OFELIA – A Secure Mobile Attribute Aggregation Infrastructure for User-Centric Identity Management

Alexandre Augusto, Manuel Correia

OFELIA - A secure mobile attribute aggregation infrastructure for user-centric identity management

Alexandre B. Augusto, Manuel E. Correia
aaugusto@dcc.fc.up.pt , mcc@dcc.fc.up.pt

Center for Research in Advanced Computing Systems (CRACS-INESC LA);
Department of Computer Science, Faculty of Science, University of Porto;
Portugal

Abstract. Personal mobile devices with real practical computational power and Internet connectivity are currently widespread throughout all levels of society. This is so much so that the most popular of these devices, the smart phone, in all its varied ubiquitous manifestations is nowadays the de facto personal mobile computing platform, be it for civil or even military applications. In parallel with these developments, Internet application providers like Google and Facebook are developing and deploying an ever increasing set of personal services that are being aggregated and structured over personal user accounts were an ever increasing set of personal private sensitive attributes is being *massively aggregated*. In this paper we describe OFELIA (Open Federated Environment for Leveraging of Identity and Authorization), a framework for user centric identity management that provides an identity/authorization versatile infrastructure that does not depend upon the massive aggregation of users identity attributes to offer a versatile set of identity services. In OFELIA personal attributes are distributed among and protected by several otherwise unrelated AAs (Attribute Authorities). Only the user mobile device knows how to aggregate these scattered AAs identity attributes back into some useful identifiable entity identity. Moreover by recurring to an IdB (Identity Broker), acting as a privacy enhancing blind caching-proxy, in OFELIA the identity attributes location in the Internet is hidden from the RP/SP (Relying Party, Service Provider) that wants to have temporary access to the users personal data. The mobile device thus becomes the means by which the user can asynchronously exercise discretionary access control over their most sensitive dynamic identity attributes in a simple but highly transparent way.

Keywords: Secure Digital Identity management, User centricity, Mobile Identity Wallet, XMPP, OpenID Connect, Attribute aggregation, Access control

1 Introduction

Due to the massive organic growth of the Internet, with its unaccountable number of unrelated services, users personal data is currently completely scattered

all over the network. This is the direct result of the current need to create different user accounts (identity personas[1]) for the numerous Internet services that are being run by different operators. However this fragmentation of identity data can in some way be seen as a positive feature, because this means that no single system is capable of completely identifying a person identity attributes, in other words, user identity data on the Internet is naturally decentralized and this is a very useful tendency we should explore to improve upon the users privacy.

The interest on users digital identity has been increasing dramatically over the recent years due to its highly strategic commercial value for the market [21]. Internet application providers, companies like Google, Facebook and even Microsoft, are currently under a fierce competition over the hearts and minds of users for their personal data. Their main purpose is to create enormous monopolized centralized databases of user identity attributes as they allow them to produce highly accurate user profiles that they can then monetize very efficiently for marketing purposes. These global companies harvest and aggregate personal data in such a large scale that, lest it is put under some kind of control, it will very soon represent a major global threat to personal security and privacy the like of which the world has never seen.

Moreover interoperable Internet applications flourish in the presence of standardized and simple to use Identity, Authentication and Authorization services. This is manifested on the push Google, Facebook and other major players have been given lately to open identity and authorization protocols like OpenID [19] and OAuth [14]. These are employed as standardized mechanisms to build single sign-on systems and attribute sharing based on valet keys [13], which are nowadays essential to keep and follow the user navigating within the same service provider set of managed services. At the moment OpenID Connect [18] is under development, as a single solution for aggregating both Identity and Authorization into one single open standard.

