Persona-aware Identity Management (PIdM):

Towards a framework for managing persona identity

Sejin (Eva) Choi

Supervised by Professor Clark Thomborson

A dissertation for the partial fulfilment of Bachelor of Science Honours in Computer Science at the University of Auckland

November 2013

Abstract

User personas are fictional characters representing the goals and behaviours of a hypothesized group of users. For example, a person might have two personas: Stella Student and Tully Tutor. When she is acting as Tully, this person wants to access Cecil with her Tutor rights and she wants to access the course Facebook page. When she is acting as Stella, she wants to access Cecil with her Student rights and she wants to access her personal Facebook page.

This dissertation describes the specification and high level design of a user-centric identity management system regarding user persona. Identity management systems usually require high standard of security and privacy to be fully functional. I propose a design for a Persona-aware Identity Management System (PIdM), to make it easier and safer for Stella Student and Tully Tutor to use the same handheld devices and personal computers.

Identity management systems are traditionally built on service-oriented approach, which means that a service provider has authority to manage identities of users. Traditional approach to identity management has had adverse effects on the user experience, so identity management research has emerged with user's perspective.

To preserve usability of the user-centric identity management but enhance security and privacy, Persona aware Identity management system (PIdM) is introduced in this dissertation. A current single sing on and user-centric identity management systems are examined comparison to PIdM. We use few user scenarios to explain how Persona aware Identity management works.

The paper then presents possible implementation of persona concept through manipulation of existing methods. The benefits of inclusion of persona identification and managements in a user-centric management system are discussed. The main problem is to apply PIdM in the business model. The purpose of the paper is to improve security and privacy takes place in persona-aware identity management with user-centric perspective.

Acknowledgements

I would like to express the deepest appreciation to my supervisor, Professor Clark Thomborson, who continually and persuasively conveyed a spirit of adventure in regard to research, and an excitement in regard to teaching. Without his supervision and constant help this dissertation would not have been possible.

I would like to thank my security group members, Jason Li and Helena Ju, who demonstrated to me that concern for global affairs supported by an “engagement” in comparative literature and modern technology, should always transcend academia and provide a quest for our times.

In addition, a thank you to Jaysen Magan, who consistently gave me opinion for the research idea as a third person, and whose passion for the “underlying structures” had lasting effect.

Table of Contents

1. Introduction

An identity is a representation of an entity such as people or organisations in a specific application domain (Jøsang & Pope, 2005). For example, the personal data in online banking and characteristics as observed by the bank staff establish the identity of the customer within the bank domain. An emerging technology is the user centric identity management, where the user is able to take control on their identity with better user experience.

In the context of user-interface design, Cooper (1999) defined persona as a fictitious character that is played by a user who is goal-oriented. In other words, a persona is a portrayal of the user and what the user wants to achieve. Blomkvist (2002) offers a similar definition: “A persona is a model of a user that focuses on the individual’s goals when using an artefact.”

In this dissertation, we review current designs for identity management systems. We explore the concept of “persona” in the context of identity management. We define a “persona identity” based on behavioural analysis. We provide a specification for a novel identity management system, which we call a “persona-aware identity management system” (PIdM). We offer a high-level design of our PIdM, and we analyse this design with respect to functionality, privacy, security and usability. We conclude that our PIdM design would have similar functionality and usability to current Identity Management systems, and that our PIdM design would improve privacy and security.

2. Background: Current Identity Management Systems

This chapter begins with defining the general concept of identity management. Core element and functionalities of identity management systems are explained in Section 2.1 and 2.2. There are two types of commonly used identity management models, Single Sign On and User-centric Identity management, are explored in Section 2.3 and 2.4. Identity management systems based on those two models are reasonably functional, but there are several security and privacy flaws in managing identities. Security and privacy issues in the current systems are the main drives to introduce new type of identity management system considering user persona into identity.

2.1 Core Element of the Identity Management

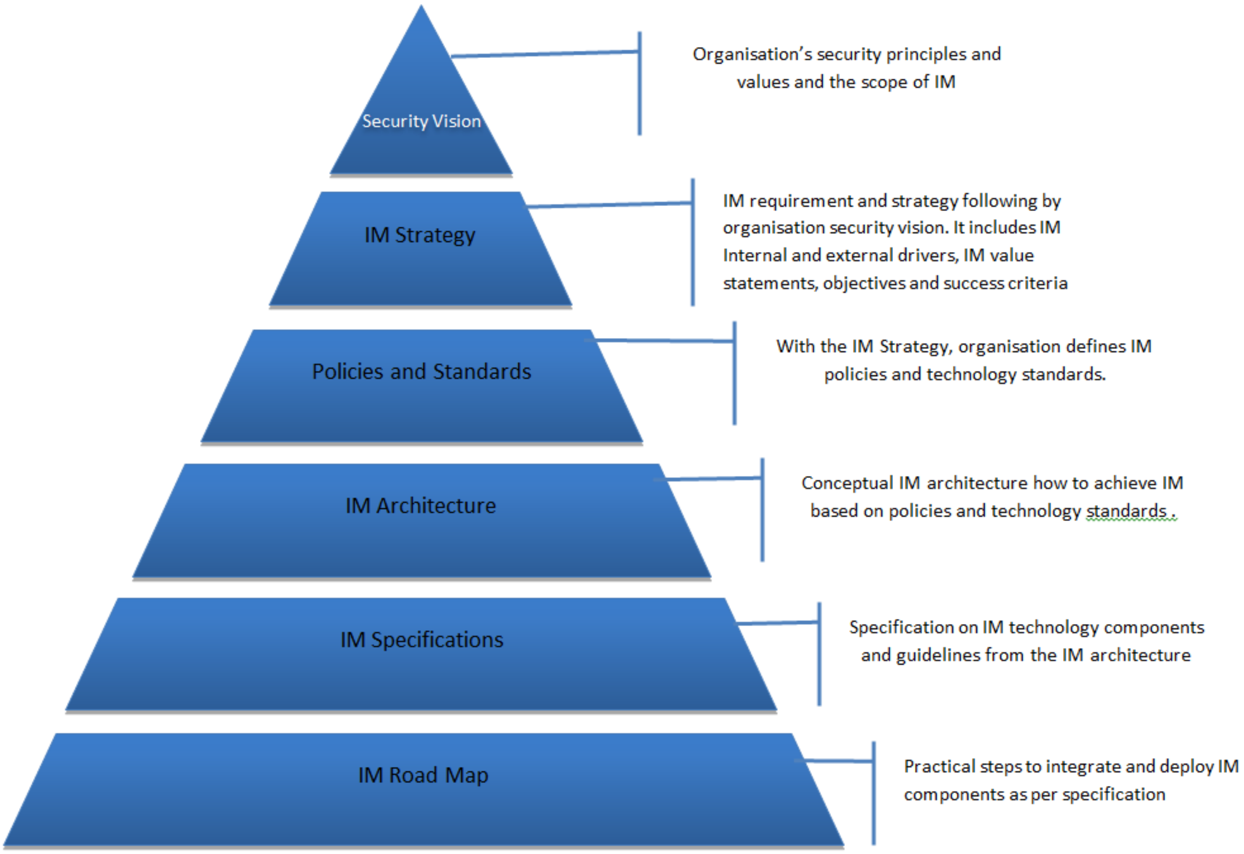
Traditional identity management systems are built to meet the organisation's need for managing and provisioning user identities under business processes. In the various business processes, all types of identities in the organisation from enrolment and retirement are dealt with identity management tool. The aim of the identity management system in the business is to integrate business processes and technology to provide high level of security and privacy in connecting user and the systems. Therefore, in service oriented identity management, the main objective is to centralise and standardise business process to make service as consistent across the organisation.

Vanamali (2004) defines the six key components of an identity management framework to combine identity management initiatives with organisation's business goals and security strategy. She lists the business goals and security strategy towards identity management as below:

- Delivering business value
- Data confidentiality and integrity
- Non-repudiation
- Authentication and authorization
- Provisioning and de-provisioning
- Audit
- Compliance and monitoring

The six key components of an identity management framework are summarised in the figure 1 in below.

