developed another model by introducing a new SP called a linking service (LS). This conceptual model satisfies most of the identity management requirements and allows the collection of attributes from various sources. However, this model is difficult to deploy and maintain. It does not follow the typical conception of identity federation systems, as the first point of contact to authenticate an end user is an SP instead of an IdP. Moreover, important technical modifications should be made at SPs' level, which could make the latter unmotivated to join systems based on this model. In addition, this model sends the total list of IdPs with end users' accounts, even those who manage attributes that are not requested by the SP. Thus, the second law of identity (data minimization) and the privacy requirement are not respected.

The authors of [35] give an overview and analyze the strengths and weaknesses of seven different models: application database, identity proxcing, identity relay, client-mediated assertion

collection, identity federation/IdP mediated attribute aggregation, SP-mediated attribute aggregation, and linking service.

The proposed work in [36] provides a taxonomy of the attribute aggregation models discussed in the work of [35], and categorizes different requirements in a systematic manner. The results have been presented in tabular form to compare all models side-by-side.

The authors of [37] enrich the study of the attribute aggregation model by analyzing other approaches like the SWIFT model [38,39] and user-centric identity management using trusted modules [40].

Prior to designing our approach to deal with interoperability issue for current identity federation systems, we have studied all models previously mentioned to gain a thorough understanding of each one. Taking into consideration the perspectives expressed to strengthen the current models of attribute aggregation, we have formulated a set of functional, security, privacy, and trust requirements that we want our model to fulfil in order to gain a wide acceptability. These requirements are prepared in accordance with the digital identity laws [3] and have been rephrased with the reference of attribute aggregation.

The essential requirements that are selected as comparable metrics for this study are the following:

- Attribute aggregation from many IdPs in a single session: the model has to have the ability to select user attributes from multiple IdPs;
- Signing of attribute assertions by their authoritative sources: to provide adequate assurance of the attribute value correctness, each attribute assertion must be signed by the authority managing this attribute and who the SP is willing to trust;
- Linking and mapping attributes to IdPs with user permission: the user should have the control and be able to select the attributes that will be provided by each IdP;
- Respect of the typical operating principle of identity federation: the model should follow the standard design of an identity federation system;
- Single authentication in one session: end users need to be authenticated only once without asking them to authenticate separately into each IdP;
- Privacy protection of user attributes: during data transmission, the model must ensure the controlled release of attributes and the unlinkability between sessions;
- Efficiency of trust relationships management: the model should optimize the trust relationships, while at the same time avoiding the establishment of trust relationships that are not useful and mandatory.
- Data minimization: user attributes will be processed only if it is necessary for the SP with limited access to personal data;
- Mitigation of implementation complexity: the design and the implementation of the model should be as simple as possible by avoiding additional investment and technical complexity;
- Availability: the system should be online and ready to conduct business 24 hours a day, 7 days a week. Besides, the design of the model should take into account the absence of the single point of failure (SPoF) to grant the reliability of the system.

Table 1 summarizes the results of our study of the previous models and points out the strengths and limitations of each approach. We have used the tick (\checkmark) mark to indicate that the model satisfies a respective requirement, while the character (\times) has been used to indicate that the model does not satisfy the respective requirement. The dash (-) character has been used in cases where it was difficult to explain the analysis precisely.

Table 1. A comparative analysis of attribute aggregation models. IdP—identity provider; SP—service provider.

	Attribute Aggregation Models							
	Application Database	SP-Mediated Attribute Aggregation	Identity Proxying	Identity Relay	Client-Mediated Assertion Collection	Identity Federation or IdP Mediated Attribute Aggregation	SWIFT Identity Framework	Linking Service
Attribute aggregation from many IdPs in a single session	×	√	√	√	√	×	√	√
Signing of attributes assertions by their authoritative sources	×	√	×	√	√	×	×	√
Linking and mapping attributes to IdPs with user permission	×	×	×	×	×	×	×	×
Respect of the typical operating principle of Identity Federation	√	√	√	√	√	√	√	×
Single authentications in one session	√	×	×	×	×	×	√	√
Privacy protection of user attributes	×	×	×	×	×	×	×	×
Efficiency of trust relationships management	√	√	√	√	-	-	√	×
Data minimization	×	×	×	×	×	×	×	×
Mitigation of implementation complexity	√	×	√	√	×	×	×	×
Availability	×	-	×	×	-	-	×	×

4.2. Analysis and Interpretation

Surveying related work reveals that each model has a set of requirements with their own strengths and weaknesses and with approaches that are sometimes complex and intolerable by a wide audience. There is, therefore, a real need to develop a satisfactory solution that will overcome the interoperability challenges of current identity management systems. From this perspective and to counteract this deficiency, it is up to us to build the required model to make this vision a reality by proposing a new approach of identity federation with appropriate policies, procedures, and controls in order to aggregate attributes from multiple sources, without a need to authenticate each IdP separately, taking into account the enhancement of privacy and security aspects.

5. Description of the Proposed Model

5.1. Bricks of the Proposed Model

Managing access to resources and services, maintaining their availability, integrity, and the confidentiality of sensitive information are the main goals of our model, which relates to an interoperable identity federation system. The primary purpose of this model is to develop a consistent approach flexible enough to support new scenarios, requiring user attributes managed by different attribute authorities, particularly in academic, e-Government, e-Health, e-Business, and e-Banking fields. The proposed model allows users to access different services of different domains in a transparent and secure manner after a single authentication with a trusted third party. More precisely, our proposed model is based on the attribute aggregation technique, the mechanisms of identity federation, and the identity relay model, while extending its benefits and minimizing its drawbacks. The essential components composing the architecture of our model are as follows:

- Service provider/ relying party: entity providing IT solution/services to end users;
- Identity provider: entity managing users' identities and providing system authentication;
- Account linking provider (ALP): a new component that acts as a gateway between SPs and IdPs allowing users with multiple accounts into several IdPs, in order to federate their identities

and aggregate their attributes, while improving the trust relationships between the various stakeholders and respecting the security and privacy concepts;

- ALPs' discovery service: entity holding the predefined list of all ALPs having trust relationships with the SP.