However to share or give access to highly sensitive data [22] like bank accounts, electronic health record or the current geographic position to monopolized identity providers, nowadays constitutes a highly risky proposition. Once a user shares this kind of data he immediately loses control over it, not to mention that if the IdP suffers an attack, millions of highly detailed personal attributes can be immediately compromised. Personal data is also subject to change, and depending upon its nature it can quickly become stale. With a centralized and "distant" identity provider it can become quite difficult to manage the staleness of massive amounts of personal data. For these reasons we thus strongly believe that user data should be kept and managed as much as possible close to its origin by its owner, its *Authoritative Source*, and should only be made accessible with its owner explicit authorization. The disclosed data should also only be readable by the original requester, therefore a monopolized centralized intermediary Identity Provider (IdP) should not be trusted with the requested attributes. These characteristics of identity data lead us to propose the development of a fully decentralized privacy and user oriented model for identity management. The necessity for user digital data aggregation from many different authorita-

tive sources in a secure and user centric way [17] is our major motivation behind project OFELIA[1] (Open Federated Environment for the Leveraging of Identity and Authorisation).

In this project we are developing an identity infrastructure that is tackling digital identity related problems like: how much information service providers (RP/SP) and IdPs should have access to ? who should aggregate the user data? what authorizations and proofs are needed to request personal data? how a RP/SP can be sure that who provided the data is really its Authoritative Source? These are all problems we need to solve if one wants to provide a highly distributed user identity management based on the aggregation of scattered attribute authorities.

To a better comprehension of these problems and the possible solutions, we proceeded with a research about the already existing identity attribute aggregation models:

- *Identity relay[16]*: The SP trust in a single master federated IdP that is responsible to request all attributes to the SP, these attributes are returned directly to SP, in other words SP is responsible to aggregate the attributes. This model is like Identity proxying but with a reduced level of trust on master IdP.

- *Identity proxying or chaining[9]*: The service provider(SP) fully trust in a single master federated IdP that is responsible to request and aggregate all requested attributes before send it back to SP in other words the master IdP can request attributes from others IdPs that are part of its federation. This model have no control about how many IdPs will be requested to fulfill a request and was typified by myVOCS.

- *RP/SP mediated attribute aggregation[2]*: Based on SP-IdP federated model, SP redirect the user to each IdP, obliging the users a high level of interaction and is responsible to attribute aggregation.

- *Identity Federation model [3]*: Based on federated network, after user authentication a secret is generated and shared with each requested federated IdP by a user agent, the first contacted IdP provides SP the details of others IdP allowing the SP request the needed attributes. IdPs can create wrong assumptions about the attributes that others IdP issues.

- *Linking Service [5]*: In this model only the user knows about all his IdPs, a service called linking service is responsible to hold minimal information to allow SPs to obtain their queries from others IdPs. After a user authenticates, the IdP offers the possibility of attribute aggregation and if the user accept it the information to access the linking service is shared with SP, the aggregation of attributes can be done by the liking service itself or at SP.

[1] OFELIA-PTDC/EIA-EIA/104328/2008

– *Client mediated assertion [16]*: Based on an intelligent user agent that guide the user to the different IdPs, obliging the users a high level of interaction, the user agent is responsible for the attribute aggregation and the delivery to SP.

It is also currently widely accepted[4] that user centricity, in particular user authorization, is not only advisable but essential for attribute assertions to be considered reliable. Digital identity attributes should also be digitally signed by their respective Authoritative Sources and the end-user interactions related to identity management should also be kept as simple and sporadic as possible. Unfortunately there is no agreed upon final conclusion on the literature about the place where attributes should be kept aggregated. This is manifested by the high diversity of attribute aggregation models existing on the literature[4].

In this paper we propose a dynamic user centric identity attributes aggregation model with persistent user managed authorization mechanisms where the user smart-phone acts as the authorization and attribute management node in other words we intend to deploy user smart-phones as secure digital wallets with a full list of the user associated authoritative sources of his identity attributes. We strongly believe that it is essential to set the user as the unique authorization and revocation agent and the best way to materialize our vision is by employing smart phones because these devices are nowadays ubiquitous, have more then adequate processing CPU power to run modern operating systems, are being deployed with full Internet access, are accompanied by fully matured development systems and constantly follow their owners everywhere as the de facto personal mobile device.

The rest of the paper is organized as follows. In Section 2, we review the system architecture, describing each node, their functionality and how data flows between the different actors involved. In Section 4 we describe a representative usage case scenario that helps us to better understand the interplay of the different actors involved in OFELIA attributes authorizations and exchanges, its applicability and the its main advantages. In Section 5 we describe what has already been implemented, present some preliminary conclusions for the work we have developed thus far for OFELIA and delineate our plans for the immediate future.