Figure 1. Key Components of the Identity Management(IM) Framework


Security Vision
Organisation's security principles and values and the scope of IM
IM Strategy
IM requirement and strategy following by organisation security vision. It includes IM Internal and external drivers, IM value statements, objectives and success criteria
Policies and Standards
With the IM Strategy, organisation defines IM policies and technology standards.
IM Architecture
Conceptual IM architecture how to achieve IM based on policies and technology standards .
IM Specifications
Specification on IM technology components and guidelines from the IM architecture
IM Road Map
Practical steps to integrate and deploy IM components as per specification

Srinivasan (2004) claims that the key components of the framework are security vision, IM strategy, policies and standards, IM architecture, IM specifications and IM road map.

This dissertation is focused on the Identity management specification and architecture to improve privacy and security by adding persona into user identity.

- Identity Management Specifications:

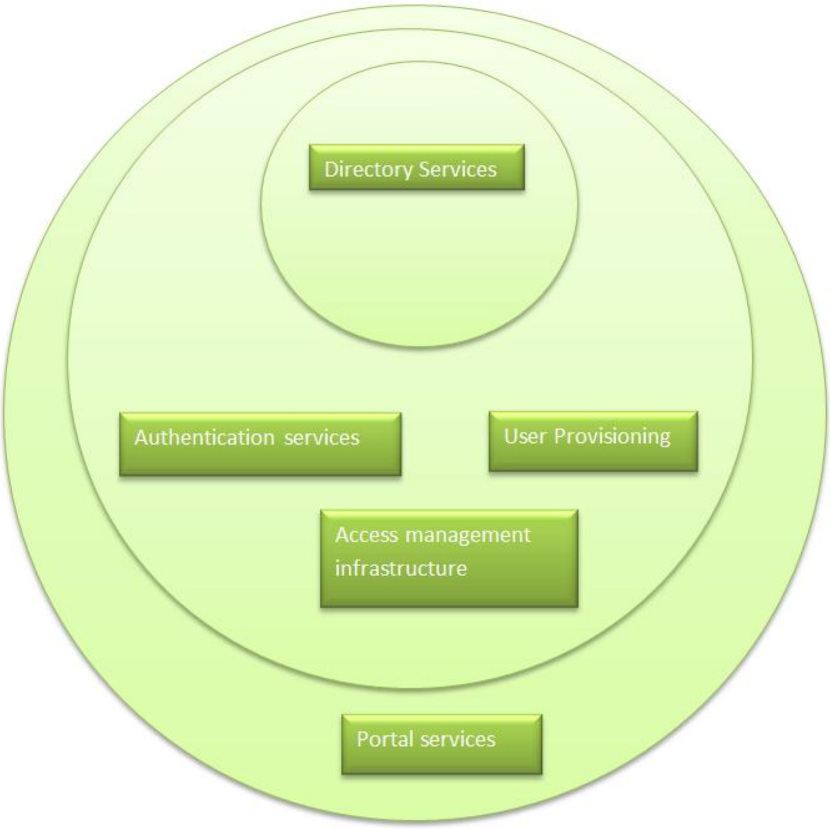
  An organisation chooses the detailed specifications guide for technology based on its required features. A key requirement is to understand how each component works and roles of components as part of the identity management framework. The specification should also cover evaluation criteria for acquiring or integrating identity management solutions, and guidelines for effective implementation.

  For example, a detailed specification for a user access control system addresses acceptance criteria to meet technical and business requirement for the solution. It also specifies the possible impact of the legacy system and existing business process and suggestion of reengineering existing system.

- Identity Management Architecture:

The architecture of the identity management must cover the design, implementation, maintenance and management of the identity management infrastructure. In order to architecture practical and manageable identity management solution, there are four identity management components to be considered as in figure 2.

Figure 2. Identity Management Components of an identity management solution



According to Srinivasan (2004), main features of identity management provide a standardised infrastructure, which includes directory services, authentication services, access management infrastructure, user management capabilities, such as user provisioning and de-provisioning, and portal services.

- Directory services reside in a name-based object model and acts as a repository for user ID and user profile information. The key roles of directory services are user authentication and enabling on-demand service delivery.
- User provisioning overview user life cycle management from enrolment to retirement of the different name-based systems. A directory service provision user with a role-based approach.
- Authentication services identify the user with various authentication methods, including digital certificates.
- Access management infrastructure is for authorisation and access control to the system based on the business policy. Access management consists of user validation,

authorisation services, and providing appropriate privileges to users to access authorised systems as well as auditing.

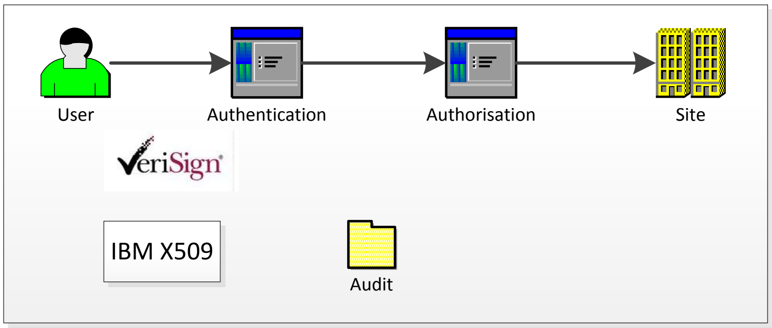
- Portal services are a user interface in a system which is personalised to the user profile. It resides in a presentation layer.

2.2 Functionalities of the Identity Management

There are various types of identity management systems addressing different aspects of identity management. Hansen (2004) classifies there are two operational areas in identity management system. Those are access management and pseudonym management.

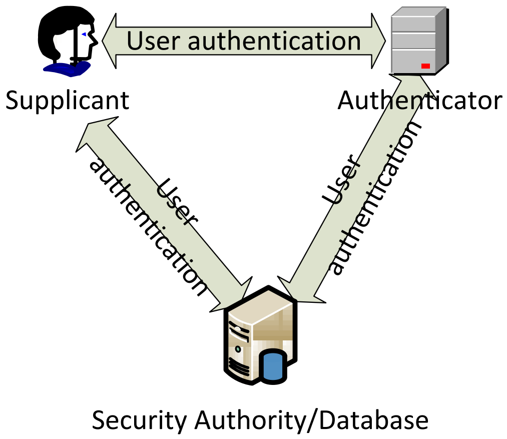
The main feature of the identity management systems is access management. It manages and controls user identity by providing authentication, authorisation and accounting (AAA). Feature 3 depicts identity management flow how the user gets access to the site.

Figure 3. Access management in identity management



- Authentication
  According to (Todorov, 2007), There are three components involved in the user authentication process.

Figure 4. Authentication system



- Supplicant: A user, client or supplicant provides its identity and requires authentication to the authenticator and security authority.
- Authenticator: An authenticator or a server provides resources to the supplicant and authorises user identity. It involves in audit on user access to resources.
- Security authority/database: A file or a server on the network which is storage to check user credentials.

- Authorisation

  Authorisation is the process of determining whether authenticated user is able to grant access information resources in a specific way (Todorov, 2007).

  For instance, when a user tries to access file in the FTP server, the authorisation process considers whether the user should be allowed to read, write, or delete the file.

- Accounting (Audit)

  Once the user is authorised to access a resource, the operating system or application needs to track user action on the resource to store historical data. It is called an audit trail. Accounting is very important for a security perspective to determine an attempt to violate system authorisation or authentication policies (Todorov, 2007).

Another feature of the identity management is pseudonym management to keep different partial identities separately, designated by pseudonyms. In the Some email clients use various pseudonyms in email addresses and signatures. Different sets of personal data bound to pseudonyms can be managed, i.e. form filling solutions like Mozilla21 or Microsoft Internet Explorer and the local proxy CookieCooker (Hansen, 2004).

Identity management system should be trustworthy. If the context or namespace of the identities to be authenticated is important, the attribute authentication should be robust.

2.3 Single Sign On

Service-oriented identity management system heavily relies on persistent data stored at the user's local machine (Alp´ar, 2011). However, a user should be able to access a Reliable Party using the identity management system from a computer in any location or from other devices.

The traditional type of identity management causes issues when the user has several identities in a single domain. Distinction in identities should manifest itself when people have different roles. For example, an accountant may use an electronic banking system either to enter personal or a business transaction. An ICT system administrator may sign in to system either as a system administrator or as an ordinary system user. Those users have different roles to do different action within a service and the impact of the actions depends on their role. In the service-oriented identity management systems, the users are forced to maintain and manage several identifies to separate these roles, and it leads to confusion. For instance, if a user has previously signed in at its Identity Provider using a particular identity through single sign-on, the user may automatically be signed in using this same identity to access a different service some time later. If the financial officer executes a personal transaction, he does not want to be signed in as financial officer of the company, because the actions performed in a certain role may be visible to others that can also access the role.

