Preliminary Security Specification for New Zealand's igovt System

Yu-Cheng Tu[1] **Clark Thomborson**[1]

[1] Department of Computer Science,
The University of Auckland,
Auckland, New Zealand,
Email: ytu001@aucklanduni.ac.nz, cthombor@cs.auckland.ac.nz

Abstract

The New Zealand government has proposed an identity management system, to provide an effective and convenient alternative for citizens to access online government information and services. The proposed system is branded as "igovt", which offers two types of authentication services. The first service provides people and businesses with logon identities. The second service provides semi-anonymised identities to government agencies. Each semi-anonymised identity carries a strictly limited amount of information about a logon identity along with an assurance that it corresponds to a living New Zealand citizen or a registered business entity. The New Zealand government has carefully designed the system with clearly-articulated policy principles. It has also conducted several privacy impact assessments and public consultations. However, the New Zealand government has not published any security analyses for igovt, and we are not aware of any unpublished ones. In this paper, we propose a lightweight methodology for the elicitation of security requirements of a complex but incompletely unimplemented system, such as igovt. We illustrate the use of our methodology by developing preliminary security specifications for a portion of the igovt system.

Keywords: Identity management, E-government, Security Requirements Engineering.

1 Introduction

Identity management (IdM) is often described as the administration of identity in IT systems. A managed identity is, generally, unique within an organisation and is associated with a specific user. IdM can be considered as the infrastructure for identity-authentication services. A full-featured IdM system will create user accounts and their associated identities; it will manage all identity activities during an account's lifetime; and it will revoke all identities and associated privileges when a user account is closed. In order to achieve these tasks, accurate user identification and authentication will be essential to IdM systems (Harding et al. 2007).

Generally, in a commercial context, IdM expresses the goals and procedures for managing identity through a combination of business policy and IT practices (Josang et al. 2007, Slone 2004). The underlying security principles in IdM aid in business operations for achieving effective identity provisioning and access control. Thus, IdM is often included as a part of the business strategy for improving the efficiency and the security in managing identities (Slone 2004)

Similarly, IdM is often integrated in E-government applications. It plays an important role in assuring the security of individual identities (Kreizman & Rust 2004). Unlike commercial IdM systems, governmental IdM systems require stronger means of security and privacy mechanisms. This is because governments bear greater responsibilities and expectations for delivering services to the public. They have the obligations to support all of their constituents while protecting individual privacy (Joshi et al. 2001). Therefore, IdM systems in governmental applications are not only important to people and governments for utilising digital identities, but they are also crucial to the security and privacy of individuals.

An example of the IdM system for E-government can be found in New Zealand government's Authentication Programme, which had been established in 2000. The main initiative of the programme is to improve the online delivery of government information and services to the public. It is also aimed to improve the internal performance of government agencies (SSC 2006). With these initiatives, the IdM system proposed in the scheme had been branded as "igovt". The igovt consists of two separate online authentication services, Identity Verification Service (IVS) and Government Logon Service (GLS). The IVS intends to enable people to verify their identities to government agencies online with verified identity assertions. The GLS, as suggested by its name, manages the logon process which will enable people and businesses to access multiple government services with single logons. Currently, the IVS is under development and it will be piloted with limited services in 2009. On the other hand, the GLS is now available and in place for government agencies to adapt to. Together, igovt aims to provide an "all-of-government" solution, which will standardise the authentication mechanisms across government agencies. Therefore, reducing the number of identity verifications and logons for accessing different online services (McKenzie et al. 2008, SSC 2008*b*).

In order to support this all-of-government solution, the New Zealand government has identified key policy and implementation principles during the initial stage of the programme. These principles covered (McKenzie et al. 2008, SSC 2008*a*):

- 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.

In addition to the principles specified, the programme has conducted privacy impact assessments for analysing the potential influences of the IVS and the GLS on privacy respectively. Besides the privacy impact assessments, research of issues on the Maori people relating to the Authentication Programme had also been carried out. Examples of the issues raised from these assessments include concerns in multiple identities and collective privacy of the Maori people (SSC 2004, 2005*a*,*b*).

Furthermore, the New Zealand government has recently conducted a public consultation for the general public as well as businesses and organisations to provide feedbacks about online authentication and the proposed igovt services. From the consultation, the government has identified several key views which are important for ensuring that the igovt will be usable and valuable for both people and businesses in New Zealand. In order to encourage the uptake of igovt, these key views include (DIA 2008):

- The services of igovt shall be user-friendly to any types of users with low fee or no cost at all;
- The igovt services shall be accessible and available for use in a wide range of government agencies and government services;
- The security and privacy protection aspects of igovt shall be considered and managed;

From the above key principles, assessments and public opinions for the two igovt services, we find that the New Zealand government displays a well-defined design of IdM. It clearly identifies the goals and policy for what is to be achieved in igovt. Moreover, it also demonstrates government's attempt to appreciate its citizens with user-focused IdM design and public consultations. These can possibly avoid rejections of the services from the public.

However, we cannot find any related security requirements analysis for igovt even though the security as well as its importance in the services was mentioned in both the key principles and the public consultation report. Security requirements analysis, also known as security requirements engineering, is crucial to systems as the security requirements elicited from such analysis can prevent or mitigate owners' losses from security threats and attacks (Dwaikat & Parisi-Presicce October 2004, Tondel et al. 2008). Moreover, according to Haley et al. (2008), organisations are likely to face great financial impacts without proper security analysis or security requirements of the complete system. On the other hand, applications with adequate security requirements are more likely to be trusted and accepted (Haley et al. 2008). Thus, in order to minimise the risks of financial losses and to increase people's confidence as well as acceptance level about igovt, it is important to analyse the security of the system. Since the IVS of igovt is still at the development stage and there is little detail about the exact design or implementation, the security requirements elicited for igovt will be at a higher level of abstraction and will not be specific to any particular security mechanisms.