5.2. Key Components of the ALP

To ensure the attribute aggregation, our scheme is based on a particular identity provider, which is the ALP. This latter requires a detailed description of its architecture, as it is one of the building blocks and the core of the proposed model. As illustrated in Figure 6, the main components of the ALP are as follows:

- Authentication authority: this is the brick responsible for the authentication and the authorization process on the ALP;
- Centralized user database: a local database holding the identities of users who are authorized to access the ALP by means of a UserID and password;
- Discovery service: this module holds the predefined list of all IdPs having trust relationships with the ALP. It interacts with end users, allowing them to select an identity provider that manages one of their identities;
- Attribute authority: unlike an ordinary IdP, this brick does not produce SAML attribute assertions. Once the ALP receives user attribute request from an SP, the attribute authority triggers a search process for the corresponding IdPs;
- Account linking table (ALT): the attribute aggregation process is based on the establishment of an ALT (Table 2), which illustrates, for each user, the set of IdPs on which they have accounts with the corresponding attributes that will be provided by these IdPs to SPs. The ALT table also contains authentication assertions for each user in an IdP.

Table 2. Account linking table. ALP—account linking provider.

	Identity Providers (IdP)	UId (at IdPs Level)	AttributeID	Authentication Assertion
UserId (at ALP level)	IdP1	UId1	Email NIN ^a	OK
	IdP2	UId2	GivenName DisplayName	OK

	IdP _n	UId _n	Telephone Number	OK

NIN^a: national identification number.

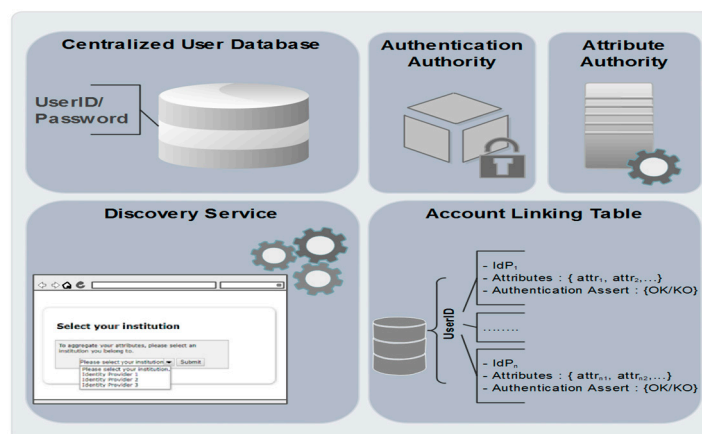


Figure 6. Key components of the account linking provider (ALP).

5.3. Properties of the Proposed Model

Preferred, but non-limiting features of our scheme are as follows:

- The access to resources requires a single authentication with the ALP. Therefore, end users do not need to be authenticated with each IdP during a single access session. Moreover, the system is based on the single sign-on (SSO) mechanism to avoid re-authentication of end users each time they access protected services during a specific period of validity;
- Users have complete control and visibility of the dissemination and the use of their identities and attributes. In addition, no IdP should be aware of user identities on other IdPs so that the privacy requirement is insured;
- IdPs communicate the attribute identifiers (attributeIDs) to ALPs and not the values of those attributes that are stored in appropriate directories;
- The management of trust relationships between stakeholders is optimized. Each IdP must have a trust relationship with the SP and the ALP so that they can communicate successfully. However, IdPs do not need to have trust relationships between each other;
- The SP must be aware of the IdP that initially asserted attributes of the end user and all assertions must be signed by trustworthy sources;
- The ALP communicates to the SP only the selective list of the IdPs managing the required attributes to allow the resource access;
- The proposed model is mapped on the standard protocol SAMLv2 and follows the typical principal of identity federation systems.

The findings of the comparative analysis, as shown in the Table 3, highlight the strengths of our model, which adopts a cost–benefit analysis approach by adding valuable assets in term of security, privacy, and simplicity of implementation. The new model meets the majority of the requirements expected by end users, SPs, and home IdPs.

Table 3. Strengths of the proposed model.

	Attribute Aggregation Models								
	Application Database	SP-Mediated Attribute Aggregation	Identity Proxying	Identity Relay	Client-Mediated Assertion Collection	Identity Federation or IdP Mediated Attribute Aggregation	SWIFT Identity Framework	Linking Service	Our proposed Model
Attribute aggregation from many IdPs in a single session	×	√	√	√	√	×	√	√	√
Signing of attributes assertions by their authoritative sources	×	√	×	√	√	×	×	√	√
Linking and mapping attributes to IdPs with user permission	×	×	×	×	×	×	×	×	√
Respect of the typical operating principle of identity federation	√	√	√	√	√	√	√	×	√
Single authentications in one session	√	×	×	×	×	×	√	√	√
Privacy protection of user attributes	×	×	×	×	×	×	×	×	√
Efficiency of trust relationships management	√	√	√	√	-	-	√	×	√
Data minimization	×	×	×	×	×	×	×	×	√
Mitigation of implementation complexity	√	×	√	√	×	×	×	×	√
Availability	×	-	×	×	-	-	×	×	×

6. Operating Principal of the Proposed Model

The operating principle of our model goes through two stages:

6.1. Registration and the ALT Filling

During the registration and the ALT filling phase, the end user, the ALP, and one or more IdPs interact with each other, as described in Figure 7. The end user attempts to access the ALP by sending an access request to the ALP via their web browser (1). Once the request received by the ALP (2), this latter asks the end user for authentication (3). After receiving of the authentication request (4), the end user sends his authentication credentials to the ALP (5). This latter receives and validates the correctness of these credentials (6):

- If the user credentials are not valid, the ALP denies the access request and notifies the end user (7.1) who gets an error message (8.1). In this case, the end user may either attempt to retry the access process or decide to withdraw.
- If the user credentials are valid, the ALP initiates the research process in the ALT table (7.2). A treatment of the research request will be launched (8.2) with the verification of the related data 0 existence (9):
 - In the case of the prior existence of the end user entry in the ALT, the ALP allows the end user to update his data (10.1). He can view information related to his accounts and aggregated attributes, and he can also update accounts and attributes (11). The ALP receives, prepares, and sends the updated data to the ALT (12). This latter adds and saves the updated data (13).
 - If the ALT does not contain any data relating to the end user, a registration phase will be started (10.2).

In Section 6.2, a detailed explanation of the registration process is presented (see Figure 8).

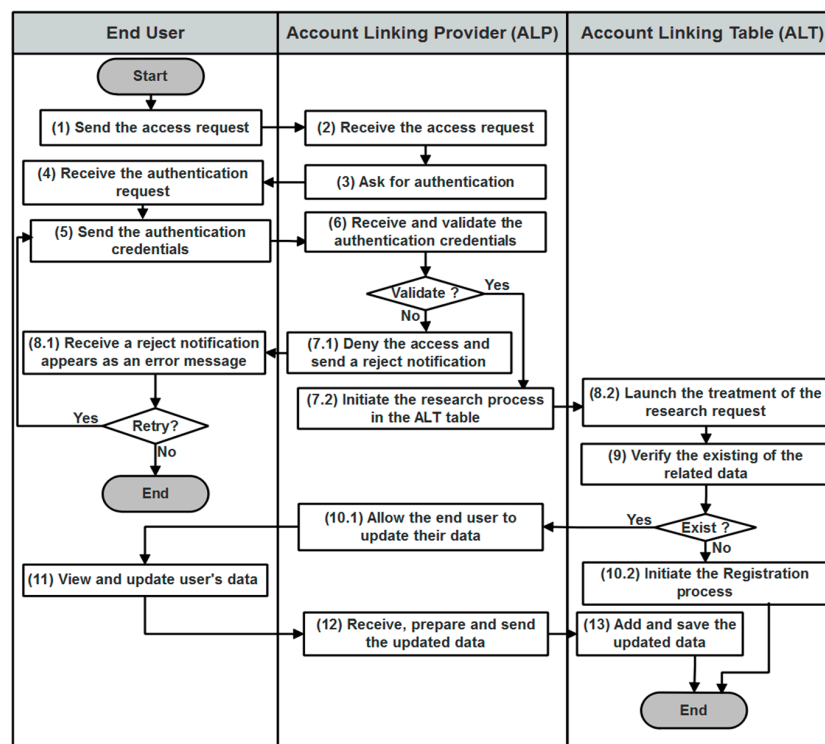


Figure 7. ALT filling algorithm.

6.2. Detailed Description of the Registration Phase

For a better understanding of the registration phase, we have designed Figure 8 to illustrate a detailed description of the registration process, which follows the steps below:

After the authentication of the end user, as is already detailed in Figure 7 (step 1 to 7.2), the ALP redirects the end user to a discovery service (1) that displays a predefined list of all IdPs having trust relationships with that ALP (2). After having chosen an IdP (3), the end user is then redirected to this IdP (4) and he is asked to log in (5). In the case of a successful authentication, a list of attributeIDs managed by this IdP is displayed (6), and the end user can seamlessly select the attributeIDs (7) that will be provided by this IdP to SPs. The list of selected attributeIDs, the local user identifier (UIId) at this IdP, and the user authentication assertion into this IdP will be sent to the ALP (8), and an entry for that user will be created at the ALT (9) (see Table 2). The user may be asked to choose another IdP and the process described above will be repeated again (10).

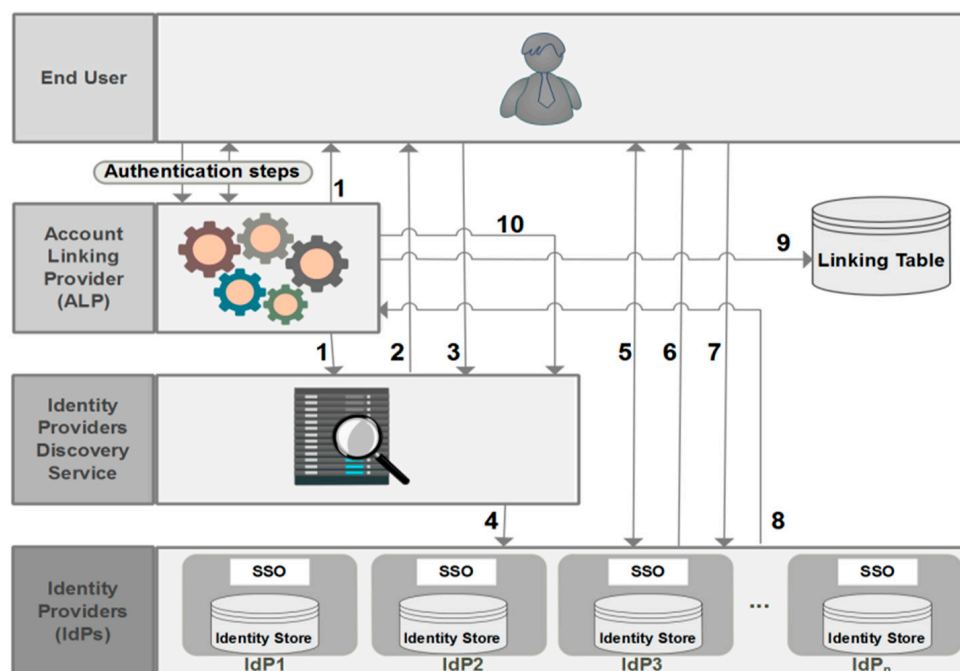


Figure 8. Detailed registration process. SSO—single sign-on.