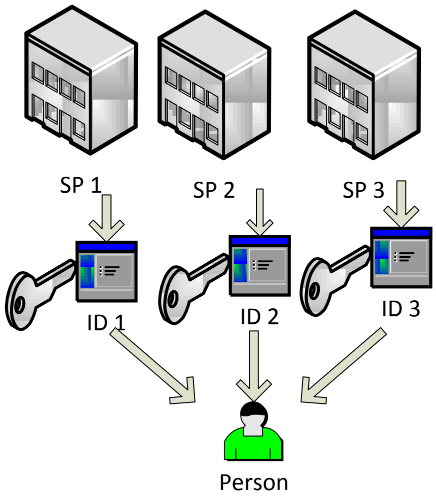
Identity management should allow users to see and select their identity even if explicitly signing in, because the user has already authenticated with an Identity Provider that is recognised by the trusted party. Asking users each time which role they want to use is not usable.

When the complex transaction requires multiple credentials, for example, in Service Oriented Architectures, where one application consists of multiple software services. The problem arises if the user needs to present credentials for more than one service, and the credentials depend on the role the user assumes. The user needs to have all the credentials required to perform the transaction, but can only present them if he logged in using the right role. In this case, the user has no means to select his role or identity for a particular session. If identity management plays a role only partially, then it could provide a way to automatically determine the full set of required credentials and the minimal role the user can assume that covers those credentials.

Single Sign-On (SSO) is unified from the Federated Identity Management (FIM) system. Federated identity management is effective in sharing resources among multiple organisations. It enables users from one organisation to access services provided for other federated organisations. A FIM system consists of a number of Identity Providers (IdPs) and Service Providers (SPs). IdPs manage their local user identities and profiles, and SPs are the services that users consume. It carries over the feature of sharing network connectivity which means a user can get network connectivity at any organisation within the federation. In SSO, users can get network connectivity and application level SSO with single time authentication.

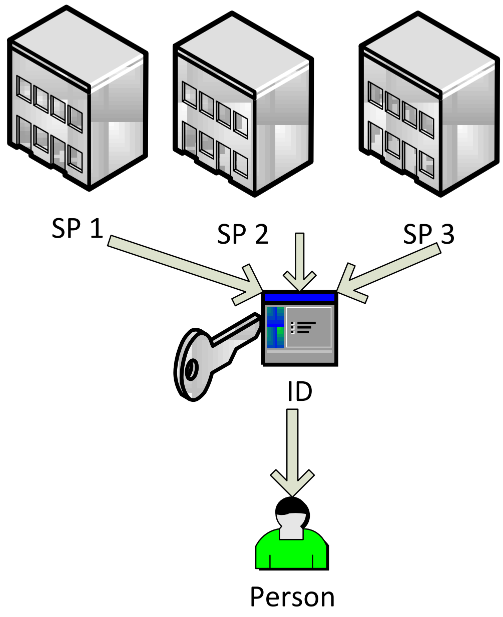
The problem of the federation of isolated identifier domains was to that users need to have multiple identities and credentials for all service providers (Jøsang & Pope, 2005) as figure 5. There are numbers of technology standards for identity federation such as the OASIS Security Assertion Markup Language(SAML) and the Liberty Alliance framework, and Shibboleth .

Figure 6 Federated Identity Management system



Single Sign On is derived to let user manage single set of identifiers and credentials as figure 6. Kerberos based authentication solutions, where the Kerberos Authentication Server acts as the centralised identifier and credential provider, are the common example of SSO.

Figure 7 Single Sign On



Microsoft .Net Passport uses email addresses adopted as user identifiers, so the credential issuance and authentication are controlled under Microsoft (Jøsang & Pope, 2005).

2.4 User-centric Identity Management

Service-oriented identity management system heavily relies on persistent data stored at the user's local machine (Alp´ar, 2011). However, a user should be able to access a Reliable Party using the identity management system from a computer in any location or from other devices.

The PIdM is based on the user-centric identity management model that is introduced by Jøsang and Pope (2005). They study identity management architecture with automation and system support at the user side in order to increase usability of an authentication. Personal authentication device (PAD) is introduced for identity management support. The idea of the PAD is derived from Personal Transaction Protocol which is a user centric security mechanism to help user to security related action remotely at a Personal Computing Device (Veijalainen et al, 2003)

An authentication solution must take into consideration how the identifiers and credentials are to be handled by the user and usability is important to let uses to handle their credentials. Users manage credentials manually while service providers usually have automated systems to manage identities and authentication.

To let users store identifiers and credentials from different service providers in a single tamper resistant hardware device which could be a smart card or some other portable personal device. This approach opens up a multitude of possibilities of improving the user experience and of strengthening the mutual authentication between users and service providers.

Signs of this type of solution are already emerging. For example, the Mozilla browser provides virtual SSO capabilities for users so they do not have to remember their usernames or passwords for web sites. A master password protects the PKCS11 security device, which can be either a software or hardware device that stores sensitive information associated with their identity, such as usernames and passwords, keys and certificates. Recent releases of Mozilla have a software-based security device, and can also use external security devices, such as smart cards, if the user's computer is configured to use them. The master password for the browser's built-in software security device protects the user's master key, which is used to encrypt sensitive information such as email passwords, web site passwords, and other sensitive data (Mozilla Project, 2004).

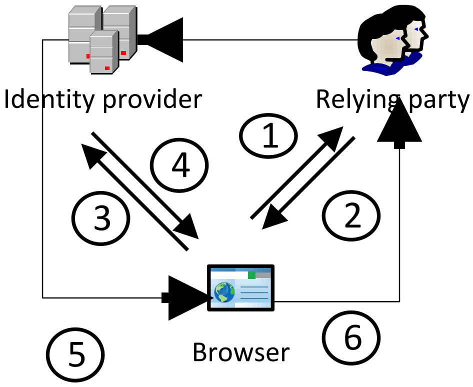
The advantages of the user-centric identity management architecture are that 1) the user only needs to remember one credential (e.g. the PAD PIN), 2) that virtual SSO is possible, and 3) that the traditional legacy identity management models can remain unchanged. The PAD should be under the control of the user and the purpose of having a single device for simplification identity management for the users.

However, to be more practical, PAD should be able to handle many types of identities and credentials and organise them to let users aware of different identities. This issue takes into consideration of modelling persona aware identity management system, Persona aware identity management system.

Good example of the user centric identity management is OpenID. OpenID is an URL based identity management protocol which enable a decentralised and open source based solution for IdM. An

OpenID-URL can be used to log on other websites (OpenID-Consumers). Account data will took just once on OpenID server.

Figure 8. Open ID identity authentication process



1. Send user's URL
2. Redirect user to get token from IP
3. Get token from IP
4. User must post Credentials to IP
5. Redirect token back to RP
6. Redirect token back to RP

According to Recordon & Reed (2006), there are two approaches of user-centric identity management architecture, which are address-based identity and card-based identity.

- Address-based identity
  It uses a unique digital address to identify the user in the context of a relationship. This digital address is dereferenced to discover various associated identity services.

- Card-based identity
  It uses a digital token that contains or references a collection of attributes or identifies the user and provides the information to achieve an identity-based transaction. For example, Microsoft's cardspace and The Higgins project is based on this approach.

3. Specification and Architecture of the Persona aware Identity Management System

The key elements of the Persona aware identity management system (PIdM) are persona identification, how to select persona of the user and link user persona with user identity, and management of generated persona identity. In this chapter, the process of identity construction and persona identity creation are explained in section 3.1. To give better understanding about persona identity, the definition of persona identity related terminologies are introduced in section 3. Section 3.3 specifies how core functionalities in identity management presented in previous chapter is applied in PIdM.

