Lessons from Implementing Federated Identity Management within the Research and Education Sector

by

Brent Coetzee

Lessons from Implementing Federated Identity Management within the Research and Education Sector

by

Brent Coetzee

Dissertation

submitted in fulfilment
of the requirements
for the degree

Master of Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela University

Supervisor: Prof. Reinhardt A Botha

April 2018

Declaration

I, Brent Coetzee, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognised.
- This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institute.

Brent Coetzee

Abstract

Collaboration between academic and research institutions has become fairly common. Traditional methods of identity management do not scale across institutional borders and this places an increasing responsibility on users to remember a large number of credentials. As a result, collaboration has become a risky and expensive task. Federated Identity Management facilitates the cooperation of identity processes, policies and technologies and fosters an environment of secure resource sharing in heterogeneous IT environments (Jensen, 2012; Malik, Anwar, & Shibli, 2016).

The adoption of Federated Identity Management has been lower than expected across industries. The research and education sector has had relative success in this regard (Landau & Moore, 2012). However, there is little literature on the practices of federations in this sector. As a result there is little insight into the challenges of implementing Federated Identity Management within the research and education sector. Similarly, there is also little insight into the solutions deployed to overcome these challenges.

This research study aims to compile lessons learnt from the implementation of Federated Identity Management within the research and education sector. Semi-structured interviews are conducted to learn the experiences of seven federations from around the globe. Literature and stakeholder input is used as a filter to analyse and structure data into themes.

Identified themes are used to derive eight lessons learnt from the implementation of Federated Identity Management within the research and education sector. These lessons provide guidance to new federations in this sector, capitalizing on its strengths and avoiding its weaknesses.

Acknowledgements

Foremost, all praise belongs to Allah, the most gracious, the most merciful. I thank Allah for his guidance and I pray that he continues to guide me and grant me ease until my dying day and I pray that Allah grants me Jannah Firdaus, the highest level of paradise. Ameen.

I would like to express my gratitude and appreciation to my mother and father who have supported me throughout my education. It is through them that I have reached my potential. I pray that I will be able to show them the same support that they have shown me, in the future.

Similarly I would like to express gratitude to my wife who has undoubtedly influenced me and this dissertation for the better. I pray that Allah increases the love he has put between us.

For his patience, motivation, enthusiasm and beneficial guidance, I would like to extend my most sincere gratitude to Prof. Reinhardt A Botha. It was an absolute pleasure.

Furthermore, I would like to thank the following benefactors for their financial assistance:

- The financial assistance of the South African National Research and education Network (SANReN) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors, and are not necessarily to be attributed to the South African National Research and education Network.

- The financial assistance of the Nelson Mandela Metropolitan University's Post Graduate Research Scholarship (PGRS) is also hereby acknowledged.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Collaboration amongst institutions and organizations in similar sectors of industry has been on the rise coming into the 21st century. This is especially true for national and regional research organizations, for whom collaborating has become the norm (Broeder et al., 2013).

Traditional forms of identity management such as the isolated model are limited and do not scale well outside institutional borders. Federated Identity Management is a response to the limitations of isolated identity management in environments where cross institutional, local and international collaboration is required. Federated Identity Management enables the cooperation of identity processes, policies and technologies and fosters an environment of secure resource sharing in heterogeneous IT environments (Jensen, 2012; Malik et al., 2016).

The concept of Federated Identity Management has been readily accepted by academic literature, in which wide-spread adoption was predicted. However, industry has not been as enthusiastic about Federated Identity Management and the adoption of Federated Identity Management has not met the expectations of literature (Jensen & Jaatun, 2013; Landau & Moore, 2012; Smith, 2008).

The research and education sector has had relative success implementing Federated Identity Management (Landau & Moore, 2012). Literature has attributed this success to the highly collaborative nature of the research and education sector together with its more trusted environment (Smith, 2008).

The EduGAIN federation is proof of the compatibility and supportive nature of the research and education sector with regard to Federated Identity

Management. EduGAIN is a global federation consisting of a number of national federations with more than 40 members as of 2017. Shibboleth and SAML (Secure Assertion Mark-up Language) have been key enablers of EduGAIN and Federated Identity Management in general in the research and education sector (Ferdous & Poet, 2013; Arias-Cabarcos, Almenarez-Mendoza, Marin-Lopez, & Diaz-Sanchez, 2009).

Literature has identified challenges responsible for the low adoption and failure of Federated Identity Management through industry. Smith (2008) states that Federated Identity Management is not rocket science, but that there is confusion as to what it delivers and the complexity it entails. The lack of understanding and perceived complexity of implementing Federated Identity Management has created a barrier to its adoption.

1.1 Problem Statement

Literature has shown concern for the low adoption of Federated Identity Management (Jensen & Jaatun, 2013). Failed implementations of Federated Identity Management have revealed unique challenges facing specific parts of industry (Chadwick, 2009). Despite this, Federated Identity Management has been relatively successful within the research and education sector (Landau & Moore, 2012). Literature has identified the mutual desire for collaboration in the trusted environment of the research and education sector as the primary reason for this (Smith, 2008).

However, literature has not given much attention to the research and education sector as a whole. Federated Identity Management has only recently been standardized with the help of Shibboleth. Earlier implementations of Federated Identity Management relied on proprietary software and differed from country to country.

> ***There is little insight into the challenges of implementing Federated Identity Management within the research and education sector. Similarly, there is also little insight into the solutions deployed to overcome the aforementioned challenges.***

New federations such as the South African Identity Federation (SAFIRE)

must identify and address the challenges of implementing Federated Identity Management in this sector to achieve the desired rate of adoption. Learning from the failures and capitalising on the successes of already established federations will reduce the time and increase the chance of implementing Federated Identity Management successfully within the research and education sector.

1.2 Research Objectives

With the problem statement in mind, the primary objective of this research is to identify lessons learnt from the implementation of Federated Identity Management within the research and education sector.

Fulfilling this primary objective will provide insight into the unique challenges and opportunities faced by the research and education sector. To achieve the primary objective, a number of sub-objectives must be met.

- Describe the state of Federated Identity Management within industry
- Identify the benefits and challenges of Federated Identity Management
- Determine the current state of Federated Identity Management within the research and education sector
- Collect the experiences of implementing Federated Identity Management throughout the global research and education sector

The completion of the four sub-objectives will allow Federated Identity Management literature and the experiences of federations within the research and education sector to be combined and the primary objective to be fulfilled.

1.3 Delineation

By increasing insight into the experiences of implementing Federated Identity Management in the research and education sector, young identity federations such as the South African Identity Federation (SAFIRE) have the opportunity to accelerate growth and to participate in the global federation, EduGAIN. Value is drawn from lessons when common errors are avoided and advantageous opportunities are not missed.

This research is also applicable to young, established, and future federations within the research and education sector.

1.4 Research Methods

The review of prior literature is an essential part of any academic research project (Webster & Watson, 2002). Therefore, literature is used to understand and to discuss the benefits of Federated Identity Management, the challenges of implementation and the individual components which make up typical federations throughout industry. Literature is also used to discuss the current state of Federated Identity Management within the research and education sector.

Interviews provide insight into the world, opinions, thoughts and experiences of those being interviewed (Hove & Anda, 2005). Semi-structured interviews are used to collect the experiences of established identity federations within the global research and education sector. The semi-structured nature of the interviews allows the researcher to control the direction of the conversation, but makes provision for the flexibility and freedom essential to gain new insights.

Qualitative analysis and argumentation combining interview data and literature are used to derive the lessons learnt from implementing Federated Identity Management within the research and education sector.

1.5 Layout of Study

Chapter 1, provides an introduction to Federated Identity Management and the purpose of the study. Details of how the study will be organized and conducted is found in Chapter 2, Research Methodology.

To gain a better understanding of the research topic, Chapter 3, Federated Identity Management, describes the current state as well as identifies the benefits and challenges of Federated Identity Management. Chapter 4, FIM in Research and Education, provides more focus by describing Federated Identity Management within the research and education sector.

Interviews are a qualitative method of data collection. Chapter 5 explains the choice of interviews as well as how they were constructed using Federated

Identity Management literature as a primary input. After the interviews have taken place, they must be analysed in an appropriate way. Chapter 6, Analysis, describes how the interviews were transcribed, coded and then separated into logical themes with the use of Federated Identity Management literature and stakeholder input.

The study cumulates in Chapter 7, Lessons, with the discussion and presentation of lessons learnt from implementing Federated Identity Management within the research and education sector. Eight lessons are derived from argumentation together with Federated Identity Management literature and interviews.

The conclusion of the study comes Chapter 8, where a reflection on the processes and output of the study together with limitations and the direction of future research is presented.

Figure 1.1 illustrates the layout of the chapters. The upcoming chapter, Research Methodology, contains a detailed layout and description of how the study is organized and what each chapter entails.

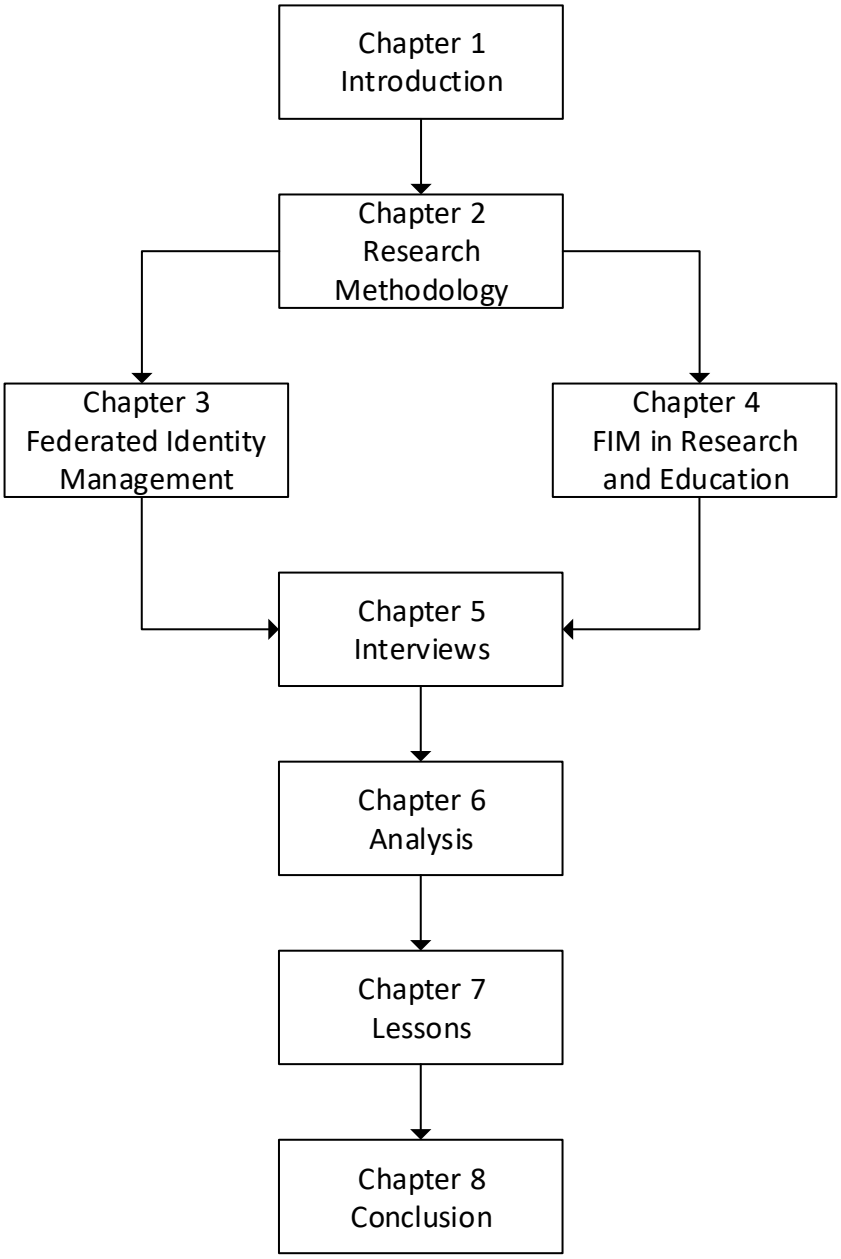

Figure 1.1: Chapter Layout

Chapter 2

Research Methodology

Most qualitative research includes a chapter titled research methodologies or at least a specific portion dedicated to "data and methods" (Silverman, 2013). The purpose of the research methodology chapter is to inform the reader about how data was gathered, how the data was organized and analysed, and how the final output was reached.

The chapter begins by outlining the qualitative nature of this research. The rest of the chapter elaborates on the three phases this research has been divided into to. First the initiation and planning phase, then the knowledge and data phase and lastly the analysis phase. The intention is to convey to the reader, the systematic thought process and series of steps followed throughout the execution of the research.

2.1 Overview

From the beginning of the 17th century, the importance of objectivity and evidence was emphasized in the search for truth. In the 19th century, Auguste Comte asserted that the social world could be studied through invariable laws in the same way as natural sciences. This school of thought or paradigm is known as positivism (Ritchie & Lewis, 2003).

In 1781 Immanuel Kant published his Critique of Pure Reason. Kant's argument was that there are other ways of knowing about the world other than direct observation and that people use these ways all the time. Max Weber (1864 - 1920) believed that analysis of material conditions as used in a positivist approach was important but not sufficient in understanding

people's lives and experiences. Additionally, Max Weber emphasized that the research must understand the meaning of social actions within the context of the material conditions in which people live. This school of thought that stresses interpretation as well as observation is known as interpretivism (Ritchie & Lewis, 2003).