6.3. Attribute Aggregation and Access Phase

After the registration and the ALT filling, the end user can access resources and services whose authorization requires users' attributes managed by multiple IdPs. As can be seen from Figure 9, the attribute aggregation and access process is described as follows:

When the end user attempts to access a protected resource via an access request (1), an authentication dialog appears with a list of required attributes asking the end user if he would like to use the attribute aggregation with this resource (2). If the end user accepts, he will be redirected to the ALP's discovery service (3). From the appeared ALPs list (4), the end user chooses his ALP (5). By doing so, he will be redirected to the chosen ALP (6) by asking him to log in (7). Once authenticated, the ALP sends back to the SP an authentication assertion with user identifier (UserId) at this ALP (8). Before granting access to the resource, the SP sends an attribute request to the ALP (9), which initiates a lookup process in its ALT based on the UserId. Once it has located the appropriate entry for this user, the ALP sends a selective list of IdPs managing the required attributes (10). For each IdP, the ALP sends to the SP a combination of the authentication assertion and the user identifier (UIId) relating to this IdP. The SP sends attribute requests to each IdP with the UIId and the relating authentication assertion (11) (the user does not need to be authenticated into these IdPs). Each IdP returns a response

with the requested attributes (12) so that the SP can make a decision to deny or grant access to the protected resource based on the attributes received by all IdPs (13).

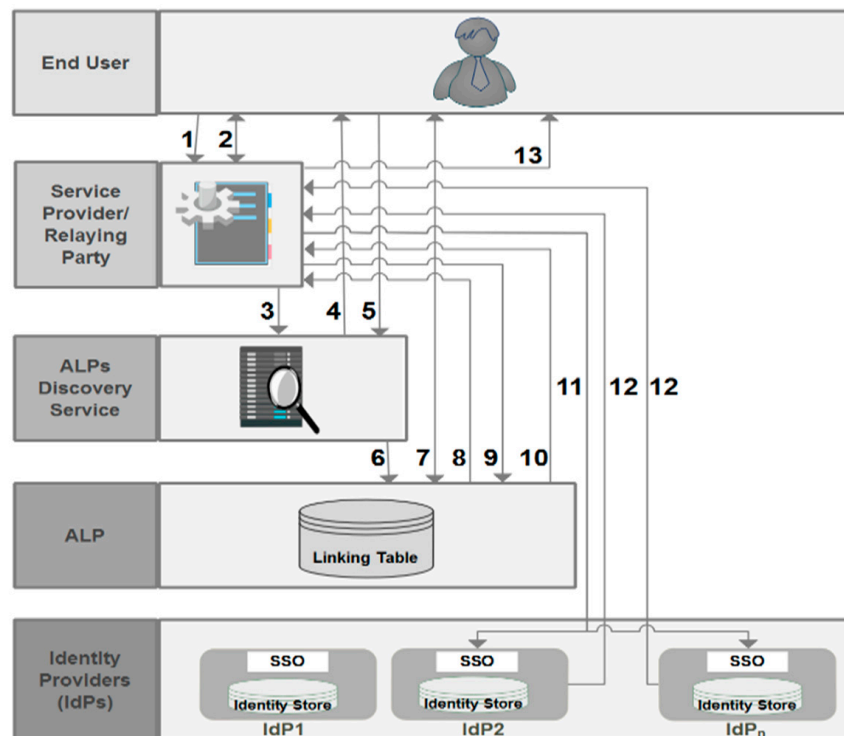


Figure 9. Attribute aggregation and access phase.

7. Prototype Implementation

The Shibboleth software was chosen as the adopted solution to perform the technical implementations of the prototype of our proposed scheme. Shibboleth follows the SAML standard and is among the most widely deployed federated identity solutions, especially in the academic sector. Besides its larger user community and its strength, Shibboleth is built to ensure the proxy feature by handling the delegation of the end user authentication to another IdP, and then releasing the attributes to an SP via a SAML assertion once the end users have been authenticated. However, attribute aggregation from multiple IdPs in a single session is not allowed with the ordinary concept of the Shibboleth package. In other words, it could not be considered as a rely IdP. Nonetheless, and despite of its limitations, the Shibboleth package has given us a solid basis to carry out our implementations, while making appropriate changes to the base code of Shibboleth bricks, as it is an open source software. The results of the prototype implementations are represented via a series of screenshots displaying web interfaces of the proposed system. The web-based workflow of registration and accounts linking process of the proposed scheme is illustrated in Figure 10.

7.1. Registration and the ALT Filling

7.1.1. Authentication Process

The ALP acts as the entry point to start the attribute aggregation process. Thus, the authentication of the end user is required before beginning any activity. The authentication home page of the ALP was personalized, as illustrated in interface 1 of Figure 10. After a successful authentication, we developed an application to start the search for the data related to the authenticated user. Interface 2 of Figure 10 shows the result obtained when any data relating to the end user are found in the ALT, knowing that at this stage, the end user can initiate the registration and the ALT filling process by clicking on the

“OK” button. In the case of the prior existence of the data in the ALT, the end user gets, as shown in interface 3 of Figure 10, a table indicating his accounts that will be used in the attribute aggregation process. At this stage, the end user can also initiate the registration and the ALT filling process to add other accounts via the “Link another account” button.