2 Architecture

In this section we describe the main components of the OFELIA architecture and discuss the main reasons behind some of the options and compromises we had to make to realize our vision. We also take some time to describe the conceptual model for attribute aggregation and its most relevant aspects like the protocols and services we have employed to devise the OFELIA secure communication infrastructure. We are currently developing and testing four different components, one API and library components for the RP/SP, another for Attribute Authorities, an implementation for an IdB[12] and an android

OFELIA app, implementing the Digital identity Wallet authorization broker to aggregate AAs and authorize, manage and revoke access to their identity attributes. Figure 1 illustrates the relationship between the main OFELIA components and the type of communication that can occur between them in a simplified way.

In what follows we provide a more detailed description of the functional role played in OFELIA by each one of these OFELIA architectural components.

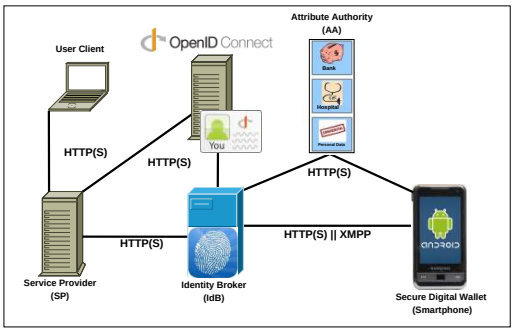


Fig. 1: OFELIA nodes relationship

2.1 OpenID Connect Identity Services

The OpenID Connect protocol is a simple identity layer built on top of the OAuth 2.0 protocol. It allows SPs to verify the identity of their end users by taking advantage of the authentication services provided by an associated OAuth service. This protocol is also capable of providing basic profile information about the end user by providing the web application developer with an identity/authentication API based on RESTful web services [18]. OpenID Connect allows users to sign into multiple different web applications with a single account, in Single Sign On (SSO) mode and at the same time control which of the user identity attributes can be shared with each one of these web applications.

In OFELIA we employ OpenID Connect as an authenticator and the provider of the OFELIA bootstrapping information required by the RP/SP to enroll into OFELIA. The essential information needed to bootstrap a RP/SP into OFELIA, for a particular user, consists of two identity attributes provided by OpenID Connect to the RP/SP, the Identity Broker Internet domain name and the user public key.

2.2 The RP/SP (Relying Party/Service Provider)

In OFELIA, a RP/SP is a web application that requires users attributes that are being managed and protected by the OFELIA identity infrastructure. We are currently developing an API and OFELIA software library components to allow for a much more simple integration of current existing web application into the OFELIA infrastructure.

Th OFELIA software for the RP/SP provides functionalities for X509 certificate management, supports OpenID Connect authentication and is capable to asynchronously request and store OFELIA user attributes. To this effect it must also be capable of managing OFELIA's authorization tokens, user identifiers, expiration dates, decryption of attribute values and recognize AA identifiers

according to the OFELIA's specifications. It must also allow for the caching of conditional authorizations tokens provided by OFELIA, which must then be presented each time the RP/SP wants to renew an access to the associated OFELIA identity attribute.

2.3 Attribute Authorities

In OFELIA, *Attribute Authorities(AAs)* are network entities responsible for the security and management of the data owner identity attributes. The user mobile phone needs to be enrolled into each one of the users AA, in order to determine which personal attributes are being held and maintained by each one of these AAs. The mobile phone can then act as an authorization broker where access for each one of these attributes can then be announced and further negotiated with each one of the participating RP/SP.

The OFELIA framework for AAs provides appropriate security mechanisms for authentication and authorization to ensure the appropriate level of access control necessary to protect these assets from unauthorized access, and provides the SPs with the means to negotiate with the IdBs and mobile phone the authorization needed to be able to access the resources being protected by each one of the user registered AA. This type of framework allows a simple and fast integration of already existing AAs into OFELIA's infrastructure.

