IADIS International Journal on Computer Science and Information Systems
Vol. 4, No. 2, pp. 1-12
ISSN: 1646-3692

CONSOLIDATING FRAGMENTED IDENTITY: ATTRIBUTES AGGREGATION TO SECURE INFORMATION SYSTEMS

Ghazi Ben Ayed. *Information Systems Institute, Faculty of Business and Economics, University of Lausanne.Internef #137, Lausanne 1015, Switzerland*

ghazi.benayed@unil.ch

ABSTRACT

Modern organizations become distributed and maintain multiple identity repositories. This reality promotes spreading identity attributes across information systems and landscaping identity silos. Many security use cases require identity silos consolidation that can be set through identity aggregation. In this paper, we explain within identity management parlance and compare between attributes aggregation conceptual models: meta-centralization, virtual-centralization, and identity federation. We propose also a framework would help organizations to conduct implementation projects of attributes aggregation. A great attention should be paid simultaneously to strategic purpose, aggregation models, architectures, and implementations.

KEYWORDS

Identity aggregation project framework, meta-centralization, virtual-centralization, and identity federation.

1. INTRODUCTION

A famous ancient proverb says: “The larger the fortress, the more vigilant must be its defense”. The advent of Internet-compliant technologies and open standards are easing the extension of information systems by lowering the barriers to connecting disparate business applications both within and across corporate boundaries. Increasingly, information technology architects are asked to define end-to-end business processes that span borders to enable inter-enterprise collaborations and mass integration with partners. Therefore, the current fortress landscape becomes a puzzle of partnering enterprises that should be working hand-in-hand toward building a common defense program in order to fortify the security of critical resources available within and across information systems.

An effective identity silos consolidation through maintaining relationship between distributed attributes is considered as one of the current challenges and a critical step to secure access to information systems' assets (Benantar, 2006) and (Windley, 2005). [Merriam] defines "to consolidate" in the meaning of to strengthen and to unite. Identity attributes are rarely stored in one place but rather in diverse and various stores residing within multiple information systems (Benantar, 2006). We use the term 'silos' to convey that identity is fragmented and distributed across multiple stores and a user is in one-to-many relationship with his identities. Several use cases explain and illustrate the need of data consolidation for security purpose. We detail three of the use cases as illustrations of how identity aggregation could respond to organizations' security needs: 1) applications and services may require more attributes to authorize the user accessing resources. This is reflected in the real world as a person, who is asked to provide more than one identity proof comprising different identity information to get a customized service. For instance, a customer is asked to provide a credit card and fidelity saving card in a movie store to take advantage of DVD prices rebates. Moreover, to get into some mistrusted or restrictive environments, such as national security organizations, a visitor is asked to provide more than one identity card; 2) provisioning an employee who leaves. Consolidating employee identity attributes across information systems and synchronizing them would allow recognizing the validity of his authentication performed inside and outside the information system; 3) online reputation systems are in use to trust parties and conduct secure online business. For instance, EBay reputation mechanism unifies member's transaction feedback history to calculate community members' reputations in the form of colored and shooting stars. In addition, we need not only just a consolidation but an effective attributes because a poor administration and maintenance of duplicated, out-of-date, and low-quality identity attributes may expose enterprise assets and resources at a high risk.

(Windley, 2005) presents a list of four choices to make identity attributes aggregation a true reality. It could be trough 1) building a single central attributes store; 2) creating a meta-directory; 3) creating a virtual-directory; or 4) federate directories. We exclude the first option because it is an organizational-class directory deployable only locally and does not respond to the inter-organizational realm needs.

In the present paper, we present aggregation models: meta-centralization, virtual-centralization, and identity federation and compare between them based on a set of criteria. We also propose a framework to guide the projects of identity aggregation system implementation. The comparison and framework could help organizations to better choose the aggregation model that respond to their security needs. The remainder of the paper is organized as follows. In section 2, we define major identity and attributes concepts. In section 3, we present several use cases to detail and illustrate origins of identity silos. In section 4, we describe attributes aggregation models. In section 5, we discuss the aggregation system adoption and, in section 6, we propose aggregation project framework. We conclude in section 7.

