A Preliminary Security Analysis of New Zealand's igovt System

by

Yu-Cheng Tu

Supervisor: Clark Thomborson

A Thesis Submitted in Fulfillment of the

Requirements for the Degree of

MASTER OF ENGINEERING

in

Software Engineering

The University of Auckland

Acknowledgement

Firstly I would like to thank my supervisor, Professor Clark Thomborson. I am very grateful for his advice and expertise throughout the year. Without his guidance, I would never have been able to finish this thesis.

I would also like to thank my parents and my brother for their support and encouragement throughout the year.

ABSTRACT

Identity management is the emerging technology for organisations to administer identities. It consists of business processes and policies as well as current practices for supporting such administration.

Since governments often deal with a large amount of people and identity information, identity management in recent years have become more important for delivering services to the public electronically. New Zealand is an example of this, where an identity management system is being developed for its people. The system is known as igovt, where it aims to manage the identities of New Zealand citizens when they interact with government agencies online.

In this thesis, we propose a method for analysing the security requirements of the New Zealand's igovt system. We first identify the primary security objectives of the identity management system in general as well as the igovt system. We then analyse the types of information held in the system using a novel extension of the FIDIS methodology. And finally we use misuse case analysis to elicit security requirements for the igovt system. Together, we present the preliminary analysis of the igovt system for illustrating our methodology.

Contents

1 Introduction **1**

1.1 Introduction 1

1.2 Organisation 3

2 Identity Management **5**

2.1 Overview of Identity Management 5

2.1.1 Objectives of IdM 6

2.1.2 Functionality of IdM 8

2.1.3 Existing IdM Models 10

2.2 Fundamental Concepts 16

2.2.1 Identity 16

2.2.2 Lifecycle of Identity 18

2.2.3 Authentication 19

2.3 Security of IdM 20

2.3.1 Security Objectives 20

2.3.2 Privacy Protection Objectives 23

3 E-government **27**

3.1 E-government and IdM 29

3.2 New Zealand E-government 30
3.3 IdM in New Zealand E-government 31
3.3.1 The Authentication Programme 31
3.3.2 Overview of igovt 33
3.3.3 Government Logon Service 35
3.3.4 Identity Verification Service 36

4 Our Methodology **41**
4.1 Overview 41
4.2 Identifying Security Objectives 42
4.3 Information Analysis 43
4.4 Threats Analysis 44

5 Results and Discussion **47**
5.1 Security objectives for user-centric IdM 47
5.2 Information in New Zealand igovt 48
5.3 Analysing Misuse Cases for IdM 52
5.3.1 Actors in IdM 52
5.3.2 Overview of IdM Use Cases 54
5.3.3 Register Identity 54
5.3.4 Manage Identity 55
5.3.5 Use Service 57
5.3.6 Security requirements elicited 59

5.4 Analysing New Zealand igovt 61

5.4.1 Secrecy 61

5.4.2 Integrity 62

5.4.3 Availability 62

5.4.4 Accountability 62

6 Conclusions and Future Work **63**

6.1 Conclusions 63

6.2 Future Work 65

List of Tables

5.1 Security objectives for user-centric identity management. 49

5.2 Information Principle for the users of New Zealand igovt. 50

List of Figures

2.1 Conceptual IdM Frameworks Model (reproduced from [38]) 10

2.2 Centralised IdM models (reproduced from [35]) 12

2.3 Federated SSO identity model (reproduced from [35]) 15

3.1 E-government practices categories (reproduced from [41]) 29

3.2 Conceptual Model of igovt. 34

3.3 Sequence diagram for the GLS processes. 36

3.4 Sequence diagram for a user enrolling in IVS. 37

3.5 Sequence diagram for a user establishing a service. 38

4.1 Principles of Information Management (reproduced from [48]) 45

5.1 Overview of the main use cases for IdM 54

5.2 Overview of use and misuse cases for Register Identity 56

5.3 Overview of use and misuse cases for Manage Identity 57

5.4 Use Service 58

5.5 Requesting a service and prove identity to service provider in New Zealand igovt 60

Chapter 1

Introduction

1.1 Introduction

Identity management is the emerging technology for organisations to administer identities. It is often seen as a part of the organisation's business strategy to enhance security and privacy in business operations [55]. Generally, it aims to build a more secure identity infrastructure while consistently managing identity information as well as user accounts, passwords and tokens throughout its lifecycle [32].

Since identity management aims to improve security with better access control to information and services, governments in recent years have started to consider using identity management. As governments have responsibilities for assuring privacy and security to the public, identity management becomes useful for governments to deliver services electronically [43]. New Zealand is an example of this, where an identity management system is being developed for its people. The system is known as igovt, where it aims to manage the identities of New Zealand citizens when they interact with government agencies online [43].

In this thesis, we propose a method for analysing the security requirements of the New Zealand's igovt system based on security requirements engineering (SRE). Requirements engineering, also known as requirements analysis, is the procedure for analysing the requirements of a system. This procedure is often conducted during the initial phase of software development projects and usually iterates throughout the entire development lifecycle. The requirements captured from the analysis are descriptions of what capabilities or conditions a system must conform to in accordance to the demands and expectations of the stakeholders [18]. Generally, the requirements are being classified into two main categories, functional and non-functional requirements. According to [18], functional requirements describe the required behaviour of a system, whereas, non-functional requirements specify the constraints that a system must comply with. Likewise, SRE has similar concepts to requirements engineering, where it concentrates on eliciting the security requirements of a system.

Throughout the literatures reviewed, there are many researches in identity management focusing on privacy and functional requirements. However, to our knowledge there was no previous work that focused on SRE for identity management in E-government. Thereby, as one of our research goals, we intend to find a lightweight methodology for analysing security in identity management systems, particularly with E-government.

Therefore, as the first step of SRE, we identify the security objectives of the identity management system. We then analyse the types of information held in the system using a novel extension of the FIDIS methodology [47]. Afterwards, we enumerate threats with a misuse case analysis. Together, we demonstrate our methodology with the preliminary analysis of the igovt system.

1.2 Organisation

There are six chapters in this thesis. Chapter 2 reviews identity management in general and discusses the underlying concepts in identity management. It also discusses the security and privacy objectives for the identity management systems. Chapter 3 examines the current identity management system in New Zealand E-government. Chapter 4 describes our methodology for analysing identity management with common practices found in requirements engineering. In Chapter 5, we present the findings from our analysis. And finally in Chapter 6, we give a summary of our research and then conclude with any possible areas for future research.

Chapter 2

Identity Management

In this chapter we introduce identity management and its fundamental concepts. We first give an overview of identity management with its objectives and functionalities as well as three types of existing models. In Section 2.2 we discuss the fundamental concepts in identity management. And in Section 2.3 we examine the security and privacy objectives for identity management systems.

2.1 Overview of Identity Management

Identity Management (IdM), according to The Open Group, is often seen as a part of the organisation's business strategy to enhance security and privacy in business operations. It consists of business processes and policies that define the goals and procedures for administrating identities. Moreover, it also combines current technologies and practices for supporting such administration [35, 55].

The administration of identities in IdM generally involves the management of identity lifecycles, which include activities such as creating identities and maintaining related profiles as well as removing these from applications. It also defines how these identities can be authenticated as well as be used to access resources [34]. Hence, IdM can also be referred to as Identity and Access Management, which this term had been used by Microsoft Developer Network and Gartner Research in [23] and [58]. We conclude that identity and security control principles are fundamental to IdM.

Before looking at the identity and security principles of IdM, we first give a brief overview of IdM. Firstly, we discuss the objectives and functions of IdM based on the research conducted by The Open Group as it provides greater detail about the concepts and objectives of IdM than other literatures reviewed. We then examine existing models and current solutions for IdM.

2.1.1 Objectives of IdM

Generally, the main objective for IdM is to provide an effective solution for managing identities securely and efficiently. Underneath this main objective, individuals and organisations have their own set of concerns and expectations for IdM. The Open Group has identified and specified these in accordance with the "SMART" (Specific, Measurable, Actionable, Realistic and Time-bound) objectives of a good business scenario [32].

According to The Open Group [55], the aims of individuals for IdM are to preserve individual's ownership of identity and privacy while providing efficient and personalised services. Specifically, IdM shall enable individuals to achieve the following objectives [32]:

- Publish identity and address information, as well as give information to others and make the information available for public access;

- Authenticate identity for service entitlement in IT-based transactions. The same identity shall also be recognised and accepted in different applications;
- Pay for goods and services through electronic payment;
- Manage own identity information, as well as keep record of the different identities used;
- Manage others' identity information, so that individuals can make contacts with others or identify them using the information already available.

On the other hand, organisations are required to provide efficient and secure services to individuals as well as to conform to regulations. Moreover, they tend to focus on minimising the costs in managing identities [55]. Therefore, organisations will need to realise the following IdM objectives, which had been defined by The Open Group [32]:

- Support the above objectives for individuals;
- Manage identity information within the organisation. It includes creating new identities and changing identity records as well as revoking identities;
- Achieve data consistency;
- Manage mobile members;
- Achieve seamless E-client management, which also aims to provide a single view of the client;
- Prevent Fraud, as well as prevent unauthorised access and keep information confidential.

Overall, the objectives of IdM are aiming to achieve a more secure infrastructure for managing identities and related attributes through their lifecycles. Furthermore, they

also aim to support identity authentication. In addition, these objectives include the goal of standardising and simplifying identity information from multiple applications. And finally, IdM needs to consider reducing operational costs while providing a consistent and efficient solution for controlling identities and protecting information.

2.1.2 Functionality of IdM

In order to satisfy the above objectives, IdM will be required to provide functions that have the capabilities of administering identity and enforcing controls on identities. Based on the literatures from [44], [55], and [58], we find a typical IdM system will include the following functionalities: user provisioning, control, and metadirectory. We discuss each in turn below.

User Provisioning

User provisioning in a typical IdM system manages the accounts of the users and their associated identity information throughout the accounts' lifecycle. It deals with the creation, modification and revocation of user accounts as well as entitlements and credentials for the individuals [44, 58] And yet, user provisioning includes establishing the identity of an individual with verified information before making a new user account [53]. In addition, according to Gartner Research [58], user provisioning also provide other functions such as password management for password rest and password synchronisation.

Control

The control functionality of IdM offers enforcement of access control, which includes authentication, authorization and auditing services [44]. Authentication is the process for identifying and validating the identity of a user, which ensures that the user using the

identity is the person who claims it to be [53]. Often, technical mechanisms such as biometrics or PKI are used for this [55, 58]. Authorisation, on the other hand, is the process for permitting users to access resources or services depending on their eligibility. It also consists of mechanisms like role-based access control or policy-driven authorisation [44]. Coupling with these services is the auditing functionality, which is to ensure that the IdM system meets its objectives by capturing and examining the assets, data and operations of the system [34].

In addition, many IdM systems nowadays also promote single-sign-on (SSO) and identity federation, particularly for communications across different application domains. SSO is one of the access control methods, which allows the users to access multiple applications through only one single authentication process [58]. Moreover, SSO can also be used for identity federation among different organisations. Identity federation allows associated organisations to share and trust each other's information about its users. Thereby, users from one organisation can use services from another organisation without extra registration or authentication [34, 58].

Metadirectory

Metadirectory, which can also be referred to as enterprise directory [53], is an important component in IdM systems for organising and synchronising identity information in directories and databases [58]. It acts as a data repository, which stores identity information and user credentials. In addition, metadirectory will need to provide standard APIs and protocols such as LDAP or X.500 for retrieving and publishing as well as protecting this set of data. [44, 55].

Besides the above functionality, in many instances, IdM will need to fulfil additional requirements such as conforming to legislation and supporting system integration. And

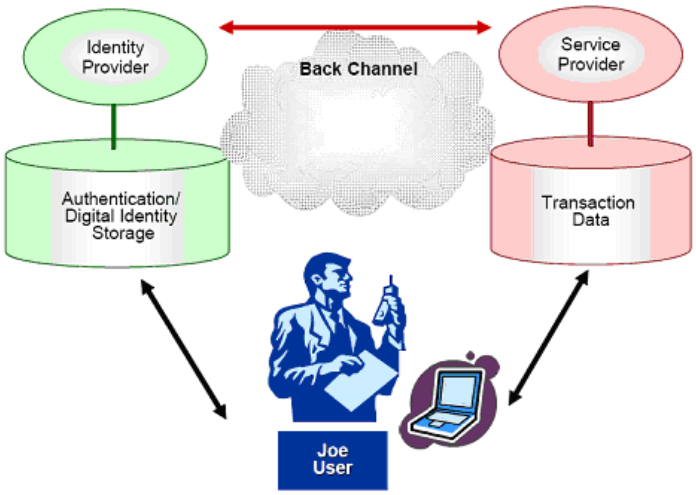


Figure 2.1: Conceptual IdM Frameworks Model (reproduced from [38])

yet, providing user self-service and supporting user control over own information also essential capabilities for IdM to realise [34].

2.1.3 Existing IdM Models

Generally, an IdM system involves with at least two types of entities including identity provider and service provider. An identity provider is responsible for managing user identities and authentication, whereas a service provider, which some articles refer to as a relying party, is responsible for providing services to users with correct privileges [16, 17]. At a higher conceptual level, IdM consists of these two entities, and for which the users interact with them respectively. Figure 2.1 shows this conceptual framework, which had been discussed by Gartner Research in [38].