Each participating AA must be in the possession of a public key pair whose legitimacy can be attested by a valid OFELIA's PKI X509 certificate containing the AA's OFELIA identity. The also AA stores, for each one the OFELIA user identity attributes, their respective currently valid authorization tokens and for each one these tokens their expiration dates and the related RP/SP and IdB involved in that particular user authorization.

2.4 The Identity Broker

In OFELIA, the Identity Broker(IdB) acts like a privacy enhancing blind caching-proxy for identity attributes that hides from the SP the real network location of the AA responsible for that data. We need to keep in mind the importance of catering for the situations where the RP/SP cannot be fully trusted and it is therefore important to hide the AA real network location behind a trusted IdB. Moreover for privacy and security reasons, in OFELIA the IdB does not know the content of personal attributes it is proxying because they are encrypted with the asking RP/SP public key by the custodian AA before they are delivered to the IdB to be sent to the requesting RP/SP.

In OFELIA we aim for a trusting equilibrium where the RP/SP does not need to know the location of the AAs and the IdB does not need to know the nature and value of the personal attributes he his proxying for the RP/SPs. For authentication purposes and to prevent men in the middle attacks it is mandatory for the IdB to be in the possession of a public key pair whose legitimacy can be attested by a valid OFELIA's PKI X509 certificate containing the AA's OFELIA identity.

2.5 The smart-phone as a Secure Digital Wallet

In OFELIA we are employing android smart phones as highly decentralized personal access authorization management devices for identity management, empowering the use with the creation a management of the access control policies he fins most adequate for his own personal data. This means that user does is no longer obliged to comply with the abusive identity management policies implicitly normally in place at major sites where the user is made to share or give full control of his data to network entities he does not fully know or does not fully trust, as happens with the majority of current Internet applications. OFELIA also brings some advantages in security due to the full "hidden" decentralization it imposes on the storage of identity attributes.

All mechanisms related to authorization token creation, token revocation, attribute access authorization and the enrollment into AAs and IdBs is conducted by OFELIA application installed on the smart-phone. More details about tokens authorization and AA and IdB enrollment process are discussed on 3.1 and 3.2.

The smart phone OFELIA application is the critical component of the users digital identity and should thus be always reachable over the Internet. Unfortunately this is not always possible. Network aware smart phone application are highly demanding on terms of phone battery usage and therefore cannot be always left running. In OFELIA we circumvent this problem by having the IdB to send a SMS message requesting the mobile phone to reconnect to OFELIA, every time the IdB needs to communicate with the phone but cannot reach it via the usual OFELIA channels, namely XMMP messaging. The phone has one SMS handler service installed on the phone that on receiving OFELIA reconnect SMS messages, launches the appropriate application thus reconnecting the phone back into OFELIA. After a certain period of inactivity the OFELIA application terminate to save on phone battery.

2.6 The XMPP messaging protocol

The XMPP messaging protocol is an open technology for real-time communication that uses the eXtensible Markup Language (XML) as a base format for exchanging information encapsulated into small pieces of XML [20]. XMPP provides a complete standard set of services like authentication, asynchronous one-to-one messaging and other very useful messaging oriented services[7].

Arguably, in the cellular mobile world an implicit direct Internet communication with a personal device is generally not possible due to the shortage of public IPs addresses faced by Internet service providers. In the near future, IPv6 is supposed to have solved this problem, however we believe that the mobile Telecommunications operators (Mobicomms) will not allow for directly addressable mobile devices from the Internet due to their less flexible business plans and business culture that regards the mobile devices, smart phones in particular, as a strict consumer device, not as a provider of services. Towards this end, XMPP messaging is proving to be an almost ideal communication infrastructure for OFELIA to circumvent these communication restrictions because of its ability to

efficiently operate over HTTP by the means of the BOSH(Bidirectional-streams Over Synchronous HTTP)[15] protocol where two non directly addressable devices, located on private closed intranets and with minimal Internet access, can locate each other over the Internet and then freely exchange messages between themselves in a reliable and safe way.