Therefore, in this paper we attempt to identify the preliminary security specifications for New Zealand's igovt system with a proposed set of security analysis methodology. The remainder of this paper is structured as follows. In Section 2, we briefly describe igovt with a conceptual diagram of the entities involved in the system based on the standard UML notations. We also discuss the authentication procedures in both the GLS and the IVS through sequence diagrams. In Section 3, we discuss our methodology for analysing the security of igovt. Then we present the results of our analysis of the system. And in Section 5, we end with our conclusions.

2 New Zealand's igovt system

The New Zealand government's igovt system intends to offer people an option to verify their identities to different government agencies online without going through multiple identity documents. It also aims to reduce the number of logons needed for different public services. The igovt system is roughly consistent with the user-centric IdM system, which seeks for the consent of the user before passing the identity information to the service provider.

However, unlike the standard IdM system, the New Zealand government separates user authentication into identity verification (IVS) and logon management (GLS). At the front-end, these services will be integrated and presented to the public through a single interface. At the back-end, the two services are being maintained by two independent government agencies. The reason for the separation of identity information and logon activity is to enhance privacy protection and to minimise the probability of data matching in government agencies (DIA 2007*b*, McKenzie et al. 2008). While these services handle user authentication for the agencies, each service-providing government agency still retains the responsibility for its user authorisation and access control. Therefore, by separating authentication and authorisation, privacy protection can be improved further and the elevation of user privileges can be prevented in igovt (McKenzie et al. 2008).

In Figure 1 we have depicted the igovt system in an Entity-Relationship Diagram, where there are seven main entities involved:

- 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;
- igovt: a governmental IdM system designed 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 manages the logons. It is associated with one or more key providers for confirming the validity of the keys provided by the citizens. It also authenticates citizens' identities to service agencies;
- Key provider: an agency for issuing keys for logon to citizens and checking the validity of the keys when requested by the GLS;
- Review Body: an independent government agency such as an Ombudsman for making advices or handling complaints and investigations about the authentication process. It also ensures that the igovt complies with legislation and regulations such as the Privacy Act.

In the following sections, we discuss the main authentication services of igovt in more detail. We also describe the procedures for the logons and the identity verification in the GLS and the IVS respectively.

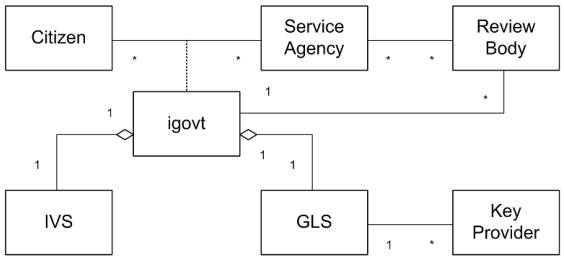

Figure 1: Entity-Relationship Diagram for the igovt system.

2.1 Government Logon Service (GLS)

The GLS enables people as well as businesses and organisations to access various online government services with single logons. It is operated by the State Services Commission and has recently become available to all government agencies in New Zealand. Most of the agencies are now expected to adapt their logon management to this newly designed services (McKenzie et al. 2008).

Currently, the GLS is offering two levels of authentication mechanisms for access to online services. The first authentication mechanism consists of only the low strength logons, i.e. username and password. This is used for services that are of low identity risks. The second is used for services that possess moderate identity-related risks, where multifactor authentication is required. For this level of authentication, a GLS token, which is a small device that generates unique token numbers, will be issued to the user for use along with username and password.

The logon process in GLS conforms to the single sign-on profile in the Security Assertion Markup Language (SAML) as the GLS as well as the IVS have been designed to use SAML to exchange authentication data within the igovt system. The authentication data exchanged with the GLS is a unique number specific to that service agency (or IVS) and the user. This number is known as the federated logon tag (FLT). It contains no identity information and is used as a persistent identifier for service agencies as well as the IVS to recognise the users whenever they logon through the GLS (McKenzie et al. 2008, SSC 2007). Since the GLS only delivers unique numbers without any specific identity information, McKenzie et al. (2008) describe the service as a pseudonymous identity provider. Moreover, as depicted in Figure 1, in order to enhance individual privacy, the GLS has separate key providers which limit the amount of information known by a single component about a particular user (McKenzie et al. 2008). Figure 2 shows an example sequence of the logon process in the GLS. A user makes an online request to government's service agency for a service. The service agency redirects the user to the GLS for logon. Then the user presents a logon key identifier such as username and password to the GLS. Where, the GLS passes the logon key identifier to a key provider for confirming with the root key about the validity of the identifier. After validation, another key identifier is returned to the GLS. This key identifier is used for finding the FLT associating the user and the service agency (FLT_sa) stored in the GLS. Subsequently, FLT_sa is passed to the agency and the user is redirected back to the agency's browser. With FLT_sa, the service agency is able to reference the user to its own record. And thereby, the agency can determine user's eligibility to the requested service.

2.2 Identity Verification Service (IVS)

The proposed IVS plans to verify the identities of the users online with security assertions to government agencies. It provides an alternative means for the public to complete the identity proof process for different government services without presenting the same identity documents multiple times. At present, the IVS is not available to the public yet. It is planned to be introduced in phases with the first identity verification service limited to New Zealand citizens in 2009 and then gradually to any person who wishes to join the igovt services (DIA 2007*a*).

The primary design goals of the IVS are, in general, consistent with the primary goal of user-centric IdM system (Bhargav-Spantzel et al. 2007), in that the IVS attempts to maximise the control exerted by individual users over their identity information. In particular, the IVS will obtain permission from the identity owner before forwarding personal information to other government agencies. Protection of individual privacy is an important property in a user-centric IdM, and it is also important to the IVS. Several aspects of the IVS have been designed specifically to improve the privacy of the users.