On top of the conceptual framework, IdM can be distinguished into server-centric and user-centric systems. A server-centric (or a provider-centric) IdM system is mainly a centralised system for managing accounts, profiling user data and associating data to individuals reliability [24, 46]. In most cases, users of a server-centric IdM system rely on the identity provider to present credentials to others. Consequently, users have less

control over their credentials and thus limiting the use of their identities [16].

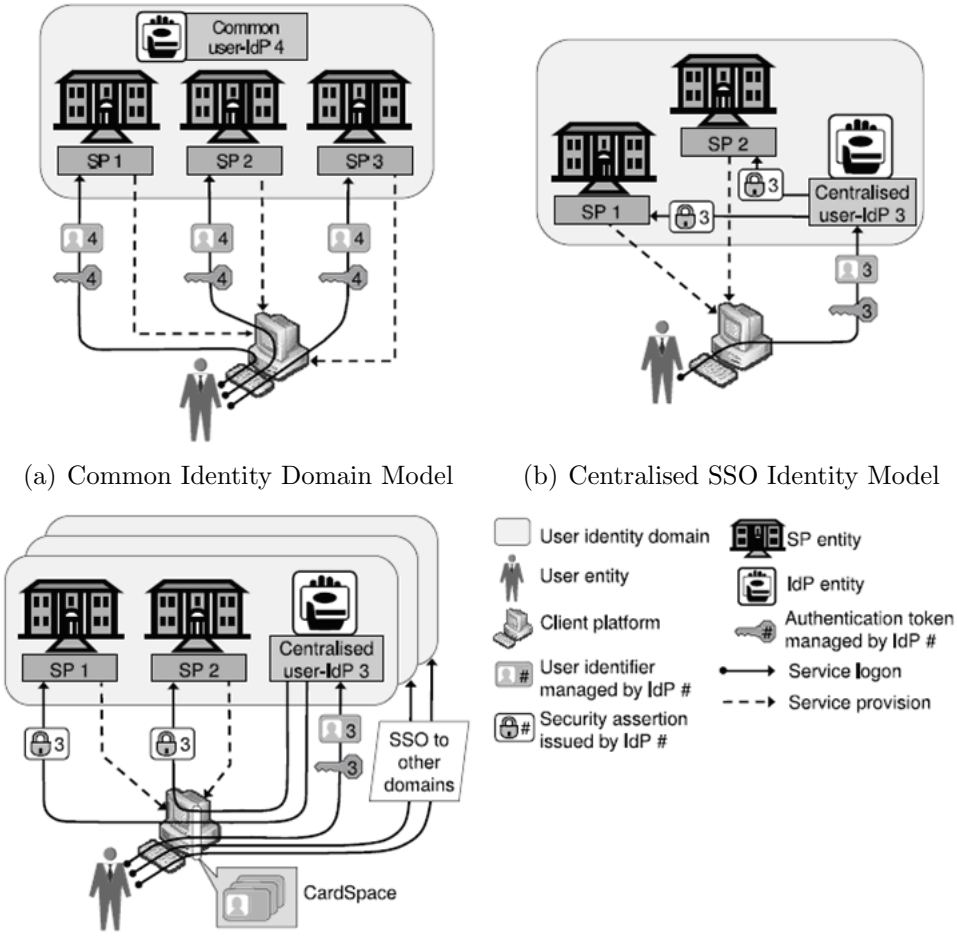
On the other hand, a user-centric IdM system is mainly a user-oriented system that allows users to have more controls over their identities and credentials. Usually, the users have the capabilities to decide on what identity information to be disclosed. And yet, they become less dependent on identity providers as long term credentials can be obtained and stored under their control [16, 51]. In addition, recent user-centric IdM has been focusing on privacy protection, which aims to minimise the disclosure of identity information and to protect the real identities of the users from being recognised for malicious intent. Therefore, it is also being referred to as a privacy-enhancing IdM [24, 51].

Besides server-centric and user-centric classification, IdM systems can also be deployed mainly into three kinds of models: silo, centralised, and federated IdM model.

Silo Model

The silo model is an isolated IdM system, where each system manages the identities of the users and related information in its own domain. This means that each system consists of only one identity provider and one service provider. Normally, the service provider in such model can also act as an identity provider for authenticating users and managing tokens [35].

The silo model is easy to implement and it provides tight controls over identities as only one entity, i.e. the identity provider, is exposed to the information [35]. But, it is inconvenient for users who wish to obtain access to services from multiple service providers. This is because each service provider has its own set of rules and processes. Therefore, the users will be required to register at different service providers for different services [35, 54].



(a) Common Identity Domain Model

(b) Centralised SSO Identity Model

(c) Centralised Model with Browser Support

Figure 2.2: Centralised IdM models (reproduced from [35])

Centralised IdM Model

The second type of model is the centralised IdM, where there is only one identity provider responsible for managing identities and administering authentication across different service providers. It simplifies the control procedures within the service providers and also improves user convenience over the silo model by offering the SSO functionality. However, the involved service providers will need to trust the only identity provider for providing identity services, and for which the identity provider can become the single point of failure. Yet, a malicious user may be able to access to all the services from the involved service providers if the identity provider is compromised [13, 16, 54].

Josang et al. [35] had distinguished three variants of the centralised IdM, as shown in figure 2.2.

The Common Identity Domain variant of the centralised IdM model has a central authority, referred to as the common identity domain. This authority takes the role of the identity provider for managing identities and tokens, but it does not authenticate the users. Generally, PKI is implemented for this common domain, which issues and manages public-key certificates as authentication tokens. This model has the above advantage of simplifying management in service providers. As well as easier management for the users as they only need to obtain one unique identifier and authentication token from the common identity domain. Despite the advantages, the model may compromise the privacy of the users as the SPs may be able to match identity information using the common identifier. Moreover, it is difficult to implement this kind of model, particularly in defining unique identifiers that satisfy users from different regions.

The Centralised SSO Identity variant of the centralised IdM model has the SSO functionality for authenticating users. It will also send security assertions directly or indirectly to service providers once the users have been authenticated. Microsoft's .NET Passport, now renamed to Windows Live ID, is an example of this type of centralised model. This model has similar advantages of the centralised IdM model mentioned from the above, where users have a more convenient way to access services. However, it also suffers from the above disadvantages. And yet, closed environments will be more suitable for this model than open environments as it is easier to implement a central identity provider for service providers under the same organisation and authentication policies. According to Josang et al. [35], Kerberos Authentication and Active Directory can be useful mechanisms for implementing this model in closed networks.

The Browser Support variant of the Centralised IdM model is similar to the centralised SSO identity model with an additional browser support known as Windows CardSpace or InfoCard. The Windows CardSpace is the client component of Microsoft's implementation, which acts as an intermediary between the identity providers and service providers [38]. When users request for services, they will first be asked to select identities stored in CardSpace. Next, the CardSpace will communicate with the identity providers that contain sensitive information about the selected identities. The identity providers will return security assertions to the CardSpace and for which the CardSpace then pass these to the service providers for approving service access. This type of model aims to improve over Microsoft's .NET Passport and to avoid single point failure with support in multiple identity providers. However, Windows CardSpace is platform-specific to Windows and thus limits its usability [38]. Moreover, this model as well as the other two centralised IdM models supports users or SSO within one identity domain. Hence, if users wish to access services from another domain, they will need to obtain new sets of identifiers and authentication tokens from identity providers of that particular domain.

Federated IdM Model

The last type of model that the IdM system can be deployed into is the federated IdM model. A federated IdM has the functionality of identity federation, which was mentioned in the previous section. Generally, the model consists of many independent IdM systems or silo domains, where each system has its own service provider and identity provider for providing services and managing identities. In order to establish identity federation, a set of policies, standards and practices, which the participating organisations had mutually agreed on, will be used for collaborating with service providers

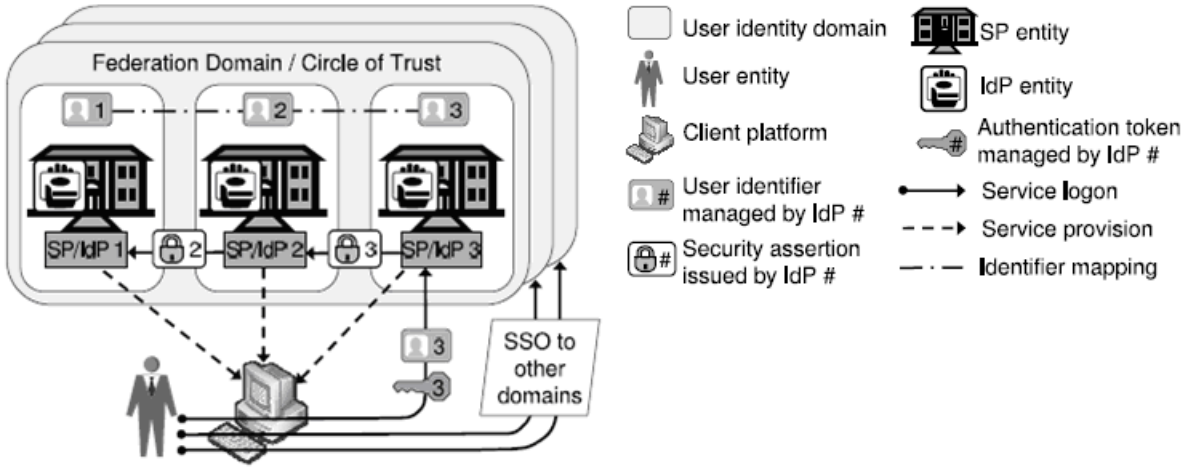


Figure 2.3: Federated SSO identity model (reproduced from [35])

and identity providers across different domains. Normally, the SSO approach will also be applied to the federation for improving user convenience. Like the centralised SSO identity model, an identity provider will give security assertions about its authenticated users to service providers within the identity federation. The service providers will in turn trust the identity provider and accept the assertions, which allowing the users to use the services provided. However, unlike the centralised model, federated IdM model can implement the SSO functionality in open environments. On the other hand, it is difficult to build a federation as the service providers and identity providers must trust each other. Moreover, the privacy of the users may be compromised as identifiers in different service providers are mapped. Furthermore, it too suffers from the scalability and password fatigue problems as the SSO functionality cannot offer users to communicate across multiple domains that have no federation agreements [13, 35]. Figure 2.3 shows an example of federated SSO IdM model, where the federation of the identity domains is also known as the circle of trust. Other examples of federated IdM can be found in the Liberty Alliance project [11], where it also aims to provide open standards for building such model.

2.2 Fundamental Concepts

From the previous section, we find that IdM aims to provide services that involves with managing identities and associated security controls, particularly in authentication, through their entire lifecycle. Underlying this aim, we find three fundamental concepts including the concept of identity, identity lifecycle, and authentication. We discuss each in turn below.

2.2.1 Identity

Identity is the foremost concept for IdM. An identity is a set of information and characteristics about an entity. The entity usually refers to a person or a user in the context of IdM. Generally, the identities are unique within an environment [55]. This identity is generally in the form of digital identity, which depicts individual's physical identity in electronic formats for computer applications [20, 35]. Therefore, various aspects of the person's attributes can be used to represent the person in IdM. These attributes include the name of the person, biological characteristics and other properties such as the person's reputations and affiliations [46].

Usually, the identity within an IdM system can be established with only a subset of the person's attributes. Hence, an individual user can have many identities using different sets of personal attributes for different roles and purposes [52]. Sometimes, these identities are referred as partial identities of a user, whereas a complete identity is the union of all the user's partial identities and associated attributes [52].

Furthermore, attributes associating with the identity have different perspectives from different parties. And yet, the identity can be dynamic as these attributes like the user's reputations can change over time. Hence, Mont et al. from HP's trusted system laboratory describes a digital identity as "a view on the identity information associated

to an entity, at a specific point of time" [44].

According to NIST [42], a view on identity information can either be intrinsic or extrinsic. The intrinsic view consists of users' own perspectives and controls on the identity attributes, which can be helpful for designing the authentication mechanisms. Examples of this include memories and biological features of the users.

On the other hand, the extrinsic view is an observation on the identity information made by third parties. For instance, the reputation of a user is an extrinsic view on the identity perceived by others. The observation is often recorded in logs, and for which it can be useful to establish trust and accountability within the application [42]. Often, the user will know about such observation and may have some indirect control on it. However, in most cases, there will be some observations that the user is not aware of and has no control over them [44].

Moreover, in a typical IdM system, the identity of a user not only composed of personal attributes, it also includes identifiers and credentials. Identifiers are pointers for uniquely describing the user within the context of the system [32]. Credentials, usually a set of secrets, are used to prove and validate the identities of the users [19]. In addition, user's preferences for the application are also stored with the identity [42].

Therefore, the identity in the IdM system is more than a static set of personal attributes. It composes of attributes about the user from multiple perspectives that varies over time. These attributes can also be used for users to create different identities across various contexts. Moreover, it forms the basis for authorisation through the identifiers and credentials stored. And yet, it enables personalised services with the preferences specified by the user.