Positivism aims to produce law-like propositions and immutable truths, where interpretivism, including qualitative research, aims to understand people's experiences and perspectives to increase general understanding of a particular station or topic (Ravitch & Carl, 2015).

2.1.1 Qualitative Research

Qualitative research emerged as a formal field in the late 1960s (Ravitch & Carl, 2015). However qualitative paradigms were in practise well before the 1960s. From the late 19th century and throughout the 20th century, qualitative research methods evolved and became more sophisticated as researchers became aware of the research process and responded to challenges from other methodologies and paradigms such as positivism (Ritchie & Lewis, 2003).

During the 20th century, positivism was the dominant paradigm. Qualitative research was often criticised as 'soft' and 'unscientific'. In an attempt to combat this view, qualitative researchers formalised their methods and stressed the importance of rigour in data collection and analysis.

Qualitative research exists within many disciplines. For this reason qualitative research can be difficult to explain as it has no theory or paradigm of its own (Denzin & Lincoln, 2011). However, qualitative research methods do have features in common. Data collection methods are context specific and flexible. Methods involve understanding as well as detail and context.

Qualitative research can be difficult to define as it is used as an overarching category and covers a wide range of approaches and methods from a number of different research disciplines (Denzin & Lincoln, 2011). Ravitch and Carl (2015) broadly defines qualitative research as the methodological pursuit of understanding the ways that people see, view, approach and experience the world and make meaning of their experiences as well as specific phenomena within it.

2.1.2 Relevance to this research

The primary objective of this research is to produce a list of lessons learnt from implementing Federated Identity Management in the research and education sector, globally. Literature on the subject of Federated Identity Management highlights a number of the benefits together with the challenges of implementing Federated Identity Management. This literature is useful for any federation looking to implement itself successfully by capitalizing on benefits and avoiding potential points of failure.

However, literature is general and includes all sectors of industry. Landau and Moore (2012) state that Federated Identity Management has enjoyed more success in the research and education sector than in other parts of industry. Smith (2008) mirrors this statement when he says that the adoption of Federated Identity Management is already well established in communities of trust such as the research and education sector. To produce lessons on implementing Federated Identity Management successfully in the research and education sector specifically, literature cannot be the only source of information.

The success of Federated Identity Management relies on solving sensitive challenges and concerns such as privacy and security. User perception, organizational risk appetite and national law differ substantially on issues such as these from country to country. It is therefore necessary to accommodate the experiences and perspectives of national research and education federations to increase ones understanding on this topic.

A delineation of this research is to produce lessons that can be used or adapted by the South African Identity Federation as a primary stakeholder. For these lessons to be useful to the South African environment, they will need to be viewed through the unique lens of the South African research and education sector, its students and researchers.

A qualitative method of data collection provides the structure and means to collect the experiences of identity federations from selected national identity federations within the research and education sector around the globe. These experiences, together with literature will provide a more complete set of lessons learnt from implementing Federated Identity Management in the research and education sector.

2.2 Overall Research Design

This research is divided into three distinct phases. Each phase comprises two components, as can be seen in Figure 2.1

Phase One is the Initiation and Planning Phase. This phase consists of an initial literature review of Federated Identity Management, followed by a description of the stakeholder visit.

Phase Two is the Knowledge and Data Acquisition Phase. A second literature review is conducted with a primary focus on Federated Identity Management in the research and education sector. Interviews with federations in the research and education sector are conducted as the primary means of data collection.

Phase Three is the Analysis Phase. Firstly, important themes are identified from the primary data. Lessons are synthesized by means of argumentation and combining identified themes with both literature reviews.

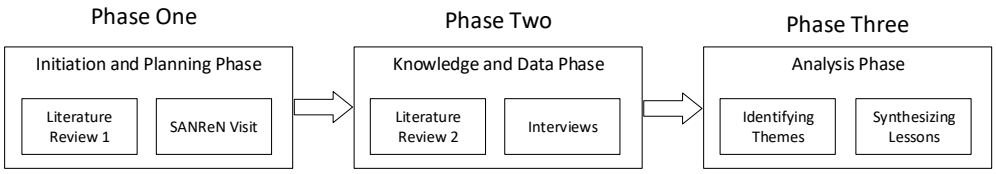

Figure 2.1: Research Layout

2.3 Initiation and Planning Phase

This section will introduce and explain the contents of the Initiation and Planning Phase. This phase consists of a literature review and details of the interaction with major stakeholders. The literature review titled, Federated Identity Management can be found in Chapter 3.

2.3.1 Literature Review of Federated Identity Management

A literature review will be conducted to gather and organize the history and current state of Federated Identity Management structurally within academic

literature. Chapter 3, titled Federated Identity Management contains the literature review. The reader is first introduced to Federated Identity Management within the context of identity management as a whole. The literature review proceeds to inform the reader of the components of Federated Identity Management together which a short history of early implementations. The benefits of Federated Identity Management are identified and explained to inform the reader of the value of Federated Identity Management. The literature review concludes with the challenges of Federated Identity Management, to make the reader aware of the the major reasons that literature has shown concern for low rates of adoption.

2.3.2 Stakeholder Visit

The South African National Research and education Network (SANReN) is a major contributor to the formation of the South African Identity Federation (SAFIRE). As such, both organizations are stakeholders in this research.

In the early stages of the research proposal, I visited SANReN at their main campus in Pretoria, South Africa. The visit lasted for three weeks during which time I gained first-hand exposure in setting up a federated service together with the operation of Shibboleth, software used to enable Federated Identity Management in educational environments.

During my visit I met with several engineers who played a role in the formation of SAFIRE. Discussions were centred on the state of SAFIRE at the time, particularly the challenges it faces. The unique South African environment with it's young democracy and wide range of cultures, languages and privacy/security perspectives were mentioned.

In conclusion, the primary area of concern is the successful adoption of SAFIRE in the unique environment of South Africa. Even though the global sector of research and education is enthusiastic to provide guidance, it became clear that simply implementing an identity federation in South Africa would not work unless it was significantly tailored to the South African environment.

The SANReN team of engineers contain an impressive amount of talent within their ranks including backgrounds in electronic engineering, project management, cyber security, computer sciences, data handling and enterprise level networking technicians.

2.4 Knowledge and Data Acquisition Phase

With a broad understanding of Federated Identity Management and direction from the stakeholders, the research can enter the second phase, the Knowledge and Data Acquisition Phase.

This section explains the reason for a second literature review. Then the method of primary data collection, interviews, will be introduced and explained.

The literature review titled, FIM in Research and Education can be found in Chapter 4. An in-depth explanation and report of the interview process can be found in Chapter 5.

2.4.1 Federated Identity Management in Research and Education Extended Literature Review

The first literature review titled, Federated Identity Management gives a broad description and history of Federated Identity Management and highlights its benefits and challenges.

The second literature review described in this second phase of research is titled FIM in Research and Education. The purpose of this literature review is to gather and to organize structurally academic literature of Federated Identity Management specifically within the research and education sector.

The reader is introduced to the history of Federated Identity Management in higher education as well as past and present enablers such as Athens and Shibboleth respectively. EduGAIN is introduced together with the South African Identity Federation (SAFIRE)

2.4.2 Interviews

The second literature review together with the first literature review provides a complete picture of Federated Identity Management in research and education. However, literature on Federated Identity Management is general throughout all parts of industry. To fulfil the primary research objective of producing the lessons learnt from implementing Federated Identity Management in the research and education sector, academic literature must be supplemented with primary data.

Federated Identity Management has been implemented in the research and education sector, globally for well over a decade. Learning the experiences and strategies of these federations can offer insight into the unique benefits and challenges of Federated Identity Management in this sector. The research and higher education sector encourages cooperation and progress throughout. This collaborative nature allows SAFIRE to benefit from federations around the globe.

Rubin and Rubin (2011) suggests that if questions cannot be answered briefly and it is anticipated that respondents may need to explain, describe and give examples, then interviews are the preferred method of data collection. Qu and Dumay (2011) strengthens this statement by confirming that interviews are one of the most important qualitative data collection methods. Therefore, interviewing selected federations from around the globe will be the method of primary data collection.

Interviews can be divided into three main categories: structured, semi-structured and un-structured. Semi-structured interviews make use of both structured and un-structured components. They involve prepared questions divided into themes with probes designed to encourage more elaborate responses. Semi-structured interviews are the most popular of all categories owing to their flexibility and their ability to uncover hidden information (Qu & Dumay, 2011). Figure 2.2 describes interviews as a spectrum where a semi-structured approach would fall in the middle. This shows that interviews are not rigid, but can be adjusted along the spectrum to suit the needs of the specific research they are used for.

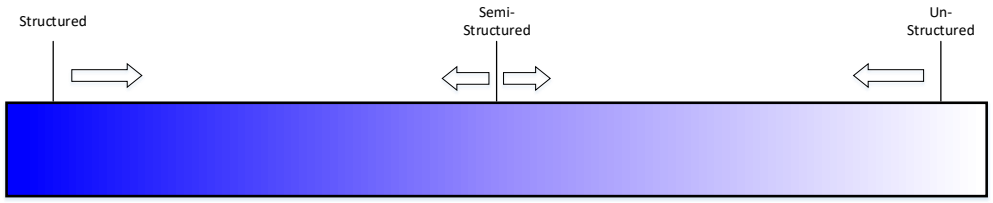

Figure 2.2: Interview Spectrum

Semi-Structured interviews were chosen as the primary method of data collection for this research. Literature has provided themes and a basis on which to formulate questions for interviewees. However, in order to capture

the specific attributes of Federated Identity Management in the research and education sector, the interviewer is given the freedom to follow up on any unexpected or interesting answers provided by the interviewees.

2.4.3 Participant Selection

The South African National Research and education Network SANReN provided the contact details of persons within six established federations, as well as that of the director of the South African Identity Federation (SAFIRE). Each identity federation was contacted via email and asked to participate in an interview regarding their experiences within their respective identity federations. All six identity federations agreed and interviews were arranged at the convenience of the interviewees.

Although a number of the interviewees were eager to reveal their identity, if was decided that the individual identities of the interviewees would be kept private. Therefore, the names and contact details as well as other details will not be included in this research.

The pool of interviewees consists of a number of different titles and positions within their respective federations, including:

- Technical Engagement and Support Manager
- Network Operations and Administration
- Associate Vice President for Trust and Identity
- Principal Technical Support Specialist
- Project Development Officer
- Developer
- Project Director

An argument can be made for interviewing current and potential members of SAFIRE in South Africa. Documenting the concerns and limitations of institutions within the South African research and education sector can provide SAFIRE with information on how to proceed in South Africa's unique environment. However, the aim of this research is to fill the gap in academic literature with regard to implementing Federated Identity Management specifically in the research and education sector.

2.5 Analysis Phase

With a complete understanding of the literature of Federated Identity Management in higher education together with primary data, the third phase, the Analysis Phase can begin.

This section describes the process of identifying themes in the data as well as synthesizing lessons as the final part of fulfilling the primary objective of this research. This phase can be found in Chapter 6, Analysis.

2.5.1 Identifying Themes

The first step of data analysis is to convert the recorded interviews into a more usable format. Rubin and Rubin (2011) stresses the importance of real-time recording and later transcription of interviews. Interview transcription is more reliable than interview notes which rely on memory. Silverman (2013) emphasizes the fact that although field notes can provide a summary of what people said, memory simply cannot be relied upon for pauses, overlaps, in-breaths, out-breaths, etc.

Transcripts are academic records and can be revised and re-analysed from several angles. Furthermore, (Silverman, 2013) goes on to point out that preparing transcripts should not simply be seen as a technicality prior to analysis. The convenience of transcripts for presentation purposes is an added convenience. Ravitch and Carl (2015) state that simply listening to interview recordings, lacks a kind of deep interaction with the text of the interview and without transcripts it is difficult to engage in intensive, iterative data analysis.

Atlast.ti 7 was used to transcribe the interview recordings as well as to code the transcriptions into segments. Atlast.ti is considered to be one of the most sophisticated qualitative research coding software in existence (Silverman, 2013).

Rubin and Rubin (2011) discuss the precision to which transcripts must be written. They mention that at the most precise level, everything is recorded including grammatical errors, digressions, abrupt changes in focus, profanity, exclamations and other indicators of mood such as laughter or tears. However, they also point out that the level of detail in the transcription should match the type of research being done. It may only be necessary

to include “uhmms” and “ahhs” to retain the feeling of conversation that was had between the interviewer and interviewee. In this regard, I included pauses, digressions and changes in focus to understand the importance that the interviewees put on certain topics. I did not include all grammatical errors, profanities or additional factors that were not core to the topic of this research. A brief example of the transcription detail can be seen in Figure 2.3

I: I believe the UK federeation was one of the first federations that got set up.

A: Sure which means we got certain uh, you'll always have uh, uhm problems with being kind of first movers as well.

Figure 2.3: Transcription extract

Coding involves assigning codes to ’chunks’ of data. Axial coding, also called Thematic clustering coding is a process of transition from coding data to seeing how the codes come together into coding categories or clusters (Ravitch & Carl, 2015).

I began by creating codes based on themes from literature such as Adoption, Privacy and Security. As the processes of coding the transcripts proceeded, more complex codes such as Value proposition and Weaknesses of identity federation were created.

Family codes were created to group individual codes together in logical themes. A list of the family codes are shown in Figure 2.4.

