Persona Concept for Privacy and Authentication

Kal Toth, (E-Mail: ktoth@cs.orst.edu), Oregon State University

Mahesh Subramanium, (E-Mail: subramma@cs.orst.edu), Oregon State University

Ike Chen, (E-Mail: chenjia@cs.orst.edu), Oregon State University

Abstract

This paper describes ongoing research and development aimed at creating a trustworthy software-based model called the Persona Concept. The "Persona Architecture" uses "web services" to implement this model and is designed to provide the consumer direct control over their identity, credentials and private data. Credentials are expressed as third-party assertions encapsulated in certificates using Secure Assertion Markup Language (SAML) and are digitally signed. The architecture also supports distributed management of electronic credentials and aims at operating across various fixed and mobile platforms including cell phones and wireless Portable Digital Assistants(PDA's).

Introduction

Although authentication systems are meant to serve both users and web service providers (WSPs), implementations have not always respected the privacy needs and rights of the individual consumer. This paper introduces a concept and strategy aimed at better serving individual e-business users. The motivation for this work comes from our observation that despite best intentions, the web offers little direct control or accountability to the consumer over their personal and private data. For example, the FBI recently exposed a major identity theft, reported in [14] and [15] where it was estimated that up to 30,000 consumer identities were stolen from a credit bureau and used to produce millions of dollars worth of fraudulent transactions.

Consumer privacy is currently in the hands of the web service providers they use. Although the branded web service providers may be trusted in most cases, they too are subject to hacking, viruses and mistakes. And there are plenty of WSPs that do not take proper care or are not aware of the privacy rights or concerns of the consumer and their obligations to protect consumer data. Therefore, the more web services a given consumer uses, the greater the exposure is likely to be.

The good news is that the power of the web has the potential of increasing control and privacy of user data. We have already seen technologies like SSL (Secure Sockets Layer) [1] and PGP (Pretty Good Privacy [2] implement security effectively on the web. However, fully deployed PKI (Public Key Infrastructure) [3] and SET (Secure Electronic Transactions) [4] have not lived up to promises or predictions – mostly to do with the complexity of deployment we think.

More recently, SSO (Single Sign-On) solutions like MS Passport [5] have been attempting to address some of the problems. And several companies have banded together recently to develop the SAML (Secure Assertion Markup Language) [6] to support an open web interoperability standard.

The Persona Concept

"Persona" has sometimes been used to represent a user's profile in cyber space. It has also been used to denote a software agent or assistant interacting with the user to provide advice while brokering web transactions [12]. Our own usage is akin to the first two examples and is not aimed at modeling an individual per the latter example. On the contrary, our Persona concept focuses on providing the user with control over her personal profile maintaining and tracking her identification, authentication, authorization, security assertions (credentials) and other privacy data.

We consider the persona to be an active software agent that encapsulates private and personal data and performs a range of authentication and personalization services on behalf of its owner. It its most broad incarnation, the persona carries out tasks ranging from user authentication and provisioning of credentials to WSPs, through to personalization and customization activities such as channel selection, user interface adaptation, auto web form filling and automated searching and bidding. In this paper we will restrict our persona discussions to authentication, credential handling and accountability mechanisms for the most part. Fig. 1 illustrates the conceptual framework for the persona.

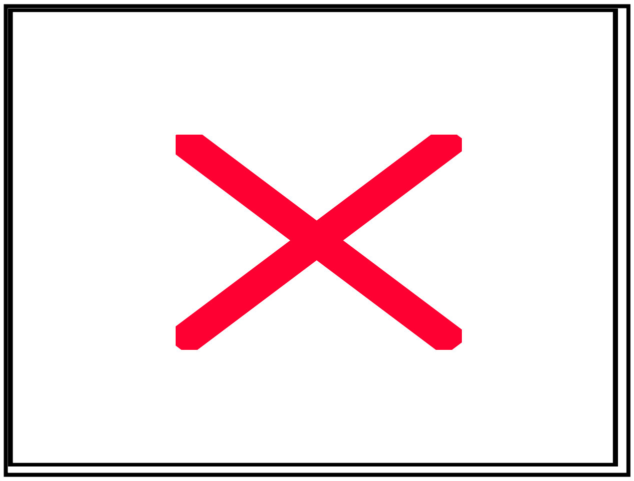


Figure 1.