2.2.2 Lifecycle of Identity

The lifecycle of an identity within a typical IdM system comprises of three fundamental stages: [55]

1. Enrolment of identity
2. Maintenance of identity
3. Disposal of identity

In the first stage of the identity lifecycle, users register with the organisation using their personal attributes and credentials. Once the information provided by the users had been verified, the IdM system will add the users and create unique identifiers for them in the directory. After the enrolment, the identities will be provisioned with access controls as well as services entitled to the users. These identities will be maintained in the directory for later stages of the identity lifecycle.

During the operational life of the identities, users can read, modify and delete their identity information stored in the directory. In the meantime, the IdM system maintains the information and audits or reviews the operations to ensure that the changes made by the users are valid. It can also suspend and resume identities from accessing to services. Moreover, the identity information may be shared with other applications.

Finally, the last stage of identity lifecycle is the disposal of identities. In this stage, the identities of the users will be deleted and removed from the directory. And consequently, the services entitled and associated rights will also need to be revoked. After this process, generally the identities and their information will be archived.

To manage identities throughout these lifecycle stages, user provisioning can be applied, which was mentioned previously as one of the main functionality of IdM systems.

The provisioning handle identity information associated with individuals, resources and services for entitled users, and termination of identities [55].

2.2.3 Authentication

Authentication is another important concept for IdM systems, especially for enabling user provisioning and control processes. By definition, authentication in IdM is "the process of gaining confidence in a claimed identity" [55]. In other words, it is to ensure the validity of the person whom he or she claims the identity to be. Generally, underneath authentication is the concept of identification, which is to recognise an individual as a particular identity. It aims to associate personal identifier with the individual who had presented such attribute to the application, and for which provides some support in linkability [22, 46].

In IdM systems, authentication is operated in two areas. Firstly, it is applied in establishing the identity of the user before account provisioning, which is also known as verification [55]. This process involves verifying the identity of the user with the identity documents supplied by the user. These documents are often checked with the issuers of the documents or with an authoritative source [42].

Furthermore, authentication is also required for ensuring the identity is the person qualified, and for which it becomes the basis for authorisation and access control. According to The Open Group [55], only authenticated identities can be bound to permissions that allow the users to have access to certain services. Thus, the authentication process prevents malicious users from gaining access to resources using stolen identities.

And yet, the authentication provides some level of confidence in the validity of the identity. NIST [5] has defined the level of confidence in identity as the identity authentication assurance level, particularly for e-government transactions. The level ranges from

level 1 of little or no confidence to level 4 of very high confidence in the asserted identity's validity [5].

Besides the assurance level, there are three types of methods for users to prove the authenticity of their identities:

- **Secret (something you know):** usually secrets are shared among the involved parties, and users prove their identities with these shared secrets [25]. Usernames and passwords are an example of this, which are the most common authentication method.
- **Biometric (something you are):** to prove the users' identities based on their physical characteristics such as handwriting and fingerprint [25].
- **Token (something you have):** usually a physical token for proving users' identities [25]. This can also be used with secrets to provide two-factor authentication [55].

2.3 Security of IdM

Generally, the security of IdM is realised by the control functionality (as seen in Section 2.1.3) to prevent identity theft and identity fraud, as well as to protect identity information from corruption. It usually consists of security and privacy objectives for the IdM system to apply with. We discuss these two types of objectives identified in the following sections.

2.3.1 Security Objectives

The security objectives for IdM systems generally reflect on the process of managing identities of the users as well as their interactions with the service providers. Moreover,

since IdM acts as a part of the organisation's business control, these security objectives will need to be defined in a way to ensure that the application can provide some auditable evidence to its stakeholders as well as assurances that the involved activities will fit for purpose. Thereby, according to The Open Group [55], the underlying objectives for such control will include the descriptions of the following security control processes:

- Authentication: this is to verify credentials in a message or transaction.
- Authorisation: this is to verify the identity of an individual and grant permissions for the individual to do some tasks or access some information.
- Audit: this is to examine the logs of the actions and data of the involved parties for monitoring and investigative purposes.

In addition, identification will also be introduced as a part of the control for creating unique identities from verified credentials provided by individuals, which these can later be used for authentication and authorisation [55]. And yet, [55] has included accountability as one of the underlying objectives to record the actions taken with associated parties. This will then become some form of references to past events, which the involved parties can be identified and held accountable for their actions [28, 55]. Therefore, according to [55], accountability provides an evidence trail for satisfying the purposes of auditing and non-repudiation [55].

Similar to the control objectives by The Open Group, Gartner Research [58] has recognised four security objectives, also known as the "A's of information security" for IdM systems to realise. These objectives include authentication, authorisation and audit as well as administration for managing user access. Similarly, [56] has suggested that these four security objectives should be applied to the application for implementing user-centric IdM systems. As discussed from the previous section, these objectives become the

control functionality of IdM. In particular, authentication is fundamental for establishing identities and proving user authenticity, which had been discussed previously.

Furthermore, the security objectives for IdM systems also concerns with the general goals found in information security such as confidentiality, availability and integrity. For instance, according to [54], in order to ensure information assurance in a federated IdM system, it has to consider the availability of the system, and for which system's reliability and its ability to make timely delivery of information will need to be taken into account. And yet, integrity and confidentiality are required to prevent unauthorised modification and disclosure of information [54].

Besides the control objectives and the general information security objectives, Kim Cameron from Microsoft [21] has proposed the "seven laws of identity" for developers to consider when building IdM systems. Four of these laws reflect on the security issues raised in the application. From these laws we derive four additional security objectives to achieve.

- User control and consent: this is to protect the privacy of the users by allowing them to control the release of their own information as well as to inform users about others using their information.

- Minimal disclosure for a constrained use: this is to reduce the ability of any parties including users, IdM systems and adversaries identifying any particular individuals. It also aims to minimise information aggregation by disclosing the minimal amount of identifying information and limit its use.

- Justifiable parties: this is to ensure that the system is designed in a way that all the users of an IdM system have some valid justification for all of their uses of this system.

- Directed identity: this is to ensure that the system is designed in a way to support different identifiers for public and private entities, and for which provides transparency in public entities without exposing excess correlations between private entities.

From the last security objective, we find that the IdM must distinguish an entity as either private or public and that the level of controls differs depending on the view of the entities. For example, IdM should place more controls in any extrinsic view, such as reputational information (see Section 2.2.1), on private individuals than a similar view on a public entity.

2.3.2 Privacy Protection Objectives

Privacy is also another important goal for IdM systems as they store and handle a large amount of personal information. Privacy, defined by OECD [7], is

> the status accorded to data which has been agreed upon between the person ... and the organisation receiving it...

Since privacy relates to the status of data, breach of confidentiality such as intrusions to personal data or disclosures of unauthorised information will violate the privacy of the individual. Therefore, according to [7], confidentiality and privacy are directly correlated, and that the concept of confidentiality will reinforce privacy by preventing exposure of personal information.

Additionally, there are three other basic properties relating to the protection of privacy, which will also strengthen the confidentiality of personal information. The first privacy-related property is anonymity, which means that the person is not identifiable within a set of people [52] or the associated identities is not identifiable from the information or messages released [28]. With the property of anonymity, the application can

ensure that an individual's privacy is full protected in a transaction. However, this may create some difficulties in identifying the parties responsible for things that had gone wrong. Thus, with anonymity, the information or the message presented needs to be reliable and that the parties need to be or assumed to be trustworthy.

The second property for protecting privacy is unlinkability. Unlinkability is to prevent a malicious user from understanding the associations between two or more entities, attributes or transactions [52]. It will thereby avoid data aggregation and identity matching. According to Pfitzmann and Hansen [52], a privacy-enhancing IdM system will thus be described as the system that "sufficiently preserves unlinkability between the partial identities of an individual person required by the applications".

Lastly, the basic property for protecting privacy is pseudonymity, which uses pseudonyms as identifiers that are not of individual's real attributes [52]. Hence, the real identity of an individual may not be easily recognised by malicious users. Therefore, anonymity of an identity will be dependent on the unlinkability of the pseudonyms. For instance, anonymity is stronger when there is less personal attributes linked to pseudonyms. Likewise, it is strong when there is less use of the same pseudonyms [52]. Generally, a pseudonym also requires authentication so that the real identity of the pseudonym can be revealed for liabilities if something had gone wrong in the application [24].

Furthermore, deriving from the above definition for privacy, there will need to be an agreement between the party holding the information and the party receiving the information. Hence, we find that giving controls to the users and acquiring users' consents are common practices for privacy, where these have been suggested in many literatures concerning the protection of personal information. For instance, one of Cameron's laws of identities on "User control and consent", in the previous section. Moreover, [28] stated that users must have control over their identities and uses as well as over what information to be revealed to others. In addition, a related concept to "User control and consent"

is the "Selective disclosure" of identity information, which has appeared in [31] as one of the privacy-enhancing properties for identity credentials and [16] for user-centric IdM systems. As explained in [16], selective disclosure is the concept of allowing the user to control what identity information to be released when using a service.

Another practice known as "Data minimisation" is also common to privacy protection, which is to minimise the information revealed in transactions. This can be found from the previously discussed Cameron's laws of identity for "Minimal disclosure for a constrained use". Similarly, Josang et al. [35] have defined that the fundamental principle of privacy protection as the "exposure of personal information must be minimised", which the IdM systems should be adhered to. Data minimisation will also be dependent on the three underlying privacy protection properties and user control for consenting to what information is disclosed to the SPs.

In addition, the supports for user access to modify own information and notification about organisation's information practices are often included as the protection objectives for privacy [14, 54]. Furthermore, the IdM system will need to ensure the integrity and security of personal information. And yet, it is also vital to adopt the accountability principle, which ensures that the application complies with business policies and regulations [13, 45].

With the above security objectives and privacy protection objectives, we find that the IdM system becomes more user-centric focused. Bhargav-Spantzel et al. [16] have composed a list of properties for achieving a user-centric IdM system. They have distinguished two types of properties in their list, basic and compound, where the compound properties are compositions of other properties. After comparing with the security and privacy objectives discussed previously as well as removing the functional properties, we find the following additional list of security and privacy properties:

- **Notification,** which aims to enhance user control by enabling the user to receive and retrieve notifications about the credential usage;
- **Conditional Release,** which is related to selective release. The identity information is only released to the recipient once a condition has been fulfilled;
- **Illegal sharing prevention,** which prevents users from giving credentials to other parties to use without being authorised;
- **Non-replay,** which prevents replay of messages or transactions;
- **Non-repudiation,** which prevents users or service providers to later deny about a particular transaction that had taken place;
- **Non-transferability,** which prevents a recipient of identity information to reuse this information using the obtained security tokens;
- **Revocability,** which IdM revokes identity and related identity information in order to maintain the validity of credentials and information;
- **Selective Disclosure,** which means that the user has control over what identity information to be released;
- **Stealing prevention,** which aims to protect identity information and credentials from theft, viruses, and other malicious means;
- **Verifiability,** where the users give consents and verifications to the identity provider about their identity information and transactions. Together with selective disclosure, these two properties correspond to the user consent law in Cameron's laws of identity.

Chapter 3

E-government

In this chapter we discuss the identity management system designed for New Zealand E-government. We first give a brief overview of E-government in general and then discuss the role of identity management in E-government. In Section 3.3 we discuss the E-government programme in New Zealand. And in Section 3.4 we examine the identity management in New Zealand E-government with its goals and procedures for identity verification and authentication.

E-government, also known as electronic government or digital government, is typically a web-based application for delivering online government information and services to both public and private sectors. It provides a platform for the government to interact with private individuals, businesses, and other government organisations. It also promotes internal communications between its employees and departments. Through the use of internet and other IT practices, E-government aims to deliver better services to the public while improving internal operations within government agencies [29, 36].

In general, E-government covers a wide range of operations for both internal and external government activities. It has the functionality of encouraging citizen participation in political activities, providing prompt access to information and services, as well as integrating government systems for greater operational efficiency. Normally, E-government can be categorised according to its functionality and the type of interactions between the government and other entities. For instance, providing public services to private individuals belongs to the category of Government-to-Citizens (G2C). According to Lee et al. [41], there are five categories in E-government, where each category is analogous to the technologies used in E-commerce. Figure 3.1 shows these categories along with the descriptions and example practices.

Although these categories can be mapped with business metaphor, E-government is still different to E-commerce. Particularly, they differ in the motivation for providing services as well as in the expectations from the stakeholders [15]. Generally, E-commerce is motivated by competitions and demands in the marketplace. Whereas, E-government has no such pressure and that it is usually driven by the government making the initiative. However, unlike E-commerce, where only the customers need to be satisfied, E-government has to take its entire population into account [43].

Moreover, individuals usually have higher expectations in E-government than in E-commerce. This is because, from an individual's perspective, government is obligated to provide public services and protection to all of its constituents without fail. Hence, any personal information and communications need to be secured and protected. And yet, better accountability and transparency in E-government are also required [27, 43].