The first aspect of privacy protection is the design of storing only a minimal amount of core identity information in the electronic database maintained by the Department of Internal Affairs. The core identity information stored includes only the name(s), date of birth, place of birth, and the gender of the user (DIA 2007*b*). The second aspect is the use of unique identifiers for different government agencies. Furthermore, information obtained from the GLS is not stored together with the IVS. Therefore, these aspects reduce the possibility of the IVS knowing too much about the identity activities of the users and thus prevent data aggregation or identity matching from linking transactions (DIA 2007*b*).

Before using the IVS, the identity of the user must be established to a higher level of confidence. Generally, the process of establishing an identity is based on the Evidence of Identity Standard, which checks the identity with relevant documents for ensuring that the identity truly belongs to the claimed user (SSC 2005*a*). Currently, people with New Zealand passports or citizenship certificates are not required to go through the establishment process again as these identity documents had already demonstrated higher levels of confidence in the claimed identities (DIA 2007*a*).

After the process of establishing the identity, the IVS can enrol the identity and create an identity verification credential (IVC) for that identity. The IVC contains the core identity information as well as other data for internal use. Usually, each individual can only have one IVC which expires every five years. In order to use the IVC, the IVS relies on the GLS to provide high-strength logons for its users. Generally, a GLS logon will be requested by the IVS for the user during the enrolment process. As depicted in figure 3, the IVS asks the GLS to create a logon identity for the user after having verified and established the identity of the user. The GLS then creates a logon and asks a key provider to provide a logon key for the user. The key provider will create and pass a logon key to the user while giving the GLS a key identifier for associating with the appropriate FLT. Accordingly, the GLS will pass an FLT_ivs to the IVS for referencing the user. Like the service agencies, the IVS will store

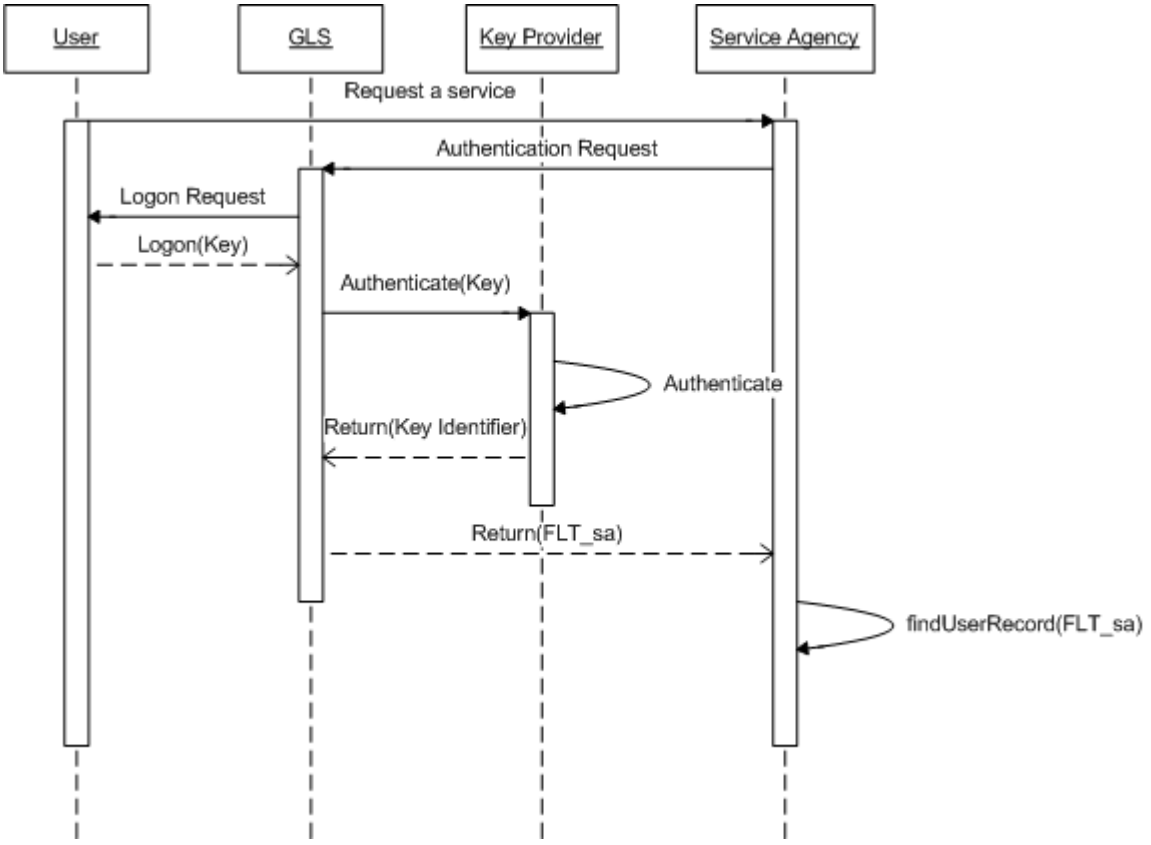

Figure 2: Example sequence diagram for the GLS.

the FLTs from the GLS and map these tags with the IVCs (SSC 2005*a*).

After the enrolment process, users can access to the IVS through the GLS when they want to prove their identities to government agencies for services. As shown in the sequence diagram of Figure 4, when a user first establishes a service with the service agency, the agency directs the user to IVS for identity verification. In turn, the IVS redirects the user to the GLS for logon. At the GLS, the user authenticates using the second level of authentication mechanism as mentioned previously. After the completion of the authentication process, the GLS returns a tag (FLT_ivs) back to the IVS for retrieving user's IVC. Subsequently, the IVS makes a request to the user for consent to release some of the identity information stored in the IVC to the service agency. Once the user agrees, the consented identity information with an associated federated identity tag for the service agency (FIT_sa) is sent. The agency can then use this tag to attach the identity information received to its own database. If the user continues to use the service, the service agency will ask the GLS for subsequent authentication. The GLS will then return an FLT_sa to the service agency, where the agency will reference the tag with its database for that user (McKenzie et al. 2008, SSC 2007).