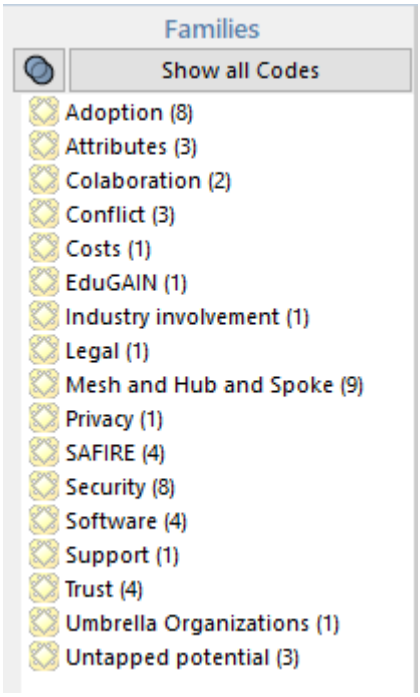

Figure 2.4: Family Codes

With the interviews transcribed and coded into themes, final analysis and argumentation can begin.

2.5.2 Synthesizing Lessons

With the interview data organized into themes as explained in the previous section, together with the findings from the literature reviews in Chapters 3 and 4, the final part of the Analysis Phase can begin.

It is important to distinguish the difference between data analysis and interpretation. Qualitative research is inherently subjective by definition and this subjectivity or researcher bias is seen as a positive thing. Interpretation is the way that individuals make sense of their world and this occurs all the time as a natural part of humanity. Data analysis, on the other hand, is an intentional and systematic process of interpreting data. Unlike interpretation, data analysis describes data in ways that reflect both process and insight (Ravitch & Carl, 2015).

Therefore, argumentation will be used to combine literature with the real world experience of federations to produce a list of lessons learnt from implementing Federated Identity Management in the research and education

sector.

2.6 Conclusion

This chapter has explained how data will be gathered, how the data will be organized and analysed, and how the final output will be reached.

Chapter 3 and Chapter 4 contain the two literature reviews in respective order. Chapter 5 contains the process of the interviews. Chapter 6 contains the analysis of the resulting data and synthesizes the data with the two literature reviews to produce a set of lessons learnt from implementing Federated Identity Management in the research and education sector. Chapter 7 will conclude the research.

Chapter 3

Federated Identity Management

To use an online web service, a user is generally required to login with a username and password. For a long time, passwords have been the most common means for user authentication on the web (Hühnlein, Roßnagel, & Zibuschka, 2010). Today the number of web services that a user interacts with on a daily basis is increasing. This puts strain on users who are expected to remember unique credentials for each service they use (Pashalidis & Mitchell, 2003).

Traditional methods of identity management are struggling to cope with the highly collaborative nature of the present IT environment. In response to this, Federated Identity Management is a promising approach to establish secure resource sharing and collaboration among industry partners in heterogeneous environments (Jensen & Nyre, 2013). Federated Identity Management reduces the number of credentials a user is required to memorize by facilitating cooperation on identity processes between federation members (Jensen, 2012).

However, the adoption of Federated Identity Management has been lower than the initial predictions of academic literature (Jensen & Jaatun, 2013; Landau & Moore, 2012; Smith, 2008). Furthermore, there have been a number of failed Federated Identity Management implementations. Therefore, this literature review will collect and examine academic literature in order to gain an understanding of the current progress of Federated Identity Management and to identify its benefits and challenges.

The chapter begins with an overview of identity management and where

Federated Identity Management fits in. Then Federated Identity Management is dissected and examined in terms of its actors, protocols and architecture. The benefits of Federated Identity Management are identified and discussed, followed by the challenges of Federated Identity Management.

3.1 Identity Management Today

One half of identity management is the issuing, management and termination of user credentials. The second half of identity management is authenticating and controlling access to services and resources (Josang & Pope, 2005). Identity management is usually the first layer of security and accountability (Bhargav-Spantzel, Squicciarini, & Bertino, 2006).

Identity management can be separated into three categories or models. They are the isolated model, the centralized model and the distributed model (Ahn & Lam, 2005; Shin, Ahn, & Shenoy, 2004).

3.1.1 Isolated Identity Management

Of the three models, the isolated model is the oldest and most conservative (Shin et al., 2004). The conservative nature of the isolated model is its down fall, but is also the reason it is still in use. The isolated model does not interact with any outside implementations of identity management and thus retains full control of the entire identity management cycle (Josang, Fabre, Hay, Dalziel, & Pope, 2005).

The institution implementing an isolated model of identity management is the sole identity provider and service provider for its users. This requires users to create new credentials in order to use services outside institutional borders. As institutional collaboration is becoming more widespread, authentication at each service provider is no longer the preferred method of identity management (Kylau, Thomas, Menzel, & Meinel, 2009).

Figure 3.1 illustrates the conservative nature of the isolated model.

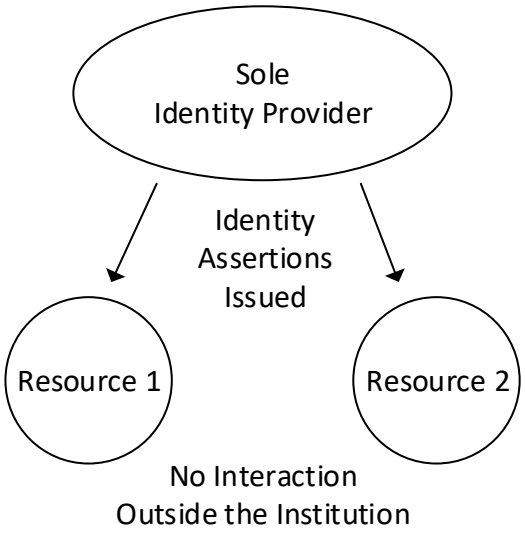

Figure 3.1: Isolated Model

3.1.2 Centralized Identity Management

A centralized model of identity management allows a user to access several service providers and resources using a single identity provider. A single authority acts as the identity provider for all participating services (Dhamija & Dusseault, 2008). Users can access all resources across participating institutions with as few as a single credential.

Although industry is embracing cross-institutional collaboration more and more, a single identity authority raises several privacy and security concerns. Landau and Moore (2012) point out that in the competitive nature of industry, who gets to keep transactional information has been a major contributor to the failure of federations in the past. Even if users create multiple identities in an attempt to mask their activities, patterns in user attributes and use can allow the identity provider to link the various identities to a single individual (Birrell & Schneider, 2013).

A central identity authority provides a single target for DoS (Denial of Service) attacks (Han, Mu, Susilo, & Yan, 2010). All relying institutions must trust the central authority to be available continuously and to risk delays in the case of an incident.

Figure 3.2 illustrates the central identity authority and resource sharing among institutions.

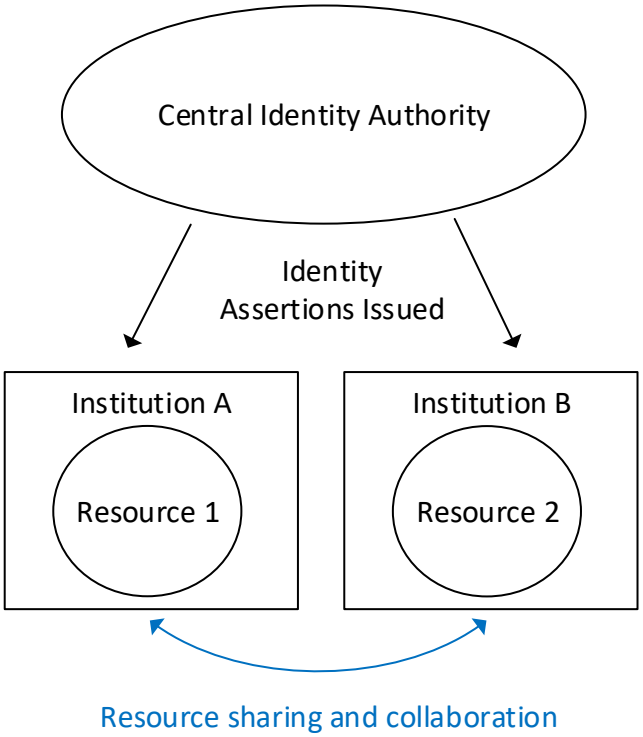

Figure 3.2: Centralized Model

3.1.3 Distributed Identity Management

The distributed model of identity management is a de-centralized version of the previous model. Instead of authentication being the responsibility of a single authority, it is shared amongst all members (Jensen & Nyre, 2013). A participating member may implement its own identity system while trusting other participants to authenticate users on their behalf, thus sharing the cost of identity management (Ahn & Lam, 2005).

This approach still requires a certain level of trust between participants, however there is no clear single point of failure and through the use of assertions, explained later in the chapter, privacy can be preserved to a much greater degree.

Figure 3.3 illustrates the sharing of identity costs and resource sharing among institutions.

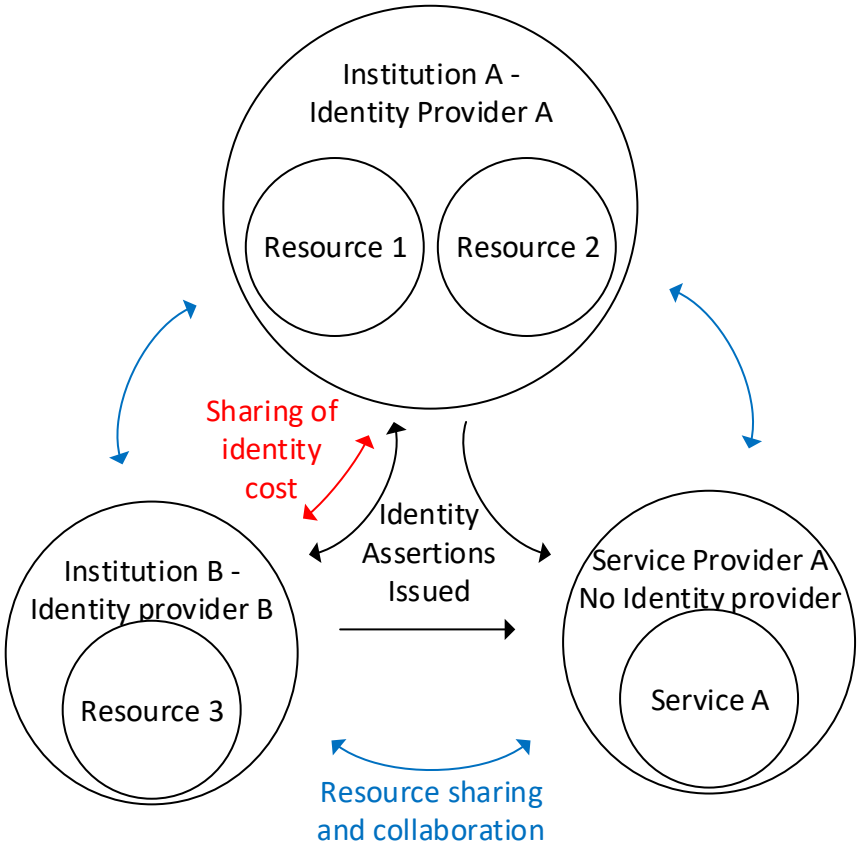

Figure 3.3: Distributed Model

Federated Identity Management allows and facilitates cooperation on identity processes, policies and technologies across institutions borders (Jensen, 2012). A federation consists of two or more institutions cooperating according to agreed rules. Both the centralized and distributed models of identity management satisfy this definition, and are considered part of Federated Identity Management.

3.1.4 Single Sign-On

Single Sign-On is a synonymous term with Federated Identity Management. However, the concept of Single Sign-On and Federated Identity Management

should not be used interchangeably or thought of as being the same. Single Sign-On gives a user the ability to access a protected resource by authenticating themselves once, and then to access other protected resources without having to re-authenticate.

Single Sign-On is commonly used within enterprise networks, where employees are provided with a security assertion that can be used to access services throughout the institution, such as e-mail, file servers and internet access (Jensen, 2013). Employees authenticate themselves once and remain authenticated throughout the institution until the security assertion is terminated or times out.

Single Sign-On was implemented to address one of the most prominent issues at the turn of the 21st century, the high cost of user-management (Gross, 2003). A study conducted at the time by the Network Applications Consortium showed that the majority of calls to help desk were password related. Single Sign-On allows administrators to deal only with one set of credentials per user. Similarly, the help desk only needs to keep track of one entry for each user in their data base (De Clercq, 2002).

Pashalidis and Mitchell (2003) categorizes Single Sign-On into four systems: Local pseudo Single Sign-On , Proxy-based pseudo Single Sign-On , Local true Single Sign-On and Proxy-based true Single Sign-On systems. Understanding these four categories of Single Sign-On assists in making a distinction between stand alone Single Sign-On and Federated Identity Management.

Pseudo Single Sign-On allows a user to experience Single Sign-On in its most basic form. A User's credentials are stored either on the user's local machine or on an external proxy server. A user authenticates himself once and then relies on the pseudo Single Sign-On system to authenticate him on his behalf every time a service requires authentication.

True Single Sign-On requires predetermined trust agreements between services and identity providers. Local true Single Sign-On is under the control of the user and therefore requires mechanisms to ensure integrity. Proxy-based true Single Sign-On is the more commonly implemented Single Sign-On system within enterprises. The user's institution takes responsibility for being the identity provider and has trust relationships with all supported services.