Remark: The Persona will be deployed on the user's PC and replicated on his/her cell phone, PDA or on a host computer at work, at work, at the bank or on a web service provider. Such a distributed Persona will need to have its copies synchronized in a secure and efficient manner. To support off-line access, say from a site with a need to access certain persona data, adequate permissions and protection features will need to be provided. Hence the Persona will need strong tamper resistance, access controls and intrusion detection mechanisms.

An over-riding purpose of a persona is to provide direct control over its owner's personal and private data. This personal agent encapsulates personal identification, authentication, credentials and other personal data and exposes selected information to web service providers on a strictly enforced need-to-know basis. If possible, the Persona should also track where, when and what data has been left in the care of web service providers accessed by its owner. This will allow the user to keep data updated at all WSPs of concern and also support follow-up when privacy misuse and/or abuse are suspected.

Single Sign-On and MS Passport

SSO is meant to simplify web access by requiring only a single user ID and password. Kerberos [15] is perhaps the first such SSO model. It mitigates the problem of remembering many passwords and reduces the vulnerability of using the same password to access many web services.

Single sign-on systems attempt to address these problems. MS Passport [5] and the Liberty Alliance Project [7] are highly visible SSO initiatives worth tracking at this time. Instead of requiring users to establish separate identities and authentication mechanisms for every web service they may use, users register with an SSO authentication server using a single user ID and password.

Unfortunately, single sign-on does not necessarily totally solve the problem. Provided the authentication server is highly trusted and cannot be impersonated, and provided access between the user and the authentication server cannot be penetrated, SSO is indeed an improvement over poor password management by the user. However, several authors [8] and [9] have already provided sufficient evidence that MS Passport is indeed vulnerable to certain types of misuse and attack and may indeed offer a false sense of security. High-jacked sessions, masquerade, web site penetration attacks and unattended login sessions can compromise MS Passport and potentially expose all of a given user's web accounts. We understand that Microsoft has reacted to plug several of weaknesses brought to their attention so far. Microsoft received a raft of negative publicity in 2002. Some of them voiced deep concerns about the prospects of putting so much private information into the hands of a major private corporation like Microsoft.

Meanwhile, the Liberty Alliance Project [7] seems to be addressing many of the shortcomings of MS Passport while avoiding the single caretaker model. However, it introduces new concepts such as trust circles and federations that users and organizations will need to embrace for this model to gain a large following.

Public Key Technologies

For more than 10 years, public key (a.k.a. asymmetric key) technologies have made enormous positive contributions to security over the web. Most notably, SSL has become a critical mechanism for providing levels of trust that have enabled web-banking and on-line credit-card processing over the last few years. SSL is a key to enabling technology for both MS Passport and Liberty Alliance. Companies such as VeriSign, have become de facto commercial Certificate Authorities (CA), are conducting basic due diligence and providing signed digital certificates to qualifying web service companies.

PKI, and the SSL as implemented by most web browsers, is designed to support 2-way authentication. Yet most web sites support only 1-way authentication. This is most likely because of the required knowledge and relative complexity for a user to obtain a digital certificate.

Conceptual Requirements for the Persona

The Persona Concept endeavors to achieve the benefits of SSO while employing the strengths of PKI to support web authentication and management of the consumer's identify, credentials and other private data.

We have chosen to model the persona agent in object-oriented terms identifying the key use cases. We will begin with an overview of the requirements as we see them. Although we are distinguishing between mandatory and desirable requirements with "shall" and "should" respectively, this paper presents a work in progress and the identified requirements are subject to ongoing refinement and change.

Persona Data

The persona shall contain data items such as identity, passwords, certificates / credentials, user profile data, ewallet information and personal preferences.

Identity, Authentication and Authorizations

A given persona instance for a user shall contain a unique and widely accepted identifier associated with the persona owner – normally the full legal name. Aliases may be useful to support. Private authentication code(s) bound to the persona identifier, such as passwords or private keys, shall be supported. Authorizations asserting various capabilities attributed to the persona owner shall be recorded in the persona in the form of credentials. The persona shall also be capable of supporting the authentication of web services by obtaining and maintaining related authentication data such as digital certificates. The persona shall also be capable of providing the owner's profile, personalization and other authorizations and credentials to web service providers on a need-to-know basis.

Controlling Access to Persona Data

Access control rules are typically expressed in the form of a security policy. In the context of the persona, the implementation of the security policy by the persona shall mediate access to persona data by external services and users. In other words, it will decide which persona data elements to expose to given web service providers and collaborating users.