E-government category	Business metaphor	Description	Sub-category	Example practice
Government to citizens (G2C)	Customer Relationship Management (CRM)	Providing opportunities for greater citizen access to and interaction with the government	Managerial interaction	Government's informational Web sites
			Consultative interaction	E-voting, instant opinion polling
Government to businesses (G2B)		Seeking to more effectively work with businesses	Businesses as suppliers of goods or services	Government's e-procurement
			Businesses as regulated economic sectors	Electronic filing with various government agencies
Government to government (G2G)	Supply Chain Management (SCM)	Enabling government agencies at different levels to work more easily together	Vertical integration	Sharing a database among agencies within the similar functional walls but across different levels of government
			Horizontal integration	Sharing a database among agencies at the similar levels of government but across different functions
Government internal efficiency and effectiveness (IEE)	Enterprise Resource Planning (ERP)	Focusing on internal efficiency and effectiveness	Government to employee	Web-based payroll/health benefits system
			Integrating internal systems	Implementing ERP-like systems to integrate different functions within a single agency
Overarching infrastructure (Cross-cutting)	Enterprise Application Integration (EAI)	Facilitating the interoperability across different practices	Hardware and software interoperability	Public-key infrastructure interoperability
			Authentication	e-Authentication across different e-government initiatives

Figure 3.1: E-government practices categories (reproduced from [41])

3.1 E-government and IdM

Since individuals have higher expectations of E-government, it is important for the government to ensure that all of its services are always available and accessible. Moreover, as mentioned in Section 3.1 that E-government must support all constituents, it is crucial to protect privacy and identity information of individuals as well as to ensure that individuals are entitled to the right services and resources. Hence, E-government requires the functionality of controlling and protecting personal information with strong means of authentication as well as other security mechanisms such as access control and audit process [36].

Therefore, identity management system plays an important role in E-government as it provides means for government agencies to utilise individuals' identities and personal data. It also comprises of security mechanisms that are essential for assuring security in E-government. Moreover, IdM ensures greater confidence about individuals' identities with

privacy protection objectives and mechanisms, which can be found in the previous chapter, for reducing the risks of data aggregation and information matching in government agencies [37]. In addition, with a user-centric approach IdM can also satisfy individuals' demands in E-government for greater personal control over information [27, 43]. Thus, IdM is crucial to the usability as well as the confidence levels of private individuals in E-government.

3.2 New Zealand E-government

The New Zealand E-government programme was established in July 2000 to improve the delivery of government information and services to the public through the use of web-based applications and tools. It aims to enable both people and businesses to do things remotely such as paying tax and finding regulations online. Like the E-government in general, it also aims to improve the internal performance of the public sector. Moreover, the programme plans to assist government agencies with standards and guidelines in developing the necessary components for E-government [12].

Currently, in the New Zealand E-government strategy, government agencies need to consider two sets of requirements regarding E-government. The first is the mandatory requirements set by the Cabinet, which all of the public service departments in New Zealand must give effects to. These requirements include adapting the online authentication strategy for E-government as well as implementing the "Security in the Government Sector" (SIGS) guideline set by the Cabinet for information security. On the other hand, government agencies are encouraged to take the discretionary requirements into considerations. The discretionary requirements include Shared Workspace, which is a tool for agencies to share and work online with their partners [1].

3.3 IdM in New Zealand E-government

IdM in the New Zealand E-government programme is a part of the Authentication Programme initiated by the State Services Commission. The Authentication Programme had designed an all-of-government approach, which aims to standardise the authentication mechanisms within government agencies while providing a cost-effective solution for authenticating identities. It consists of work on policy, authentication standards and all-of-government shared services, which are now mandatory for government agencies to comply with [1, 2].

In the following sections, we give an overview of the Authentication Programme in New Zealand with some important policy and implementation principles. We then briefly discuss the all-of-government shared services that had been developed in this programme, which are now branded as "igovt". We also give an overview design structure of igovt and describe the authentication services in detail. Finally, we discuss the issues relating to the Authentication Programme.

3.3.1 The Authentication Programme

The Authentication Programme concentrates on the authentication of G2C transactions, which is one of the E-government category found previously in figure 3.1. It also focuses on user control, privacy and security of personal information to ensure that the citizens have greater confidence and trust in using identities with the government [43]. These can be found from the key policy and implementation principles specified during the initial development stage, which include the following [3, 43]:

- Security and privacy protection of information;
- Acceptability to users and fit for purpose;

- All-of-government approach;
- Opt-in for users, where users can choose different means for identity authentication;
- User focus;
- Enduring, affordable and reliable solution;
- Legal compliance and certainty;
- Non-repudiation of transactions.

Furthermore, as one of the key principles for authentication, the work in the Authentication Programme as well as government agencies implementing the authentication standards must comply with relevant New Zealand laws and regulations. These include the Privacy Act and Human Rights Act, as well as the principle of Government-held information which covers principles such as availability, integrity and collection of information [6, 25].

In the Authentication Programme, the all-of-government shared services or igovt serve as the IdM system for E-government, which enable citizens to identify themselves online and to gain access to resources securely and conveniently. Currently, the designed services comprise of two independent authentication services that separate online authentication from identity verification [43].

The first service is the logon management system, which is also known as the Government Logon Service (GLS). It provides the logon management system to government agencies, where the agencies simply redirect users to GLS for online authentication. Moreover, GLS also supports the SSO mechanism, which enables users to obtain access to multiple services with a single logon. And therefore reduce the costs in building separate logon systems for government agencies as well as encourage users to use more online services with fewer logons [43, 50].

The second service is the Identity Verification Service (IVS), which is based on the user provisioning functionality of IdM. IVS aims to establish the identities of individuals and to maintain personal information in a user-centric manner. In addition, it also aims to verify identities and forward the agreed personal information to government agencies when individuals first apply for services [43, 50].

By separating these two services, it becomes more difficult for others to link personal information with interactions between private individuals and the government. Hence, the separation of services enhances privacy and thus meets one of the above key principles [43, 50]. Yet, government agencies still retain the responsibility for authorisation and access control of individual users, and for which it will further enhance privacy as well as preventing elevation of user privileges [43].

Furthermore, both services have been designed to use the Security Assertion Markup Language (SAML) for communicating security assertions to government agencies or service providers, which is an open standard that can be supported by many vendor products [43]. Together, these services deliver the main functionality of IdM, and for which the New Zealand government plans to provide to the public by 2010 through a single front-end known as igovt [43, 50].

3.3.2 Overview of igovt

In Figure 3.2, we have depicted the seven main players of igovt in an entity-relationship diagram:

- Citizen: an individual user who wishes to interact with one or more service agencies;
- Service agency or service provider: a government agency for delivering services to one or more citizens;

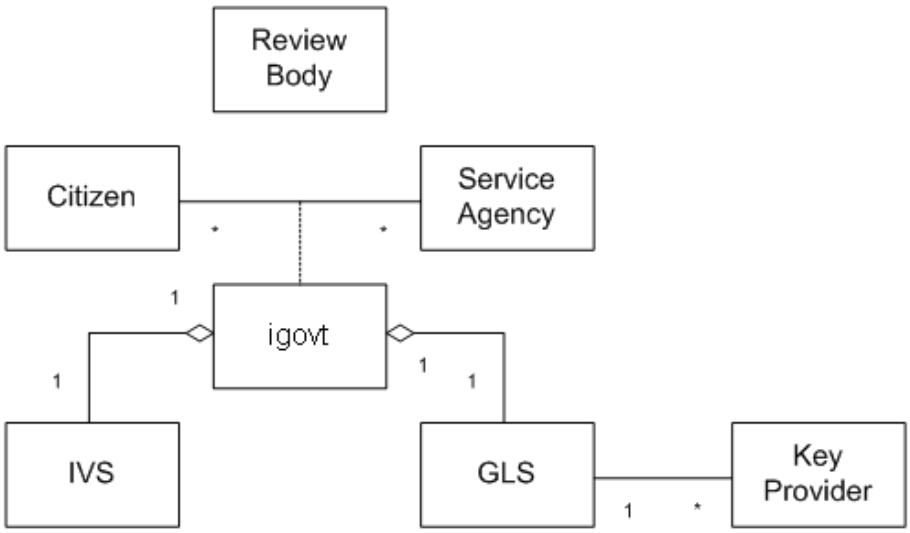


Figure 3.2: Conceptual Model of igovt.

- igovt: an all-of-government shared service for citizens to identify themselves and access to government services;
- IVS: a part of igovt for verifying identities to service agencies;
- GLS: a part of igovt that also associates with one or more key providers. It confirms the validity of the keys provided by the citizens and then authenticates their identities to service agencies;
- Key provider: an agency for issuing keys for logon to citizens and checking the validity of the keys when requested;
- Review Body: an independent government agency for making advices or handling complaints and investigations into the authentication process.

From the conceptual model, we find that this authentication design is similar to the centralised SSO model mentioned earlier in Chapter 1. This is because despite the separation

of identity verification from authentication, there is only one single authority responsible for the authentication task and one for handling identity information.

3.3.3 Government Logon Service

The GLS is a part of New Zealand's igovt, which offers single logons for people, businesses and organisations to access online services provided by government agencies. It has recently become available and that all of the public service departments as well as other relevant state service agencies in New Zealand are now expected to adapt the GLS for online authentication services [8]. An instance of the current participating agencies include Auckland City Council, which uses GLS for its ratepayers to view information about their rates online [4].

Currently, the GLS offers two levels of authentication. Generally, username and password are used for accessing online services that are of low risks to users. Services with moderate risks require two-factor authentication, and for which an additional GLS token that generates a unique token is used along with username and password [9].

For each correct logon to a particular service, GLS creates a unique number specific to that service provider if not already existed. This number contains no identity information and is used as a persistent identifier, also referred as a federated logon tag (FLT), for the service provider to recognise the user with its own record of identity information in future transactions [43]. It also records transaction information automatically for managerial and statistical purposes [4].

According to McKenzie and Crompton [43], the GLS is a pseudonymous identity provider that delivers a FLT to the service provider. Since GLS is designed to use SAML for communicating security assertions, it operates in accordance with the SSO profile of SAML [43]. As shown in figure 3.3, when a user request a service, the service agency

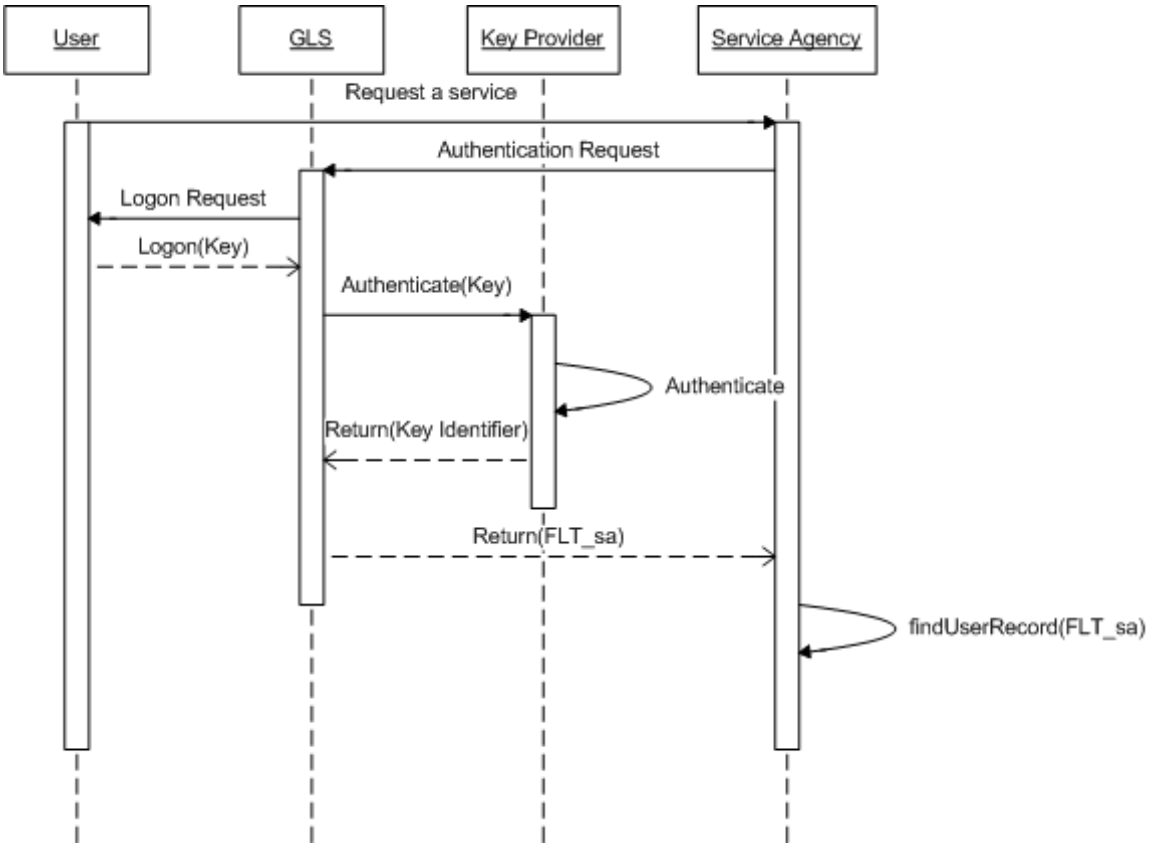


Figure 3.3: Sequence diagram for the GLS processes.

redirects the user to the GLS for logon. The user then presents a logon key identifier, which the GLS passes this to the key provider for confirming its validity with the root key. After validation, a key identifier is returned to the GLS for finding the FLT associating the user and the service agency (FLT_sa). This tag is subsequently passed to the agency and the user is redirected back to the agency's browser. The FLT_sa tag is then used by the agency to reference the user with its own record and thereby determining the eligibility of the user to services and resources.