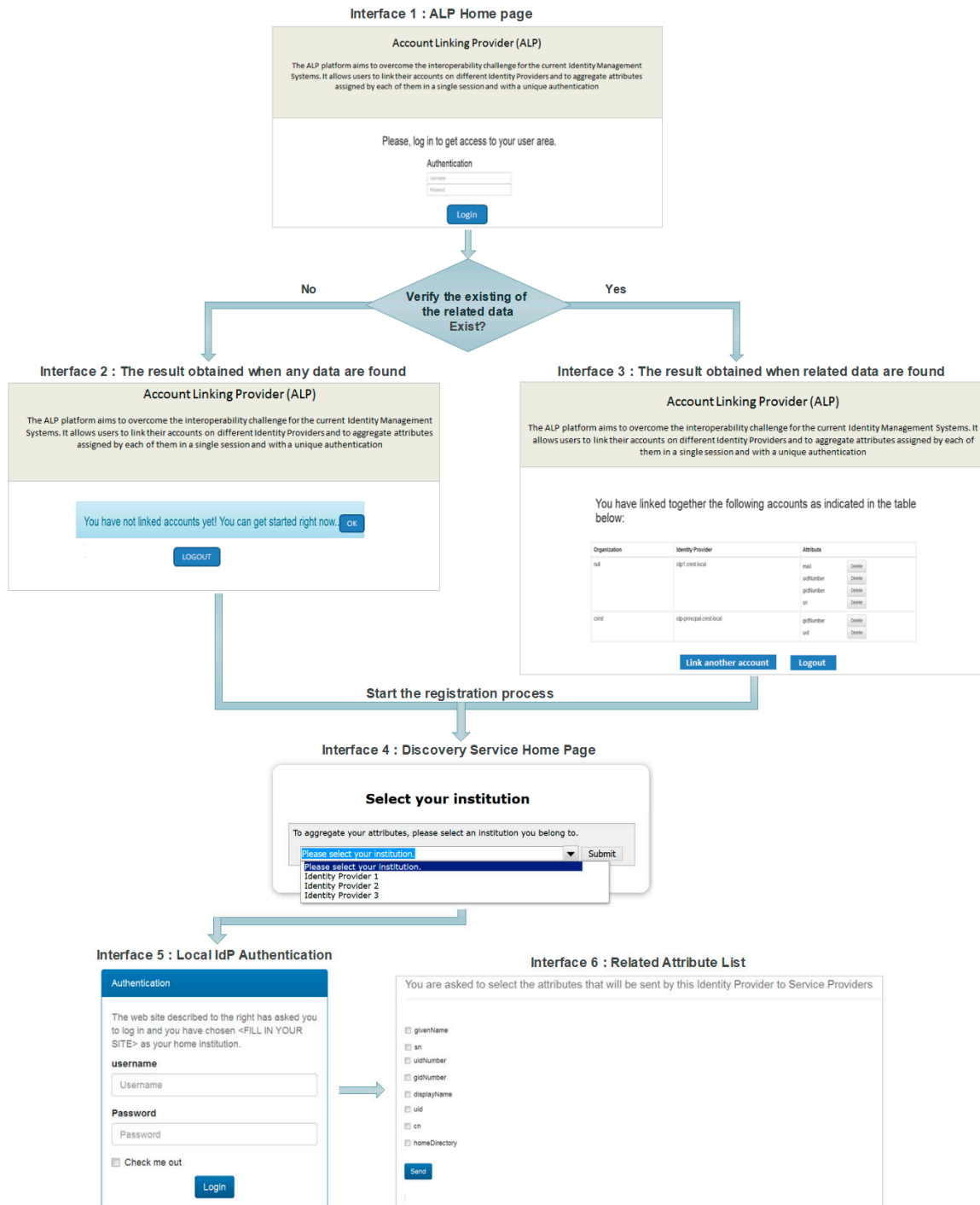


Figure 10. Web-based workflow of registration and accounts linking process.

7.1.2. Integration of the Discovery Service into the ALP

To display a predefined list of trusted IdPs once the end users accept to aggregate their accounts, we have installed on the ALP a WAYF (where are you from) application. Then, we have included the \$commonDomain element to add the ALP as a resource that will use the discovery service (WAYF).

Hence, once the end user initiates the attribute aggregation, the ALP will redirect him to the WAYF home page with a list of trusted IdPs (see interface 4).

7.1.3. Retrieval, Display, and Transmitting of the Selected Attributes to the ALT

We implemented an application that has to be running within each home IdP. This application allows the retrieval of all attributeIDs from the user data directory based on the UID of the authenticated user. The attributeIDs are displayed on a consent form that gives the user the ability to choose those that shall be revealed to SPs. The recovered attributes will be sent to the ALP on a secure socket layer (SSL). The ALP stores these attributes associated with UID, the IdP name, and the authentication assertion on the ALT.

7.2. Interaction between SP, ALP, and Local IdPs

7.2.1. Extraction and Sending of the Required Attributes by the SP

When an end user tries to access a protected resource managed by an SP, this latter displays the required attributeIDs list to grant access to the requested resource, with a possibility to use the attribute aggregation mechanism. Once the end user opts for this mechanism, the SP behaves as usual by redirecting the end user to a WAYF service to choose an ALP. Then, the end user is forwarded to the chosen ALP where the authentication takes place. After a successful authentication, we have configured the SP to extract the required attributeIDs and send them to the ALP. To achieve this, we have changed the */secure* URL with */secure2*, which is linked to the script *shibenv.php* in the *shib.conf* web server file. The default URL */secure* is used to extract the required attributes from the *attribute-map.xml* file. A PHP script is elaborated to retrieve the extracted attributes and send them to the ALP.