2. IDENTITY, ATTRIBUTES, AND RELATED CONCEPTS

We use several terms and definitions that are derived from (Benantar, 2006), SAML-OASIS glossary (Hodges, 2005), Liberty Alliance Technical glossary (Hodges, 2006), and (Miyata et al., 2006). An "identity" consists of a set of "attributes". An attribute describes an entity such

as a physical trait or a network address. A "Service Provider" (SP) provides service to the user through a medium such as a portal (e.g. an online retailer, a financial institution, a government agency). An "Identity Provider" (IdP) provides identity attributes to other providers (e.g. telecommunication company) and it may act as an authentication service provider. A "provider" could refer to either SP or IdP. Specifically, Liberty Alliance and Security Assertion Markup Language (SAML) specifications point out that the providers can interact and discuss details behind authentication. "Attributes Authority" (AA) manages the identity store and provides to IdP the requested attributes in the desired format such as through an attribute assertion. "Attribute aggregation" is the ability to collect user attributes from IdP(s) and express the union to SP(s). Attribute "scheme" or "schema" represents the definition of the structure and the form of attribute held in a directory or database. "Identifier" is an attribute used for user identification within a specific domain. Finally, identity "store", "repository", and "directory" refer to any technology that could be used to store identity attributes such as the LDAP directories, databases, and files.

3. ORIGINS OF FRAGMENTED IDENTITIES

Different enterprise directories store different pieces of identities. We illustrate identity silos shaping and origins with the following seven use cases: 1) managing finance and preserving privacy. Rather than using a single credit card for shopping, most of the people prefer to use multiple credit cards to better manage finances and assure anonymity. A man buys a birthday's gift for his spouse with one of his credit cards rather than using the jointly held credit account. Therefore, each credit card issuer maintains a different set of user attributes; 2) managing attributes schema and policies restrictions. The restriction occurs when a number of identity stores do not allow write permission for several reasons, such as technical, governance and political reasons. In addition, the directory schema could be static and cannot be changed without major repercussions on the whole infrastructure. Hence, attributes would be stored only in a limited number of repositories and could not be distributed over all identity stores. We can extend this use case to point out that having identity attributes within different semantics, such as languages and cultural considerations could foster the identity fragmentation; 3) context-based nature of identity and governance issue. Each context requires a specific form of attributes to authenticate an identity holder. In the real world, a traveler is asked to provide a passport at the counter of customs or immigration and the same person, being a car driver, is asked to show his driving license to a police officer, who stopped him. For access limitation and governance needs, patient record is strictly maintained in the medical identity store and travel information in the passport issuer authority's identity store; 4) technological advent and emergence. The identity management and access control related technologies have evolved within different computing waves that range from mainframes, mid-size systems to personal computing, and from enterprise distributed network infrastructure to the internet and web. The history of computing shows that new fragmented identities are created with the emergence of each discipline; 5) business dynamics. As a consequence of corporate mergers and acquisitions over time is a complex fragmented identity infrastructure; 6) Simple authentication and access management. Often, different lines of business or divisions maintain separate identity repositories in order to easily manage users' access to different and heterogonous business applications such as CRM and HR; 7) multiple

Web subscription. Many web sites require user subscription before providing services. As a result, a growing array of online fragmented identities is maintained by the Web sites' back-ends.

4. IDENTITY ATTRIBUTES AGGREGATION

Identity silos landscape raises several issues. (Benantar, 2006) stresses that managing and maintaining identity repository separately would inhibit scalability and multiply attributes inconsistencies. More dramatically, he adds that attributes that are stored in heterogeneous stores within different formats and schemes (e.g., databases, directories, HR repository, and Web application server) would increase management difficulties. As a consequence, security manager should establish relationship between fragmented identities through identity silos consolidation. In the next sub-sections, we explain how to consolidate identities through meta-directory, virtual-directory and federated identity services.