3.3.4 Identity Verification Service

The IVS aims to provide government agencies with assertions about the identities of the online users when applying for services. It offers the means of presenting verified

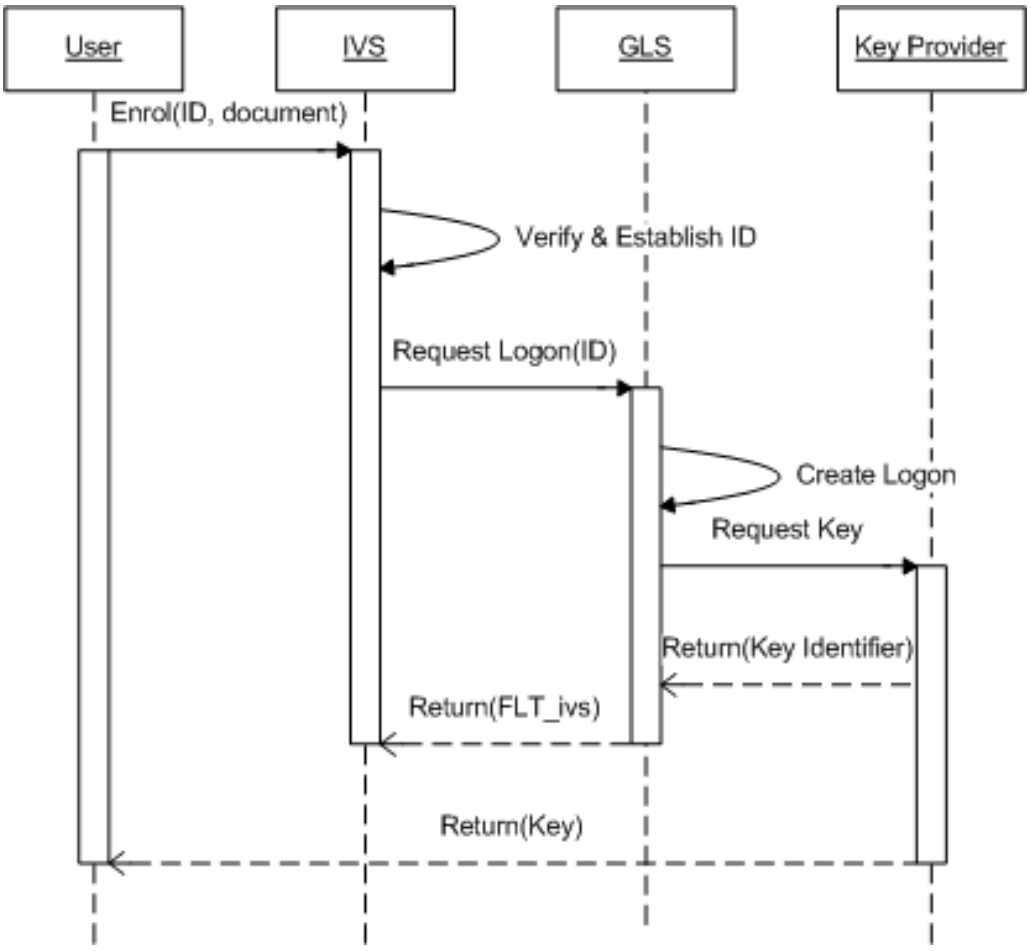


Figure 3.4: Sequence diagram for a user enrolling in IVS.

identity information or documents to government agencies through the use of internet rather than in person [10, 49]. Thus, individuals can complete the identity proof process for government services such as applying for an IRD number online.

Currently, the IVS is still under development. It plans to introduce the service in phases, first in 2009 for people with New Zealand passports or citizenships, then gradually to permanent residents and to anyone else who wishes to join [49].

The IVS is proposed to take a user-centric approach, which aims to put people in control of their personal information. And for which the proposed IVS cannot forward identity information to government agencies without the permission of the identity owner [10].

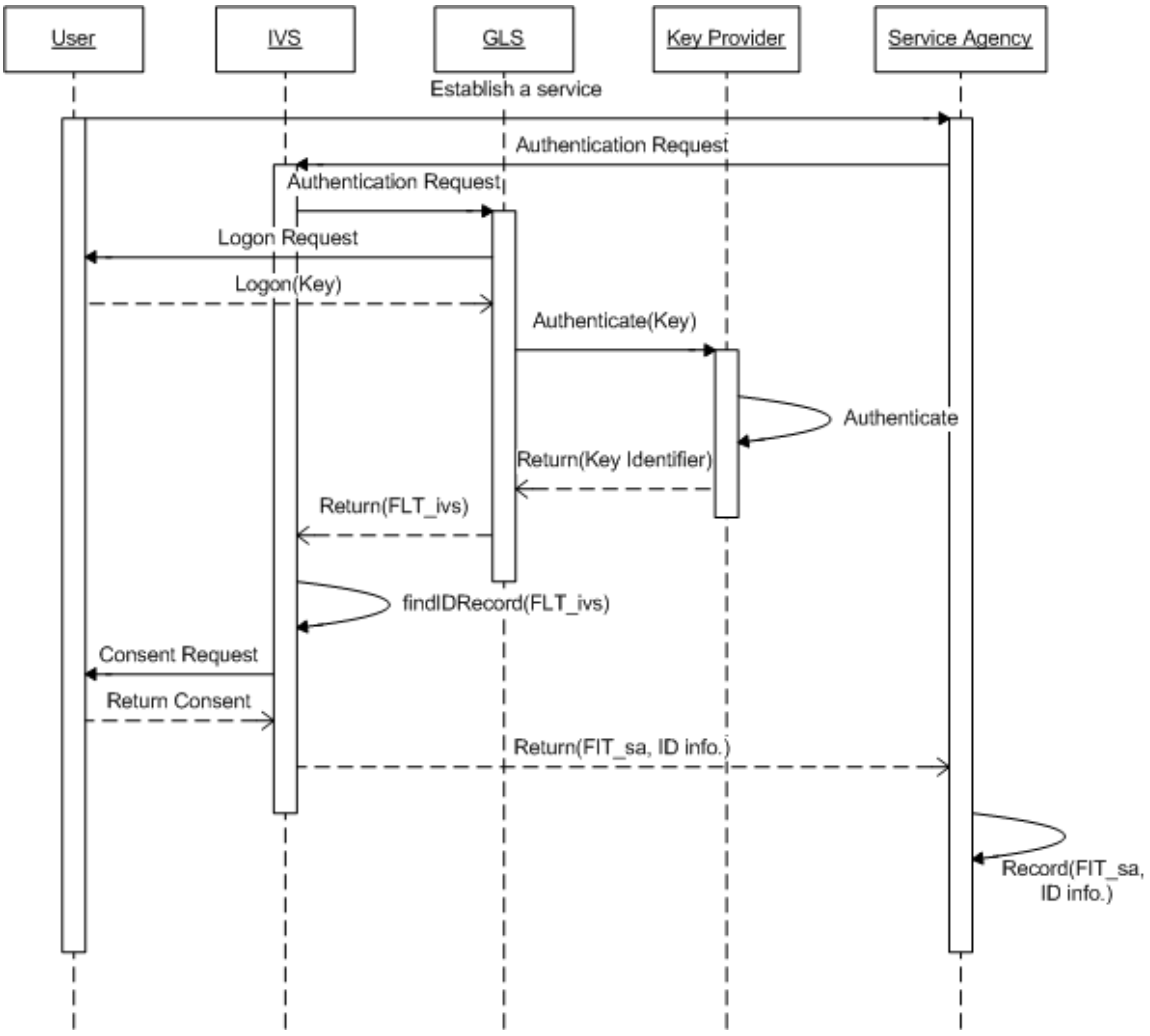


Figure 3.5: Sequence diagram for a user establishing a service.

Moreover, privacy protection is also an important concept for the users of IVS. The IVS aims to protect the privacy of its users in several aspects of the service. Firstly, it only stores a minimum amount of core identity information in the electronic database held by the Department of Internal Affairs (DIA) The core identity information includes name(s), date of birth, place of birth and sex of the person [10, 50]. The second aspect for privacy protection is that each government agency identifies the users using identifiers that are unique to that agency, and that these identifiers are stored internally in the database with the DIA. Moreover, data obtained from the GLS is not stored with the information

held in the IVS. Therefore, reduces the possibility of knowing what services the users had requested as well as preventing linkability of transactions that may lead to data aggregation and identity matching [50]. And yet, IVS is claimed to be more privacy-enhanced and differs from a national identity card as it is not compulsory for people in New Zealand and it contains no biometric information [50].

Before using the IVS, the identity of an individual must first be established to a higher level of confidence. The process of establishing an identity is based on the Evidence of Identity Standard, where the IVS checks the identity against the databases administered by the DIA to ensure that the identity truly belongs to the sole claimant [26]. At present, people who have New Zealand passports or citizenships do not need to go through the establishment process as passports and citizenships already represent higher level of confidence about the claimed identities [49].

After establishing the identity, an identity verification credential (IVC) is created and stored with IVS. The IVC contains the core identity information and other data such as an IVC number for internal use within the IVS. Generally, an individual has one IVC, which expires every five years. In order to access and use the IVC, the IVS relies on the GLS to supply a high-strength logon usually with a token to the user. And subsequently the IVS associates the FLT from the GLS with the IVC [26]. Figure 3.4 shows this enrolment process.

After the enrolment process, users can gain access to the IVS through logons using the GLS whenever they want. As shown in figure 3.5, when a user first establishes a service with the service agency and also wants to verify the identity using igovt, the service agency directs the user to the IVS, which then directs to the GLS for logon. At the GLS, the user authenticates with username, password and a token. After completing the authentication process, the GLS returns a tag FLT_ivs to the IVS for retrieving user's IVC. Subsequently, the IVS requests user's consent for releasing identity information to

the service agency. Once the user agrees, the identity information with an associated federated identity tag for the service agency (FIT_sa) can be sent. The service agency then uses this FIT_sa tag to attach the identity information received to the user record stored locally [26, 43]. Afterwards the user can continue using the service, where the GLS returns the FLT_sa to the service agency for referencing the user to the record stored in the agency.

Chapter 4

Our Methodology

In this chapter we describe our methodology for eliciting the security requirements. We firstly give a brief overview of our approach. Then we discuss each step of the approach in more detail.

4.1 Overview

Among different SRE practices, we identified three important steps in eliciting security requirements for an IdM system. The first step is to identify the security objectives of an IdM system. Since security objectives are the high-level requirements that had been derived mainly from the security need of the stakeholders [57], we could therefore elicit and prioritise security requirements from these objectives while assuring that the expectations of the stakeholders could be met. Secondly, information involved in IdM could be identified for understanding the importance of each piece of the information as well as for recognising the necessary information protection mechanisms. Finally, the last

step for eliciting security requirements was to analyse threats and vulnerabilities within the system.

Generally, after acquiring security requirements for the application, the SRE process is iterated for adapting to any changes in the goals of the stakeholders or the design of the system [33]. In addition, security requirements can be documented with functional requirements, and together they can later be used as a guide for design and specification of the application [57]. Moreover, these requirements can be described using a formal specification language such as JML to avoid any ambiguities in the natural language. However, it is not easy to read or understand a formal specification language and thus out of scope for the purpose of our research.

Since our research is to analyse the security requirements for IdM at a higher level, we would not specify any design or mechanisms for building the system. Hence, a lightweight approach for our research would be adequate. Therefore, we have decided to use the three steps that we had just briefly discussed from the above for eliciting security requirements. Again the steps are:

1. Identifying the security objectives of an IdM system.
2. Analysing the information involved in an IdM system.
3. Analysing the threats and the vulnerabilities of an IdM system.

4.2 Identifying Security Objectives

The first stage to elicit security requirements is to identify the security objectives for an IdM system. In some literatures, the term "security goals" has been used instead of "security objectives". Security goals, according to [33], are often statements within security policies or principles for the system to comply with. Generally, the security goals

are then realised through the specification of security requirements [33]. And yet, most security requirements are based on the security goals specified [30]. Thus, security goals, similar to security objectives, can be seen as a higher level representation of security requirements. In our research, we will not distinguish between these two terms and will use them interchangeably.

The security objectives, which had been discussed in previous chapters, cover general information security goals and control objectives such as authentication. Besides these, we also consider privacy objectives and security properties of a user-centric IdM system as many applications including New Zealand E-government aim to deliver user-centric solutions for their users. Hence, the security objectives for our analysis would primarily be based on the taxonomy of user-centric IdM properties composed by Bhargav-Spantzel et al. [16].

4.3 Information Analysis

The second stage of security requirements elicitation is to identify any relevant assets, resources and information within an IdM system. This stage will be helpful to determine what information needs most protection and thus aids in later stages of eliciting and prioritising security requirements [57].

In order to analyse the information in IdM, we have considered the information management principles in the IdM best practice developed by FIDIS (Future of Identity in the Information Society) [47]. The information management principles are used as guidelines for developing business procedures and checking the completeness of existing operations [47]. According to FIDIS [47], there are five information management principles:

1. **Information:** to identify all types of information including any data, input and

output, and interoperability activities involved in the system.

2. **Roles and responsibilities:** to understand all the legal issues as well as to carry out the responsibility of duty of care.

3. **Processes and procedures:** to recognise business processes and procedures including specifying both internal and external processes.

4. **Enabling technologies:** to support business processes and procedures.