Selected credit card information may be made to be explicitly available to designated web service providers. Personal information, such as meeting times and locations, may be made available to designated collaborating users. User preferences may be made available to specific application programs (e.g. for form filling and message routing).

Multi-Channel Access Support

The persona owner shall be free to transact with any WSP or any user of its choosing on the web. The user shall be able to employ PCs, laptops, cell phones and/or PDAs at home, at work or at some other location such as an Internet café (such PCs may need access to persona data but should leave none behind.

These devices may or may not be capable of supporting all persona data and capabilities. Furthermore, there may be scenarios where persona data may not be stored on the device being used because of security and capacity reasons. Finally, to support off-line (autonomous) transactions, a user may wish to expose certain persona data to WSPs and collaborating users.

The persona should therefore be capable of providing controlled and secure access to persona data directly from a WSP or collaborating user in accordance with owner-specified access control rules.

Transaction Support

The persona shall support both on-line and off-line transactions between the persona owner and external web service providers (i.e. consumer to business) and other users (i.e. consumer to consumer).

Accountability / Transaction Logging

Ideally, the persona should be able to log all events. Due to various implementation constraints, this may not be practical. At a minimum the transaction log should be able to log the last access to any given site and accumulate a record of all persona data released to that site.

Security and Trust

As discussed above, an important objective is to be able to deploy a Persona copy on other host computers to provide redundancy and off-line asynchronous access including synchronization and update transactions for PDAs and cell phones. Persona design and supporting system architecture must therefore address the following security and trust requirements:

- tamper-proof according to trustworthiness of the host
- positively authenticate the persona instance
- prevent hijacking, masquerade and sniffing
- provide secure channels between the persona and WSPs.

Operational Requirements: Use Cases

The operational requirements can be expressed in terms of use cases where the principle actors are the persona owner, external web service providers and collaborating users. We are ignoring administrators and other possible actors at this stage.

We are also assuming that the system design will need to incorporate multiple persona copies and/or fragments to support availability and reliability requirements, off-line transactions, and transactions from cell phones and PDAs including the following:

- Create a Persona Instance
- Maintain an Instance
- On-Line (Synchronous-Pull) Access:
  - Authenticate Owner
  - Exchange Credentials
  - Exchange Other Private Data
- Deploy Instances
- Synchronize Instances
- Off-Line (Asynchronous-Push) Access
  - Authenticate Transaction
  - Exchange Other Private Data

Implementation Challenges

The Persona will be implemented in the form of an object-oriented software agent. User identity and attributes will be encapsulated and protected using encryption, an adapted form of PKI, digital signatures and access control lists. In addition, intrusion detection mechanisms will be used to detect and prevent tampering. The implementation will provide controlled access to services supporting owner maintenance (update), web authentication, copy synchronization and backup. The Persona will be designed to overcome deficiencies of current SSO and PKI architectures and will be designed for ease of deployment using web services, possibly SOAP.

Persona Distribution

It is apparent that the persona will need to be distributed to support availability, reliability, off-line operation and support for hand-held devices. This suggests that a persona-based architecture will need to be logically integrated yet physically distributed. The owner will need to be able to create and deploy persona components and as well as access and manage these components as if they were a single entity.

Hosting and Accessing Components

Given that the persona architecture will be distributed, the question of deployment of the persona components needs to be considered. Our primary objective of giving the persona owner direct control motivates one to seek out an architecture that has the potential of providing that control. The approach we are proposing is an open approach (something akin to the open software movement) based on the Simple Object Application Protocol (SOAP). SOAP provides mechanisms for easy deployment on hosts using open source tools like Apache SOAP Server.

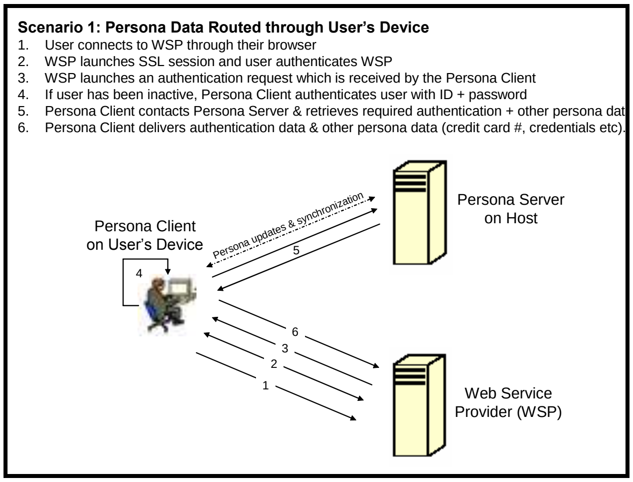
Interoperability

For the persona concept to work, it must be capable of supporting the use cases identified above. SOAP with WSDL will support transactions among persona components and between WSPs and persona components. SAML has the potential of standardizing such transactions.