2.7 OFELIA secure access authorization tokens

An OFELIA authorization token can be seen as something that the RP/SP has, that gives temporary access to some identity attribute and can be easily validated by an AA. The tokens are also very hard to falsify and take the form of a small base64 encoded XML excerpt, containing elements for a large pseudo-random number[6], and a simple statement describing the authorization validity restrictions applying to this particular authorization. This statement can express for example temporal restrictions. This XML is then digitally signed by the users phone OFELIA private key and the resulting XML document is then encoded into a base64 string which constitutes the OFELIA authorization token. The token is then installed by the phone into the AA responsible for the requested identity attribute. A copy is also sent by the phone to the IdB that then forwards it to the requesting RP/SP. These authorization tokens provide a more flexible security mechanism for smart-phone users to provide RP/SPs with a restricted more controlled access to their AAs identity attributes without having to share more permanent and hard to manage credentials.

2.8 The OFELIA TRUST infrastructure

One of the critical components of OFELIA is the management of trust among the participating components. This role is played by a PKI infrastructure responsible for the management of the security certificates that constitute the core of the privacy, trust and authentication infrastructure we need to put in place to secure the OFELIA architecture.

To establish a stronger and therefore more trustworthy identity/authentication between the different OFELIA actors, RP/SP, AAs, IdBs and the personal smart phone, we rely on the existence of a standard compliant PKI that signs the X509 certificates we employ as id wallets for each one the OFELIA participating actors. Due to to the critical role played by the personal smart phone, that acts as the core authorization broker, in OFELIA we are taking advantage[8] of micro-SD mobile security cards[10] to better protect the mobile private keys associated with X509 certificates issued by the OFELIA PKI to the mobile devices. The smart phone OFELIA X509 certificate can also be doubly signed by the government issued electronic identity (eID) smart-card of the user's country to further ascertain his real civil identity.

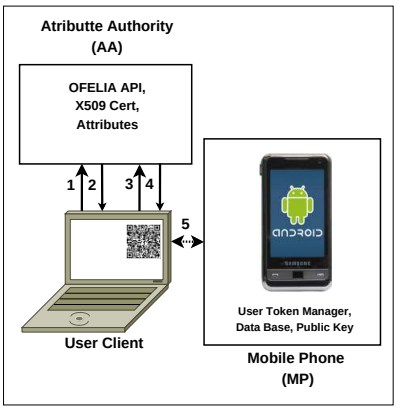
3 Entities enrollment and communication schemes

In OFELIA the mobile device must be enrolled into the each one of the aggregated AAs and into the IdB. The mobile device enrollment into each one of the user Attribute Authorities constitutes the main attribute aggregation mechanism employed by OFELIA. The mobile phone must also enroll into the IdB so it can then be announce and manage the list of attributes names and respective types that can then be made available to the requesting RP/SPs. These are maintained within the AAs aggregation sets that are being controlled by the user mobile device. This list is dynamic and must thus be updated each time the mobile phone is enrolled or unrolled from an AA, thus increasing or decreasing the number of attributes announced by the IdB for that particular digital identity that is being managed by the user mobile device

3.1 Attribute Authority enrollment

The enrolment process should be as painless and automatic as possible for the users, and for that we can rely on the services provided by the OFELIAs AA framework infrastructure (already mentioned on subsection:2.3) and QR-codes[11].

In the OFELIA's AA framework, after being authenticated, the user is provided with the option to link his digital wallet (mobile phone). The set of parameters that must be provided to the mobile phone to achieve this linkage can be transmitted by the means of a web session screen QR-code that provides the mobile device with the necessary URL locations, the AA X509 certificate and the access token needed to officialise this connection in a secure way. To link his mobile device (digital wallet) into the AA, the user employs his OFELIA mobile application to scans the AA web session QR-code that provides the application with all the parameters it needs to conclude the enrolment process. Figure 2 illustrates this process and provides for a more detailed explanation of the AA enrolment process.



1. User requests authorization by sending the necessary credential.
2. AA Answers by granting authorization if credential are accepted.
3. User request a full access token.
4. AA answers with an access token and the AA information encrypted with the users public key, aggregated and encoded as a QR code.
5. The User uses a QR code scanner to register the AA on his digital wallet(mobile phone).