3.1 How the persona should be added to user identity

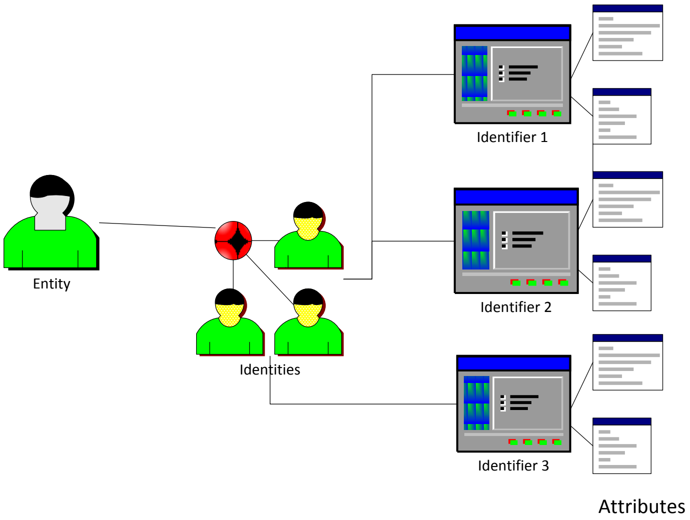
A user identity consists of attributes for the individual in current identity management systems. In PIdM, user identity is specified based on user persona as persona identity in the context of system usage.

3.1.1 How the identity is defined in existing identity management systems

An identity is constructed from an entity's set of attributes. In the real world, all identities in a given namespace must be unique and represent a specific relationship corresponding to entities and services. In general, an entity has multiple identities and each identity contains multiple attributes. This is a conceptual relationship between identities and entities.

According to Camp (2003), digital identity is "the digital representation of network entities by the individuals, communities and governments". The digital identity is categorised into three major classes, which are people, objects and organisations. Identity management is to allow a user to reliably prove certain characteristics, which are attributes.

Figure 5. Structure of digital identity



An entity is a user who wants to acquire the privileges or access to the system. It includes people, objects or organisations. An entity needs its E-format identities to grant access to the system, like User ID. Not only individual user, but a group of people may require the same access control based on their roles, such as system administrators.

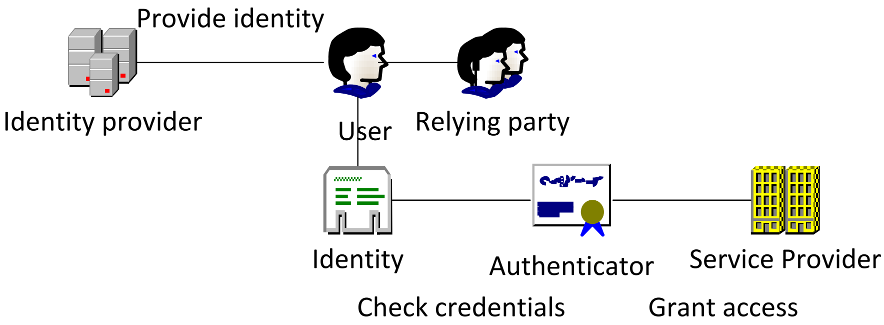
Objects can get access to the system. Object refers to the devices, such as computers, printers, and mobile phones, and each object has its unique digital identity to be assigned into the user of the system. Identifier needs to be a unique format to represent the object. A set of attributes are in the each identifiers.

Organisations establish their digital identities in a same way with objects to get the access to the system. For instance, universities, hospitals and banks need to access to the system with their own organisation digital identity.

3.1.2 How the identity is created and who creates identity

According to the system model provided by Barisch (2009), this is how the identity is created.

Figure 6. Digital identity construction

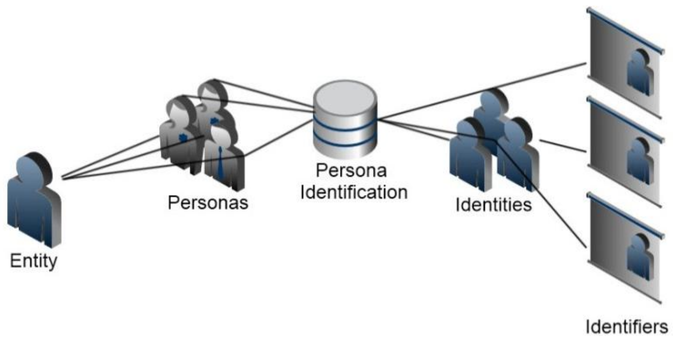


An identity provider (IP) has user accounts, and stores all attributes for these users for the account. Once the user is registered to an identity provider, an IP provides user identity. A user might have a relying party(RP) who protects access to user resource based on user credentials, which are attributes of the user identifier on business rule in the service. RP asks the IP directly to get user attributes and it asks user to sign in to the identity provider.

Service Providers offer services for attribute providers and relying parties to connect to the system. For example, a service provider may offer a relying party to do the validation of credentials in its place, and only return whether the credentials verified correctly.

3.1.3 How the persona is added into user identity

Figure 7. Persona identity consturction



Cooper (1999) develops the concept of personas at a goal directed design tool for software design. He claims that using personas in the design process helps system to deal with specific user needs. The figure explains how persona identification extracts user identities from user personae input.

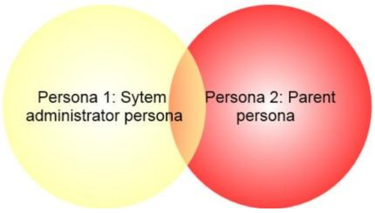
The persona identification concept is the system's feature to identify a user's persona or personae in order to process user information relating to personae. This concept of persona identification or management is incorporated as a feature in the user-centric identity management model described in section 3. A persona identification system collects list of personas detected from an entity and renders to persona identity to produce identifiers.

Identity management system store information about a user's profile such as personal preference, name, login and communication channel details and so on. Bunney(1999) explains an Internet based system with numerous user terminals that includes a Profile Manager preserving a database of user profiles. Each user has mandatory profile that is shared across different servers, and can have additional profiles for different usage. In Bunney's system, those profiles are managed dependent on a different personality for that user and each profile shows the status of invisible, busy, away or available for communication.

3.1.4 Example of the persona identity with user scenario

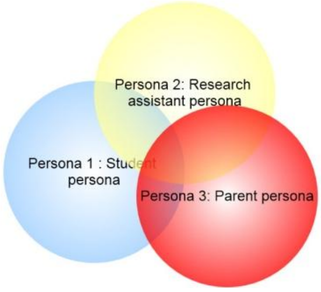
Steven is a full time system administrator and a single father of a teenage child.

- Uses work device
- Wants to control internet usage of his child while he is at work
- Wants to have better communication with his child by understanding their culture
- Sometimes uses work device as personal usage, such as online shopping, internet banking and web surfing


Persona 1: Sytem administrator persona
Persona 2: Parent persona

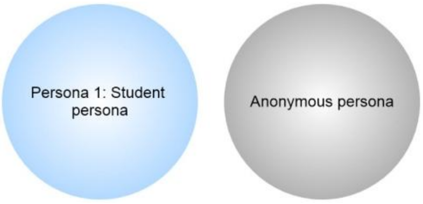
Rachael is a mother of two teenagers, a part time research assistant and a PhD student at the University of Auckland.

- Brings own device to the university
- Wants to control internet usage of her children
- Communicates regular basis with students and supervisors about her PhD research
- Spends lot of time on communication with internal staff and students regarding to her research work at university
- Often confuses the context of communication, as she involves various researches as an assistant and has own PhD research


Persona 2: Research assistant persona
Persona 1 : Student persona
Persona 3: Parent persona

Amy is a tertiary student who wants to access the system anonymously

- Has own device
- Generally access to university student system with student credential
- Wants to access to different religious group without showing her religion



3.2 Definition of "persona identity"

According to Camp(2003), Identity is defined as "a set of permanent or long-lived temporal attributes associated with an entity."

Following by Camp's definition of Identity, persona identity is defined as below.

- Persona Identity: A subset of permanent or long-lived temporal attributes which are associated with an entity, and which are relevant to a particular goal-directed context for that entity.

- Persona Identifier: Persistent identifiers consist of a set of identifiers associated with an individual's persona based on attributes. It should be unique to distinguish a distinct persona in the context of specific goal.

- Persona Attributes: A characteristics associated with an persona, such as student persona. Attributes consist with persistent value, long-lived attribute, and temporary attributes. Example of persistent attributes include for student persona is date of birth that is recorded in the system. Example of temporary attributes include for student persona is research submission id number. Example of long-lived attribute for student persona is the student is student id number

- Anonym persona: An authenticated attribute that is not liked to any of persona identifier to be used as single use. An anonymous persona identifier identifies an persona attribute ad used more than once becomes pseudonym.