Interoperability between WSPs and users will be more challenging. This will require integration with browser technologies using cookies, URL query strings or accessing the browser APIs. MS Passport, for example, uses encrypted cookies and encrypted URL query strings to co-ordinate authentication transactions.

Persona Architecture

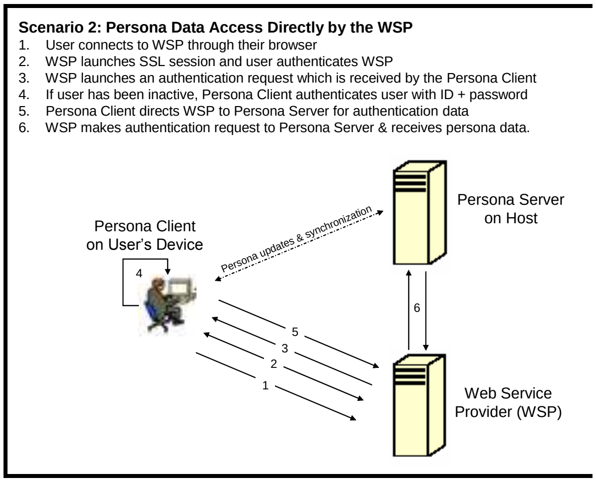
Fig. 2 & fig. 3 illustrate two scenarios currently being studied. Both of them assume that the persona is composed of two parts: a small Persona Client component on the user's device that is integrated with the browser[1]; and a Persona Server component deployed on a trusted host. These approaches may be compared to MS Passport, which accomplishes similar coordination by re-directing the user's web browser from the web server, to the authentication server, and then back to the web server again.



Scenario 1: Persona Data Routed through User's Device

1. User connects to WSP through their browser
2. WSP launches SSL session and user authenticates WSP
3. WSP launches an authentication request which is received by the Persona Client
4. If user has been inactive, Persona Client authenticates user with ID + password
5. Persona Client contacts Persona Server & retrieves required authentication + other persona dat
6. Persona Client delivers authentication data & other persona data (credit card #, credentials etc).

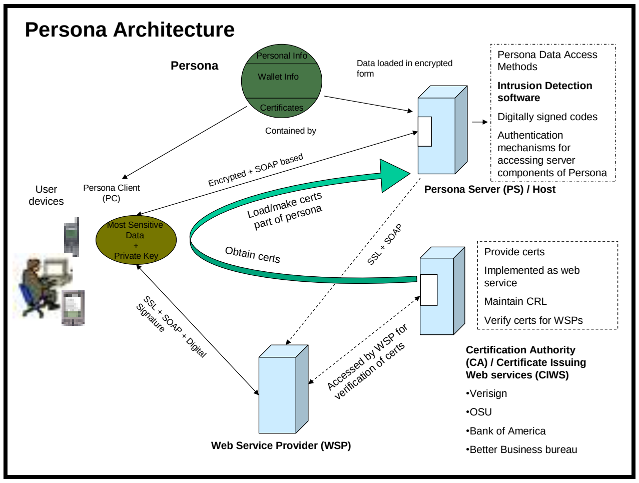
Figure 2.



Scenario 2: Persona Data Access Directly by the WSP

1. User connects to WSP through their browser
2. WSP launches SSL session and user authenticates WSP
3. WSP launches an authentication request which is received by the Persona Client
4. If user has been inactive, Persona Client authenticates user with ID + password
5. Persona Client directs WSP to Persona Server for authentication data
6. WSP makes authentication request to Persona Server & receives persona data.

Figure 3.



Persona Architecture
Persona
Personal Info
Wallet Info
Certificates
Contained by
Data loaded in encrypted form
Persona Data Access Methods
Intrusion Detection software
Digitally signed codes
Authentication mechanisms for accessing server components of Persona
Persona Server (PS) / Host
Encrypted + SOAP based
User devices
Persona Client (PC)
Most Sensitive Data + Private Key
Load/make certs part of persona
Obtain certs
SSL + SOAP
Provide certs
Implemented as web service
Maintain CRL
Verify certs for WSPs
SSL + SOAP + Digital Signature
Accessed by WSP for verification of certs
Certification Authority (CA) / Certificate Issuing Web services (CIWS)
•Verisign
•OSU
•Bank of America
•Better Business bureau
Web Service Provider (WSP)

Figure 4.