7.2.2. Retrieval of IdPs Managing the Required Attributes

When an ALP receives an attribute request from an SP, a JSP script is programmed to launch a research process at the ALT level in order to retrieve all IdPs managing the required attributes on the basis of the UserId. To facilitate the research operation, a *split()* method is used to split the string of required attributes into an array of substrings. The JSP script is programmed in such a way that the result of the research into the ALT must include, for each attributeID, the name of the related IdP, the UID, and the authentication assertion at this IdP. The final result is inserted inside an *AttributeStatements* element, which accommodates one or more *AttributeStatement* elements.

7.2.3. Interaction between an SP and linked IdPs

Before granting access to the requested resource, the SP relies on the received statement from the ALP to form follow-up attribute requests to the related IdPs. The SP sends selective attribute queries to each IdP, along with the UID and the authentication assertion at this IdP. To issue several SAML attribute queries to the set of IdPs managing the required attributes, we used the *SimpleAggregation* *AttributeResolver*. The IdPs return assertions to the SP, which validates these assertions as required by the SAML protocol and extracts the embedded attributes to make an authorization decision according to the data in these attributes. Without identifying the source of each attribute, it might be difficult for the SP to make access control decisions.

8. Analysis and Evaluation

In the analysis process of our model, we focus mainly on design and implementation benefits and issues related to the security aspects according to threats that could impact its practical use. To identify potential threats and validate security and privacy assumptions of our proposed model, we have based it on the threat modeling concept, which is an integral process for building a secure system [41]. The process of this concept typically includes three high-level steps: *Identifying Assets*, *Identifying Threats*, and *Outlining Mitigation Strategies* [42]. Additionally, there are some works that deal with

threat modeling for identity management systems [43,44]. On the basis of these works, the threat modeling of our model followed the steps outlined below:

- **Identifying Assets:** in the work of [45], Schostack describes assets as valued things that should be protected from attackers. In an identity federation system, user identity is a central part that can be considered as a potential target of attackers. Thus, the main assets of our model are as follows: (a) partial identity with related attributes, (b) associated processes with partial identities (authentication, authorization, . . .), and (c) web services.
- **Identifying threats:** among possible threats against assets of our proposed model, we list the following threats:
 - *Spoofing (Th1):* information of user identities stored on IdPs and the ALP may be disclosed to unauthorized users that impersonate legitimate users from trusted sources.
 - *Information Disclosure (Th2):* attributes can be disclosed to SPs without user's consent.
 - *Tampering (Th3):* exchanged data between stakeholders, through communication channels, can be intercepted by attackers.
 - *Reply Attacks Threat (Th4):* user messages may be captured and used by an attacker to launch a replay attack on SPs.
 - *Denial of Service Threat (Th5):* attackers may send several modified requests to render the ALP unavailable for its intended users.
- **Outlining Mitigation Strategies:** after the identification of threats, strategies should be planned and implemented to effectively mitigate the underlined threats. In the next subsections, we will highlight the main mechanisms adopted to minimize the identified threats as much as possible.

8.1. Advantages of the Proposed Model

There are a number of benefits to implementing the proposed model in order to aggregate attributes seamlessly, by satisfying almost all requirements that are selected as comparable metrics as illustrated previously in Section 4.1.

At the IdP and ALP levels, user registration and authentication mechanisms have been established in order to limit access to only authenticated and authorized users. As a result, Th1 is reduced. The implementation of our model allows end users to be aware beforehand of the required attributes to access SP resources by displaying the list of required attributes for each specific service at the SP home page. In addition, the first step of the attribute aggregation process is to explicitly link together various user accounts from different IdPs. Hence, the user's consent is satisfied. To achieve the data minimization requirement, the ALP ensures a selective disclosure of IdPs managing the required attributes to an SP with a user's consent. Thus, Th2 is undermined. The ALP also maintains the session active while the SP is interacting with IdPs managing the required attributes, thus satisfying the single authentication requirement during an access session. As is evident from the SAML implementation approach, attribute and authentication assertions are encrypted and digitally signed by IdPs, and user attributes are transmitted over secure https channels so that data, during transmission, are not disclosed to any party. Thereby, Th3 and Th4 are weakened.

8.2. Limitations

Despite the strengths and significant potential of our model to overcome the interoperability the challenges of existing identity federation solutions, there are some limitations with our current implementations. Indeed, the SPoF is a potential risk posed by the conception of the proposed model in which one fault or malfunction of the ALP would cause the entire system to stop operating. In addition, the issue of SPoF becomes particularly severe with the exposure to serious vulnerabilities.

Furthermore, the authentication mechanisms represent one of the most promising ways concerning trust and security enhancement. However, the strength of the authentication is more related to the

strength of the underlying authentication methods. In the conception of our model, passwords have been taken as a standalone authentication method; thereby, the security level could be decreased. Thus, it leads to the need for combining more than one factor to authenticate users, taking into account that the combined authentication methods (multi-factor authentication) should offer an elegantly simple end user experience. In addition, the central storage of valid authentication assertions at ALP level (via the ALT), which is responsible for providing identifiers of users with authentication assertions to interact with home IdPs, presents a prime target for attackers so that it is susceptible to Th5. Furthermore, there is no guarantee that the trusted ALP will not abuse the stored data in its ALT.

Finally, the proposed model is limited to an attribute aggregation system that integrates user's information from IdPs that are members of one identity federation domain. It will be interesting to investigate how this model can be deployed into an interfederation like eduGain for the academic sector.