- Pseudonym persona: An identifier associated with persona attributes or set of transaction by persona identity but with no permanent identifier of the persona.

3.2.1 Who provides persona identity

In PIdM, Persona provider is the one who generates persona identity and it is a user or a relying party (Hussain, 2008).

- Persona identity is uniquely identified by a user so that any persona identity belongs to at least individual.
- Persona identity can be labelled by an individual. A user can create a user persona identity whenever they need.
- An individual can generate many persona identities for different usage, or even same contexts. These persona identities belong to the same individual and may be able to track each other's behaviour if the persona identity is granted access.
- Persona identities can include attributes about the properties, rights and desires of the individuals. These are used for authentication.

- Persona identities may have shared attributes and access controls.
- Persona identification agent identifies shared persona attributes and suggests default persona attributes.

3.2.2 Restriction on persona identity

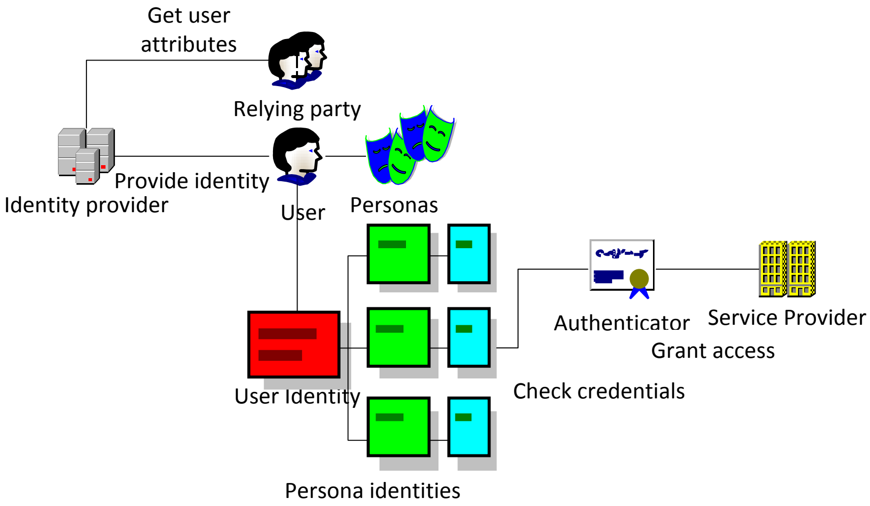
The associated attributes of a persona identifier is packaged as tokens that allow other entities to prove to themselves that the persona identifier has the attributes rather than its values.

For example, to demonstrate an individual eligible to purchase alcohol, a persona identifier does not need to have value of individual's age as an attribute, but instead true or false value that the individual's age is greater than 18.

3.2.3 How the persona identity is consumed

Persona identity is used instead of user identity in the PIdM. User identity that is provided by the identity provide exists but the user acts as a persona provider. Persona Provider generates persona identities and credentials of the persona identities are checked by the authenticator to get access to the service delivered by a service provider.

Figure 8. Persona identity management process



3.2.4 Suggesting default persona identity based on cluster analysis

Cluster analysis has been used in the market research to divide the target users into clusters, subsets defined by a set of observations, based on the similarities. In PIdM, cluster analysis is used to extract default user persona based on the questionnaire. User questionnaire is designed following a template. The attributes collected from the survey is used for defining personas.

In suggesting default personas by the persona agent, the first thing to keep in mind is to how many and which subgroups of attributes are used in creating Persona

Copper (1999) discussed the idea of using limited amount of Persona to aid the design process. He summarized the idea into a slogan 'Design for one and design for all'.

Once the user personas is defined by a clustering method, the number of clusters are determines automatically. Third, we show how our approach can be extended to cope with variation in nuisance parameters. Fourth, we provide a thorough quantitative evaluation by comparing to ground truth for a publically available persona database.

Then persona generation model is from Tu et al(2010) where the persona attribute x_{ij} from the j'th example of the i'th person's answer as a sum of signal and noise components.

$$x_{ij} = \mu + Fh_i + \epsilon_{ij} \ (1)$$

The first component μ denotes the constant attributes derived from the user identity. Fh_i represents the basic attributes for the persona which is derived from the accessible role provided by SP. Fh_i represents the identity signal that depends on the particular instance j of the given person's persona answer. ϵ_{ij} is an idealised representation of attribute for the persona.

3.3 Specification of Persona aware identity management

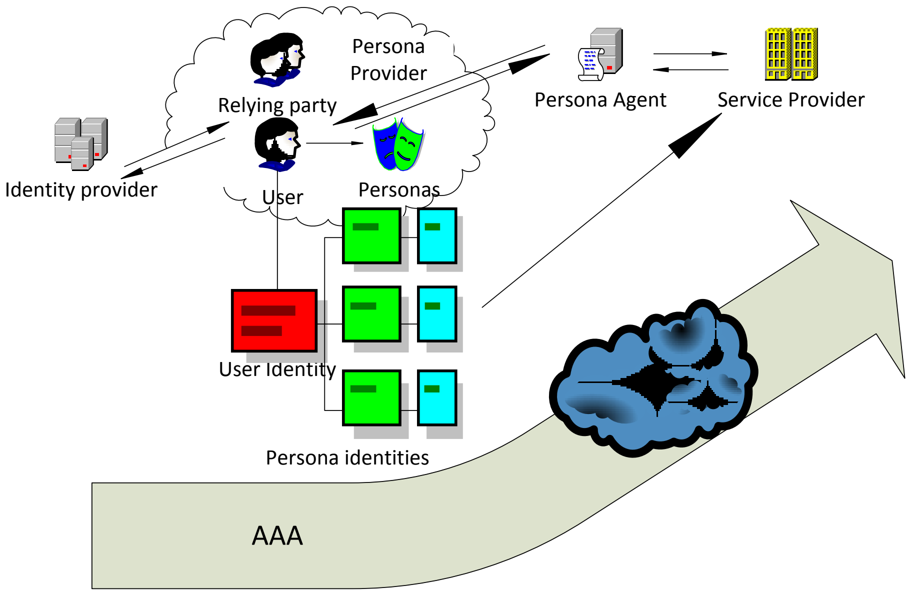
3.3.1 What is persona aware identity management

Persona aware identity management system consists of a set of user's personal information, proposed information from the persona identification module and the set of rules required for identity management.

The PIdM uses 6 components of identity management to the system for creating and using persona derived from identity management components suggested by Hussain (2008).

1. A user who wants to use personas
2. Identity providers who generates identity of the user
3. Persona provider who generates persona, and acts as guarantee that each persona belongs to real persona and has the properties representing that persona
4. Service provider who interacts with personas to provide services.
5. De-anoynimisation authorities who trace personas with the help of PP, to individuals
6. Persona agent who suggests the default persona to the user.

Figure 9. PIdM components



The figure depicts how six components act in persona identity management

The user first asks to the Identity Provider (IP) with his real identity and any relevant attributes that they want to be associated with this persona. In the context of online transaction, an attribute should be amount of credit associated with the persona.

IP takes this information and returns a user identity to the individual who asked for it, keeping a record of the identity for de-anoymisation.

Persona Agent contacts to Service Provider(SP) to get the list of accessible roles in the service. It also asks the user questionnaires to render user answers to possible personas. Once the Persona Agent detects the list of personas, it maps the persona list with the provided roles from SP to discover which persona matches the role in the service. Once the Persona Agent extracts service accessible personas, it suggests them to the user to select as default personas.

Persona Provider (PP) creates persona identities or configures persona identities based on the default personas generated from Persona Agent. It can be a user or a relying party that the user delegated. Persona identity includes a list of attributes that have been guaranteed by the PP, packaged into prevented the user identity. Once the PP is signed in as persona identity, the audit of the persona historical activities can be viewed.

Service Provider acts as other identity management systems in terms of providing service where the user wants to access resources from. The difference in PIdM is that the SP accepts persona identities configured by PP instead of a user identity.

De-anoymisation Authority (DA) tracks all persona activities in authentication, authorisation and accounting processes. The DA extracts a persona identifier which allows the government to trace to an individual if government requires. When the police needs to track online transaction fraud, they should be able to find out identity of the criminal with its persona identifier.