The persona system architecture also incorporates a certification authority (CA) as is illustrated in Fig. 4. In addition to the above mentioned persona services, CA services will include the ability to provide CA and user certificates in response to user requests and to create, deliver and sign digital certificates for end-users on request. Both the CA and the Persona will be hosted using SOAP services to provide open but protected access.

[1] For example, IE, Netscape, AvantGo for PDAs and HDML or WAP for cell phones.

Research Plans

The work to date has focused on persona requirements and alternative technologies, standards and models. We have conducted a preliminary investigation of existing and emerging technologies and standards and have begun to examine various usage scenarios. Our next steps will include conducting a more in-depth analysis of architectural alternatives and security mechanisms; developing prototypes of software agents; and assessing the performance and security properties of these alternatives.

Summary

The persona concept has been specifically designed to provide functions and features that will empower the consumer. The consumer's identity, credentials and other private date are stored in persona components and maintained by persona agents. Credentials are expressed as third-party assertions, encapsulated in certificates using SAML and digitally signed. The Persona Architecture uses SOAP to implement "web services" for certificate issuing, exchange and authentication among consumer devices, certificate issuers, persona agents and web service providers.

References

[1] Logan Bodia "Real World SSL Benchmarking", www.ciscoworldmagazine.com/webpapers/2002/05_rainbow.shtml

[2] Michael K. Johnson "Lurking with PGP" Linux Journal, December 1996

[3] Verisign, www.verisign.com/whitepaper/enterprise/pki/index.html

[4] William Stallings "The SET standard and E-commerce", Dr. Dobb's Journal, November 2000

[5] Microsoft, www.microsoft.com/netservices/passport/passport.asp, March 2002

[6] Documents on SAML found at OASIS website www.oasis-open.org/committees/security/#documents

[7] Liberty Alliance Specification, www.projectliberty.org

[8] David P. Kormann, Ariel D.Rubin, "Risks of the Passport Single Sign On Protocol", Computer Networks, Elsevier Science Press, Volume 33, pages 51-58, 2000.

[9] Marc Slemco, "Microsoft Passport to Trouble", http://online.securityfocus.com/library/3632

[10] The Web services (r)evolution: Part 1 Applying Web services to applications, Graham Glass Nov, 2000,www-106.ibm.com/developerworks/webservices/library/ws-peer1.html

[11] **Deploying Web services with WSDL,** Part 2: Simple Object Access Protocol (SOAP), Bilal Siddigui Mar 2002, www-106.ibm.com/developerworks/library/ws-intwsd2

[12] Junichi Suziki and Yoshikazu Yamamoto, Document Brokering with Agents: Persona Approach, JSSST WISS'98 (Workshop on Interactive Systems and Software).

[13] Clarke, R., "Computer Matching and Digital Identity", Prepared for Presentation at CFP'93, Feb. 4, 1993, www.anu..edu.au/people/Roger.Clarke/DV/CFP93.html

[14] Associated Press. "Feds Charge 3 in Massive Credit Fraud Scheme", CNN.com. November 26, 2002, http://www.cnn.com/2002/LAW/11/26/ID.theft.ap/index.html

[15] J. Leyden. "Feds Break Massive Identity Fraud", The Register, http://online.securityfocus.com/news/1718

Bibliographies

Kal Toth, Ph.D, P.Eng.

Kal Toth is an Associate Professor in Electrical Engineering and Computer Science at Oregon State University and a faculty member supporting the Oregon Master of Software Engineering. He has a Ph.D. in Computer Systems Engineering from Carleton University. His current research interests include software engineering, information security, mobile commerce and messaging, and intelligent agent based collaborative systems and personalization.

Mahesh Subramanium

Mahesh Subramanium is a graduate student at Oregon State University completing the requirements for a Master of Science degree in computer science. He has a Bachelor of Technology in Computer Engineering from Kannur University, India with research interests in information security, intelligent agents and distributed systems.

Ike Chen

Ike Chen is a graduate student at Oregon State University registered to complete a Master of Science degree in computer science. His research interests include information security, web services and distributed systems.