Fig. 2: AA enrollment flow

3.2 Identity broker enrollment

In order to establish an OFELIA authorization flow the user must have his mobile device (aggregating digital wallet) enrolled into the OFELIA IdB.

A similar process happens with the enrollment into the IdB as has already been described for the enrollment into an AA. The user logins/authenticates into the IdB by OpenID Connect which provides the IdB with the XMPP identity and the public key of the mobile device. The user is then presented at his PC screen with a QR-code that can then be scanned by the mobile device and contains the information the smart phone needs to automatically enroll into the IdB, again via the appropriate invocation of enrollment web-services made available by the IdB, and be thus semi-automatically associated with the user OpenID identity. The IdB also provides the user with a web interface where he can list a history of the RP/SP attribute requests that have been made for that particular OFELIA identity, the enrollment process ends after the mobile OFELIA application sends an attribute name list of all attributes linked on mobile. This list is classified into generic groups like: Banks, Hospitals, Sports and etc. This enrollment process is illustrated on figure 3.

After the enrollment process has been completed, the user interacts with the mobile OFELIA application to decide upon and determine the restrictions that should be associated with each access requests being made by RP/SP web applications. He can also use the OFELIA application to revoke previously given and still valid authorizations.

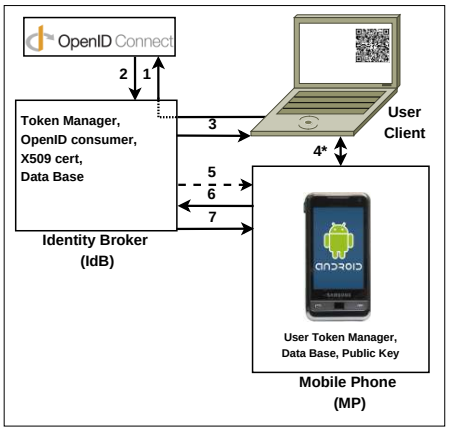


Fig.3: IdB enrollment flow

1. User authenticates at IdB via Openid Connect allowing IdB to request users jabber Id and public key.
2. Openid Connect answers to IdB with the requested data.
3. IdB sends back to user browser a Q-R code holding IdB information: Certificate, users identification and IdB addresses (jabber and web).
4. User using a Q-R code reader pre-register the IdB on his digital wallet. (mobile phone)
5. IdB sends via XMPP a signed challenge encrypted with user mobile public key.
6. Mobile phone answers the challenge to IdB and send the list of attribute names holden by itself.
7. IdB confirms the registration.

3.3 Service provider enrollment

Every time the user decides to use a new SP an enrollment process is trigged in order to allow data exchange. This process is a bit longer than the others since all nodes have to act.

The user logins/authenticates into the SP by his OpenID Connect account which provides the IdB link, then the user is redirected to the IdB with a generic request list from the SP, now the user has to interact and decides the attributes he will give access based on the SPs generic list. After authorization is given, the IdB sends via XMPP a request to confirm the authorization to the mobile OFELIA APP that must be confirmed by the user mobile thus triggering an authorization token creation phase. Now the mobile OFELIA APP has to create signed access tokens for the respective requested AAs, sending the tokens to them and to the SP by using the IdB, in other words encrypting the tokens with SP certificate and requesting IdB to delivery it. This scenario is exemplified on figure 4.

Now the SP can request attributes from IdB until authorization given by the user is valid.