5. **Audit and control:** to monitor and control business processes and procedures.

Moreover, when identifying the personal information, as required by the information principle, we believe the information of an individual should be further analysed according to the type of identifier or credential as well as recording who is authorised to possess this information. The table at the top of Figure 4.1 shows the personal information held in a simple IdM system. In Chapter 5, we will expand this table to show the additional types of personal information held by the New Zealand E-government system. We will also show our additional analysis of this information. The FIDIS group, as far as we know have not named this table, nor have they extended their analysis in the directions we suggest here. Because this table is central to our analysis in Chapter 5, we give it a special name, calling it the "information principle table".

By considering the information management principles, we aim to understand the type of personal information used in IdM and in New Zealand E-government. We will also analyse any requirements for protecting information.

4.4 Threats Analysis

The last stage of our method is to analyse the threats and vulnerabilities of IdM. There are several techniques available for analysing threats including attack trees and misuse

Identity	Information			
	Identifier / Credential	Importance	Held by person	Held by other stakeholders
Person	Name (n)		Yes	All stakeholders
	Signature		Yes	All stakeholders
Location	Address (n)		Yes	All stakeholders
	Location address (n)		Yes	All stakeholders
	Phone Numbers (n)		Yes	All stakeholders
	e-mail address (n)		Yes	All stakeholders

Roles & Responsibilities	Processes & Procedures	Enabling Technologies	Audit & Control
Secure and protect: Information Computer systems Ensure stakeholders & representatives are bona fide Protect: Credit card usage Passwords PIN numbers Comply with statutes & regulations	Purpose for use Application Lifecycle: Input Storage Access Maintenance Deletion Authorisation Confidentiality Security Interoperability	Paper Electronic Web E-mail Cards: Credit (n) Store (n) Licence (n) Membership (n) Etc RFID	Ensure all items are bona fide: Stakeholders & their representatives Documents and copies Compliance with statutes & regulations

Figure 4.1: Principles of Information Management (reproduced from [48])

case analysis. Attack trees analyse all the possible attacks and threats to the system and place these in a tree structure [57]. Whereas, misuse case analysis models the threats to the system in terms of use cases.

Use cases are the most common software engineering approach for capturing and documenting the functional requirements of a system. They are useful in a way to help customers and developers to understand and communicate requirements efficiently and consistently [18].

Like use cases, misuse cases are also helpful in a way for understanding undesirable behaviours of the system. Generally, a misuse case can be seen as an extension of use cases that describes a negative scenario or a use case with hostile intent [57]. Therefore, misuse

cases can be used to elicit security requirements of a system efficiently and consistently.

Furthermore, according to Lee [40], misuse cases provide a better way to convey the threats in diagrams than attack trees. And yet, misuse case diagrams also depict any countermeasure to the threats, which can be helpful for identifying requirements to mitigate such threats. In our research, we use both use and misuse cases with standard UML notations to demonstrate the functionality provided by IdM and to analyse any threats to the system.

Chapter 5

Results and Discussion

In this chapter, we present the findings from our analysis. In Section 5.1 we classify the security objectives for user-centric IdM. In Section 5.2 we analyse the type of information used in New Zealand igovt. Then we present and analyse the use and misuse cases for user-centric IdM and New Zealand igovt.

5.1 Security objectives for user-centric IdM

We found that most of the security and privacy objectives discussed previously in Chapter 1 could be described under Lampson's four security headings. These security headings are [39]:

1. Secrecy
2. Integrity
3. Availability

4. Accountability

These security headings, according to Lampson [39], are useful for describing the user's needs for security, and in which are often expressed in the security policy of the system. By using these headings, we could ensure that the security objectives defined cover the main security aspects of IdM.

Moreover, we also recognised that the security objectives could be applied to either the information or the transaction level of the system. At the information level, the security objectives aim at protecting identity information from any operations conducted by the user or by the system. Generally, the information is associated with some security conditions or levels. At the transaction level, the security objectives aim to protect the transactions in the IdM system. Yet, in some cases, the security objectives can also apply to both the identity information and transactions in IdM.

We have attempted to classify the user-centric IdM taxonomy composed by Bhargav-Spantzel et al. [16] in accordance with the security headings and the two levels discussed from the above. This is shown in table 5.1. From the table, we found that there was no property related to availability from the user-centric taxonomy.

In addition to the above security headings, the control objectives can also be applied to user-centric IdM. The main control objectives that we have identified in Chapter 1 include authentication, authorisation and auditing. These three objectives are being referred by Lampson as the "gold standard", which can be implemented as security mechanisms for the system. [39]

5.2 Information in New Zealand igovt

Based on the information management principles, we have first identified all the possible information that related to the identity of a user in New Zealand igovt services. In the

Security Objectives	Information Level	Transaction Level
Secrecy	Conditional Release Confidentiality Illegal Sharing Prevention Non-transferability Selective Disclosure Stealing Prevention	Anonymity Confidentiality Data minimisation Unlinkability
Integrity	Integrity Revocability Verifiability	Notification Verifiability
Availability		
Accountability		Accountability Non-repudiation Non-replay

Table 5.1: Security objectives for user-centric identity management.

igovt services, there are four main sets of information regarding the user. As shown in table 5.2, the four main sets are:

1. Person: this set contains identity attributes such as name and date of birth, which are used for joining the IVS and for establishing services with service agencies.

2. Status: this set refers to the citizenship as well as the legal status of the user, which can be represented in legal certificates and documents. The documents in the status set can be used by IVS to verify the identity of the user before creating an IVC.

3. IVC: this identification credential is stored in IVS, which consists of identity data attributes, FITs and information about IVC. The identity data attributes belong to the person set, where a subset of the attributes along with an associated FIT are usually forwarded to the service agency that a user has established a service with.

4. GLS: this set includes keys for the user to logon as well as associated key identifiers and FLTs for the GLS and service agencies to identify the user respectively.

Category	**Classification of Personal Information**		
	Identifier/Credential	**Type of Identifier / Credential**	**Possessors**
Person	Name(s)	Descriptor	IVS, Person
	Date of birth	Descriptor	IVS, Person
	Place of birth	Descriptor	IVS, Person
	Sex	Descriptor	IVS, Person
	Mother's birth name	Descriptor	IVS, Person
Status	Birth Certificate	Token	Govt, Person
	Civil Union Certificate	Token	Govt, Person
	Death Certificate	Token	Govt, Person
	Marriage Certificate	Token	Govt, Person
	NZ Citizenship	Token	Govt, Person
	NZ Passport	Token	Govt, Person
	NZ Residency Number	Token	Govt, Person
IVC	Identity data attributes	Descriptor or secret	IVS, Person, SA
	IVC creation stamp	Secret	IVS
	IVC creator	Secret	IVS
	IVC number	Secret	IVS
	IVC status	Secret	IVS
	IVC version number	Secret	IVS
	FIT(s)	Secret	IVS, SA
GLS	Key(s)	Secret	KP,Person
	Key identifier(s)	Secret	GLS, KP
	Root Key(s)	Secret	KP
	FLT(s)	Secret	IVS, GLS, SA
Other	E-mail address(s)	Descriptor	GLS,Person
	Referee's declaration	Token	Govt, Person
	Session ID(s)	Secret	GLS, SA
	Transaction logs	Secret	GLS, SA

Table 5.2: This information principle table shows our classification of personal information held by New Zealand igovt. We identify five categories of identifiers or credentials: Personal, Status, IVC, GLS, Other. Each identifier or credential is a Descriptor, Token, Secret, or a combination of these basic types. Our table also indicates the entities that are authorised to hold each identifier or credential.

In addition to the four sets of information, other data may be requested or created in igovt. For instance, the current GLS requires the user's email address for registering a logon. A referee's declaration may be needed as secondary evidence for identity verification in IVS.

Moreover, we have modified the information principle table, which an example is shown in Section 4.3. As shown in the same table, table 5.2, we have identified the entities that own the identifier/credential or hold the record of it. We have also distinguished the identifier/credential into three types (this is similar to the three types of authentication methods discussed in Chapter 2):

- Descriptor: is simply a description of an identity, which is difficult to monitor and control as the description can be reproduced or forwarded easily;
- Token: is something that the user has physical possession of, which is generally issued by an authoritative source with controls over reproduction. It ensures higher level of confidence in the authentication of the user as well as the integrity of personal information. And yet, copies of the tokens can be verified against the original ones;
- Secret: is something only known to a limited number of parties, in other words it is a descriptor with controlled distribution.

Since both IVS and GLS in igovt mostly deal with identifiers or credentials that are secret, as seen from table 5.2, it is important to secure and protect these sets of information. Generally speaking, the other four information principles for the information held in igovt would include the following requirements:

- **Roles and responsibilities:** both IVS and GLS have the roles and responsibilities to protect information and secret and destroy out of date information while complying with regulations;

- **Processes and procedures:** the processes and procedures in igovt have to consider information lifecycle, matching checks as well as the information used in authentication and authorisation;

- **Enabling technologies:** the technologies for the information used in igovt range from paper to electronic databases;

- **Audit and control:** ensures everything involved in igovt is genuine and compliant with regulations.

5.3 Analysing Misuse Cases for IdM

Before analysing New Zealand igovt, we first examine the misuse cases for a simple IdM system based on the conceptual IdM framework model found in Chapter 2. We considered this IdM system to be user-centric and in a centralised environment with one identity provider and multiple service providers.

In the following sections, we describe the main actors involved in the simple IdM system. We then give an overview of the use cases and subsequently the relevant misuse cases for the simple IdM. After these, we examine New Zealand igovt with the user-centric security objectives as well as the information principle identified from Section 5.1 and Section 5.2.

5.3.1 Actors in IdM

We have identified the four main actors for a centralised user-centric IdM system. These are:

User

The user has different identities, credentials and physical possession of tokens. He or she can make use of one of the identities to access a resource, fulfil a goal or to carry out some tasks.

Identity Provider

The Identity Provider (IdP) can be both an authenticator and a manager of identities. As an authenticator, the IdP authenticates the user as the claimed identity based on the credentials and tokens presented. Once the user had been authenticated, it also passes security assertions about the claimed identity to service providers that the user wishes to gain access for. On the other hand, as a manager, the IdP does not provide any authentication services. It simply creates identities and manages associated information as well as authentication tokens for the user.

Service Provider

The Service Provider (SP) offers services to users, usually to the ones whom had been authenticated by an identity provider. It also specifies and enforces access control policies for the services it provides.

Misuser

The misuser can be any individual person (or group) with malicious intents to benefit from the information, services and transactions of an IdM system. Generally, a misuser tends to achieve his objectives through unauthorised observations or inappropriate operations on the IdM system. In some cases, a misuser can be a normal user who had unintentionally harmed the system with some misused behaviours.

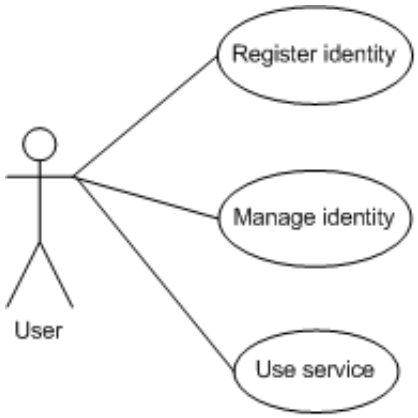


Figure 5.1: Overview of the main use cases for IdM

5.3.2 Overview of IdM Use Cases

As we considered IdM to be more user-centric, we have identified three main use cases based on individual's objectives for an IdM system found in Chapter 2. As shown in figure 5.1, the three use cases derived from such objectives with a user as the main actor are:

1. **Register Identity.** This use case describes how a user registers his identity to the identity provider.

2. **Manage Identity.** This use case describes how a user manages his account with the identity provider. The user can view and update his identity information.

3. **Use Service.**This use case describes how a user uses his identity to obtain access to services provided by service providers.

5.3.3 Register Identity

This use case describes how a user registers an identity to the identity provider. Generally, when a user registers with the identity provider, the identity provider will check the

identity and then create a new account for the user. This process is a part of the user provisioning functionality discussed in Chapter 2.

There are two major misuse cases that exploit this use case. These misuse cases are:

- **Repudiate a registration:** a misuser denies a valid registration of identity and may later on re-register with his own identity. And consequently, the link between the user and the identity is lost. Thereby, the user can no longer use his identity for the services he was entitled to.

- **Impersonate an identity:** a misuser claims an identity that he does not represent and for which the identity created in the system does not correspond to the actual user. False or stolen credentials maybe presented by the misuser to prove the validity of the identity he tries to pretend.

Figure (to appear) shows an overview of the misuse cases identified for the registration process.

In order to mitigate these misuses, it is important to have some auditing mechanisms as well as some procedures for verifying the identity of the user in the system. Figure 5.2 illustrates the use case for a user registering an identity with the two main misuse cases. It also shows associated use cases that can be used to reduce the possibility of the misuse cases succeeding. For instance, in this figure, we have the use case "verify identity" that mitigates the misuse case "impersonate an identity". This implies that the misuser has less chance of successfully registering a false identity to the identity provider.

5.3.4 Manage Identity

In the use case of manage identity, a user can view and modify identity information in own account. For a user-centric IdM, this use case also includes the use case of "notify

Figure 5.2: Overview of use and misuse cases for Register Identity

and consent". The "notify and consent" case enables the user to receive notifications and consent requests from the system for using identity and associated information.