3 Our Methodology for igovt's Security Specifications

Among different practices of security requirements analysis, we have identified three major steps in eliciting the security specifications for New Zealand's igovt system. The initial step of the analysis would be to identify the security objectives of the igovt system. This step is essential as the security objectives could be seen as the high-level requirements derived from the security need of the stakeholders (Tondel et al. 2008). Therefore, we could take these objectives into account when stating the security specifications while assuring that the stakeholders' expectations could be met. After identifying the security objectives, information involved in the igovt would be identified for understanding the importance of the information in the system as well as recognising any necessary information protection mechanisms. Lastly, the final step for analysing the security of igovt system would be to identify the threats and vulnerabilities within the system, for which any countermeasures for preventing or mitigating such threats would also be recognised.

Generally, for a complete security requirements analysis, the process is iterated to adjust any changes made in the system goals or design throughout the development lifecycle (Haley et al. 2008). Furthermore, the security requirements can be documented, which can later aid the design and specifications of the system (Tondel et al. 2008). In addition, formal specification language such as JML can be used for security specifications for avoiding any ambiguities in the natural language. Moreover, there are different approaches such as SQUARE to security requirements engineering that can also be applied. However, the main objective of this paper is to demonstrate a preliminary methodology for analysing security of IdM systems. Thus, the security specifications identified would be at policy-level, where it does not specify any design or mechanisms for building the system. Thereby, the three main steps identified previously would be sufficient for the initial security analysis and any iterations or the use of formal specification language is out of scope for the purpose of this paper. In the following sections, we describe each of the steps in more detail.

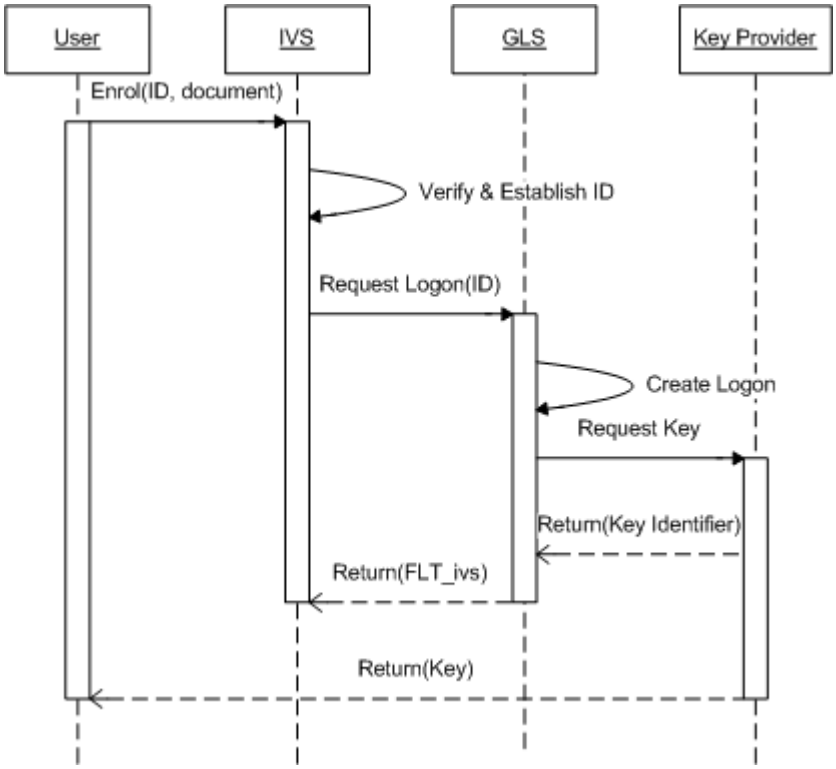

Figure 3: Sequence diagram of the identity enrolment process in the IVS and the GLS.

3.1 Security objectives

The first step to elicit the security specifications is to identify the security objectives of the igovt system. We found no information about the igovt's security objectives, aside from one brief statement in the key policy principles about the security and privacy protection of information. In order to analyse the security of the system, we must have some goals. Because participation in the igovt system is fully voluntary on the part of New Zealand users, igovt must be attractive to users. It is far beyond the scope of this paper to survey the New Zealand population to discover their preferences. As proxy for these preferences, we adopt the privacy objectives and security properties of the user-centric IdM system (Bhargav-Spantzel et al. 2007). These objectives and properties were chosen to comply with OECD principles, and to provide a maximum of user control over their identity credentials. We think it very likely that these properties would be attractive to potential users of igovt, and we leave it to future researchers to validate this assumption.

3.2 Information analysis

The second step in our security analysis is to identify the information used, stored or created within the igovt system. This step would be helpful to determine the importance of the information in the system and thus aids in later stages of eliciting and prioritising the security requirements (Tondel et al. 2008).

In order to analyse the information in igovt, we have considered the information management principles from the IdM best practice developed by FIDIS. The information management principles are being used as guidelines for developing business procedures while checking the completeness of the existing operations (FIDIS 2006). According to FIDIS (FIDIS 2006), there are five information management principles, which include information, roles and responsibilities, processes and procedures, enabling technologies, and audit and control.

From the five principles, we have further analysed the information principle according to the type of identifier or credential and recognised the stakeholders that were authorised to possess the information. In the later section of this paper, we will show this additional analysis of the information held by New Zealand's igovt system.