9. Conclusion and Future Work

With the increasing use of e-services in different fields, especially in e-Government, e-Health, e-Business, and e-Banking, the interoperability and privacy in current identity management systems are emerging as mounting concerns. In this article, we studied and discussed ongoing issues related to the interoperability and the attribute aggregation for existing identity federation systems. These analyses led us to design and build a new model that covers the missing parts of the most recent approaches to attribute aggregation. In addition, our scheme takes into account the majority of identity management requirements that are especially related to security and privacy aspects. The proposed approach follows identity federation technologies and the operating principle of the identity relying model. The ultimate goal of this model is to allow users to link their multiple IdP accounts together in order to get access to protected resources that require attribute aggregation from various authorities. To achieve this, we introduced a special IdP, an account linking provider (ALP) with attribute linking table (ALT). The ALP acts as a gateway between IdPs and SPs and allows users to federate their accounts by having total control of the dissemination of their data and attributes by each IdP. To mitigate difficulties in adoption, the model is based on the standard protocol SAMLv2, extending it where necessary while avoiding major technical changes at the SP level that may make these latter unmotivated to join the proposed system, and stand in the way of its success. Similar to existing models regarding attribute aggregation, the availability and reliability requirements remain the most serious issues for our model for as long as the ALP is considered as a single-point of failure. This concern will be further investigated in future work.

Author Contributions: Conceptualization, S.E.H. and M.D.E.-C.E.K.; Methodology, S.E.H. and M.D.E.-C.E.K.; Investigation, S.E.H., M.D.E.-C.E.K.; Writing—original draft, S.E.H.; Writing—review and editing, S.E.H.; Validation, M.D.E.-C.E.K.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bertino, E.; Takahashi, K. *Identity Management: Concepts, Technologies, and Systems*; Artech House: Norwood, MA, USA, 2010.
2. Ferraiolo, H. *A Credential Reliability and Revocation Model for Federated Identifiers*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012.
3. Cameron, K. The laws of identity. *Microsoft Corp.* **2005**, *12*, 8–11. Available online: <http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf> (accessed on 3 June 2019).
4. Shavers, B.; Bair, J. Digital Identity. In *Hiding behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis*; Syngress: Amsterdam, The Netherlands, 2016; pp. 187–202.
5. Mobile Identity Management, Enisa Position Paper. 2010. Available online: <https://www.enisa.europa.eu/publications/Mobile%20IDM> (accessed on 3 June 2019).

6. Roussos, G.; Peterson, D.; Patel, U. Mobile Identity Management: An Enacted View. *Int. J. Electron. Commer.* **2003**, *8*, 81–100. [CrossRef]
7. Rose, J.; Rehse, O.; Rober, B. The value of our digital identity. *Boston Consult. Group* **2012**. Available online: <https://www.bcg.com/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity.aspx> (accessed on 3 June 2019).
8. Jøsang, A.; Pope, S. User centric identity management. In Proceedings of the AusCERT Asia Pacific Information Technology Security Conference, Vienna, Austria, 7–8 July 2005; p. 77.
9. Conklin, G.D.; Walz, D. Password-based authentication: A system perspective. In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2004.
10. Zhao, Z.; Dong, Z.; Wang, Y. Security analysis of a password-based authentication protocol proposed to IEEE 1363. *Theor. Comput. Sci.* **2006**, *352*, 280–287. [CrossRef]
11. Zviran, M.; Erlich, Z. Identification and authentication: Technology and implementation issues. *Commun. Assoc. Inf. Syst.* **2006**, *17*, 4. [CrossRef]
12. Zimmerman, M. *Biometrics and User Authentication*; SANS Institute, 2002. Available online: <https://www.sans.org/reading-room/whitepapers/authentication/biometrics-user-authentication-122> (accessed on 3 June 2019).
13. Ambalakat, P. Security of biometric authentication systems. In *21st Computer Science Seminar*; 2005; p. 1. Available online: <https://pdfs.semanticscholar.org/e1d7/7b951c55d7d1f322d1f96942daa77ec6c4ee.pdf> (accessed on 3 June 2019).
14. Multi-Factor Authentication—Australian Cyber Security Centre (ACSC). Available online: https://acsc.gov.au/publications/protect/multi_factor_authentication.htm (accessed on 3 June 2019).
15. Karp, H.; Haury, H.; Davis, M.H. From ABAC to ZBAC: The evolution of access control models. *J. Inf. Warf.* **2010**, *9*, 38–46.
16. Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L.; Youman, C.E. Rolebased access control models. *Computer* **1996**, *29*, 38–47. [CrossRef]
17. Hurwitz, J.S.; Bloor, R.; Baroudi, C.; Kaufman, M. *Service Oriented Architecture for Dummies*; John Wiley & Sons: Hoboken, NJ, USA, 2006.
18. Hu, V.C.; Ferraiolo, D.; Kuhn, R.; Friedman, A.R.; Lang, A.J.; Cogdell, M.M.; Schnitzer, A.; Sandlin, K.; Miller, R.; Scarfone, K. Guide to attribute based access control (abac) definition and considerations (draft). *Nist Spec. Publ.* **2013**, *800*, 162.
19. Armstrong, M.W. *An Introduction to Xacml*. 2003. Available online: <http://courses.cs.vt.edu/~cs5204/fall05-kafura/Papers/Security/XACML-Short-Introduction.pdf> (accessed on 3 June 2019).
20. Federation and Attribute Based Access Control: Realization of the IAM (r)Evolution. 2010. Available online: https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/AXIOM_SE/A100901F.pdf (accessed on 3 June 2019).
21. Windley, P.J. *Digital Identity: Unmasking Identity Management Architecture (IMA)*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2005.
22. Boujezza, H.; Modher, A.-M.; Ayed, H.K.B.; Saidane, L. A taxonomy of identities management systems in IOT. In Proceedings of the 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrakech, Morocco, 17–20 November 2015; pp. 1–8.
23. Buecker, A.; Filip, W.; Hinton, H.; Hippenstiel, H.P.; Hollin, M.; Neucom, R.; Weeden, S.; Westman, J. *Federated Identity Management and Web Services Security*; IBM Redbook, 2005. Available online: https://www.academia.edu/6726901/Federated_e-Identity_Management_across_the_Gulf_Cooperation_Council_048_ (accessed on 3 June 2019).
24. Refeds Survey. 2016. Available online: <https://geant.app.box.com/s/8f30ptw5houmauurfqfupw3ruz3x9enu> (accessed on 3 June 2019).
25. Field Mesh Guide to Internet Trust Models: Federation. 2014. Available online: <https://identitywoman.net/field-guide-to-internet-trust-models-mesh-federation/> (accessed on 3 June 2019).
26. Shibboleth Consortium. Available online: <https://www.shibboleth.net/> (accessed on 3 June 2019).
27. Cantor, S.; Kemp, J.; Philpot, R.; Maler, E. Assertions and Protocols for the Oasis Security Assertion Markup Language (saml) v2.0 Oasis Standard Mar.15, 2005 Oasis Open. Available online: <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf> (accessed on 3 June 2019).
28. Federation Architectures. 2017. Available online: <https://wiki.geant.org/display/eduGAIN/Federation+Architectures> (accessed on 3 June 2019).