We borrow IdP, SP, and AA federation-specific concepts to explain the meta-centralization and virtual-centralization models for the following main two reasons: 1) to explain and compare between the three models with the same parlance for convenience and clarity purposes; and 2) to highlight communication and attributes convey between providers. In the three following sub-sections, we provide high level descriptions of the three aggregation models and describe issues related to each of them.

4.1 Meta-centralization

The meta-directory defines a centralized repository that is built directly on the top of the existing systems. It also provides a unique consolidated and centralized view by unifying distributed attributes across different identity stores. In figure 1, Meta-AA represents authority that manages the meta-directory and plays the role of a middleware between SPs and AAs. Within services provider envelope, we represent different types of services by different shapes with colored borders. AA represents authority that manages the repository and provides the requested attributes to Meta-AA. However, Meta-AA manages a unique master account for all participating AAs. In this structure, a user is in one-to-many relationship with his sets of attributes in the underlying AAs. IdP manages all the identity attributes provided by AAs and Meta-AA and conveys attributes to SPs through namespace connector. (Benantar, 2006) and (Windley, 2005) point out that Meta-AA administers two main services: attributes aggregation (push up) and attributes synchronization (push down). In one hand, identity attributes aggregation process allows collecting all the attributes from different AAs and pushing them up to the central Meta-AA. Technically, a join operation is performed to copy attributes from various underlying directories that are keyed by joint points through a join-link. These links are configured separately to filter the desired attributes. In the other hand, identity attributes synchronization propagates and pushes down the changes from Meta-AA to AAs. Meta-AA maintains a master identity scheme, which comprises either all the attributes provided by AAs or only some of the attributes that were considered relevant during system configuration.