By considering the information management principles, we aim to understand the type of personal information used in the igovt. We also aim to discover any requirements for protecting this information.

3.3 Threats Analysis

The last step of our security analysis is to identify the threats and vulnerabilities of the igovt system. There are several techniques available for analysing threats. These include attack trees and misuse case analysis. Attack trees analyse and place all the possible attacks in a tree structure. Whereas, misuse case analysis models the threats to the system in terms of use cases (Tondel et al. 2008). 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 for helping customers and developers to understand and communicate requirements more consistently and effectively (Bittner 2002). Like the use cases, misuse cases are also helpful in a way for understanding the undesirable behaviours of the system. Generally, a misuse case is seen as an extension of the use cases for describing negative scenarios or cases with hostile intent (Tondel et al. 2008). Thus, misuse case analysis can be used effectively for threats analysis and for eliciting security requirements of the system.

Furthermore, according to Lee (2006), misuse cases provide a better way to convey the threats in diagrams than attack trees. Misuse case diagrams also depict any countermeasure to the threats, which can

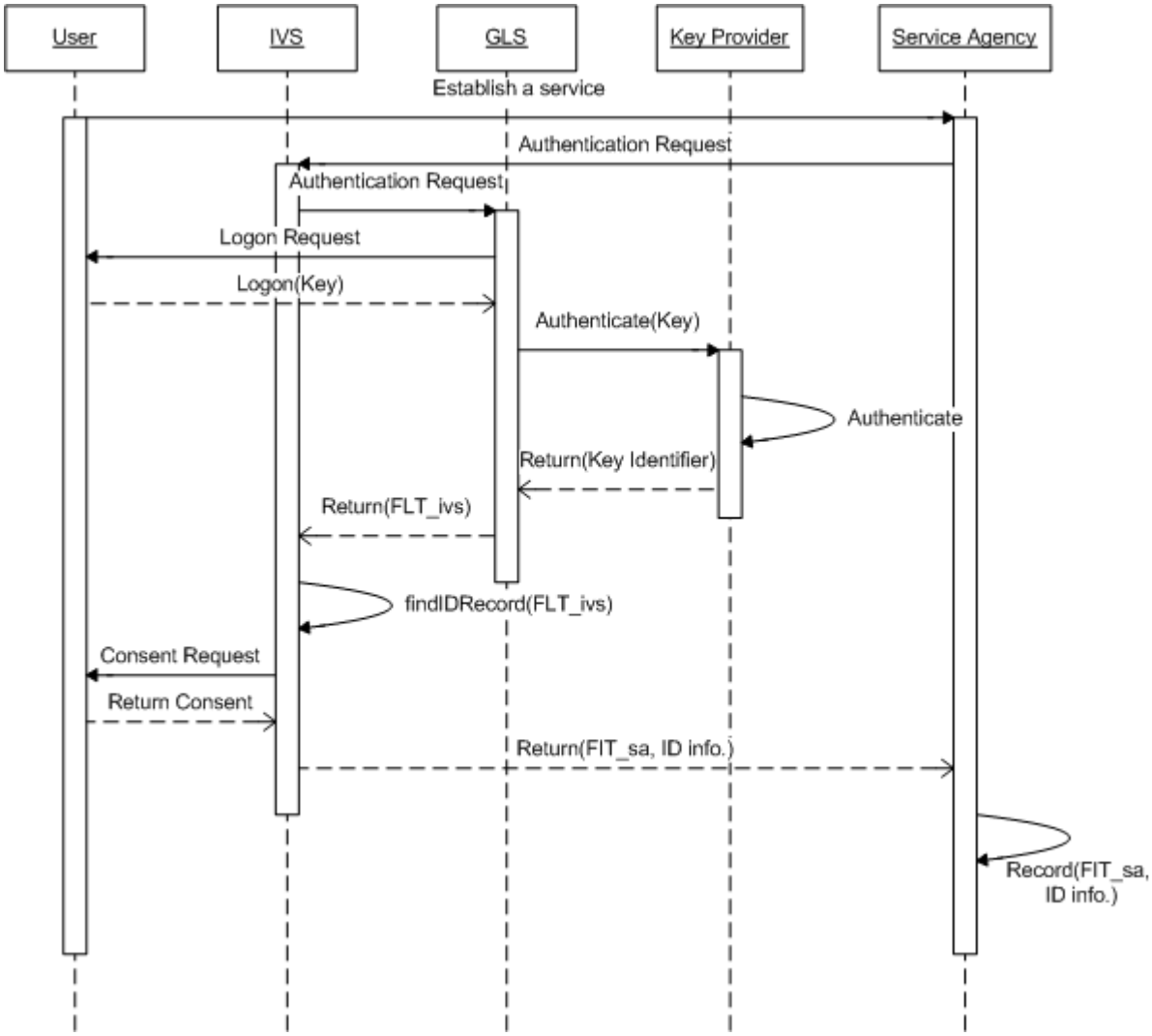

Figure 4: Sequence diagram for using the IVS to verify identity.

be helpful for identifying the requirements to mitigate such threats. Since we are only to find out the preliminary security specifications of igovt, it is more crucial to first analyse the risks and threats to the most valuable parts of the system rather than considering all the possible attacks. Therefore, misuse case analysis is more useful in the context for our security analysis. Later in this paper, we will present both the use and misuse cases using the standard UML notations for analysing the threats.

4 Results

In this section, we present the results from analysing the security of igovt based on the methodology proposed from the previous section.

4.1 Security objectives for governmental IdM

When identifying the security objectives for governmental IdM, we found that most of the security and privacy objectives could be described under Lampson's four security headings, secrecy, integrity, availability, and accountability (Lampson 2004). According to Lampson (2004), these security headings are useful for describing the security needs of the users, where these needs are often translated into the security policy for the system. By using these headings, we can ensure that the security objectives defined cover the major security aspects of the system.