29. Scudder, J.; Jøsang, A. Personal federation control with the identity dashboard. In Proceedings of the IFIP Working Conference on Policies and Research in Identity Management, Oslo, Norway, 18–19 November 2010; pp. 85–99.
30. Watson, T. Introduction to the Liberty Alliance Identity Architecture. 2003, Volume 1. Available online: <http://www.projectliberty.org/Revision> (accessed on 3 June 2019).
31. Lawrence, K.; Kaler, C.; Nadalin, A.; Monzillo, R.; Hallam-Baker, P. Web Services Security: Soap Message Security 1.1 (Ws-Security 2004). OASIS Standard 2006. OASIS. Available online: <https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf> (accessed on 3 June 2019).
32. Lockhart, H.; Andersen, S.; Bohren, J.; Sverdlov, Y.; Hondo, M.; Maruyama, H.; Nadalin, A.; Nagaratnam, N.; Boubez, T.; Morrison, K.; et al. Web Services Federation Language (Ws-Federation) Version 1.1. 2006, 15, 2008. Available online: http://seine.afnet.fr/referentiel/gestion_identites/documents/normes_travaux_spec/WS-Federation-V1-1B.pdf (accessed on 3 June 2019).
33. Inman, G.; Chadwick, D.W.; Klingenstein, N. Authorisation Using Attributes from Multiple Authorities—A Study of Requirements. In Proceedings of the HCSIT Summit-ePortfolio International Conference, Maastricht, The Netherlands, 16–19 October 2007; Volume 366.
34. Chadwick, D.W.; Inman, G.; Klingenstein, N. A conceptual model for attribute aggregation. *Future Gener. Comput. Syst.* **2010**, *26*, 1043–1052. [[CrossRef](#)]
35. Hulsebosch, B.; Wegdam, M.; Zoetekouw, B.; Dijk, N.; Wijnen, R. *Virtual Collaboration Attribute Management*; Surf Net: Utrecht, The Netherlands, 2011; Volume 1.
36. Ferdous, M.S.; Poet, R. Analysing attribute aggregation models in federated identity management. In Proceedings of the 6th International Conference on Security of Information and Networks, Aksaray, Turkey, 26–28 November 2013; pp. 181–188.
37. Haddouti, S.E.; Kettani, M.D.E.C.E. Towards an interoperable identity management framework: A comparative study. *Int. J. Comput. Sci. Issues (IJCSI)* **2015**, *12*, 98.
38. López, G.; Cánovas, Ó.; Gómez-Skarmeta, A.F.; Girao, J. A swift take on identity management. *Computer* **2009**, *42*, 5.
39. Pérez, A.; López, G.; Cánovas, Ó.; Gómez-Skarmeta, A.F. Formal description of the swift identity management framework. *Future Gener. Comput. Syst.* **2011**, *27*, 1113–1123. [[CrossRef](#)]
40. Vossaert, J.; Lapon, J.; De Decker, B.; Naessens, V. User-centric identity management using trusted modules. *Math. Comput. Model.* **2013**, *57*, 1592–1605. [[CrossRef](#)]
41. Desmet, L.; Jacobs, B.; Piessens, F.; Joosen, W. Threat modelling for web services based web applications. In *Communications and Multimedia Security*; Springer: Boston, MA, USA, 2005; pp. 131–144.
42. Myagmar, S.; Lee, A.J.; Yurcik, W. Threat modeling as a basis for security requirements. In Proceedings of the Symposium on Requirements Engineering for Information Security (SREIS), Paris, France, 29 August–2 September 2005; Volume 2005, pp. 1–8.
43. Khattak, Z.A.; Sulaiman, S.; Ab Manan, J.L. A study on threat model for federated identities in federated identity management system. In Proceedings of the 2010 International Symposium on Information Technology, Kuala Lumpur, Malaysia, 15–17 June 2010; Volume 2, pp. 618–623.
44. Abdu, N.J.; Lechner, U. A Threat Analysis Model for Identity and Access Management. In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016), Rome, Italy, 19–21 February 2016; pp. 498–502.
45. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA, 2014.