3.3.2 Persona identity management model in the PIdM

- **User persona identification model**

The PIdM has an ability of persona identification based on user persona identification model extended from Bunney's system. User persona identification model is a mechanism to build user persona according to personality of the user. Persona Identification in the PIdM store and identify information regarding user's personae. It process user persona to identity through a set of predefined rules which persona was in operation at which kind of web services. Persona Template has a set of predefined rules which persona is appropriate in type of web services. Rules to define persona in the persona template should be carefully designed to prevent problems with persona identification.

For example, Steven defined two personas in the system which is a personal persona and a professional persona. Persona identification checks his persona and matches with Persona Template to produce identity based on the persona. Persona Template has history of his access to the system with his system administrator role and personal account. During his work hours, all emails that are identified by the system as professional are directed to his work email account and the system will direct to personal emails to his personal account.

Persona identification feature gives user confinement user to redefine a persona within a persona. Steven can set parent persona under personal persona to monitor his child's internet usage and identity. Personal persona deals with all matters unrelated to work.

- **One persona management model**

Once user personas are processed by persona deification system as user identities, user should manage their own persona using PIdM. One persona management model is examined to manage persona aware identifiers. One persona management model applies to the user who records one persona as identity. Persona manager matches persona to identity and produces identifier. The identifier has access to the system that can be used by the predefined persona.

In this model, the persona identification can store multiple personas of the user, but the multiple persona aware identifiers cannot be processed simultaneously. Only one persona identifiers can be log in to the system and the audit of each persona is not visible to the others. If the persona is not set by user, or set by user as anonymous, the persona is identified as exception and processed in anonymous persona management which is described in next section.

PIdM adopts a one persona management model to increase privacy level to restrict access to information not relevant to the persona.

- **Anonymous persona management model**

Jøsang and Pope(2005) address that the users should be able to access system as anonymous or pseudonyms that are not linked to any user transactions in order to enhance user privacy. User-centric identity management model does not allow identity providers to view all user transactions.

UK e Envoy(2002) defined a pseudonym as a unique identifier to use an anonymous identity for privacy purposes. The pseudonyms should be self-assigned, and the pseudonym is hidden to all other parties. However, pseudonym can be delegated to a trusted third party under special circumstances (UK e Envoy, 2002).

In PIdM, once the user privileges anonymous persona, the activity of the pseudonym is hidden status. The rest of the persona identity cannot view or manage pseudonym performance. For example, Amy wants to access to online shopping site anonymously to check the original price not discounted to its customer. In this case, she can select anonymous identity in the Persona Manager to obtain pseudonym. Once she access to the online shopping site as pseudonym, the log of the activity is hidden and not recorded. In the situation where the user information should be highly protected to certain service or group, anonymous persona management model is useful. For example, if Amy does not want to show her religion in the blog set for different religious group, she can also acquire pseudonym.

- **Multiple persona management model**

In a multiple persona management model, there is no limitation on adding persona. Personas may have overlapped characteristics which shares requirement of the functionality. Therefore, persona should be interacted with other persona. A suggested theoretical framework for implementation of management of multiple personas is Bayesian network logic.

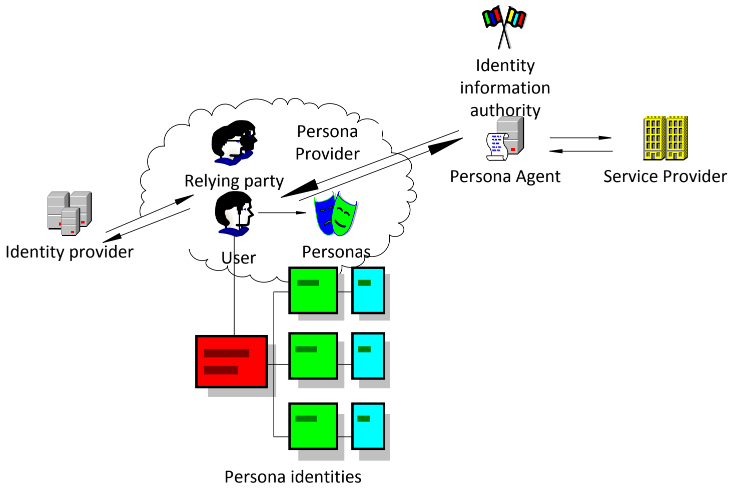
A master persona identity holds the information that required for all personas of the entity. In the same way, sub master persona identities hold information of several overlapped personas. For example, Rachael can have general persona that shares all information across research assistant persona, student persona and parent persona. She can also have researcher persona as sub master persona identity which is overlapped persona between a PhD research student persona and a research assistant persona. Persona identity may have sub persona identity as of the example of Steven.

By extension of the anonymous persona management model, it allows one way identity management where the super persona manages the child persona. The super persona can view, monitor and manage child persona but child persona cannot see any information of super persona's activity. For example, Rachael is able to monitor and manage her child's personal persona activity but her children cannot check their mother's activity.

To have better communication to the right person, multiple persona management sorts out user contacts that are related to specific persona. For example, Rachael needs to report about research progress in daily basis to her supervisors for PhD research and lecturers who she assists for research work at university. To reduce confusion of communication what research she is referring to, Persona Manager suggests the contact detail relevant to her PhD research persona.

3.3.3 Main functionalities in the persona aware identity management

Figure 10. Authentication & Authorisation in PIdM



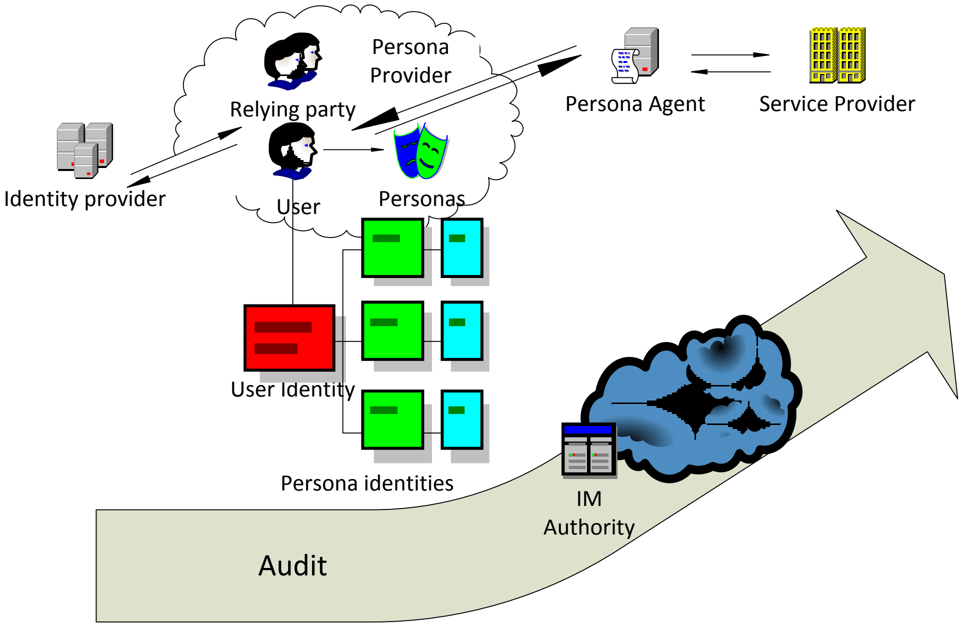
- Authentication

  Persona identity specifies required level of assurance for particular identity information and the mechanism to validation assertions. Identity information authority provides assertions on the level of assurance of the persona identity information and RP might be a third party that validates assertion. Identity information authority contacts with service provider to get the assertions and it resides in the persona agent.

- Authorisation

  As we see in the diagram, the Identity information authority in the Persona agent brings information of authentication and authorisation from the service provider and checks the credential of the user persona identity. It returns to the user whether they grant or deny information processing operations on their requested information.

- Accounting (Audit)



Identity management authority sits in the DA so that it defines persona identity actions to be logged, and incidents to for reporting. It tracks all process of persona identity management and maintains log of management actions. It also logs data access operations from identity information requests and information provisioning activities.

4. Comparative analysis of the PIdM design

4.1 Criteria for analysis

Single Sign On, User-centric identity management and Persona aware Identity management systems are designed to target different identity management. Therefore, analysing those identity management systems is significant to use in the right system.

4.1.1 Functionality

There are few properties that the Tatyana &Neumann (2008) introduced to analyse functionality in the following categories.

- End user authentication: The authentication procedure is focused on a user authentication, which connects the user and the authentication provider, and leaves the rest of authentication.