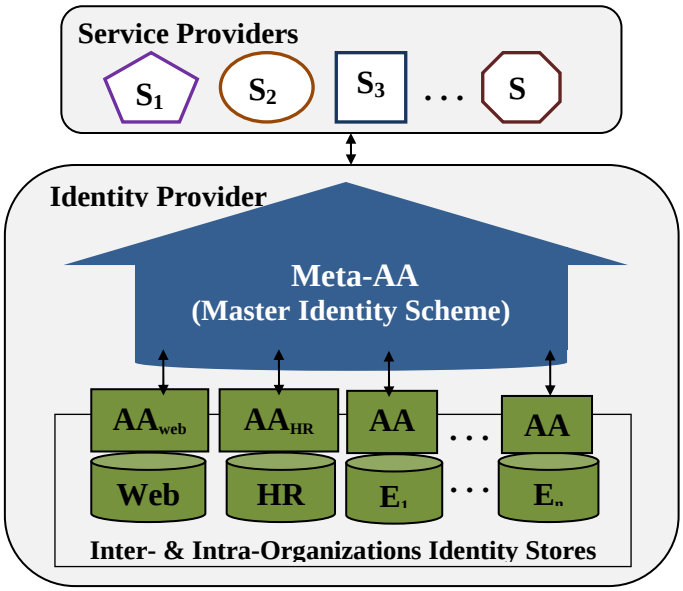

Figure 1. A high-level description of the meta-centralization model

(Benantar, 2006) suggests two ways to specify and implement the 'master identity scheme': a unified identity-representation scheme and a decoupled identity-representation scheme. In the unified scheme, master identity scheme, which is maintained by Meta-AA, encapsulates a superset of all identity attributes. Each AA may introduce attributes and contribute to master identity but AA is aware of only a subset of the common identity attributes. Multi-valued attributes on master identity scheme is allowed because the same attribute might have different values within different identity stores. Note that, attributes with no values that are assigned to them may be permitted within master identity scheme. However, a mapping may be needed to relate an attribute defined on Meta-AA to the corresponding attributes maintained by AAs. AA might have to manage new defined attributes, which might be not visible to Meta-AA and not common to other AAs, hence, a dynamic redefinition of the schema and a full reconfiguration of the meta-directory system are needed. Here, Meta-AA maintains all attributes in a unique identity vault and attributes are replicated piecewise across identity stores. Attribute retrieval operations, therefore, can be send to Meta-AA and do not require involving AAs. In the decoupled scheme, only a fixed set of attributes are maintained by Meta-AA and AA-specific attributes are not visible to Meta-AA. Adding new identity store would not impact the master identity scheme. Here, the scheme requires only one setup at the meta-directory but in the unified scheme, it requires one at the meta-directory and another at identity stores.

Data updates policies are also to be taken into consideration; If changes are allowed at Meta-AA and AAs levels, synchronization becomes complex. If the changes are allowed only at the Meta-AA level, complex authorization policy can ensure that only identity owners can modify accounts information (Windley, 2005).

4.2 Virtual-centralization

Virtual-directory participates in tightly coupled structure to create and enable a single integrated logical view of attributes within multiple directories (Benantar, 2006) and (Windley, 2005). Virtual-AA is a querying authority that manages virtual-directory and performs real-time attributes pooling from disparate trusted AAs named authoritative sources as shown in figure 2. We represent Virtual-AA in a discontinued line box to highlight the fact that virtual-directory is a logic and non-physical directory that disappears instantly when the query is completed.

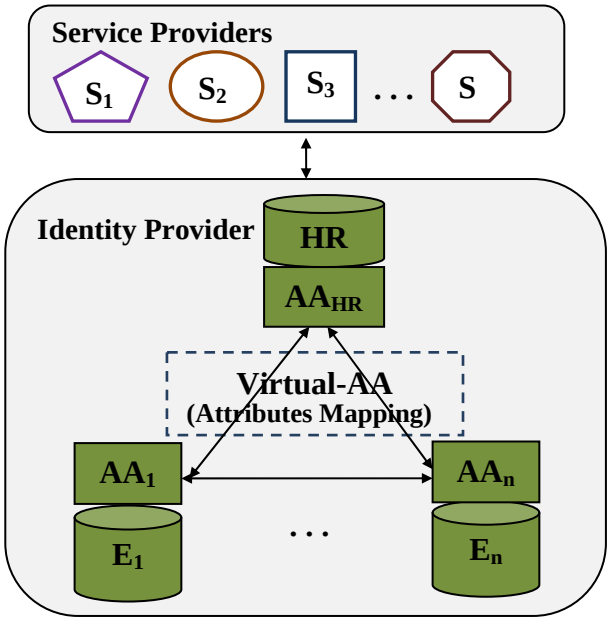

Figure 2. A high-level description of the virtual-centralization model

Attributes mapping is processed while all the identity attributes are kept intact in the underlying repositories. The main difference between Virtual-AA mapping approach and that enabled by Meta-AA is that Virtual-AA is not keeping data in a central attributes repository. A query to the virtual-directory is turned by Virtual-AA into multiple queries distributed over the participating AAs. Virtual-AA receives queries and directs them to the appropriate AAs and then the result is sent by IdP to SPs through application programming interface (API). Virtual-AA retrieves and updates attributes maintained by multiple AAs simultaneously through an initial setup of a collect operation. Virtual-AA uses one attribute as the join-key in order to match entries across different identity directories. The join-key is the name of an attribute that is used as the common link between identity stores. Mapping identity attributes across all AAs, however, creates management complexities associated with n-wise mapping issue (Benantar, 2006). Moreover, attributes updates may require synchronization across multiple directories. It is helpful to consider automated synchronization; otherwise, complexities and data errors are very likely to increase. (Windley, 2005) recommends virtual-directory use in cases where real-time access to frequently changing attributes is important.