Federated Identity Management is more ambitious than Single Sign-On and offers more value, of which Single Sign-On is only one part. Federated Identity Management enables Single Sign-On, but Single Sign-On does not enable Federated Identity Management. Cooperation on identity processes, policies and technologies in a secure resource-sharing environment are some of the benefits of Federated Identity Management (Jensen, 2012; Malik et al., 2016). The above categories of Single Sign-On were once only possible within the confines of a single organization. Federated Identity Management enables Single Sign-On across institutional and even national borders.

3.2 Federated Identity Management

Federated Identity Management is not a new concept. Academic literature has been identifying, discussing and addressing the benefits of Federated Identity Management as well as the challenges affecting its adoption for some time. Jensen (2012) defines Federated Identity Management as the cooperation on identity processes, policies and technologies across institutional borders. Jensen and Nyre (2013) add to this definition by stating that Federated Identity Management is a promising approach to establish secure resource sharing and collaboration among partners in a heterogeneous IT environment.

This section will focus on and explain the actors, protocols and architecture of Federated Identity Management.

3.2.1 Federated Identity Management Actors

Literature primarily mentions three actors in Federated Identity Management. These three actors are the identity provider, the service provider and the user (Han et al., 2010; Khattak, Sulaiman, & Manan, 2010). However, it is useful to add a fourth actor, the federation operator. Smedinghoff (2012) explains that in a federation with a large number of institutions, there is often an entity referred to as a trust framework provider or a federation operator.

A federation participant is not limited to a single role. In a distributed federation, a number of institutions are able to assume the role of both identity provider and service provider (Birrell & Schneider, 2013).

Users

Each user has an identity that consists of various attributes. These attributes describe the user. A person becomes a user when he attempts to make use of a service or resource.

A user may be an independent actor on the internet, or a user may be an employee, student or researcher at an institution belonging to a federation.

Identity Provider

An identity provider has two primary tasks: to authenticate users and to store and manage user attributes (Birrell & Schneider, 2013). Authentication is the process where by users prove their identity to the identity provider. To store and manage user attributes is a great responsibility and it is in the best interest of the identity providers to keep user information secure and up-to-date.

An identity provider may be an individual actor on the internet, or a users home institution.

Service Provider

Service providers are institutions which make their resources available for use to users. A service provider relies on an identity provider's authentication assertions about a specific user when authorization decisions are to be made.

A service provider may be an individual actor on the internet or a participating institution in a federation.

Federation Operator

The fourth actor in Federated Identity Management is the federation operator. The need for a federation operator depends on the nature and size of the federation (Smedinghoff, 2012). Similarly the role and responsibility of the federation operator is linked to the nature and size of the federation and the agreement between federation participants. Generally, the responsibility of the federation operator is to define the framework or set of rules dictating how the previously mentioned actors interact.

Execution

The process of authentication in Federated Identity Management begins when a user attempts to access a resource. In the case of a centralized federation, a user is redirected to the central authoritative identity provider. In the case of a distributed federation, a user may choose his home institution or desired identity provider from a list of identity providers, and is then redirected. Once the identity provider authenticates the user, an assertion is sent to the service provider containing relevant information about the user. Hughes, Maler, Microsystems, and Lockhart (2005) explain that assertions allow the identity provider to assert characteristics and attributes of a subject (the user) to the service provider. The service provider then authorizes the user, and the user is granted the appropriate level of access.

Figure 3.4 visually illustrates this process.

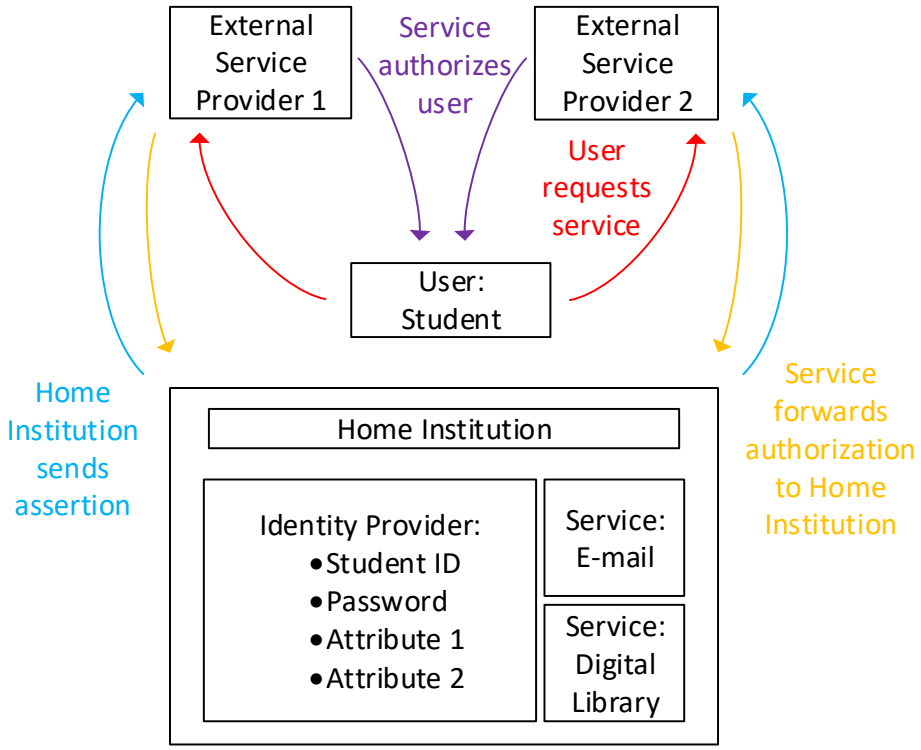

Figure 3.4: Federated Identity Management Actors

3.2.2 Federated Identity Management implementations

Over the last decade, some implementations of Federated Identity Management have been successful, and others have failed. The following implementations of Federated Identity Management have had a noticeable impact on the direction and progress of Federated Identity Management.

Microsoft Passport

Microsoft Passport was one of the first major attempts at implementing Federated Identity Management on the internet (Han et al., 2010). Microsoft Passport was the underlying authentication system of Microsoft's Hotmail and was also integrated into Windows XP (Ahn & Lam, 2005). Microsoft had the intention to become a global identity provider for multiple services, not just its own. Microsoft Passport was designed as a centralized model with Microsoft being the sole identity authority.

Bhatti, Bertino, and Ghafoor (2007) points out that trying to implement a centralized model of Federated Identity Management on this scale, contradicts the distributed nature of the internet. Although Microsoft Passport was able to attract a number of key early adopters such as eBay, it failed to gain traction and eventually early adopters started leaving (Hühnlein et al., 2010). Microsoft Passport ultimately failed to achieve the desired adoption figures (Chadwick, 2009). Security and privacy concerns about the centralized nature of Microsoft Passport have been singled out as the primary reason for its failure (Hühnlein et al., 2010).

OpenID

OpenID is not originally a Federated Identity Management protocol. Rather, it is simply a fairly popular web-based authentication protocol. Through the addition of extensions such as the Attribute Exchange extension, attributes can be exchanged between different institutions (Ferdous & Poet, 2013).

OpenID was developed and released in 2005 to provide a decentralized way of authenticating users who wish to post comments on the LiveJournal online community (Maler & Reed, 2008). Since then, OpenID has spread across the internet with many websites acting as free identity providers and several thousand websites accept OpenID as a method of authentication.

However, OpenID is has not been popular amongst organizations and has not attracted many service providers (Landau & Moore, 2012). Despite the benefits and simplicity of OpenID, there are severe limitations with regard to trust, security and privacy (Arias-Cabarcos et al., 2009). In most implementations, OpenID identity providers only provide service providers with a username and an email address.

Security Assertion Markup Language (SAML)

SAML (Security Assertion Markup Language) was originally created by OASIS (Organisation for the Advancement of Structured Information Standards). The Liberty Alliance was formed in 2001 with the objective to create guidelines and standards for identity management. The Liberty Alliance includes over 150 organizations and in 2005, joined forced with OASIS to produce SAML 2.0 (Landau & Moore, 2012; Scudder & Jøsang, 2010).

SAML is an XML based framework that allows the exchange of security assertions between entities in a federation (Arias-Cabarcos et al., 2009). Unlike OpenID, which has become popular with the internet, SAML has found great success amongst organizations owing to its strong trust, security and privacy preserving properties. As a result, SAML and all other implementations based on SAML have become the most widely used technology for implementing Federated Identity Management (Ferdous & Poet, 2013).

Additional Implementations

Facebook has developed a centralized version of OpenID that allows users to log into third-party websites using their Facebook credentials (Landau & Moore, 2012). Interestingly, Facebook's centralized approach has become more successful than OpenID and has not struggled to gain traction as was the case with Microsoft Passport.

Facebook's success lies in its ability to lure weary service providers by providing demographics of users as well as social networking information, vastly superior to most implementations of OpenID. Additionally, Hühnlein et al. (2010) states that Microsoft Passport's failure should be attributed to distrust in Microsoft, rather than to general security and privacy issues. It is also worth noting that the immense popularity of social networking together with the increased usage of Federated Identity Management over

recent years, has influenced security and privacy concerns since the initial release of Microsoft Passport.

3.2.3 Architecture

During the implementation of a Federated Identity Management system, the layout or topology of the federation must be considered. Within the research and education sector, the two main implementations of Federated Identity Management are the full-mesh and the hub-and-spoke. Each topology has benefits and shortfalls over the other which is why both must be considered in relation to the environment in which it is being implemented.

The Full-Mesh topology interconnects all identity providers and service providers directly. The role of the federation operator is reduced to creating and sharing the lists of meta data containing routes to all participating members. Full-Mesh places more technical responsibility on the institutions, requiring them to configure and maintain links with the rest of the federation. The benefit of this approach is that start up for the federation is cheap and simple. Each institution decides who in the federation they wish to participate with and works on its own to establish a connection.

Hub-and-Spoke connects all federation participants to a central hub. The central hub is managed by the federation managers, usually a neutral third party. The benefit of this topology is that the technical responsibility rests in the hands of the federation operator. Federation participants only need to connect with the hub, and the hub provides access to the rest of the federation. The hub can also implement additional features such as specialized encryption and two-factor authentication available for all members of the federation with little effort on the part of the institutions. The Hub-and-Spoke architecture is expensive to set up initially and requires dedicated staff and technical skills to maintain.

Figure 3.5 illustrates the topological differences between a full-mesh topology and a hub-and-spoke topology.

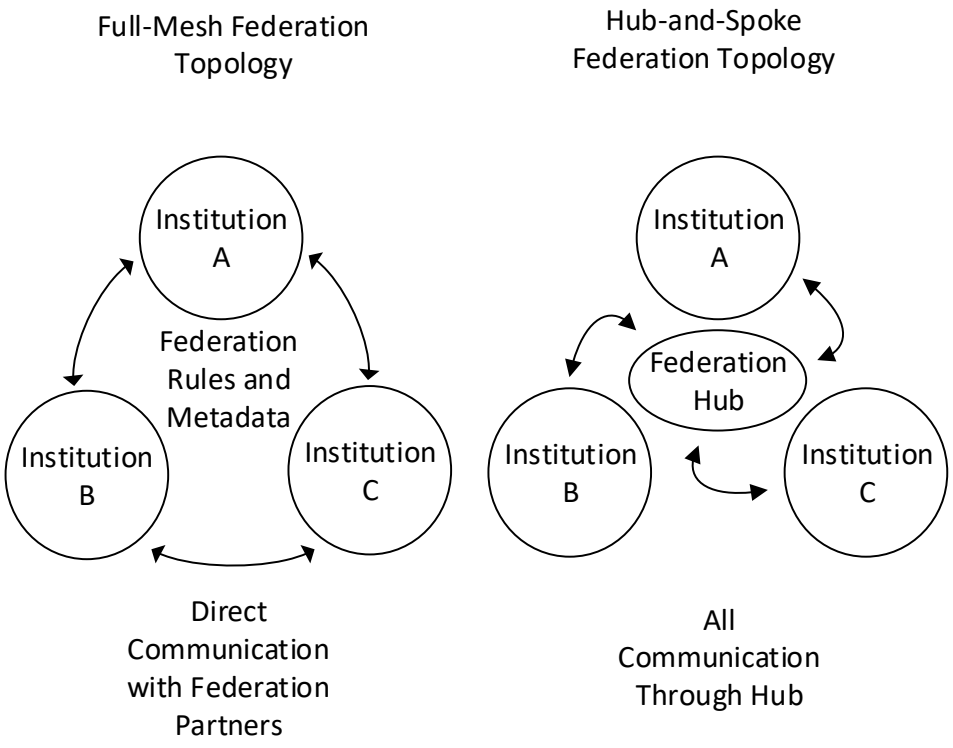

Figure 3.5: Full-Mesh vs Hub-and-Spoke

3.3 Benefits of Federated Identity Management

With the rapid increase in cross-institutional collaboration in industry, traditional isolated models of identity management do not scale well and are no longer the preferred method of identity management (Kylau et al., 2009). Federated Identity Management has been designed to facilitate cross-institutional collaboration by providing Single Sign-On capabilities amongst other benefits in a security and privacy preserving way.

SAML 2.0 is the most popular technology for implementing Federated Identity Management; and Shibboleth, based on SAML is used extensively within the research and education sector around the globe (Ferdous & Poet, 2013; Landau & Moore, 2012). For this reason, the benefits of Federated Identity Management in general will be identified and discussed with specific

emphasis on these two federation enabling technologies

This section discusses the following six benefits of implementing Federated Identity Management. The six benefits are *improved security* (Jensen, 2011; Arias-Cabarcos et al., 2009; Ferdous & Poet, 2013), *improved privacy* (Smedinghoff, 2012; Chadwick, 2009; Landau & Moore, 2012), *Reduced cost* (Ahn & Lam, 2005; Smith, 2008; Jensen, 2014), *improved data quality* (Jensen, 2013, 2014; Satchell, Shanks, Howard, & Murphy, 2011), *collaboration* (Broeder et al., 2013; Malik et al., 2016; Chadwick, 2009) and *better user experience* (Kylau et al., 2009; Scott, Wynne, & Boonthum-denecke, 2016; Landau & Moore, 2012).