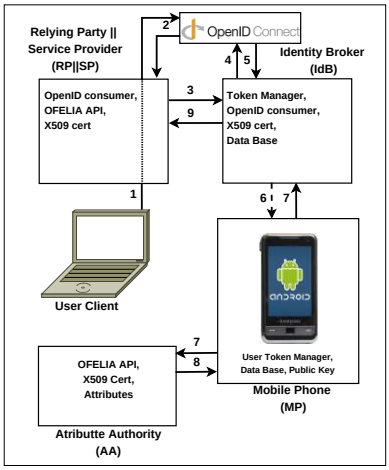


Fig.4: RP/SP enrollment flow

1. User authenticates itself at RP via Openid Connect allowing RP to request users public key and IdB address.
2. Openid Connect answers to RP with the requested data.
3. RP requests a registration to the IdB providing his certificate, OpenID request link and a details of the service with a list of requested data cyphered with user public key.
4. IdB tries the OpenID request link.
5. If the answer is a reply attack tentative the IdB will preregister the RP generating a identifier token.
6. IdB sends via XMPP to the MP a signed request message with the encrypted data request plus RP details(identifier token, certificate, details of service and address).
7. If the user authorizes, an access token is generated and sent to IdB encrypted with RP public key and to AA with RP details
8. IdB validate RP registration and send to RP the encrypted access token.

4 Usage case Scenario

For a credible illustrative OFELIA aggregation scenario imagine a chain retailer supermarket acting as a SP and for example a credit card and gas company acting as AAs. Now lets assume the user is online shopping at the chain retailer and upon completion of his purchase, if he can prove that he has a specific credit card and is a regular customer of a certain gas company, the chain retailer gives him an immediate special discount on car accessories.

At the moment of purchase after with user already authenticated via OpenID Connect the supermarket, acting as a SP will request the IdB for proof of credit

card membership and gas service for that already logged particular user. This triggers an authorization request made by the IdB that is displayed at the user mobile phone, to authorize the relevant AAs to disclose this information. On the user discretion, he then uses his mobile phone to authorize both AAs to emit a certification (signed by the AAs public certificates). These authorizations take the form of digitally signed authorization tokens that are registered on the respective AAs and delivered to the IdB but encrypted to the SP with an entropy salt, that then sends them to the asking chain retailer SP.

The SP, now in possession of these digitally signed tokens, can then present them to the IdB encrypted to the AA plus the salt each time he wants to get evidence the user is still a valid customer of the credit card and gas company. These tokens together with the consultation requests are then signed and relayed by the IdB into the appropriate AAs, which upon analyzing the validity of the accompanying authorization tokens deliver the requesting information back plus a new entropy salt to the IdB, digitally signed by the AAs and encrypted to the SP. The encryption step is important because for privacy and security reasons the IdB should not know the value of the identity attributes, otherwise the entity responsible for the IdB would be in a position of doing massive data aggregation with their users data, and that aggregation by itself would become a much more prized target for attacks. This constitutes two of the main reasons for OFELIA to have been developed in the first place, i.e, *to provide an identity/authorization versatile infrastructure that does not depend upon the massive aggregation of users identity attributes.*

Finally the IdB relays the requested encrypted information to the SP that can verify its integrity and validity by decrypting the attributes values and verifying the validity of its digital signature letting the supermarket apply the special discount on car accessories.

5 Conclusions

Nowadays we sit at a crossroads where there is a real need for users to gain back some level control about their personal data and be given the means to only disclose their most sensitive identity attributes when they need to use a network service that really requires access to this type of sensitive data. This should also only happen for a limited period of time and be kept under strict revocation control by the data legitimate owner. OFELIA infrastructure is thus an user centric empowering infrastructure where it is possible to securely dynamically manage the aggregation of identity attributes from different Authorization Authorities into a single user centric digital identity whose authorizations can be managed in a novel versatile way involving for example temporal constraints by the arbitrage of the user mobile phone.

OFELIA also possesses innovative mechanisms to protect users privacy by preventing the massive aggregation of users data into a single place. We have taken special care to prevent the disclosure of attributes values at the IdB precisely to prevent the massive disclosure of user data lest the IdB be compromised.

In OFELIA if an attacker compromises the IdB he will not have disclosed the user attributes values that should therefore continue to remain safe in a privacy aware away.

We are currently extending OFELIA with mobile phone to mobile phone communication mechanisms parametrized by QR-codes to cater for side channel authorization requests in the case where some OFELIA user, enrolled in a SP and acting as some predefined role wants to ask to some other user, permission to access some of his OFELIA managed personal attributes.