Moreover, we have 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 the identity information from any operations conducted by the user or 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 that took place as well as the actors involved in the system. In some cases, security objectives can also apply to both the identity information and transactions in the IdM system.

In Table 1, we have reclassified the security objectives for the user-centric IdM of Bhargav-Spantzel et al. (2007) under Lampson's four headings, and with respect to our informational/transactional levels. We note that the user-centric IdM has no explicit requirement for availability, but we argue that availability is necessary in a governmental IdM. If a governmental IdM is heavily used, then its heavy users are likely to rely on it for their governmental accesses, and a denial-of-service attack would then have painful consequences. If an IdM is *not* heavily used, then it was not worthwhile to build it in the first place. It is outside the scope of a security analysis to determine the cost-effectiveness of a project; instead we take a system's cost-effectiveness as a given. We have therefore

Security Objectives	Information Level	Transaction Level
Secrecy	Conditional release Confidentiality of info. Illegal sharing prevention Non-transferability Selective disclosure Stealing prevention	Anonymity Confidentiality of trans. Data minimisation Unlinkability
Integrity	Integrity of information Revocability Verifiability	Notification Verifiability
Availability	Availability of info.	Availability of trans.
Accountability		Authentication Non-repudiation Non-replay Auditability of trans.

Table 1: Security objectives for governmental identity management, at the information and transaction levels. The audit requirement at the enterprise level is not shown in this table.

inserted an availability requirement in Table 1.

Our Table 1 also includes Lampson's "gold standard" (Lampson 2004) of audit, authorisation, and authentication. These properties are not well-defined at the information level, but become important at the transaction level of a system. Regular audits of personnel, procedures, and equipment are of great importance at the enterprise level, for without these safeguards our lower-level security analyses are merely documents without any guaranteed correspondence to the currently-operating IdM system.

4.2 Information in the igovt system

We have identified all the possible information relating to the identity of a user in the igovt system, where there are four main sets of identity information. In addition to the four main sets, other data may be requested or created in the system. For instance, the current GLS requires user's email address when registering for a logon. Another example can be found in IVS when a referee's declaration may be needed as secondary evidence for identity verification.

Moreover, as mentioned in Section 3.2, we have modified the information principle table to show a more detailed analysis of the information identified. Table 2 shows the information principle table with our classification of personal information involved in the igovt system. We have recognised the identity information as identifier or credential and in which we have identified the entities that own or hold the record of the information. We have also distinguished the identifier or credential into a descriptor, token, secret, or a combination of these basic types. A descriptor is simply a description of an identity, which is difficult to monitor and control as the description can be reproduced or forwarded easily. A 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. Copies of the tokens can be verified against the original ones. The third type is secret, which is something only known to a limited number of parties. In other words, a secret is a descriptor with controlled distribution.

Since both IVS and GLS in igovt mostly deal with identifiers or credentials that are secret, it is important to secure and protect these sets of information. The remaining four information principles thus include the following requirements for igovt:

- The IVS and the GLS have the roles and responsibilities to protect information and secrets as well as to destroy out of date information while complying with regulations;
- The processes and procedures in igovt have to consider information lifecycle, matching checks as well as the information used in authentication and authorisation;
- The technologies for the information used in igovt shall range from paper to electronic databases;
- The New Zealand government needs to ensure that everything involved in igovt is genuine and compliant with regulations.

4.3 Use and Misuse cases for the igovt system

In this section, we present the overview of the use and misuse cases for the igovt system. We then elicit the preliminary security specifications for igovt.

4.3.1 Overview of the Use Cases

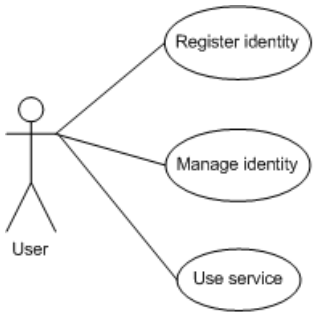

Figure 5: Main use cases in igovt for users.

Generally, in a full system analysis, use cases can consist up to 5 to 15 pages long of descriptions and for which the analysis can take some time to complete (Bittner 2002). As a preliminary analysis, it is more important to find the necessary use cases that represent the value of the system. Because our security analysis is based on a user-centric approach, we have identified three primary use cases based on the user's view of the system. These are illustrated in Figure 5, and are listed below.

1. Register identity: describes how a user registers his identity to IVS. This description can be found from the sequence diagram in Figure 3.

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 2: Information principle table of personal information held by New Zealand igovt.

2. Manage identity: describes how a user manages his identity with IVS and GLS.
3. Use service: describes how a user uses his identity to obtain access to services via GLS.

4.3.2 Overview of the Misuse Cases

We have identified ten main types of misuse cases, listed below, by considering how each of our use cases could be abused. Figure 6 illustrates three of our ten misuse cases, in the context of an igovt system. These are all abuses of the use case in which a user requests a service.

1. Disrupt service and access, of a user to their identity.
2. Data matching.
3. Disclosure of information, including shared secrets such as passwords.
4. Thievery of information, through attack methods such as password cracking, pharming and phishing.
5. Spoofing of identity, through the use of false credentials.
6. Tampering with data, where the data can be modified, deleted or disclosed by the misuser.
7. Fraudulent initialisation/termination, where the same password has been predefined or suspended account is still in use.
8. Repudiation of transactions or registrations.
9. Elevation of privilege, where a misuser gains higher privileges or full access to services and resources.
10. Insider threats, where the service agency misuses the identity information beyond the expectations of the user such as unauthorised release of data to other agencies. The misuse imposes a threat on the privacy of the user.