4.3 Identity Federation

Organizations involved in identity federations establish trusted relationships with other parties to allow users and systems accessing resources available across information systems. Based on glossaries of (Hodges, 2005) and (Hodges, 2006), "federated identity" defines an agreement between the providers on a set of attributes to refer to the user. While, "identity federation" is the act of creating federated identity on behalf of the user. (Benantar, 2006) and (Windley, 2005) mention that federated identity enables controlled linkages of attributes between heterogeneous systems while attributes stay locally. Fed-AA is the software, manager, and authority that administers the exchange of AAs' attributes in a form of assertions between IdP and SPs. The exchange of assertions is represented in figure 3 by the blue-colored arrows. The same authors stressed that establishing and maintaining trust across organizations is a core of identity federation. Specifically, identity federation can only communicate trust between organizations but it cannot establish it. As a consequence, attributes may ultimately be required to adhere to a common representation scheme and semantics. The use of XML as a means of defining attributes can ease interoperability and acceptance across organizations.

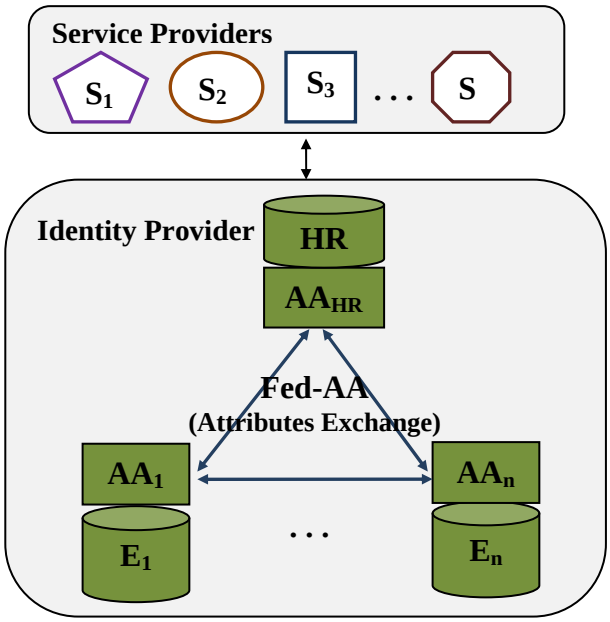

Figure 3. A high-level description of the identity federation model

Many identity federation and aggregation models are suggested in the literature. (Windley, 2005) classifies identity federation based on three patterns: 1) ad-hoc federation is established through private bilateral agreements between organizations; in 2) hub-and-spoke federation, large organizations form private federation islands; 3) identity federation network is characterized by the formation of an independent member-owned identity platform. (Benantar, 2006) presents three federation topologies categorized based on local user registration and attributes schemes: 1) local profiling topology where local attributes management and user's registration are at home organizations and other organizations would be aware of such

registration only when attributes are exchanged across them; 2) the distributed profiling topology: an organization may acquire, through additional registration, new attributes from specific organizations. Thus, identity attributes may be duplicated; 3) third party profiling scheme: a designated third party within the established federation is tasked to manage the attributes. The third party knows attributes that are common to all or to a subset of the organizations and those that are relevant to specific ones. Organizations have to establish and manage trust with only the third party, who would take care of attribute synchronization. In addition, (Klingenstein, 2007) proposes in the identity federation context three association methods that could be used for aggregation: 1) contextual association method allows multiple SAML assertions to be simultaneously propagated to providers by the same user. The attributes on assertions will be linked by a context; 2) identifier sharing method permits user identifier that is used at IdP1 to be transmitted to IdP2 through user's authentication request. If IdP2 re-authenticates the user via an identifier already knows by IdP2, the IdP1 would know that both identifiers are valid for the same user. Here IdP2 maintains user attributes. If the user is not registered at IdP2, which may need to store user attributes, it could use the identifier sent by IdP1 as an identifier in the creation of the user account locally without re-authenticating the entity; 3) identity federation method allows IdP to create a new identifier for identity that is maintained anonymously with pseudonym. Accounts may be aggregated by passing the identifier from one IdP to another by applying identifier sharing method.