Acknowledgments

This work is funded by the ERDF through the Programme COMPETE and by the Portuguese Government through FCT - Foundation for Science and Technology, project OFELIA ref. PTDC/EIA-EIA/104328/2008 and is being conducted with the institutional support provided by DCC/FCUP and the facilities and research environment gracefully provided by the CRACS (Center for Research in Advanced Computing Systems) research unit, an INESC LA associate of the Faculty of Science, University of Porto.

References

1. Baden, R., Bender, A., Spring, N., Bhattacharjee, B., and Starin, D. Persona: an online social network with user-defined privacy. *SIGCOMM Comput. Commun. Rev. 39* (Aug. 2009), 135–146.
2. Cantor., S. Shibboleth architecture, protocols and profiles. http://www.mediafire.com/?8bswqc4y47sqygw Verified on 13/01/2012, Sept. 2005.
3. Chadwick, D. Authorisation using attributes from multiple authorities. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2006. WET-ICE'06. 15th IEEE International Workshops on* (2006), IEEE, pp. 326–331.
4. Chadwick, D., Inman, G., and Klingenstein, N. Authorisation using attributes from multiple authorities–a study of requirements. *European Institute for E-Learning (EIfEL)* (2007), 366.
5. Chadwick, D., Inman, G., and Klingenstein, N. A conceptual model for attribute aggregation. *Future Generation Computer Systems 26*, 7 (2010), 1043–1052.
6. D. Eastlake, 3rd, J. S. S. C. Randomness recommendations for security. https://ietf.org/rfc/rfc4086.txt Verified on 14/02/2012, 2005.
7. Ed., S.-A. P. Extensible messaging and presence protocol (xmpp):core. *RFC 3920 , IETF* (July 2004).
8. for Android, P. S. Secure element evaluation kit for the android platform - the 'smartcard api'. http://tinyurl.com/seek4android Verified on 10/01/2012, 2011.
9. Gemmill, J., Robinson, J.-P., Scavo, T., and Bangalore, P. Cross-domain authorization for federated virtual organizations using the myvocs collaboration environment. *Concurr. Comput. : Pract. Exper. 21* (March 2009), 509–532.
10. GmbH, G. . D. S. F. S. Mobile security card ve 2.0. http://tinyurl.com/mobseccard Verified on 10/01/2012, 2011.
11. H., H. Reversible data hiding with histogram-based difference expansion for qr code applications. *IEEE Transactions on Consumer Electronics 57*, 2 (2011), 779–787.

12. Haaker, T., Smit, S., Vester, J., Shepherd, K., Ito, N., Guelbahar, M., and Zoric, J. Business models for networked media services. In *Proceedings of the seventh european conference on European interactive television conference* (New York, NY, USA, 2009), EuroITV '09, ACM, pp. 53–56.
13. Hammer-Lahav, E. Introducing oauth 2.0, 2010.
14. Hammer-Lahav, E. The oauth 1.0 protocol (rfc5849). http://tools.ietf.org/html/rfc5849 Verified on 14/04/2011, Apr. 2010.
15. Ian Paterson, P. S.-A. Xep-0206: Xmpp over bosh. http://bit.ly/xep0206 Verified on 14/04/2011, July 2010.
16. Inman, G., and Chadwick, D. A privacy preserving attribute aggregation model for federated identity managements systems. *Serbian Publication InfoReview joins UPENET, the Network of CEPIS Societies Journals and Magazines* (2010), 21.
17. Jsang, A., and Pope., S. User-centric identity management. *Proceedings of AusCERT 2005, Brisbane, Australia* (May 2005).
18. Nat Sakimura, John Bradley, B. d. M. M. B. J. E. J. Openid connect standard 1.0. http://tinyurl.com/openidc Verified on 13/01/2012.
19. Recordon, D., and Reed, D. Openid 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management* (New York, NY, USA, 2006), DIM '06, ACM, pp. 11–16.
20. Saint-André, P., Smith, K., and Tronçon, R. *XMPP: the definitive guide.* Definitive Guide Series. O'Reilly, 2009.
21. Schwartz, P. M. Property, Privacy, and Personal Data. *SSRN eLibrary*.
22. Song, D., and Bruza, P. Towards context sensitive information inference. *Journal of the American Society for Information Science and Technology, IETF*, 54 (2003), 321334.