4.3.3 Security Specifications for igovt

We have analysed New Zealand's igovt design (McKenzie et al. 2008, SSC 2007) in the light of the security objectives, control objectives, use cases, and misuse cases we have identified for generic IdMs. We describe our findings in terms of the objectives listed in Table 1 and discuss them under Lampson's four security headings.

- *Secrecy.* Most of the secrecy objectives listed in Table 1 are fulfilled in the design of igovt, for it preserves individual privacy through user consent (selective disclosure) and it provides cryptographic security for the identifiers it provides to service agencies. Furthermore, igovt stores only a very limited amount of identity information. We find a very interesting technical provision in the igovt design documents for the prevention of illegal sharing, because the IVS will establish a non-matchable identifier for each governmental agency. Because the IVS will also release names and other matchable information, agencies might still engage in improper sharing. We cannot see how any technical means could absolutely prevent such sharing, and thus legal controls such as the Privacy Act are still necessary.
- *Integrity.* In Table 1, we included the properties of revocability, verifiability, and notification under the heading of integrity. We see no technical provision for revocation, aside from a five-year time limit on the validity of a credential (IVC) issued by the IVS. With respect to verifiability: a key question to ask is whether "the user can

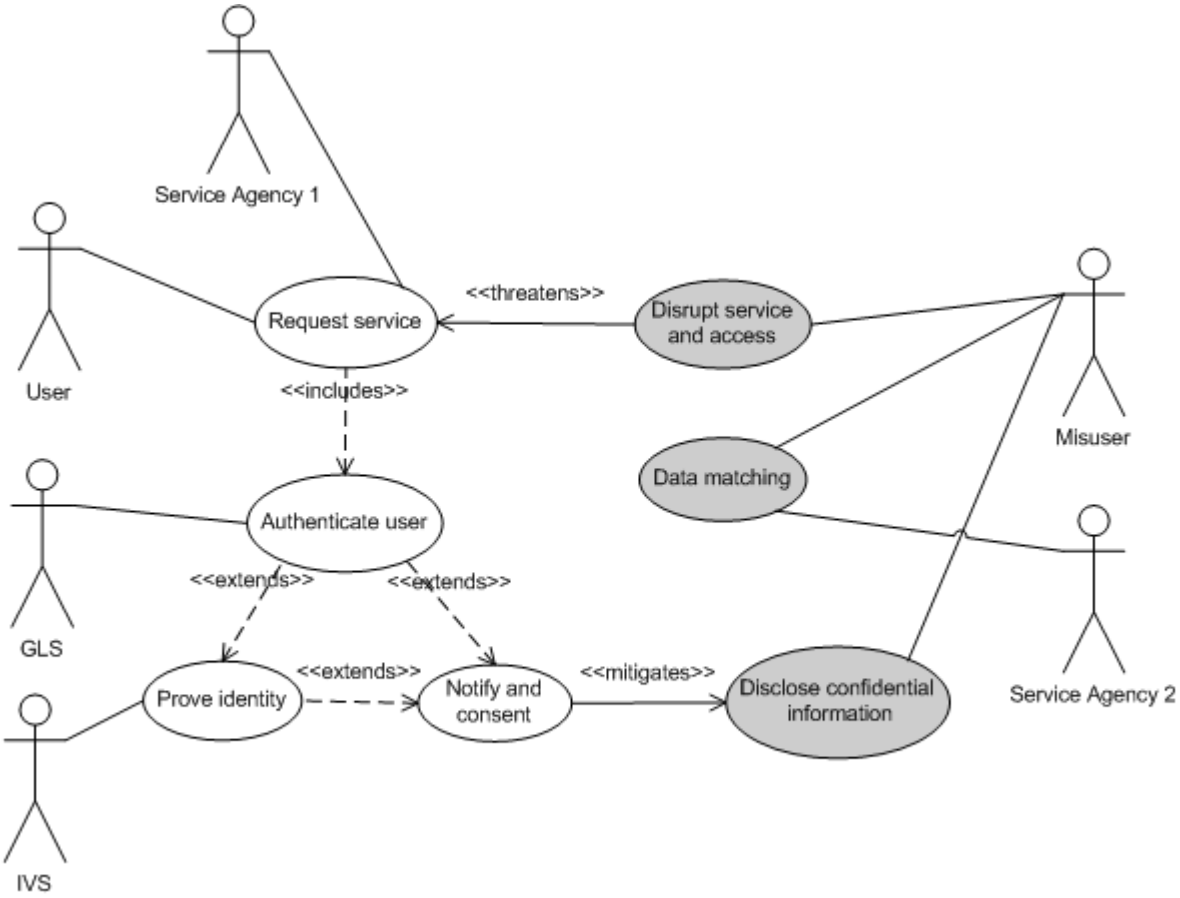

Figure 6: Example of misuses in igovt when a user requests for a service.

verify that the identity provider provides the correct identity data about the user and according to the user's intention" (Bhargav-Spantzel et al. 2007). We are unable to answer this question in its entirety. A user might make a written request, under the terms of the Privacy Act, for a copy of their personal information in their files at the State Services Commission. We see no automated provision for handling such requests. Furthermore, the published dataflows for the IVS (and GLS) strongly imply that users would not be allowed to see the FIT (and FLT) identity credentials which are provided on their behalf to service agencies by the IVS (and GLS). With respect to notification: the GLS maintains a log of the service agencies to whom they have identified each user, and we understand that a user can request a copy of their own log. We see no provision to "push" this information to the user (Bhargav-Spantzel et al. 2007), even though such pro-active notifications from igovt might be a very desirable security feature (from the user's perspective) in cases where a governmental agency has suffered a security breach which is likely to compromise any identity information held by that agency. Furthermore, if logs were routinely "pushed" at users, this might uncover some unsuspected security flaws or identity thefts. We tentatively conclude that the igovt design provides only a limited amount of technical control on the user-centric extensions of informational and transactional integrity. However, it is clear that igovt must comply with New Zealand's Official Information Act and its Public Records Act, implying that there would be strong legal and political pressures on igovt to satisfy most, if not all, of these extended integrity properties.