5. COMPARING AGGREGATION MODELS

We present the result of comparison between meta-centralization, virtual-centralization, and identity federation based on ten factors as shown in table 1. Meta-centralization is a two-level model since it requires an additional physical store that plays the role of an identity vault. Ideally, the identity manager would have only one access point, instead of multi-directories access points, to maintain identity attributes, quickly locate, and eliminate attributes duplications. The identity vault would enforce an element of control within an organization under a single authority and unifies attributes management processes (Benantar, 2006) (Pham et al., 2007). Moreover, the vault is considered as single point of reference; whether we change directory vendors, modify system implementations, or reorganize attributes, SP still query a single source (Windley, 2005). Meta-centralization is considered with a low risk of store unreliability and data unavailability since attributes have been replicated. In the other hand, having the vault would increase risks of denial service attack and attributes exposure.

While figures 1, 2, & 3 show different types of attributes authorities and two providers, (Klingenstein, 2007) mentions identifier usage by multiple IdPs in identity federation as mentioned above in section 4.3. Each implementation and configuration of the three models has critical pre-requisites. The meta-directory requires attributes replication from all the underlying identity stores and synchronization capabilities. (Benantar, 2006) explains that unified or decoupled attributes schemes should be selected before configuring the meta-directory and places emphasis on configuration complexities of attributes updates policies. Moreover, in unified scheme, attributes ownership and governance could be a very complex issue.

Table 1. Aggregation models comparison

Factors	Meta-centralization	Virtual-centralization	Identity Federation
Storage-based levels	two levels: Meta-directory & identity stores	one level: identity stores	one level: identity stores
Admin. access points	Single	Multiple	Multiple
Risk of stores unreliability	Low	High	High
Risk of denial service attack and attributes exposure	High	Low	Low
View creation of identity infrastructure	Single	Single	No
Attributes Authorities	Meta-AA & AAs	Virtual-AA & AAs	Fed-AA & AAs
Supported IdPs	Single	Single	Single / Multiple
System critical pre-requisite	Attributes duplication, synchronization & master identity scheme setup	Authoritative sources availability	Trust communication
Attributes governance / ownership issues	High	Low	Low
Global scalability	No	No	Yes

The landscape in virtual-centralization and identity federation shows multiple administration access points and attributes distributed across multiple identity stores. The landscape would inevitably lower attributes exposure risk and governance issues but increase identity stores unavailability risks. While, virtual-centralization requires a high availability of trusted attributes stores, identity federation needs trust communication between stores. While, meta-directory and virtual-directory create a single view of identity infrastructure, identity federation does not; rather, identity stores cooperatively solve identity tasks. Virtual-directory has a better scalability property over meta-directory because it does not centrally storing identity attributes but only federated identity has the most potential of global scalability (Pham et al., 2007) (Windley, 2005). (Windley, 2005) adds that meta-centralization and third party profiling topology of identity federation cannot scale to the extent to which they can accommodate a large number of worldwide identity stores. Virtual-centralization and identity federation do not violate internal or external regulations governing identity attributes because identity attributes stay at home identity stores. Within, identity federation, local profiling topology is well suited when identity attributes are well defined and understood by other organizations; otherwise it would not offer global scalability. Distributed profiling topology (Benantar, 2006) may offer global scalability but attributes duplication may pose synchronization issue. The topology offers some flexibility in term of attributes ownership since there is a separation of concerns when managing attributes among organizations. In the third party profiling topology (Benantar, 2006), scalability issue can be a serious concern

when a very large population of organizations may contend over the single third party to retrieve and update all identity attributes.