- Password-based: The authentication is based on the username and password and it has advantages of portability, mobility, and wide availability compare to other authentication method.

- Authorisation: User authentication differentiated for each service has support areas with different access restrictions. This allows for user authentication as fine grained as needed by the web application.

- Single sign-on/sign-out : It enables users to access multiple systems and datasets. It also counters logging out of the multiple systems at once.

- Accounting: Trail of the history how the identity is being used.

- Identity attributes: Identity attributes should be retrieved from the system that user accessed.

4.1.2 Security

The security requirements introduced by Suriadi et al(2009), are listed below.

- User control: User should be able to control their personal information in all operations in use of their identity. User consent must be obtained either by configuration as user prefers or per request basis. This requirement is to counter threat by providing the users with control over the information disclosed to IdPs and SPs in order to reduce the chance of misuse.

- Communication security: The communications between all interacting entities in the identity management should be secured.

- Minimal data sharing and disclosure: User's personal profile can still be shared but explicit user consent has to be obtained respecting the concept of minimum data sharing and disclosure of sensitive information. The user's sensitive information should not be shared unless it is needed. However, when it is asked, the least revealing level of data disclosure should be opted.

4.1.3 Privacy

Privacy policy relies on the trust that the IdPs and SPs will follow and enforce the agreed policy. The privacy requirements that is introduced by Suriadi et al(2009), are listed below.

- User registration: User should be able to negotiate the personal information to be registered and their disclosure level is in certain standard. A mechanism should be put to allow certification of critical information for correctness. However, to avoid having the users in a disadvantaged position whereby they have to provide certified PII all the time, there should be a provision to allow users to provide uncertified PII

- Anonymous authentication: A user should be able to be authenticated anonymously: the authenticator can verify that a user is a valid entity recognized by a trusted authority in the federation without learning the user's identity. This is to counter threat whereby the IdPs and SPs may use users' identity information for malicious purposes.

- Data storage: The storage of the user's PII should be secured from the possibility of the providers compromising the records. User's information can only be used under the collaboration with the owner of the information.

- Accountability: For transactions where accountability is important, a provider should maintain the log of the transaction activities. For privacy, the user's activities log files should be maintained. Users may perform activities that can be considered as a security breach to either the IdP or SP. In such a security breach investigation whereby the user refuses to cooperate, there should be a mechanism to allow the relevant authority to forcefully reveal the log data. If the user was anonymously authenticated, there should be a mechanism to revoke the anonymity.

4.1.4 Usability

There are three criteria to assess usability, refer to Maliki (2007).

- Password management for multiple Single Sign on: The user is able to use a single identity for multiple identity transactions

- Uniformity of identity interface: User experience increases when the user interface is consistent across the system

- Focus in context: When the user gets provided limited context that they need to be focused on, it is easier to use the system.

4.2 Analysis of SSO/UIdM/PIdM

4.2.1 Functionality

Table 1. Analysis of functionality

SSO	UIdM	PIdM	Criteria for functionality measurement
✓	✗	✓	End user authentication
✓	*	✓	Password-based
✓	*	✓	Authorisation
✓	*	*	Single Sign on and Single Sign out
✗	✗	✓	Accounting
✓	✗	✓	Identity attributes

The table 1 summaries a feature comparison of PIdM with SSO and UIdM. The result of that comparison is that PIdM is able to offer most of the features that are important in Identity management. To compare the identity management technologies in more detail, I observe OpenID and Shibboleth which represent UIdM and SSO respectively.

- End user authentication: The authentication procedure is focused on a user authentication, which connects the user and the authentication provider, and leaves the rest of authentication. The PIdM specification covers end user authentication but authentication based on the persona might not be feasible if the persona identity is not understandable to the authenticatior. OpenID does not have authentication process, as it is based on the trust between service provider and the user.

- Password-based: The PIdM authentication uses the most common method which provides username/password authentication. Each user has master username and password to select relevant persona but once the user access the system with the persona, they cannot access with other persona identifier which is not relevant to existing persona session. In OpenID, the password-based authentication is depends on the authentication provider.

- Authorisation: In UIdM, address based identity management technology does not have authorisation as it has only access value. For the card based identity management technology, authorisation is available. PIdM help user to configure their persona identity authorisation.

- Single sign-on/sign-out : Most of the UIdM technologies allow single sign on but some do not provide single sign out. PIdM allows single sign on and sign out with user persona identity. However, PIdM does not allow user to do single sign on and sign out with their user identities to access the system where persona identity granted access.

- Accounting: All service oriented systems provide audit as its aim of identity management is to control user identity management in the business. For the UIdM, user does not get audit trail of their actions. For the security purpose, it is important to make audit trail visualise to the user. To enhance security, the PIdM provides accounting to the user to track persona identity usage.

- Identity attributes: PIdM should be able to retrieve identity attributes to let user to configure and update persona identity attributes on their needs. While SSO can retrieve attributes of the user identity, UIdM cannot get those values.

4.2.2 Security

Table 2. Analysis of Security

SSO	UIdM	PIdM	Criteria for security measurement
✗	✓	✓	User Control
✓	*	✓	Communication Security
*	✗	✓	Minimal data sharing and disclosure

- User control: SSO does not have user control much, so UIdM covers the issue of lack of user control. PIdM provides full user control across persona identity management process.

- Communication security: In UIdM, there is a trust assumption that the communications between all interacting entities in the identity management is secured. However, it might not be. SSO and PIdM support this by auditing communication.

- Minimal data sharing and disclosure: Again, based on the trust assumption, UIdM does not control data sharing once the user is registered. In SSO, there is also a trust assumption that connected services must be secured, so user consent might not be available for all across the services. In PIdM, a user accesses to the system with relevant persona identity so that the unnecessary information is not provided.

4.2.3 Privacy

Table 3. Analysis of Privacy

SSO	UIdM	PIdM	
✓	✓	✓	User registration

*	×	✓	Anonymous authentication
✓	✓	✓	Data storage
✓	×	✓	Accountability

- User registration: All users in the SSO or UIdM must be registered to the system or at least provide their registration information. In PIdM, users need to be registered to do their persona identity management.

- Anonymous authentication: Some of the SSO supports anonymous authentication providing different set of identifiers not related to user. However, UIdM does not support anonymous authentication. The PIdM supports anonymous authentication in similar approach as SSO. It creates completely separate persona identity from the user identity for anonymous authentication which is not audited.

- Data storage: All three types of identity management approaches support data storage of the user information,

- Accountability: The PIdM supports accountability with Identity management authority to trail the log of actions in whole identity management process to visualise to the user. SSO does but for the business management purpose. Most of the UIdM does not support.

4.2.4 Usability

Table 3. Analysis of Usability

SSO	UIdM	PIdM	
×	✓	✓	Password management for multiple SSO
✓	✓	*	Uniformity of user interface
×	×	✓	Focus in context

- Password management for multiple Single Sign on: SSO may not provide password management for multiple SSO if the other SSOs are not connected. UIdM and PIdM provide password management for user perspective so regardless of which SSO the user accesses.

- Uniformity of identity interface: User interface is uniformed across all SSO and UIdM. There is no user interface design done for PIdM yet, but it should be uniformed across the identity management process.

- Focus in context: This is introduced by PIdM with intention that the each persona identity is focused on the goal of the user how and why they use the system.

4.3 Summary of the analysis

We conclude that our PIdM design would have similar functionality and usability to current Identity management systems, and that our PIdM design would improve privacy and security.

5. Conclusion

In this dissertation, I reviewed current designs for identity management systems. We explored the concept of "persona" in the context of identity management. I defined a "persona identity" based on cluster analysis. I provided a specification for a novel identity management system, which is called a "Persona-aware identity management system" (PIdM). I analyse this PIdM with respect to functionality, privacy, security and usability. I conclude that PIdM design would have similar functionality and usability to current Identity Management systems, and that PIdM design would improve privacy and security.

5.1 Limitations & Future works

There are two main limitation is in the PIdM.

First of all, to detect default persona of the user by cluster analysis, the survey questionnaire is critical. It is not scoped in this dissertation but it should be worked in the future.

PIdM needs to limit number of persona identities that user can create. Otherwise, the database schema will be expanded which affects serious performance issue.

In the future, market research should be conducted to find out target users and how people can accept the concept of persona in identity management. In this research, the ethical approval application was submitted to find out target users and user behaviour to each personas based on the scenario and granted conditional approval. However, there was not enough time to conduct the research.