In this use case, as shown in figure 5.3, the misuse cases include:

- **Tamper with data:** a misuser gains access to a user's account and corrupts or modifies the identity information of the user. Consequently, this may lead to disruption of user's access to own account or services.

- **Observe data and transactions:** a misuser observes and gathers information through user's account and transactions. The misuser may then match the information observed with other data or disclose information to others, and for which exploiting the privacy of the users. However, this exploitation is not explicitly

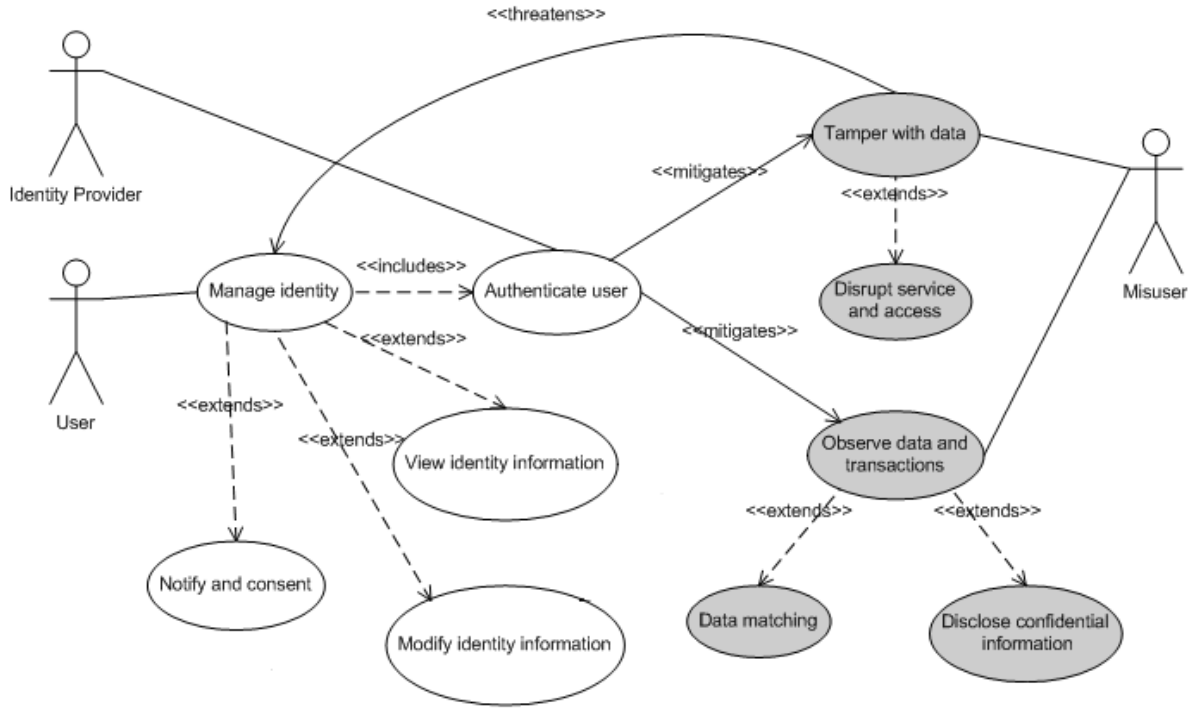


Figure 5.3: Overview of use and misuse cases for Manage Identity

shown in figure 5.3, as the actions of the user are not directly affected.

Generally, the user needs to be authenticated by the identity provider before accessing his account. This reduces the chance of making identity information accessible to wrong people and thus helps to mitigate these misuse cases for managing identity.

5.3.5 Use Service

In this use case, a user authenticates himself to the identity provider and subsequently obtains permission from service providers to use services and resources provided. Usually, the service provider also obtains and uses information about the user when he accesses the service.

Like the misuse cases from the above, the "Use service" use case is also exploited by misusers tampering with identity information and repudiating the transactions taken

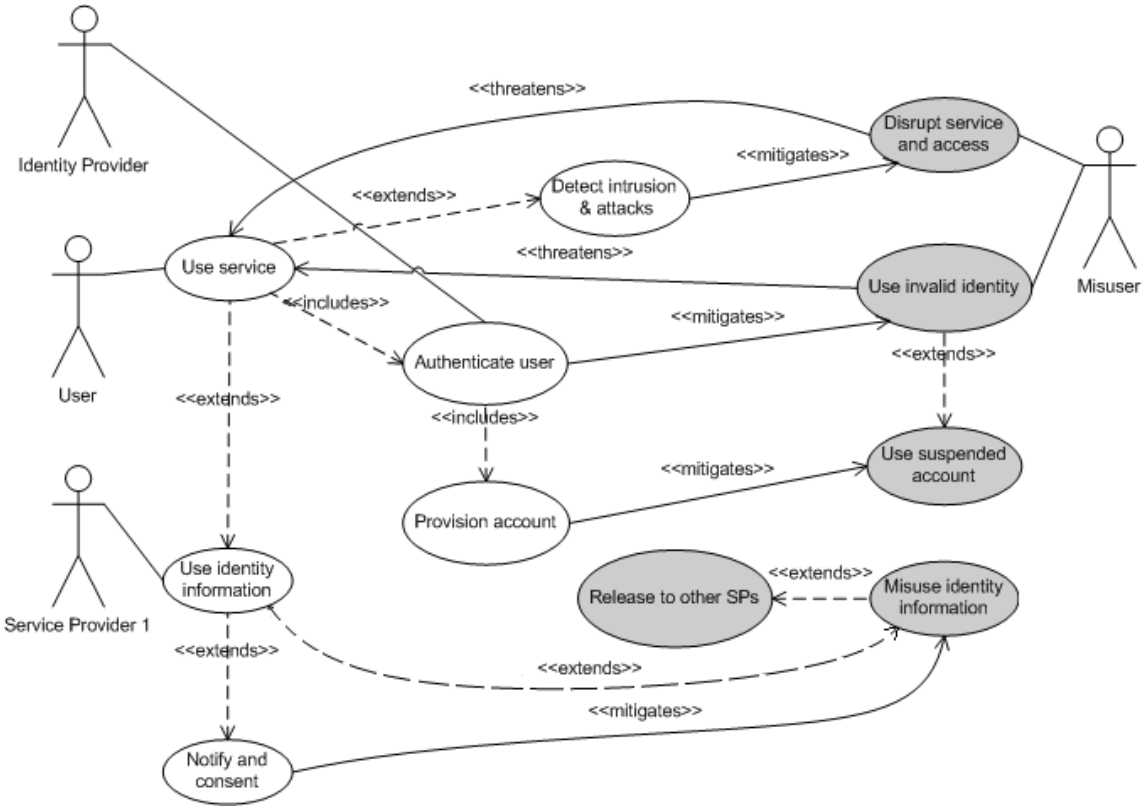


Figure 5.4: Use Service

place. And yet, the privacy of the user can be violated by unauthorised observation and access to resources, which can lead to unauthorised disclosure of user's information and behaviours. In addition to these, there are three more misuse cases that can hinder the user from accessing services and resources. As depicted in figure 5.4, the cases include:

- **Disrupt service and access:** this can be extended from a misuser tampering with data as shown in the previous section. A misuser disrupts and usurps system component, which can affect the user using services. This may also lead to denial of service.

- **Use invalid identity:** a misuser tries to use an invalid identity to access to services and resources. The misuser may also attempts to use accounts that have been suspended or deleted.

- **Misuse identity information:** this can be seen as an insider threat as the service provider may use identity information beyond the expectations of the user. It also includes releasing information to other service providers. And thereby the misuse imposes a threat on the privacy of the user, which is not explicitly shown in the figure.

Again, in order to mitigate these misuse cases, it is important to have authentication for the user. Moreover, mechanisms for availability such as intrusion detection are needed in place to ensure that the services can still be provided even under attack. Furthermore, as one of the user-centric IdM objectives, the use case "notify and consent" is included which gives more control to the user and thus lowers the risks of the service provider misusing identity information.

5.3.6 Security requirements elicited

From the above analysis of misuse cases, we find that the main security mechanisms required for an IdM system are as follows:

- Audit and non-repudiation: to provide evidence about users' interactions and to prevent a misuser from denying a righteous transaction;
- Authentication: to provide a strong verifying process for establishing identity;
- Authentication: to provide a strong authenticating process for user obtaining access to services and resources. Usually, there are three types of authentication methods that can be used (see Section 2.2.3);
- Availability: to provide some mechanisms to detect attempted intrusions as well as to survive attacks from the misusers;

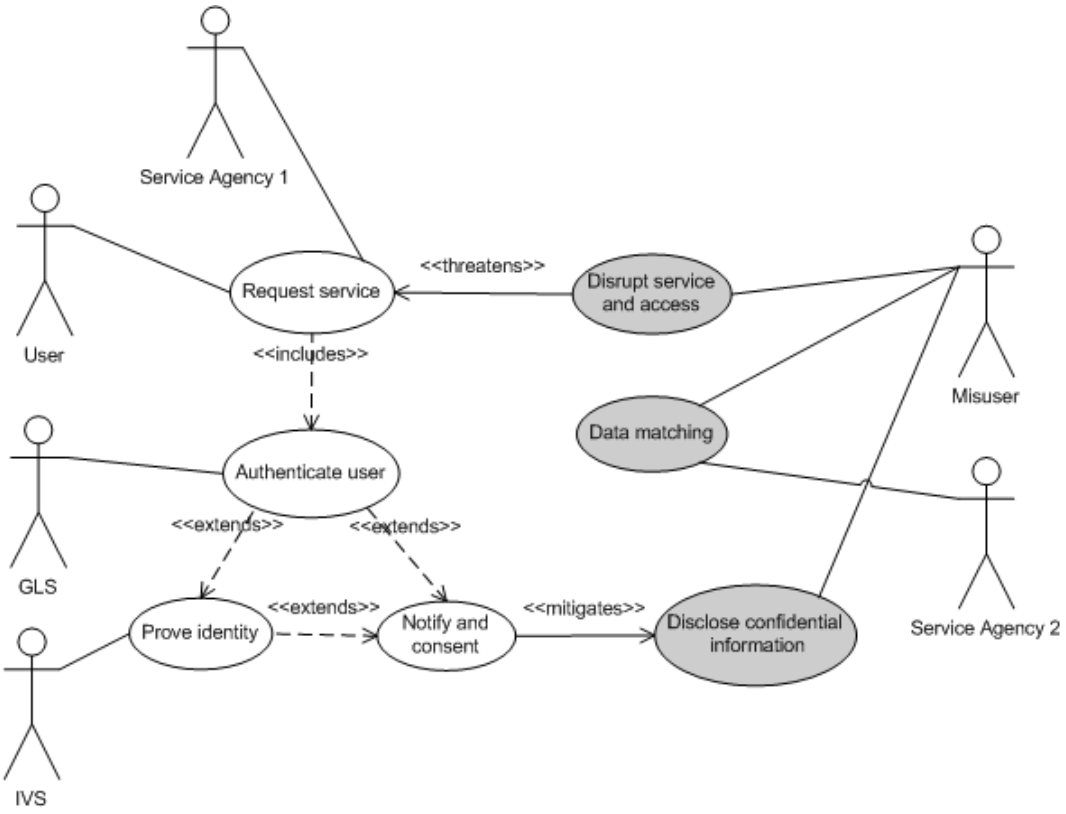


Figure 5.5: Requesting a service and prove identity to service provider in New Zealand igovt

- Privacy protection: to provide some mechanisms, including verifiability (user consent) as well as other privacy objectives identified in Section 2.3.2, for protecting privacy in identity information and transactions.

Comparing with the security objectives found in Section 5.1, we find that we can add intrusion detection and survivability to the security objectives table 5.1 under the transaction level category in availability.

5.4 Analysing New Zealand igovt

We have analysed the New Zealand igovt based on the security objectives and the misuse cases identified. Like the misuse cases from the previous section, we analysed igovt with the basic use cases of registering, managing and using identities. Figure 5.5 shows the example of a user requesting for a service in igovt. As a result, we find that the threats and the security requirements elicited from the misuse cases are similar to the ones found from the above. Likewise, from the information analysed we find that the integrity of the information, particularly of the secret or token type, are important to both the users and the igovt system as they need such information for verification and authentication.

Moreover, we have also compared the existing security designs in New Zealand igovt with the security objectives in table 5.1 as well as the additional availability objectives. We find that the design of New Zealand igovt meets with most of the general security headings. However, it is still missing some of the security properties that we have identified for user-centric IdM systems. The following sections briefly describe the findings from the comparisons.

5.4.1 Secrecy

The authentication principles for New Zealand E-government (see Section 3.3.1) have stated that the authentication programme needs to ensure the security and privacy of information. In the design of igovt, privacy of individuals is preserved in one way by giving users the control of their personal information and for which corresponds to the security objective "Selective Disclosure". Moreover, igovt also meets the objectives of confidentiality and data minimisation as it provides identifiers that are secrets to the service agencies and stores only the minimum amount of identity information. However, it has not considered some of the information level objectives such as illegal sharing

prevention.

5.4.2 Integrity

Although not explicitly stated in the design of New Zealand igovt, we find that it meets the security objectives of revocability and verifiability. It meets the objective of revocability as the IVS has some revocation policies in place for the credentials (IVC) that have only life duration of five years. It also satisfies verifiability since igovt will ask the user first before passing identity information to service agencies.