6. IDENTITY AGGREGATION PROJECTS FRAMEWORK

We propose a tower framework as a guideline for aggregation projects. We expect that following the framework would reduce implementation dangers and failure risks. We decide to organize the framework steps in a tower shaped structure for three main reasons: 1) a silo is a tower shaped structure, as of wood or concrete, used for materials storage; 2) the middle-age fortress tower is used historically mainly for security and defense purpose; and 3) many traditional lighthouses that guides sailors and warns from dangers are in a shape of tours. Hence, the tower framework might warn from falling into aggregation projects failures. The logic of the framework is inspired from the four-layered OM-AM framework for security engineering (Sandhu, 2000) and the identity management framework (Vanamali, 2004). In addition, the OM-AM framework has been applied to the identity management filed by (Daeson et al., 2002). The tower framework provides four practical steps as a basis of aggregation project roadmap.

The aggregation tower framework in the figure 4 comprises four layers: 1) purpose, motivations and planning; 2) aggregation models; 3) architectures; and 4) systems and standards. (Sandhu, 2000) points out: "These layers are roughly analogous to a network protocol stack with a many-to-many relationship between successive layers and most certainly do not imply a top-down waterfall-style software engineering process". The layers are surrounded by a sea of assurance and partners' cooperation. The top of the tower, layer1, is concerned with articulating the purpose and motivations of the cross-boundaries identity attributes aggregation project. To achieve the purpose, the projects members analyze the IS-situation and figure out the SHOULD-situation in term of short and long-term objectives using a risk management approach. Layer2 focuses on the "aggregation conceptual models", which are shortened to aggregation models for simplicity and convenience purposes. (Sherwood, 2000) highlights the importance of the conceptual model usage and emphasizes work with "conceptual security model as the pre-cursor to developing technology solution". He adds that it essential to build a solution on an accurate conceptual model, otherwise risks would increase. Three conceptual models are available meta-centralization, virtual-centralization, and identity federation. To select the right conceptual model, organizations could take into considerations the set of factors listed in table 1 and many other aspects such as trade-offs, regulations, policies, constraints, attribute schemes, trust models, association methods, mapping and synchronization approaches, data updates frequency, number of partners and counter-parties, attributes residence, and attributes ownership. In some environments, regulations might influence and limit the choice of the aggregation models. For instance, a privacy protection act might dictate that medical dossier and income/insurance information must be stored in different identity repositories. Within the restriction, virtual-centralization and identity federation are better options because meta-centralization combines all the information in one physical location. Layer3 deals with architectures: a detailed study of the aggregation models would provide all details about the target system's components and the interaction between them. Layer4 is concerned with evolving standards, systems, application services, and directories that support and meet the requirement of the system architecture. The last and foundational stone represent all disparate the intra- and inter-organizations identity

directories and repositories, which could be LDAP directories, databases, flat files, or web services. The mapping between adjacent layers is many-to-many, which means the purpose can be supported by multiple aggregation models; and with a aggregation model, multiple objectives can be supported. The same mapping is also applicable for the relationships layer2-layer3 and layer3-layer4.