- *Availability.* The igovt will need to provide some mechanisms to detect intrusions and to survive attacks from the misusers as discovered from our misuse case analysis. We found a strong emphasis on privacy and user control in the design documents, and in the privacy impact assessments, however we have not seen any explicit consideration of the availability requirements for igovt. We think an important task for future analysts would be to carefully consider the possibility of a denial of service attack on igovt, and its possible mitigations.
- *Accountability.* The accountability objectives listed in Table 1, if met fully, would provide accurate evidence about interactions between an external user and igovt. Incomplete records might allow an external misuser (or igovt itself) to deny a transaction they have conducted. Our preliminary analysis indicates that the GLS is designed to record every user logon as a transaction. We also note that there is an independent review body for reviewing and handling disputes about igovt. However, we do not see any provision for a periodic audit by an external party.

5 Conclusions

The igovt system is an expression of the New Zealand government's concern in protecting the privacy of

its citizens, and for allowing user control over online identities. We have found that the igovt design has carefully separated the authentication challenges into two components, logon management (GLS) and identity verification (IVS). This separation will make identity matching more difficult by giving different identifiers for the same person to different governmental agencies. The IVS stores only four identity attributes, which also enhances the privacy of individual users.

There have been privacy assessments and public consultations for igovt, but we know of no security analysis for the igovt system. We have demonstrated how this gap might be filled, by proposing a lightweight approach to the analysis of the igovt system. We started our analysis by identifying the security objectives for user-centric IdM systems. We then conducted an information analysis to discover security specifications. We compared the user-centric IdM objectives with the results of our information analysis, to ensure that all major security requirements were covered. Our subsequent misuse case analysis identified some threats to the igovt system. As a result of our analysis, we concluded that the igovt system has put great effort in protecting the identity information and the privacy of its users. However, we could not find any countermeasures to the threats of availability attacks, and we also noted some possible weaknesses in the area of integrity, notably in its sub-property of verifiability.

Our preliminary findings suggest that a more careful application of our lightweight analysis, or a more labour-intensive approach to analysis, would reveal additional security requirements for the igovt system. We have found some insights from the misuse case analysis, and we suggest that future researchers should consider using the more formal approach of SysML to express misuses as exceptional flows arising in "normal" use cases.

References

Bhargav-Spantzel, A., Camenisch, J., Gross, T. & Sommer, D. (2007), 'User centricity: a taxonomy and open issues', *Journal of Computer Security* **15**(5), 493–527.

Bittner, K. (2002), *Use Case Modeling*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA.

DIA (2007*a*), 'Public consultation about verifying your identity to government agencies using the internet - faq'. Department of Internal Affairs, `http://www.dia.govt.nz/idconsult`.

DIA (2007*b*), 'Public consultation about verifying your identity to government agencies using the internet - information for public consultation'. Department of Internal Affairs.

DIA (2008), 'Public consultation about the igovt service'. Department of Internal Affairs.

Dwaikat, Z. & Parisi-Presicce, F. (October 2004), From misuse cases to collaboration diagrams in uml, *in* 'Proceedings of the 3rd International Workshop on Critical Systems Development with UML'.

FIDIS (2006), 'D4.6: Draft best practice guidelines'. Future of Identity in the Information Society, `http://tinyurl.com/56oq6r`.

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

Harding, C., Mizumori, R. & Williams, R. (2007), Architectures for identity management, Technical guide, The Open Group.

Josang, A., Zomai, M. A. & Suriadi, S. (2007), Usability and privacy in identity management architectures, *in* 'ACSW '07: Proceedings of the fifth Australasian symposium on ACSW frontiers', Australian Computer Society, Inc., Darlinghurst, Australia, Australia, pp. 143–152.

Joshi, J., Ghafoor, A., Aref, W. & Spafford, E. (2001), 'Digital government security infrastructure design challenges', *Computer* **34**(2), 66–72.

Kreizman, G. & Rust, B. (2004), Government ID and authentication: The right project scope, Research note, Gartner Research.

Lampson, B. (2004), 'Computer security in the real world', *Computer* **37**(6), 37–46.

Lee, J. (2006), Perceptions of HIPAA security requirements by US dental schools, Master's thesis, University of Auckland, Auckland, New Zealand.

McKenzie, R., Crompton, M. & Wallis, C. (2008), 'Use cases for identity management in e-government', *Security & Privacy, IEEE* **6**(2), 51–57.

Slone, S. (2004), Identity management, White paper, The Open Group.

SSC (2004), 'Research of issues for maori relating to the online authentication project'. State Services Commission, `http://tinyurl.com/6gs7jz`.

SSC (2005*a*), 'Privacy impact assessment of the all of government authentication programme - identity verification service'. State Services Commission, `http://tinyurl.com/5ue5eq`.

SSC (2005*b*), 'Privacy impact assessment of the proposed government logon service'. State Services Commission, `http://tinyurl.com/6ojne8`.

SSC (2006), *Enabling Transformation: A strategy for e-government 2006*, State Services Commission.

SSC (2007), 'All-of-government authentication programme - identity verification service - build contract'. State Services Commission, New Zealand Government.

SSC (2008*a*), 'Authentication principles'. State Services Commission, `http://tinyurl.com/6p6jpd`.

SSC (2008*b*), 'igovt'. State Services Commission, `http://www.i.govt.nz/`.

Tondel, I., Jaatun, M. & Meland, P. (2008), 'Security requirements for the rest of us: A survey', *IEEE Software* **25**(1), 20–27.