3.3.1 Improved Security

The greatest information security plans are incomplete as long as end users lack proper information security awareness and education (Lebek, Uffen, Breitner, Neumann, & Hohler, 2013). Security Education Training and Awareness (SETA) programmes are designed to educate and make end users aware of proper security practices and common security threats.

Educating users on the importance of proper password etiquette is a core part of SETA programmes. Through these programmes, end users are taught how to create, store and use passwords that meet basic security requirements. One such basic security practice is to use a different password for every identity used. Dhamija and Dusseault (2008) state that in 2008 an average end user had approximately 25 different identities in total, and used up to 8 on a day to day basis.

Federated Identity Management reduces the number of login credentials users have to use to access resources within the federation. This lightens the burden on users and aids the success of information security awareness programs such as SETA by encouraging the use of a limited number of strong login credentials (Scudder & Jøsang, 2010).

SAML (Security Assertion Markup Language) makes use of assertions between identity providers and service providers. Assertions are statements that contain authentication, authorization and attribute information about a user (Arias-Cabarcos et al., 2009). SAML encourages security and privacy by allowing the identity provider to only include necessary user information. If service providers require more information to authorize a user, they can

request addition information as needed (Ferdous & Poet, 2013).

3.3.2 Improved Privacy

Privacy is an integral concern in any organizational identity management system (Smedinghoff, 2012). Privacy has been a major topic of discussion in Federated Identity Management literature and has been identified as a significant contributor to the low adoption rate of past implementations (Chadwick, 2009). Jensen (2012) states that users should be able to enjoy increased privacy protection through Federated Identity Management without a loss of information quality passed on to service providers.

Satchell et al. (2011) define privacy as an Individual's claim that information about themselves should not be available to other individuals or organizations and that the individual must be able to exercise a substantial degree of control over their data. This highlights the user's expectations of privacy in Federated Identity Management .

Integrating privacy protection is not just to please users. Bhatti et al. (2007) state that privacy protection is becoming increasingly important to businesses from a social and legal perspective. It is in the best interests of identity providers to implement adequate privacy protection to avoid privacy law violations. Satchell et al. (2011) suggest that a balance is required between effective governance, legal needs and national security needs on the one hand; and an individual's dignity and privacy on the other.

SAML implementations of Federated Identity Management disclose the minimal amount of user information needed for a service provider to authorize users (Ferdous & Poet, 2013). SAML 2.0 makes use of pseudonyms that only have meaning in the context of the relationship between the identity provider and service provider. The purpose of this is to prevent institutions from linking user identities and activities, and to maintain an appropriate level of user anonymity (Shin et al., 2004). Users still have the option to link pseudonyms to their identity if they wish (Hughes et al., 2005).

Shibboleth is an open-source implementation of Federated Identity Management and is currently the de facto standard in the research and education sector (Catuogno & Galdi, 2014). Users are identified by their rights to the resource, as a member of a particular campus, course and cross-institutional research group rather than by their user ID. The user ID is just another at-

tribute only shared if the service provider requires it to grant access (Landau & Moore, 2012). Shibboleth requires both administrators and users to have control over the release of attributes to providers insuring strong privacy protection of user details (Chadwick, 2009).

3.3.3 Reduced Cost

Being cost-effective is an important requirement for the success of Federated Identity Management (Ahn & Lam, 2005). A separation of duties allows service providers to allow trusted identity providers to authenticate users on their behalf. This potentially allows service providers to avoid the expense and responsibility of storing user information (Chadwick, 2009).

The separation of duties furthermore reduces cost by the consolidation of key business areas such as help desk pointed out by Smith (2008) and a simplified auditing process pointed out by Jensen (2014).

Furthermore, Federated Identity Management facilitates the formation of relationships between industry partners to realize common goals at lower costs (Satchell et al., 2011).

3.3.4 Improved Data Quality

To authorize users securely, service providers need accurate and up-to-date information. Jensen (2014) points out that despite policy stating that passwords must be updated every 90 days, most users will continue to reuse their password after expiry. A user who makes use of multiple credentials on a daily basis is unlikely to keep his information up-to-date at every identity provider.

Jensen (2013) highlights the security concerns of outdated identity attributes. Employees' access rights could change; users' contact numbers can change; digital certificates and credit card information can expire. Jensen concludes that it is therefore necessary for identity management processes to include procedures to keep user identity attributes up-to-date.

The approach of Federated Identity Management to establishing secure resource sharing and collaboration among partners in heterogeneous IT environments, simplifies the process and policing of updating user identities. By reducing the number of identities per user to as few as one per federation, re-

liably and consistently updating user information and levels of authorization becomes a more realistic goal.

Additionally, identity providers have more motivation to improve relationships with their users. In this way, identity providers can focus on improving the overall process of authentication (Chadwick, 2009).

3.3.5 Collaboration

Traditional isolated models of identity management do not scale well with cross-institutional collaboration. An institution would have to add users from collaborating partners to their identity management system. This not only increases the cost of collaboration, but also introduces dangerous security vulnerabilities. One such security vulnerability is account revocation (Jensen, 2013).

Broeder et al. (2013) emphasises the importance of collaboration in research and higher education. A number of institutions and service providers should be able to work together to complete research projects without users being obliged to remember a growing number of accounts and passwords.

Jensen and Nyre (2013); Jensen (2014) presents the highly collaborative environment of the Norwegian oil and gas industry, explaining the beneficial but also competitive relationship between contractors and suppliers.

Federated Identity Management simplifies and encourages collaboration between federation members (Malik et al., 2016). Using a limited number of identities per user when collaborating with federation partners addresses the concern of account revocation. Rather than contacting all the institutions a user has collaborated with in the past, a users home institution only needs to update their records and all federation members using that identity will be updated.

Additionally, by trusting another institution to manage user identification, a service provider is able to focus on improving the quality of their resources and services. Furthermore, a service provider is able to make their resources and services available to multiple identity providers, and thus to a larger audience (Chadwick, 2009).

3.3.6 Better User Experience

A major benefit of Federated Identity Management found in literature is an improved user experience (Kylau et al., 2009). Within collaborative environments, users have been expected to remember an increasing number of accounts and passwords while abiding by an organizational security policy. By reducing the number of accounts per user, Federated Identity Management encourages users to create strong passwords according to organizational requirements (Scott et al., 2016).

Additionally, Single Sign-On allows users to access several resources throughout the federation without having to re-authenticate at each service provider. This has a direct link to improved productivity and quality of work (Landau & Moore, 2012).

3.4 Challenges in Federated Identity Management

At the turn of the 21st century, literature was optimistic about the future of Federated Identity Management. Today literature has expressed concern for the relatively low rate of Federated Identity Management adoption (Jensen & Jaatun, 2013; Landau & Moore, 2012; Smith, 2008). Literature has discussed a number of challenges that are responsible for the low observed rate of Federated Identity Management adoption.

This section discusses the following six challenges of implementing Federated Identity Management. The six challenges are *trust* (Smith, 2008; Bhargav-Spantzel et al., 2006; Landau & Moore, 2012), *liability* (Jensen, 2012; Smedinghoff, 2012; Landau & Moore, 2012), *security* (Shin et al., 2004; Bhargav-Spantzel et al., 2006; Han et al., 2010), *privacy* (Morgan, Cantor, Carmody, Hoehn, & Klingenstein, 2004; Malik et al., 2016; Landau, Gong, & Wilton, 2009), *investment cost* (Shin et al., 2004; Jensen & Nyre, 2013; Smith, 2008) and the *awareness barrier* (Smith, 2008).

3.4.1 Establishing Trust

Mcknight and Chervany (1996) define trust as "the extent to which one party is willing to depend on the other party in a given situation with a feeling of

relative security, even though negative consequences are possible". Although this definition of trust is general, there are three relevant concepts that can be extracted. First, the *dependence* on a trusted party; second, the *reliability* of the trusted party; and third, a possibility of *negative consequences* in the event of an incident (Josang et al., 2005).

Dependence

Smith (2008) argues that trust is a fundamental underlying concept of Federated Identity Management. Bhargav-Spantzel et al. (2006) defines Federated Identity Management as a group of organizations which trust certain kinds of information from any member of the group as being valid.

To make authorization decisions, a service provider must trust that user information received from an identity provider is accurate and up-to-date (Landau & Moore, 2012). Identity providers must trust service providers to handle user information securely in a privacy preserving manner.

The trust dependence on federation members is apparent in the most popular Federated Identity Management specification, SAML (Secure Assertion Markup Language). The success of SAML enabled federations is largely dependent on a pre-configured trust relationship. Literature has identified pre-configured trust relationships as a barrier to Federated Identity Management adoption in some parts of industry (Ferdous & Poet, 2013).

The failure of Microsoft Passport to gain widespread adoption has been attributed to distrust in Microsoft (Hühnlein et al., 2010).

Reliability

To establish and maintain trust between institutions, reliability and assurance must be established. Identity assurance is achieved by providing transparency into how risks associated with identity information are being managed (Baldwin, Casassa Mont, Beres, & Shiu, 2010). Baldwin et al. (2010) continue to point out that while identity management is a well supported technology, and that while there are standards for Single Sign-On, authentication and authorization, many aspects remain procedural and rely on people doing the right thing. This makes it difficult to establish assurance and reliability.

Negative Consequences and Risk Appetite

Part of understanding Federated Identity Management is to understand and account for additional risk. Institutions in a federation are likely to come into contact with institutions of varying risk appetite. A difference in risk appetite will have a direct impact on the ability to establish trust relationships, as an institution with a low risk appetite may not find it acceptable to depend on an institution with a higher risk appetite (Jensen, 2012).

3.4.2 Liability

Liability is the state of being legally obliged or responsible (Jensen, 2012). In the event of a security breach or system failure, Who shoulders the blame? has become a stumbling block for many federations. Liability is not a new concern for identity management; however Federated Identity Management has introduced new complexities (Jensen & Jaatun, 2013). The boundaries of security and privacy have changed and are not as clear as they once were. This has resulted in new liability and privacy risks (Landau & Moore, 2012). Landau et al. (2009) states that the threat of being held liable has become the main motivator for privacy implementation in Federated Identity Management. Who is liable in the case of failure is clearly an important prerequisite that must be properly understood by all parties involved.

Smedinghoff (2012) states that the failure of law to address liability issues properly has presented a barrier to identity systems. Smedinghoff carries on to say that the U.S. National strategy has recognized that concerns around liability represent a key barrier to the adoption of Federated Identity Management. The U.S. National strategy has stated that liability issues would best be addressed by contractual agreements among federation participants. These agreements should be compliant with internal rules and regulations of institutions, those of partners and legal constraints (Jensen, 2012).

Returning to Smedinghoff's statement regarding the failure of law to address liability issues properly; it is important to remember that laws differ from nation to nation. In the banking industry, the U.S. provides ample protection of card holders with the Lending Act of 1968 and the Electronic Funds Transfer Act. These Acts shift the liability as a result of fraud away from the card holder, and onto the issuing banks and merchants banks (Landau &

Moore, 2012). By comparison, UK consumer protection has historically been weaker and UK banks have shifted the responsibility on to the card holder where possible.

Landau and Moore (2012) argues that a balance of liability is necessary. Once each party feels that they have a fair portion of liability then the federation is more likely to succeed.

Federated Identity Management allows identity management to be implemented with minimal data exchange. Liberty Alliance specifications enable a number of privacy protecting features, but it remains the responsibility of the implementers to conduct risk assessments and to manage liability properly, in line with the suggestion of the U.S. National strategy (Landau et al., 2009; Smedinghoff, 2012).

3.4.3 Security

Security issues are a key concern in Federated Identity Management (Shin et al., 2004). Federated Identity Management improves the overall security of cross collaboration in several ways highlighted earlier. However, like all forms of identity management, Federated Identity Management is not perfectly secure. By solving one problem, Federated Identity Management raises another (Landau et al., 2009). Allowing users to use a smaller number of credentials in exchange for a few strong credentials has obvious security advantages. However, identity theft is a serious concern (Bhargav-Spantzel et al., 2006). Identity theft occurs when a malicious user uses a honest user's credentials without his permission. Attackers who gain access to a single set of credentials could theoretically acquire access to several resources (Han et al., 2010). The reverse argument here is that with fewer passwords, users can better protect against phishing attempts. Two step authentication is a means many federations are deploying to reduce the risk of phishing attacks and identity theft.

Once a user is authenticated, they receive a token which they use to access other resources without having to re-authenticate. Much research is being put into the protection of these tokens. A token intercepted may allow attackers temporary access to multiple resources so long as the lifetime of the token persists. A trade off between user convenience and security has to be reached concerning the lifetime of these tokens.

3.4.4 Privacy

A foundational issue for any identity system is protecting privacy (Smedinghoff, 2012). A benefit of Federated Identity Management is enhanced user privacy, however solving one problem has raised others (Landau et al., 2009). Federated Identity Management blurs security borders and has created new privacy risks and vulnerabilities. Jensen (2012) labels privacy as a major challenge in Federated Identity Management, and is currently a hot topic in Federated Identity Management literature. The research and education sector has placed strict requirements on the protection of privacy and was the focus around the development of Shibboleth (Morgan et al., 2004). Despite this, privacy has not been catered for in many other implementations of Federated Identity Management (Malik et al., 2016).