5.4.3 Availability

Despite strong emphasis on privacy and user control, we find that the igovt does not focus heavily on the availability of the application. However, we think it is important to take availability into consideration. This is because, as mentioned in Chapter 3, government systems need to be more reliable and trust-worthy as people usually have higher expectations in the government. Moreover, as igovt is similar to the centralised SSO model, it can easily become a single point of failure. Therefore, intrusion detection and attack survivability are essential for igovt.

5.4.4 Accountability

The igovt also meets the non-repudiation objective as stated in the authentication principles (in Section 3.3.1) for implementation.

Chapter 6

Conclusions and Future Work

In this chapter we outline the main findings and conclusions from our study. And then we discuss any possible areas for future work.

6.1 Conclusions

In this thesis, we have conducted a preliminary security analysis on New Zealand's igovt system using the proposed methodology. Before conducting the analysis, we have first examined and understood the concepts of IdM systems in Chapter 2. Then, from this chapter, we identified the security objectives for a user-centric IdM system.

In Chapter 3, we examined the New Zealand's igovt system, which was originated from the Authentication Programme led by the State Services Commission. We examined the igovt system through its components as well as its proposed procedures for delivering authentication services to the public. We have also attempted to analyse the procedures by using sequence diagrams.

After examining the IdM systems and the New Zealand's igovt system, we have proposed a lightweight methodology to analyse the security of the igovt system. In our proposal, there were three steps involved. First was to identify the main security objectives of the system. Second was to analyse the types of information held in the system, where we have applied the FIDIS methodology. Finally, we tried to analyse the threats to the system using misuse case analysis. Afterwards, we elicit the security requirements from the misuse cases.

Finally in Chapter 5, we presented the list of security objectives identified from Chapter 2. We have also analysed the types of information held in the igovt system. We then proposed three main use cases according to the IdM objectives for individuals. From these use cases and related misuse cases, we found the main security requirements for a user-centric IdM include objectives such as authentication, non-repudiation and privacy protection. As our methodology was a lightweight approach to requirements engineering, the requirements generated would not be specific. We also found a limitation in misuse cases, where some misuse did not exploit an identifiable sequence of actions.

After the general misuse case analysis, we also discovered that the New Zealand's igovt system has similar set of security requirements. Furthermore, we have also compared the igovt design with the security objectives identified. From the comparisons, we found that the New Zealand's igovt meet most of the user-centric security objectives identified. In addition, we found that both user-centric IdM and the igovt need to consider the objective of availability.

In conclusion, we have proposed a methodology for performing a security analysis of an identity management system. We have attempted to illustrate this methodology through a preliminary analysis of the igovt system. Since this is an early stage exploratory method, the resulted security objectives and requirements are not definitive.

6.2 Future Work

This thesis has identified some of the possible areas to consider for future work. Firstly, we limited the actions of the misuse case, where a use case could only mitigate a misuse case. However, in many cases, the use case cannot prevent the actions of the misuser and thus it usually provides some mechanisms to respond after the actions of the misuser had taken place. Moreover, use case diagrams may not be sufficient to visualise all the threats and relationships within the system, as the misuse case may not always be an identifiable sequence of actions or may not exploit the identifiable actions. This was found as one of the limitations to present privacy violation in our analysis. Thus, to overcome this problem, further investigations including different notations and descriptions into misuse case analysis may be needed. Different notations such as the operational concepts in systems engineering may be considered, where the misuse cases are treated as exceptional cases.

Furthermore, there are other areas we have considered for future work. These include:

- Trust of the users. In our research we have assumed that all of the components were trustworthy. However, in the real world the users may not put full trust into the system and thereby this may affect the way of the system providing services and handling identity information.

- Validation of the security objectives. Due to the timeframe of our research we were unable to validate the security objectives for user-centric IdM. For future research, validation as well as verification can be included to check its feasibility.

- Evaluation of use cases. As our research is only a preliminary study, we did not evaluate the use cases. However, for furture work, it is important to check the completeness and correctness of the use cases to ensure that all the areas of the system have been covered.

Bibliography

[1] Agency checklist - november 2007. Available at: http://www.e.govt.nz/about-egovt/programme/agency-checklist-2007 [Online; accessed March 24, 2008].

[2] All-of-government authentication programme. Available at: http://www.e.govt.nz/services/authentication [Online; accessed March 24, 2008].

[3] Authentication principles. Available at: http://www.e.govt.nz/services/authentication/policywork [Online; accessed March 24, 2008].

[4] The convenience of an all-of-government logon. Available at: https://www2.logon.govt.nz/cls/static/homepage.jsp [Online; accessed March 24, 2008].

[5] E-authentication guidance for federal agencies. Available at: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf [Online; accessed December 6, 2007].

[6] Faqs. Available at: http://www.e.govt.nz/services/authentication/standards/faqs.html [Online; accessed March 24, 2008].

[7] Glossary of statistical terms - privacy. Available at: http://stats.oecd.org/glossary/detail.asp?ID=6959 [Online; accessed April 22, 2008].

[8] Gls - overview. Available at: http://www.e.govt.nz/services/authentication/gls [Online; accessed March 24, 2008].

[9] How the gls works. Available at: http://www.e.govt.nz/services/authentication/gls/how-the-gls-works.html [Online; accessed March 24, 2008].

[10] Ivs overview. Available at: http://www.e.govt.nz/services/authentication/ivs [Online; accessed March 24, 2008].

[11] Liberty alliance project. Available at: http://www.projectliberty.org/ [Online; accessed January 20, 2008].

[12] Overview of the e-government programme. Available at: http://www.e.govt.nz/about-egovt/programme [Online; accessed October 24, 2007].

[13] J. Altmann and R. Sampath. Unique: A user-centric framework for network identity management. *Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*, pages 495–506, 0-0 2006.

[14] A.I. Anton and J.B. Earp. A requirements taxonomy for reducing web site privacy vulnerabilities. *Requir. Eng.*, 9(3):169–185, 2004.

[15] K. Barzilai-Nahon and H.J. Scholl. Similarities and differences of e-commerce and e-government: Insights from a pilot study. *hicss*, 00:92c, 2007.

[16] A. Bhargav-Spantzel, J. Camenisch, T. Gross, and D. Sommer. User centricity: a taxonomy and open issues. *Journal of Computer Security*, 15(5):493–527, 2007.

[17] A. Bhargav-Spantzel, A.C. Squicciarini, and E. Bertino. Trust negotiation in identity management. *IEEE Security and Privacy*, 5(2):55–63, 2007.

[18] K. Bittner. *Use Case Modeling*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

BIBLIOGRAPHY

[19] K. Bosworth, M.G. Gonzalez Lee, S. Jaweed, and T. Wright. Entities, identities, identifiers and credentials – what does it all mean? *BT Technology Journal*, 23(4):25–36, 2005.

[20] D.A. Buell and R. Sandhu. Identity management. *Internet Computing, IEEE*, 7(6):26–28, Nov.-Dec. 2003.

[21] K. Cameron. The laws of identity. Available at: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf [Online; accessed September 18, 2007].

[22] J.L. Camp. Digital identity. *Technology and Society Magazine, IEEE*, 23(3):34–41, Fall 2004.

[23] F. Chong. Identity and access management. *Microsoft Architect Journal*, 3:20–31, 2004.

[24] S. Clauss, D. Kesdogan, and T. Kolsch. Privacy enhancing identity management: protection against re-identification and profiling. In *DIM '05: Proceedings of the 2005 workshop on Digital identity management*, pages 84–93, New York, NY, USA, 2005. ACM.

[25] New Zealand State Services Commission. Authentication for e-government: Best practice framework for authentication, 2004.

[26] State Services Commission. Privacy impact assessment of the all of government authentication programme - identity verification service, 2004. Available at: http://www.dia.govt.nz/Pubforms.nsf/URL/IVSPIA.pdf/$file/IVSPIA.pdf [Online; accessed October 24, 2007].

[27] F. Corradini, E. Paganelli, and A. Polzonetti. The e-government digital credentials. *Int. J. Electronic Governance*, 1(1), 2007.

[28] E. Damiani, S.D.C di Vimercati, and P. Samarati. Managing multiple and dependable identities. *IEEE Internet Computing*, 7(6):29–37, 2003.

[29] Z. Fang. E-government in digital era: Concept, practice and development. *International Journal of The Computer, The Internet and Management*, 10(2):1–22, 2002.

[30] D. Firesmith. Engineering security requirements. *Journal of Object Technology*, 2(1):53–68, 2003.

[31] S. Gevers, V. Verslype, and B. De Decker. Enhancing privacy in identity management systems. In *WPES '07: Proceedings of the 2007 ACM workshop on Privacy in electronic society*, pages 60–63, New York, NY, USA, 2007. ACM.

[32] The Open Group. Identity management business scenario. Technical report, The Open Group, 2002.

[33] C. Haley, R. Laney, J. Moffett, and B. Nuseibeh. Security requirements engineering: A framework for representation and analysis. *IEEE Transactions on Software Engineering*, 34(1):133–153, 2008.

[34] C.J. Harding, R.K. Mizumori, and R.B. Williams. Architectures for identity management. Technical guide, The Open Group, 2007.

[35] A. Josang, M. Al Zomai, and S. Suriadi. Usability and privacy in identity management architectures. In *ACSW '07: Proceedings of the fifth Australasian symposium on ACSW frontiers*, pages 143–152, Darlinghurst, Australia, Australia, 2007. Australian Computer Society, Inc.

[36] J. Joshi, A. Ghafoor, W.G. Aref, and E.H. Spafford. Digital government security infrastructure design challenges. *Computer*, 34(2):66–72, 2001.

[37] G. Kreizman and B. Rust. Government id and authentication: The right project scope. Research note, Gartner Research, 2004.

[38] G. Kreizman and R. Wagner. Waiting to catch the personal identity wave. Research note, Gartner Research, 2006.

[39] B.W. Lampson. Computer security in the real world. *Computer*, 37(6):37–46, 2004.

[40] J. Lee. Perceptions of hipaa security requirements by us dental schools. Master's thesis, University of Auckland, Auckland, New Zealand, September 2006. .

[41] S.M. Lee, X. Tan, and S. Trimi. Current practices of leading e-government countries. *Commun. ACM*, 48(10):99–104, 2005.

[42] W. MacGregor, W. Dutcher, and J. Khan. An ontology of identity credentials part 1: Background and formulation - draft. Technical report, National Institute of Standards and Technology (NIST), 2006.

[43] R. McKenzie, M. Crompton, and C. Wallis. Use cases for identity management in e-government. *Security & Privacy, IEEE*, 6(2):51–57, March-April 2008.

[44] M.C. Mont, P. Bramhall, and J. Pato. On adaptive identity management: The next generation of identity management technologies, 2003. Available at: http://www.hpl.hp.com/techreports/2003/HPL-2003-149.pdf [Online; accessed September 17, 2007].

[45] OECD. Oecd guidelines on the protection of privacy and transborder flows of personal data. Available at: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html [Online; accessed December 18, 2007].

[46] Future of Identity in the Information Society. D2.3: Models, 2005. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.3.models.pdf [Online; accessed October 15, 2007].

[47] Future of Identity in the Information Society. D4.6: Draft best practice guidelines, 2006. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.6.best_practice_guidelines.pdf [Online; accessed October 15, 2007].

[48] Future of Identity in the Information Society. D4.8: Creating the method to incorporate fidis research for generic application, 2007. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.8.generic%20application.pdf [Online; accessed October 15, 2007].

[49] Department of Internal Affairs. Public consultation about verifying your identity to government agencies using the internet - faq. Available at: http://www.dia.govt.nz/diawebsite.nsf/Files/IVSFAQ/$file/IVSFAQ.pdf [Online; accessed November 13, 2007].

[50] Department of Internal Affairs. Public consultation about verifying your identity to government agencies using the internet - information for public consultation. Available at: http://www.dia.govt.nz/diawebsite.nsf/Files/IVSInfo/$file/IVSInfo.pdf [Online; accessed November 13, 2007].

[51] T. Olsena and T. Mahlera. Risk, responsibility and compliance in 'circles of trust' - part 1. *Computer Law and Security Report*, 23(4):342–351, 2007.

[52] A. Pfitzmann and M. Hansen. Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management - a consolidated proposal for terminology (v0.31), 2008. Available at: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml [Online; accessed March 1, 2008].

[53] G. Salaway and R. Yanosky. Identity management in higher education: A baseline study. Technical report, EDUCAUSE, 2006.

[54] D. Shin, G.J. Ahn, and P. Shenoy. Ensuring information assurance in federated identity management. *Performance, Computing, and Communications, 2004 IEEE International Conference on*, pages 821–826, 2004.

[55] Skip Slone and The Open Group Identity Management Work Area. Identity management. White paper, The Open Group, 2004.

[56] M. Small. Unify and simplify: re-thinking identity management. *Network Security*, 2006(7):11–14, 2006.

[57] I.A. Tondel, M.G. Jaatun, and P.H. Meland. Security requirements for the rest of us: A survey. *IEEE Software*, 25(1):20–27, 2008.

[58] R. Witty, A. Allan, J. Enck, and R. Wagner. Identity and access management defined. Research note, Gartner Research, 2003.