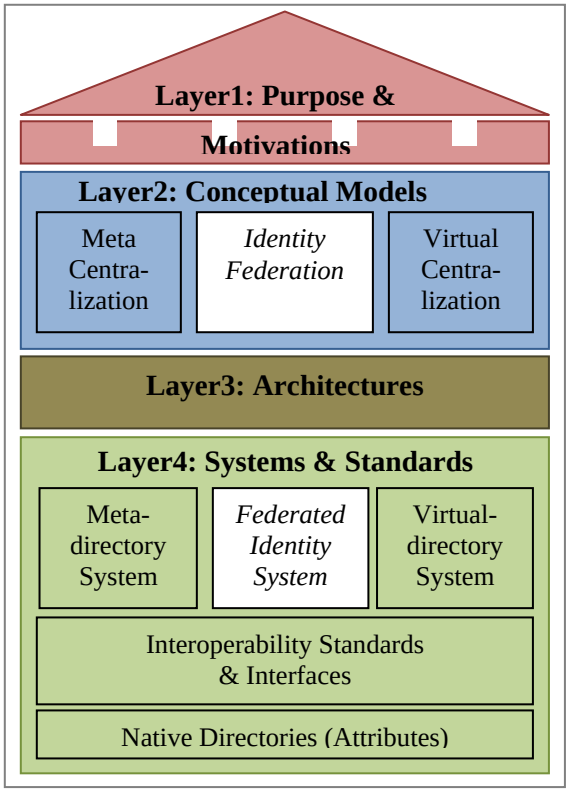

Figure 4. Identity aggregation tower framework

Each layer is composed by a set of specific activities and options that few of them are presented in layer2 and layer4. Within layer2 and in some particular cases, we may combine aggregation models but we need to have convincing reasons and clear organizational motivations. The white stones in the tower represent the level-difference between identity federation and federated identity concepts. Identity federation is a conceptual model while federated identity is a system.

In addition to technical issues, non-technical ones should be concisely resolved. A sea of partners' coordination and assurance permeates all layers in order to avoid inconstancies and mismatches. Since aggregation implies that one-party depends on the practices of another party, so it is important to work hand-in-hand with partners to agree and validate together the aggregation purpose, conceptual models, architecture and systems & standards. Note that specifying the responsibility of each party such as responding to what is required? What is expected? How liability is dealt with? What service levels are promised? and who controls what (attributes and credentials) would ease the project progress. Another aspect might be

defined is who will pay for the aggregation project costs? The tower framework presents layers as an ordered sequence, however, in practice, there is an iterative process to assure that each layer supports effectively and enforces requirements of the adjacent ones.

7. CONCLUSION

We consider identity silos consolidation important and crucial to secure information systems. In this paper, we have studied, analyzed, and compared three identity aggregation models: meta-centralization, virtual-centralization, and identity federation. We have shown that attributes aggregation models could respond to the need of identity consolidation but each model has its own benefits and limitations. Non-technical issues that face identity aggregation projects should be weighted as important as technical issues. We encourage specifying the vision and purpose with partners and understanding together business requirements such as policies, regulations, trust, and dependencies. Identity conceptual models are to be chosen to meet the strategic needs. When starting aggregation projects, we suggest using aggregation tower framework and encourage commitment to partner's coordination efforts and validation process within time and budget limits.

REFERENCES

Book

Benantar, M., 2006. *Access Control Systems: Security, Identity Management and Trust Models*, Springer, USA.

Windley, P.J., 2005. *Digital Identity: Unmaking Management Architecture (IMA)*, O'Reilly Media, USA.

Journal

Miyata, T.et al., 2006. *A Survey on Identity Management Protocols and Standards, Oxford Journals: IEICE Transactions on Information and Systems*, Vol. E89-D, No.1, pp.112-123.

Pham, Q., et al., 2007. Consistency of User Attribute in Federated Systems, *LNCS Springer-Verlag Journal*, Vol. 4657.

Sherwood, J., 2000. Opening Up the Enterprise, *Computers & Security Journal*, Vol. 19, No. 8, pp.710-719.

Shim, S.S.Y. et al., 2005. Federated Identity Management. *IEEE Society's Computer Magazine*, Vol.38, No.12.

Vanamali, S., 2004. Identity Management Framework, *Information Systems Control Journal*, Vol.4.

Conference paper or contributed volume

Daeson, C. et al., 2002, An Information Security Model for the Next Generation Application Service. *Proceedings of the 2nd International Workshop for Asia Public Key Infrastructure.* Taipei, Taiwan.

Hodges, J., 2005, Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0. *OASIS*.

Hodges, J., 2006, Liberty Technical Glossary. *Liberty Alliance Project*.

Klingenstein, N., 2007, Attribute Aggregation and Federated Identity. *Proceedings of the IEEE International Symposium on Applications and the Internet: Workshop on Middleware Architecture in the Internet*.

Sandhu, R., 2000, Engineering Authority and Trust in Cyberspace: The OM-AM and RABC Way. *Proceedings of 5th ACM Workshop on RBAC.* pp.111-119.