To understand the difference of privacy priority, one must consider the different sector and national environments. Some sectors in the US have strict privacy laws in place which influence the priority of privacy in associated implementations of Federated Identity Management. At the same time there are other sectors in the US that have very little privacy laws (Smedinghoff, 2012).

3.4.5 Investment Cost

Simplified identity management at reduced cost is a benefit of Federated Identity Management (Shin et al., 2004). However, initial investment cost is often necessary (Jensen & Nyre, 2013). Smith (2008) mentions that some institutions may need to reconstruct or replace their current system of identity management if it is not compatible with Federated Identity Management.

Changing or adapting an institution's current method of identity management can be an expensive and risky exercise. A possible strategy mentioned by Jensen and Nyre (2013) is to first adapt systems where investment cost is lower, before adapting the entire system.

3.4.6 Awareness Barrier

A lack of knowledge of Federated Identity Management may have a negative impact on the adoption. Smith (2008) says "While identity management is not rocket science, there's confusion as to what it delivers and the complexity

involved." Current knowledge about Federated Identity Management or the lack there of is a barrier to the adoption of Federated Identity Management. Even though Federated Identity Management has been around for a number of years, industry is still hesitant to give up the tried and tested methods of collaboration. Fear of the unknown causes industry to focus on negative aspects of Federated Identity Management.

The user community is also suffering from a lack of knowledge. Resulting in a lack of pressure from users pushing their institutions to invest time into gaining proper understanding of Federated Identity Management.

3.5 Conclusion

Federated Identity Management was introduced on a large scale at the turn of the 21st century in the form of Microsoft Passport. Despite its benefits, Microsoft Passport encountered a number of challenges which prevented its wide spread adoption. Since then, literature has discussed the potential of Federated Identity Management, its benefits and its challenges.

This chapter began by introducing Federated Identity Management and comparing it to traditional models of identity management. Then the defining attributes of Federated Identity Management was discussed followed by benefits and challenges found in literature.

In line with the objective of this research, the following chapter, FIM in Research and Education, will present the literature on Federated Identity Management specifically within research and education.

Chapter 4

Federated Identity Management within the Research and Education Sector

Chapter 3 identified and discussed the challenges of implementing Federated Identity Management. Literature states that the adoption of Federated Identity Management has been lower than initially predicted. However, implementations of Federated Identity Management within the research and education sector have been relatively more successful than in other parts of industry (Landau & Moore, 2012; Smith, 2008)

This literature review will focus on Federated Identity Management within the research and education sector. The chapter begins with introduction of Federated Identity Management to the research and education sector at the turn of the 21st century. The progress of Federated Identity Management in this sector such as the development of Shibboleth and the formation of EduGAIN are discussed. The chapter ends off by exploring the environment of the South African research and education sector and the challenges that SAFIRE (South African Identity Federation) must address.

4.1 Federated Identity Management in Higher Education

Literature has attributed the relative success of Federated Identity Management within the research and education sector to its more trusting environment compared to that of other parts of industry (Smith, 2008). This is strengthened by a mutual willingness to collaborate with other institutions on research projects and the advancement of education (Ferdous & Poet, 2013).

Near the end of the 1990s and the beginning of the 21st century, the research and education sector found collaboration increasingly difficult owing to rising complexities and costs. At the fifth Annual Educause Current Issues Survey, security and identity management were identified as critical IT challenges on university campuses (Morgan et al., 2004).

Without the aid of Federated Identity Management, some services such as JSTOR were forced to authorize students and researchers via network addresses, rather than via individual user accounts protected with proper authentication. JSTOR had to invest significant resources to detect and protect against security threats owing to a lack of proper identity management that could scale appropriately (Morgan et al., 2004).

It was clear that the research and education sector at large had to adopt an alternative method of identity management that would facilitate its collaborative environment.

4.1.1 Athens

Early attempts to federate identity management were isolated and not standardized throughout the research and education sector. Athens, which was a centralized implementation of Federated Identity Management was used throughout Europe and particularly the UK higher education sector (Smith, 2008).

Athens relied on proprietary protocols, creating a barrier to its adoption. Being a centralized system, Athens suffered from similar trust issues as other centralized federations, such as Microsoft's Passport. Efforts to standardize Federated Identity Management protocols resulted in Athens being phased

out from the UK higher education sector in favour of Shibboleth in 2008 (Chadwick, 2009).

4.1.2 Shibboleth

Shibboleth, based on the SAML standard is an implementation of Federated Identity Management specifically designed for the research and education sector (Gross, 2003).

In 1999 the Internet2 established its Middle-ware Initiative, and worked on issues such as authentication, authorization and directory services (Morgan et al., 2004). In June 2003, the Internet2 Middle-ware Initiative effort produced Shibboleth version 1.0. Unlike Athens, Shibboleth, being based on SAML, is open-source and standardized. Additionally, Shibboleth follows a distributed model allowing users to be authenticated by their home institution (Chadwick, 2009).

Shibboleth was developed to overcome various challenges present in the research and education sector. Challenges such as interoperability across institutional boarders, enabling home institution authorization and reducing the number of credentials per user in a secure and privacy-preserving way (Khattak et al., 2010). As a result, Shibboleth has been a success with the research and education sector and circles of trust (Landau & Moore, 2012).

The primary reason for Shibboleth's success in the research and education sector is its ability to meet the strong requirements of higher-education communities with regards to the protection of personal information (Morgan et al., 2004). Privacy was critical to the design of Shibboleth (Landau & Moore, 2012). Chadwick (2009) lists four ways in which Shibboleth protects user privacy. Firstly, Shibboleth supports anonymous authentication (Birrell & Schneider, 2013). A randomly generated identifier can be used instead of a user's permanent unique identifier. Secondly, service providers are able to request specific attributes needed to authorize users instead of simply requesting all attributes. This minimizes the opportunity for potential privacy loss. Thirdly, Shibboleth requires identity providers to provide control over the release of user attributes in the form of attribute release policies. Lastly, to prevent third parties from seeing attributes in transit, connections should be protected with SSL/TLS with strong encryption enabled.

Thanks to the standardized, secure and privacy-preserving Shibboleth,

Federated Identity Management within the research and education sector was able to expand and interconnect the globe through EduGAIN.

4.2 EduGAIN

EduGAIN is the product of an effort to interconnect identity federations around the globe within the research and education sector, allowing the secure exchange of information. EduGAIN is a service developed within the GEANT project. The GEANT project is a collaboration between European National Research and Education Network (NREN) organizations and the European Union. Today, EduGAIN serves as a federation of federations for the entire global research and education sector. Figure 4.1 shows the extent of the EduGAIN global community.

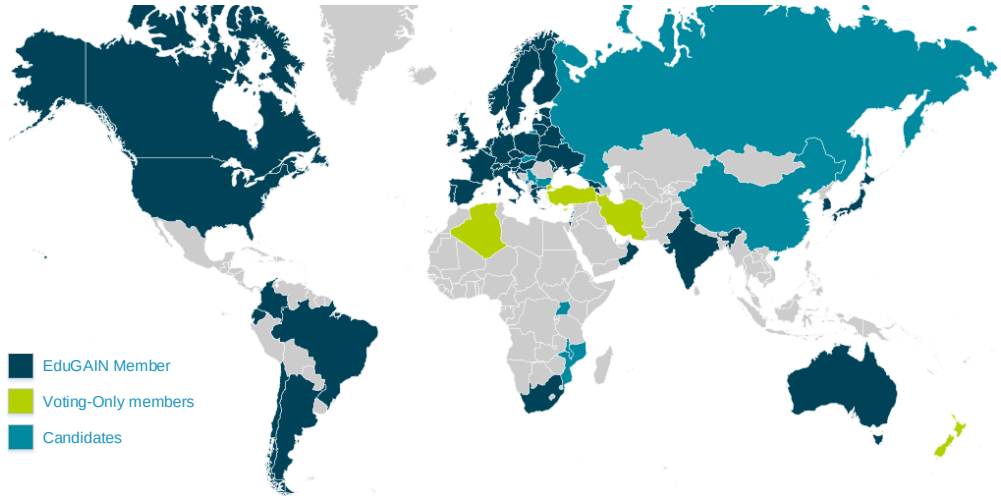

Figure 4.1: Global Map of EduGAIN As of 25/08/2017. (From https://technical.edugain.org/status.php)

EduGAIN enables researchers, students and educators to access and share online resources securely with reduced complexity and cost. At the same time, users are authenticated by their local institution, reducing the number of credentials per user. Service providers benefit by offering their services to an international community.

The EduGAIN technology retrieves and aggregates information from participating federation's services and identity providers and makes it available

through what is called a Metadata Service. The exchange of information is controlled though a policy framework. As of 31 August, EduGAIN facilitates the collaboration and exchange of information of 48 member federations.

Table 4.1 displays the number of federation members in EduGAIN. Table 4.2 shows the number of entities throughout EduGAIN. Note that the sum of identity providers and service providers equals more than the total. This is as a result of some institutions participating both as an identity provider and as a service provider.

Table 4.1: EduGAIN Members As of 25/08/2017

Federations in EduGAIN	
Members	45
Voting-only Members	7
Candidates	11

* Note: Adopted from https://technical.edugain.org/status.php

Table 4.2: EduGAIN Entities As of 25/08/2017

Entities in EduGAIN	
All	4207
Identity Providers	2513
Service Providers	1698

* Note: Adopted from https://technical.edugain.org/status.php

4.3 South African Identity Federation

The South African National Research and education Network (SANReN) together with The Tertiary Education and Research Network of South Africa (TENET) have launched the South African Identity Federation (SAFIRE) for the research and education sector. SAFIRE is an independent organization drawing a large portion of its funding from early adopters. SAFIRE currently has 8 identity providers as seen in Table 4.3 and offers 9 services as seen in Table 4.4.

Table 4.3: SAFIRE Identity Providers As of 25/08/2017

Identity Provider Participants in SAFIRE -	
(IDP)	CSIR (Council for Scientific and Industrial Research)
(IDP)	Nelson Mandela University
(Pending IDP)	North-West University
(IDP)	SANReN Competency Area
(IDP)	Stellenbosch University
(IDP)	TENET South Africa
(IDP)	University of Cape Town
(Pending IDP)	University of Western Cape

* Note: Adopted from https://safire.ac.za/participants/idp/list/

Being one of the most recently implemented federations in the global research and education sector, SAFIRE is reaping the benefits of over a decade of innovation and trial and error. Thanks to the inherently collaborative nature of the global research and education sector, SAFIRE is making use of the valuable opportunity to learn from the successes and failures of other federations in this global sector. Examples include the use of open source standardized software like Shibboleth, developed by the Internet2 and first used by InCommon.

Table 4.4: SAFIRE Service Providers As of 25/08/2017

Service Provider Participants in SAFIRE -	
(SP)	African Research Cloud
(SP)	CSIR-SANREN File Sender
(SP)	figshare
(SP)	OnTheHub
(SP)	SheerID Verification Services
(SP)	eduroam South Africa NRO
(SP)	SA NREN Mconf web conferencing
(SP)	SAFIRE Test Service Provider
(SP)	UCT DEV Filesender

* Note: Adopted from https://safire.ac.za/participants/sp/list/

In February 2017 SAFIRE became the 41st member of EduGAIN and the

first fully participating member from Africa (SAFIRE, 2017).

4.3.1 South African perspective

At the time Liberty Alliance and OASIS released SAML, and the Internet2 developed Shibboleth, South Africa was celebrating its first decade as a free country. The focus of South African research and government was to bridge the economic and social gaps left by apartheid (Brown, Hoppe, Mugera, Newman, & Stander, 2004). Around this time, no culture-specific research had been done to understand how IT should be approached for South Africa (Gefen, Rose, Warkentin, & Pavlou, 2005).

It would take another decade before SAFIRE was created. However, there are advantages to being a late adopter of a technology, especially in the research and education environment. Federated Identity Management has been relatively successful in the education sector and many of the challenges mentioned in Chapter 2 have been addressed by federations around the globe. SAML and Shibboleth have improved both in terms of simplicity and of security. Physical technology has matured and both the Full-Mesh and Hub-and-Spoke topologies have been tested and implemented with successes.

South Africa has a mix of first and third-world components, different ethnicities and cultures, 11 official languages, and large economic and educational gaps (Gefen et al., 2005). However, South Africa is also one of the leaders in IT adoption in Africa, and is the first African member of EduGAIN. There are a number of factors unique to the South African environment that must be considered to ensure the success of SAFIRE.

SAFIRE is a perfect example of a young federation working to establish itself by addressing the challenges of Federated Identity Management in a unique environment. This research, which aims to identify, gather and document lessons learnt from implementing Federated Identity Management in the research and education sector, will help young federations such as SAFIRE benefit from the past experiences of other federations within this sector.

4.4 Conclusion

The research and education sector has been relatively successful in the implementation of Federated Identity Management. Enablers like Shibboleth, developed with an emphasis on simplicity and privacy protection are key driving factors of this success. As a result, the research and education sector has become one global federation through EduGAIN.

New federations can benefit from the collaborative nature of the research hand education sector. Rather than implementing Federated Identity Management from scratch, young federations like SAFIRE have the opportunity to avoid common challenges by following the example of earlier federations.