6. References

[1] Adlin, T., Pruitt, J. Essential Persona Lifecycle: Your Guide to Building and Using Personas, edited by Tamara Adlin and John Pruitt, Morgan Kaufmann, Boston, 2010, 19-80

[2] Armando, A ; Carbone, R ; Compagna, L ; Cuellar, J ; Pellegrino, G ; Sorniotti, A. An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations. *Computers & Security*, 2013, Vol.33, pp.41-58

[3] Alp´ar, G., Hoepman, J.H., Siljee, J.: The identity crisis. Security, privacy and usability issues in identity management. Computer Research Repository (CoRR) abs/1101.0427 (2011)

[4] Barisch, M. 2009. Modelling the impact of virtual identities on communication infrastructures. In *Proceedings of the 5th ACM workshop on Digital identity management* (DIM '09). ACM, New York, NY, USA, 45-52.

[5] Blomkvist, S. The user as a personality. Using personas as a tool for design. *Proceedings of Theoretical Perspectives in Human–Computer Interaction*, IPLab, KTH, 3 September 2002.

[6] Bunney, W., *Multiple Personality Internet Account*, United States Patent, USA, Sony International (Europe), Patent Date: 26 November 2002, 1999

[7] Camp, L.J., "Digital identity," Technology and Society Magazine, IEEE , vol.23, no.3, pp.34,41, Fall 2004

[8] Cooper, A. *The inmates are running the asylum*. Indianapolis, IA: SAMS/Macmillan, 1999

[9] Dhamija, R.; Dusseault, L., "The Seven Flaws of Identity Management: Usability and Security Challenges," Security & Privacy, IEEE , vol.6, no.2, pp.24,29, March-April 2008

[10] El Maliki, T.; Seigneur, J. -M, "A Survey of User-centric Identity Management Technologies," Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on , vol., no., pp.12,17, 14-20 Oct. 2007

[11] "Federating identity for the Web; User-centric innovations CardSpace and OpenID may finally bring the promise of federation within reach." InfoWorld.com 3 Dec. 2007. General OneFile. Web. 11 Nov. 2013.

[12] Hansen, M. "Privacy-enhancing Identity Management." *Information Security Technical Report 9.1* (2004): 35-44. Print.

[13] Hussain, Mohammed, and David B. Skillicorn. "Persona-based identity management: A novel approach to privacy protection." *Proceedings of the 13th Nordic Workshop on Secure IT Systems*. 2008.

[14] Jøsang, A., Pope, S. User-Centric Identity Management. In Andrew Clark., editor, *Proceedings of AusCERT 2005*, Brisbane, Australia, May 2005.

[15] Jøsang, A., Zomai, M.A., Suriadi, S.: Usability and privacy in identity management architectures. In: ACSW Frontiers. pp. 143–152 (2007)

[16] Maliki, E. A Survey of User-centric Identity Management Technologies. *The International Conference on Emerging Security Information, Systems, and Technologies.* 2007. 12-17

[17] Mozilla Project. *Privacy and Security Preferences - Web Passwords*.URL: http://www.mozilla.org/projects/security/pki/psm/help 20/passwords help.html, 2004.

[18] Recordon, D., Reed, D. OpenID 2.0: a platform for user-centric identity management. *In Proceedings of the second ACM workshop on Digital identity management (DIM '06).* ACM, 2006. New York, NY, USA, 11-16

[19] Suriadi, S., Foo, E., Jøsang, A. A user-centric federated single sign-on system, *Journal of Network and Computer Applications,* Volume 32, Issue 2, March 2009, 388-401, ISSN 1084-8045

[20] Tatyana, R., Neuman, C. "Situational Identity: a Person-centered Identity Management Approach." identity 2: 3.

[21] Todorov, D. 2007. Mechanics of user identification and authentication [electronic resource] : fundamentals of identity management. Boca Raton : Auerbach

[22] Tu, N., He, Q., Zhang, T., Zhang, H., Li, Y., Xu, H., Xiang, Y.,
Combine Qualitative and Quantitative Methods to Create Persona Information Management, *Innovation Management and Industrial Engineering*, 2010 Nov, Vol.3, 597-603

[23] UK e Envoy. *Registration and Authentication*. UK Office of the e-Envoy, under the Cabinet Office http://www.jipdec.or.jp/archives/PKI-J/shiryou/e-auth_policy/UK_Guideline_E.pdf, September 2002.

[24] Vanamali, S. Identity management framework: delivering value for business. *Information Systems Control Journal* 4 (2004): 49-52.

[25] Veijalainen, J., Seleznyov A., Mazhelis, O. An Initial Security Analysis of the Personal Transaction Protocol *Mobile and Wireless Internet* 2003, pp 165-190

[26] Yong, J., Tiwari, S., Huang X.,&Jin, Q. Constructing robust digital identity infrastructure for future networked society. *Proceedings of the 2011 15th International Conference on Computer Supported Cooperative Work in Design*. 2011. IEEE, 570-576.

[27] Yuan, C., Lin, Y. "A survey of Identity Management technology," Information Theory and Information Security (ICITIS), *2010 IEEE International Conference,* 2010. 287-293

[28] Zimmermann, H., *Fuzzy Set Theory and its Applications, 2nd Edition*, Kluwer Academic Publishers, Massachusetts, USA, 1992

7. Appendices

Appendix 1. Glossary

In this dissertation, I adopt the terminology and definitions of Camp (2004):

> **Identifier.** An identifier distinguishes a distinct person, place or thing within the context of a specific namespace. For example, an automobile, account, and a person each have identifiers. The automobile has a license plate and the account has a number. The person may be associated with either auto or account through additional information, e.g., a serial number, or a certificate. One person, place, or thing can have multiple identifiers. A car has a permanent VIN and temporary license plate. Each identifier is meaningful only in the namespace, and only when associated with the thing being identified. Therefore, each identifier can reasonably be thought of as having a <thing identified, identifier, namespace> set, e.g., <car, license plate, state motor vehicle database>.
>
> **Attribute.** An attribute is a characteristic associated with an entity, such as an individual. Examples of persistent attributes include eye color, and date of birth. Examples of temporary attributes include address, employer, and organizational role. A Social Security Number is an example of a long-lived attribute in the American governmental system. Passport numbers are long-lived attributes. Some biometric data are persistent, some change over time or can be changed, (e.g., fingerprints versus hair color).
>
> **Personal identifier.** Persistent identifiers consist of that set of identi-fiers associated with an individual human that are based on attributes that are difficult or impossible to alter. For example, human date of birth and genetic pattern are all personal identifiers. Notice that anyone can lie about his or her date of birth, but no one can change it. Personal identifiers are not inherently subject to authentication.
>
> **Identification.** Identification is the association of a personal identifier with an individual presenting attributes, e.g., "You are John Doe." Examples include accepting the association between a physical person and claimed name; determining an association between a company and a financial record; or connecting a patient with a record of physical attributes. Identification occurs in the network based on both individual humans and devices. Identification requires an identifier (e.g., VIN, passport number).
>
> **Authentication**. Authentication is proof of an attribute. Identity as it is constructed in modern systems is an attribute, e.g., "Here is my proof of payment so please load the television onto my truck."A name is an attribute and an identifier, but it usually is not used to provide authentication.
>
> **Attribute Authentication.** Authentication of an attribute is proving an association between an entity and an attribute; e.g., the association of a painting with a certificate of authenticity. In an identity system this is usually a two-step process: identity authentication followed by authentication of the association of the attribute and identifier. The automobile is identified by the license plate; but it is authenticated as legitimate by the database of cars that are not being sought for enforcement purposes.
>
> **Authorization**. Authorization is a decision to allow a particular action based on an identifier or attribute. Examples include the ability of a person to make claims on lines of credit; the right of an emergency vehicle to pass through a red light; or a certification of a radiation-hardened device to be attached to a satellite under construction.
>
> **Identity**. In an identity management system identity is that set of permanent or long-lived temporal attributes associated with an entity.
>
> **Anonym (as in anonymous)**. An anonym is an authenticated attribute that is not linked to an identifier. An identifier associated with no personal identifier, but only with a single use attestation of an attribute is an anonym. An anonymous identifier identifies an attribute, once. An anonymous identifier used more than once becomes a pseudonym.

Pseudonym. An identifier associated with attributes or set(s) of transactions, but with no permanent identifier.