Chapter 5

Interviews

Chapter 3 discussed the current state of Federated Identity Management throughout industry, including the value it provides and the challenges of its implementation. Chapter 4 discussed the history, relevance and state of Federated Identity Management within the research and education sector. Together, these two chapters describe Federated Identity Management according to literature.

This chapter will outline and discuss the primary method of data collection, interviews. Seven identity federations from around the globe are interviewed in a semi-structured setting. Each interview comprise five distinct topic areas, derived from literature and stakeholder input. All interviews will be recorded with the consent of the interviewees and then transcribed to facilitate proper analysis of the collected data.

5.1 Interview Structure

An interview is a social interaction between an interviewer, in this case the researcher, and the interviewee, personnel from selected federations. Both the interviewer and the interviewee share in constructing a story together with its meanings. The interviewee reveals and places emphasis on information based on his subjective opinion and experiences. The interviewer or researcher, within the confines of qualitative research, analyses and interprets the data subjectively.

In Chapter 2, Research Methodology, Interviews have been described as existing on a spectrum.

Structured interviews consist of fixed questions that do not change from one interview to the next interview. The focus is to compare replies between interviewees directly. Therefore, structured interviews do not allow for probing questions, nor do they allow the interviewees to elaborate on what they previously said. The researcher must ask every interviewee the same questions in the same order to prevent previous questions from influencing the interviewee's train of thought or mood in any inconsistent way.

At the other end of the spectrum, unstructured interviews do not contain any prepared questions and each interview may take a different direction from the interviews before or after it. The interviewer introduces the interviewee to the topic with a short and general description and then allows the interviewee to answer how ever he or she pleases. Unstructured interviews are able to provide in-depth information on the topic at hand. However, unstructured interviews are limited to the interviewee's ability to communicate. An interviewee who is not fond of talking may not reveal as much information as expected. Furthermore, it can be difficult for the researcher to find patterns or common themes amongst participants, since each interview may vary substantially from the others.

Semi-structured interviews comprise structured and unstructured elements, shifting between a more structured approach at times, but allowing for sufficient depth as well. Researchers influence the direction of the interview with leading questions, derived from past research and literature, and follow up on points of interest when applicable. This allows the researcher to learn previously unknown information or to place more emphasis on topics that were previously less important. Struwig and Stead (2001) suggest following a more unstructured approach with half the interviewees, and progressively becoming more structured in later interviews. This is a good way to incorporate and to maintain a balance between structured and unstructured elements of the interview process. This approach also allows the researcher to incorporate and delve deeper into new information revealed by interviewees.

A semi-structured approach was used to interview the federation participants. Literature and input from the stakeholders were used to define five topic areas. Interviewees are asked questions related to each topic area. Additional points of interest mentioned by interviewees were followed with the relevant questions.

The following section will introduce the first topic area, Initial Adoption. There after, the remaining four topic areas, Complexity and Understanding, Incidents, Topology and Success and Failure are introduced and discussed.

5.2 Initial Adoption

Despite initially predicting the rapid adoption of Federated Identity Management, literature has shown concern for the low rate of Federated Identity Management adoption in industry. Jensen and Jaatun (2013) state that, based on the added value of Federated Identity Management, one would think that industry would be rushing to adopt it. However, this has not been the case and the adoption of Federated Identity Management has been lower than expected throughout industry.

Some implementations of Federated Identity Management have experienced modest success in a few specific parts of industry. Shibboleth has become the dominant means of implementing Federated Identity Management within the research and education sector (Landau & Moore, 2012). The reason for the wide spread usage of Shibboleth and the relative success of Federated Identity Management within the research and education sector has been attributed to the more trusted environment of higher education (Smith, 2008). Chapter 4 discusses the reasons for the success of Shibboleth in more detail.

Besides this, literature does not discuss other factors that have contributed to the success of Federated Identity Management in this sector on a global scale. Furthermore, the unique challenges affecting the adoption and implementation of Federated Identity Management within the research and education sector have not been identified or discussed within literature.

The first topic area addressed in the interviews was initial adoption and barriers to the adoption of Federated Identity Management within the research and education sector.

Interviewees are asked about the initial adoption of their federations and if it was lower than expected. Additionally, what solutions had been implemented to combat this and to encourage adoption.

The output of this topic area will aid future federations in this sector to avoid the challenge of low initial adoption and thus enable them to join the

global network of federations with less delay.

5.3 Complexity and Understanding

Smith (2008) states that Federated Identity Management is not rocket science, but that there is confusion with regard to the complexities involved. Rogers (1995) defines complexity as the degree to which an innovation is perceived as difficult to understand. It is clear from both statements that the perceived complexity of Federated Identity Management is related to industry's understanding of the risks associated with Federated Identity Management and the value it provides.

Chapter 3 discusses a number of complexities in the implementation of Federated Identity Management, such as liability, the establishment of trust and new security risks. A lack of general awareness amongst institutions and their users, is also discussed in Chapter 3 and contributes to the perceived complexity of Federated Identity Management.

While literature has attributed the general success of Federated Identity Management within the research and education sector to high levels of trust, literature has not discussed the impact of this trust, on the perceived complexity of Federated Identity Management within this sector. The purpose of this second topic area is to gain an understanding of how perceived complexity has affected Federated Identity Management within the research and education sector.

Interviewees are asked to gauge the level of complexity that is involved in Federated Identity Management in this sector and the impact it has on local potential adopters. Furthermore, interviewees are asked how they addressed members' understanding, perceived complexity and, by extension, perceived risk of Federated Identity Management.

The output of this topic area will assist future federations in simplifying and reducing the perceived risk of Federated Identity Management, tailoring it to their unique local environments.

5.4 Incidents

The previous section has addressed the impact that perceived complexity and understanding has on the adoption of Federated Identity Management. Related to this is the occurrence and handling of incidents. Federated Identity Management literature contains many discussions proposing solutions to various security and privacy breaches. Landau and Moore (2012) state that the assignment of liability in the case of information security or privacy breaches is a major stumbling block in many federations. Landau et al. (2009) give the example of identity providers who typically bear liability for the identity assertions they make and that service providers prefer to lower their own risk by relying on these assertions.

Within the research and education sector, implementations of Federated Identity Management such as Shibboleth have gone far in assigning liability to the appropriate parties. However, it is unrealistic to assume that security breaches will never happen within Federated Identity Management. Accidental breaches of information security and privacy are far more likely in a federated environment where external institutions all have a role to play in the protection of shared information. None the less, the effect of incidents occurring by accident can have the same negative impact as incidents caused by malicious parties. The purpose of this third topic area, is to learn how the research and education sector has addressed the challenges of resolving incidents.

Interviewees are asked about the relationship between members of the federation and how incidents are addressed and solved.

The output of this topic area will help new federations to adopt a realistic approach to managing the occurrence of incidents and the relationship between members of the federation successfully.

5.5 Topology

Federated Identity Management literature discusses centralized and distributed models of identity management in detail. However, the identity management model should not be confused with the underlying topology of the federation network. During meetings with the stakeholders, the choice of which topology

to implement was a topic of great importance. Both, identity management models and topologies, are discussed in Chapter 3.

There is a gap in Federated Identity Management literature with regard to the various topology options the differences between the topology options, and the decision making process one must consider when choosing a topology. Both the Full-Mesh and the Hub-and-Spoke topology are used throughout the research and education sector. Each of the topologies provides unique benefits and has certain shortfalls. The success of Federated Identity Management may be greatly affected depending on which topology is implemented. The purpose of this topic area is to discuss the importance and the nature of the underlying network topologies within the research and education sector.

Interviewees are asked to define and discuss the network topology they have implemented within their federation and the reasons that they preferred it over other topologies. Furthermore, interviewees are asked to discuss the impact that network topology has on a particular environment and on the institutions within.

The output of this topic area will assist future federations in making the decision of which network topology to implement and how it will effect their unique environment.

5.6 Success and Failure

Horbe and Hotzendorfer (2015) state that data minimization and releasing only the attributes needed to authenticate a user is well established within the research and education sector and can be considered as state of the art. Literature has also made special mention of the research and education sector with regard to the successful implementations of Federated Identity Management. This research aims to identify, discuss and compile the unique factors that have made Federated Identity Management work in this sector of industry.

However, using Federated Identity Management literature as the main source of information when creating the previous topic areas, is a potential shortfall of this research. The purpose of the final topic area is to identify additional practices unique to the research and education sector that have

aided in the relative success of Federated Identity Management in this sector of industry.

Interviewees are asked to identify and discuss addition practices that have brought success to their federation as well as practices that have not gone as expected. Interviewees are then asked to conclude with with any extra information they wish to provide.

The output of this topic area will reveal additional factors or points of interest that will aid future federations, including, how to make full use of the unique environment of the research and education sector and how to avoid potential challenges of this environment, not discussed in literature.

5.7 Conclusion

Semi-structured interviews were used to collect the experiences of seven selected federations from the research and education sector. The semi-structured approach allowed the interviewer to control the direction of the interviews through five topic areas derived from literature and stakeholder input. Interviewees were encouraged to elaborate on the topic areas as they pleased, enabling the extraction of information not found in literature.

All seven interviews were recorded, with the consent of the interviewees to allow the later transcription of the interviews in detail. The transcripts will be coded and organized into meaningful families to enable in-depth analysis. The following chapter, Analysis, will analyse and extract all relevant data from the interviews. Chapter 7, Lessons, will present the final lessons learnt from implementing Federated Identity Management within the research and education sector.

Chapter 6

Analysis

The previous chapter, Interviews, describes the five topic areas upon which the interviews were based. All seven interviews were transcribed and coded as described in Chapter 2, Research Methodology.

The purpose of this chapter is to organize the bites of coded information from the interviews and to structure it in a concise and meaningful way together with literature. Each topic area is analyzed separately, to maintain the original semi-structured nature of the interviews. The chapter concludes by summarizing the main findings in list form.

6.1 Transcription and Coding

All interviewees gave consent to be recorded. The recordings were then used to transcribe each interview using ATLAS.ti 7.

An interview transcript is an academic record of an interview used as part of the analysis process. Transcripts contain a high level of detail in a written form. The benefits of transcribing the recorded interviews are twofold. Transcripts are used for presentation purposes and allow a deep interaction with the text, which is not achieved by listening to voice recordings (Ravitch & Carl, 2015).

ATLAS.ti was further used to code the interview data into groups. Coding comprised two levels: initial codes and family codes. Initial codes are used in conjunction with the transcribed interviews, for categorizing and grouping the replies of interviewees. Family codes are high-level codes that sort the initial, low-level codes into more meaningful groups.

6.2 Topic Area 1 - Initial Adoption

At the beginning of the 21st century, literature was optimistic about Federated Identity Management and predicted wide spread adoption. Industry took a conservative approach to Federated Identity Management and therefore, the adoption of Federated Identity Management did not meet the expectations of literature. A number of factors have been attributed to the low adoption of Federated Identity Management within industry. In their paper: "Federated Identity Management - We Built It; Why Won't They Come?" Jensen and Jaatun (2013) discuss the benefits of Federated Identity Management that have been offset by challenges. The theory of Rogers (1995) regarding the diffusion of innovation has been used by researchers such as Jensen (2014) and Hühnlein et al. (2010) to explain a low initial rate of adoption in different sectors of industry.

6.2.1 The Adoption Barrier

The research and education sector has been relatively more successful in implementing Federated Identity Management and has seen a higher rate of adoption compared to other parts of industry. Smith (2008) and Landau and Moore (2012) have attributed this to the trusted environment of the research and education sector. EduGAIN is proof of the success of Federated Identity Management amongst institutions of research and education. Since 2017, EduGAIN interconnects over 40 federations globally, as shown in Chapter 4, FIM in Research and Education.

However, the adoption of Federated Identity Management within the research and education sector was not simple. Rather, it has been a continuous effort spanning well over a decade.

> *"So it was a lot of work involved. It wasn't just, it's there now people will come."* (Interviewee 1)

Interviewees have confirmed that there is a barrier to the adoption of Federated Identity Management within the research and education sector, despite its apparent success.

> *"I would say our rate of adoption was also relatively slow."* (Interviewee 2)

The purpose of interviewing federations within the research and education sector is to learn how this sector has capitalized on its unique strengths and has mitigated challenges to become one of the most successful implementers of Federated Identity Management.

Although collaboration between institutions within the research and education sector is common, and therefore well suited for Federated Identity Management, many institutions have shown resistance to and little interest in joining a federation.

Eduroam, a global service allowing students and researchers to access the internet at other participating educational institutions, using the credentials of their home institution, experienced similar challenges during its adoption phase.

> *"The roll out of Eduroam [..] took many years and in part was very slow in a large part because the people that were rolling it out weren't the people visiting other campuses"* (Interviewee 7)

Despite the fact that Federated Identity Management has been used within the research and education sector at large for well over a decade, the awareness amongst the users of Federated Identity Management, as opposed to the customers of Federated Identity Management, is low. While users such as students and researchers benefit from the value of Federated Identity Management, the customers, such as the IT department, only see the added work, challenges and risks involved.

> *"In some of the more research-intensive universities, the researchers carry a lot of weight. So, I think the problem is now that they're just not aware that this is something they should be asking for, that this is a benefit, and their IT departments in some cases are not telling them."* (Interviewee 7)

From what the interviewees have said, it is clear that a significant barrier exists to the adoption of Federated Identity Management within the research and education sector. This mirrors the adoption barrier found in the rest of industry. However, to overcome these barriers may require a unique approach. The next section describes how the research and education sector has overcome the adoption barrier.

6.2.2 Overcoming the Adoption Barrier

The previous section makes it clear that there is still a barrier to the adoption of Federated Identity Management within the research and education sector. The success of a federation is dependent on how it overcomes this barrier. Federations within the research and education sector have used different approaches to address this challenge.

It is the nature of the research and education sector to be at the forefront of many ideas and technologies. Early adopters seeking to be at the forefront of new developments should be welcomed as partners and examples to other potential adopters.

> *"So I would say part of this is identifying those individuals at those campuses that get it and really reaching out to them and engaging them in terms of case studies."* (Interviewee 2)

When the federation operator identifies potential adopters and invests resources into their smooth integration into the federation, the rest of the community has an example to follow. Additionally, a number of interviewees mentioned the integration of popular services, as a means to attracting institutions. Establishing partnerships with service providers and making their service available through the federation, adds immediate value for users.

> *"there was a singular service that everyone wanted and we made the wise decision to build the federation around this service, meaning you can only get this service if you join the federation. Since this service was so popular that's what brought us strong federation membership early on."*
>
> *"So, there was awareness in parts of our community that this is the right thing to do, but you still need the carrot that makes people jump through the hoops."*(Interviewee 6)

Exclusive partnerships with service providers such as this, is a clear real world manifestation of the value of Federated Identity Management.

Approaching the correct audience is essential to creating a demand for Federated Identity Management within institutions. Often the customers are not the users of the service. This is also true within the research and

education sector. An IT department may have different motives and goals to those of the research department.

While it is important to market Federated Identity Management to the appropriate customers, it is just as important to introduce and market Federated Identity Management to the users. Communicating with the library department is a good way to reach users and to create a demand for Federated Identity Management from the inside. Once there is a demand for Federated Identity Management amongst the users, pressure will be placed on the IT department (customer) to implement Federated Identity Management.

> *"So, for me an interesting problem is how to get into those departments without talking to the IT departments without treading on too many toes, given the fact the IT departments are in fact my customer. So, I'm going to the library conference later this year for this very reason, to talk to librarians, not to talk to IT people. I need to talk to research staff for the same reason, we need to get the other parts aware."* (Interviewee 7)

Making an example out of established federation partners, creating a need by adding services of high demands to the federation and communicating the value of Federated Identity Management to the appropriate audience are some of the ways the research and education sector is overcoming the adoption barrier.

6.3 Topic Area 2 - Complexity and Understanding

Rogers (1995)'s Theory of Diffusion of Innovation presents five attributes of innovations that potential adopters perceive. Two of these attributes are relevant to this section. Firstly, complexity and secondly, observability. Smith (2008) describes the situation as follows, "While identity federation is not rocket science, there is confusion about what it delivers and the complexity involved."

Complexity

Rogers (1995) defines complexity as the degree to which an innovation is perceived as difficult to understand and use. At an institutional level, complexity is often linked with risk. As complexity increases, so does the risk increase.

> *"I think identity management in general is difficult to understand, and uh, federated identity management uhm, is even more difficult in some ways because people jump right to the risks."* (Interviewee 2)

A more accurate description would be that the risks have changed, not necessarily increased. Interviewee 2 and interviewee 4 describe why institutions may perceive an increase of risk, but also that Federated Identity Management reduces current risks, especially with collaboration at a global scale.

> *"so Id say the risk for IT for scaling all of these services and access to them is a significant, it's significant without federated access."* (Interviewee 2)

> *"So the risk might be kind of higher, but there's no economically viable alternative to doing that, because everyone's accessing so many systems today. So it would be impossible for a user to maintain a lot of accounts of different systems without the federated identity"* (Interviewee 4)

Observability

Rogers (1995) defines observability as the degree to which the results of an innovation are visible to others. Together with a lack of awareness in general, many institutions do not understand how Federated Identity Management works and how it provides value.

> *"They're massively over reacting to a perceived threat that isn't real, because they don't understand the technology."* (Interviewee 7)

The level of understanding amongst institutions is partly dependent on their motivation or attitude towards Federated Identity Management. As stated in Topic Area 1, there is a lack of motivation to research and adopt Federated Identity Management amongst institutions. This has an effect on their understanding of Federated Identity Management. Steps must be taken to educate institutions on how Federated Identity Management works, what it requires from each player, and the value of being part of a federation.

Extending an invitation to institutions to participate in the development of the Federated Identity Management system, allows them to contribute in various stages of the development cycle, to voice concerns and to adapt themselves. Even if only a handful of institutions participate in the development of the federation, those early adopters act as an example to demonstrate the value of Federated Identity Management to the institutions who have not yet joined.

> *"Uhm everybody was asked to be involved [..] Especially in the early stages where the rules were still flexible."* (Interviewee 1)

> *"People don't really understand how it can be used, what the value is until they see it in place. So you have to get a few really key visionaries demonstrating the value of it and then just communicate the uhm, in a very consistent and repeatable way those case studies to others and they will get it."* (Interviewee 2)

Interviewees 1 and 2 emphasize the importance of involving institutions who are willing to accept initial risk for the sake of innovation. When the federation is operational, the success of the early adopters can be used to convince cautious institutions of the benefit and value of Federated Identity Management by providing them with a real world example.

6.4 Topic Area 3 - Incidents

General security and privacy and the risk of breaches is an acknowledged concern in Federated Identity Management literature. Chapter 3 discusses the issue of liability and how it can lead to the failure of a federation. As far as liability is concerned, SAML 2.0 and Shibboleth have delegated responsibility and liability to the various players of the federation.

Once it is known who is responsible and liable for each step in the Federated Identity Management process, the task of addressing incidents is less complex. However, incidents, no matter how small, have to be managed and handled in an appropriate way that will ease the concerns of federation members and potential adopters.

A number of the interviewees mentioned issues that arose from small misconfigurations and from the release of attributes. However, what is the role of the federation operator with regard to solving incidents for which it is not responsible?

> *"what does the federation handle and what does it not? Do we handle just general security problems between two federation participants, is that our role? Or is our role to really kind of, and I think we kind of collectively tryna figure this out. Or is our role to really help broker?"* (Interviewee 2)

In cases where there is a problem with the infrastructure in a Hub-and-Spoke federation or errors in meta-data issued by a Full-Mesh federation, the federation operator is liable and responsible, and so their role in resolving the incident is clear. However, in many of the examples provided by the interviewees, the federation operator's role was not clear.

The interviewees mentioned how they intervened to help resolve many of these issues even if they were not at fault, or if it was not necessarily their responsibility. Most of the issues mentioned were easily solved through communication between the affected parties. The federation operator acted as the intermediary or broker of the conversation.

> *"Or is our role to really help broker? Getting the various parties in a slack channel and talking with them about how do we address this."* (Interviewee 2)

> *"It's just a matter of us joining the dots between the service provider and the identity provider, understanding what the issue was and getting it resolved."* (Interviewee 1)

From a description of the incidents, it is clear that the members of the federation see the federation operator as a central and authoritative entity.

Encouraging and facilitating friendly cooperation when solving incidents will assist with easing the concerns of member institutions.

> *"So we've been trying to foster a sort of friendly community, not a, they're doing the wrong thing let's go and attack them sort of thing."* (Interviewee 1)

Supplementing this approach with personnel that have established good relationships with the institutions will aid in the smooth and speedy termination of incidents.

> *"And we have tried to get longevity of those kind of front line staff. I mean I've been here 5 years. One of my colleagues have been here 10 years or something like that. So these are the people who are doing the support that have now gotten a good repo [reputation]. I mean weve got a decent repo with both the SP [Service Provider] and the IdP [Identity Provider] operators. So if there are issues that arise, we've hopefully kind of built that trust up, and uhm, providing, you know decent quality advice there can generally solve those kinds of issues."* (Interviewee 3)

The federation operators have found that they play an important role in the mitigation and closure of incidents throughout the federation and between member institutions. The federation operator is able to act as a third trusted party facilitating the closure of incidents. By establishing and maintaining good relationships with federation members, incidents are able to be resolved quickly and before they can develop into more persistent problems.

6.5 Topic Area 4 - Topology

The relative success of Federated Identity Management within the research and education sector has been noted in literature. However, literature does not discuss why this is so. One aspect of Federated Identity Management that literature has not addressed is the range of and differences between the physical implementation and topology of Federated Identity Management.

The interviewees, on the other hand, were very outspoken with regard to making the decision between Hub-and-Spoke and Full-Mesh topologies.

An introduction to the Hub-and-Spoke and Full-Mesh topologies from the perspective of the stakeholders of this research can be found in Chapter 3.

6.5.1 Hub-and-Spoke

Although the Hub-and-Spoke topology has a central component, it should not be confused with the centralized model of identity management mentioned in Chapter 3. The Hub-and-Spoke topology discussed here is a fully distributed model of Federated Identity Management. Each institution can act as an identity provider and as a service provider and users are authenticated by their home institution.

The Hub-and-Spoke topology centralizes a large portion of the technology needed to implement Federated Identity Management. This reduces the technical requirements on the part of the participating institutions and thus lowers the barrier to entry.

> *"So, the big advantage is that it lowers the barrier to entry. It takes a lot of the technology away from the institutions and centralizes it. Which means we can help the institutions that arent mature enough join a federation before they would be ready to do so in a Full-Mesh world."* (Interviewee 7)

> *"an ease of integration which helps really early on I would say. In getting the service providers and the identity providers together."* (Interviewee 2)

Smaller institutions with a limited IT department that is not capable of establishing and maintaining links with all the members of the federation, will benefit from the simplified single link to the central hub in a Hub-and-Spoke topology.

By reducing the technical requirements of the institutions, the technical requirements on the part of the federation operator are increased. The federation operator must be able to establish and maintain the central hub. This requires adequate manpower and capital, which can be difficult to come by in the first few years of the federation's establishment.

> *"Do they have the manpower to support Hub-and-Spoke? It's obviously much more manpower intensive because you need the fed-*

> *eration operator to broker the relationship between services and end points."* (Interviewee 5)

The federation operator accepts the bulk of the responsibility and therefore liability, in the event of an incident. Part of this responsibility and need for capital is to build for redundancy. The central nature of the Hub-and-Spoke introduces a single point of failure and so steps need to be taken to ensure the smooth and speedy transition to a back-up in the event of a loss in availability.

> *"because you can't have a single point of failure for the whole country right, so you need to build in redundancy and clustering."* (Interviewee 6)

All of these factors make the Hub-and-Spoke topology an expensive and complex option. The environment in which the federation exists must have a need for the specific benefits that a Hub-and-Spoke topology provides.

> *"So you have to look very closely at what you think you can only do in a hub, and then weigh that against the costs it will bring in operations, in complexity .."* (Interviewee 6)

The benefits of a Hub-and-Spoke topology include a reduced barrier to entry for institutions as well as a number of centralized services offered by the federation operators. These benefits come at the expense of the federation operator who must be able to maintain the central hub both in terms of manpower and of cost.

6.5.2 Full-Mesh

The Full-Mesh topology is simpler to implement for the federation operator. Each participating institution assumes the technical responsibility of making sure they are correctly configured and connected to the federation operator and federation members. The federation operator provides the meta-data to all the members. However, since data does not move through a central hub, the federation operator is not liable for any data breaches.

> *"So any SP [Service Provider] and IdP [Identity Provider] can interoperate without reference to us as the federation operator or without the federation infrastructure coming into play. We also don't have any visibility into the uhm, the individual participants, uhm configuration [..] We're very kind of, uhm, we're very hands off in that kind of sense with the full mesh."* (Interviewee 3)

Putting more responsibility on the individual members of the federation can be a significant barrier to entry for many institutions, especially smaller institutions such an independent research unit, who may not have a large and capable IT department.

> *"There's a lot to be said for full mesh federations, don't get me wrong, but I think it relies on a level of maturity and funding."* (Interviewee 7)

Furthermore, implementing upgrades and updates or effecting change across the federation is slow and difficult. Owing to the fact that each federation member is individually connected to every other member, and is responsible for its own configuration, rolling out change must be done independently by each federation member. A Hub-and-Spoke, topology for comparison, implements change onto the central hub.

> *"But I think the problem that we find is that, it's quite difficult to effect change quickly. I think it means that we can't respond particularly quickly to uhm, as a federation, to those new developments. But this is not to say that the individual participants cant move fast. But it means that the federation as a whole can't."* (Interviewee 3)

However, the independent nature of the Full-Mesh topology allows for much better scaling. It is for this reason that EduGAIN uses a Full-Mesh topology instead of a Hub-and-Spoke topology.

Interviewee 5 explained how a Full-Mesh topology allows the federation to exist through different legal environments. Each institution makes a decision as to whether it is willing to accept additional risk by interaction with an institution governed by different local or national laws. This approach

has been used to enable EduGAIN to interconnect institutions from all over the world. If the federation operator was liable for all transactions, only institutions able to meet strict requirements would be allowed to participate. In turn, this would have a negative impact on the adoption of Federated Identity Management.

> *"because there are European data protection rules, it was unclear whether interactions through that hub, we were then responsible for the final delivery for the information. If that was the case, we wouldn't be able to let a South African log into an Australian service because we could accept the credentials into the hub, but we couldn't send it to Australia because Australia doesn't have data protection regulations which are compatible with Europe. So at the moment now South Africa, SAFIRE and the Australian Access Federation, they can actually broker a deal, a trust agreement or the institutions can individually select that to be able to send information to a service."* (Interviewee 5)

A Full-Mesh topology allows institutions to direction communication with each other without having to go through a central component. This allows the entire federation to scale well. However, institutions must understand Federated Identity Management and must be financially able to establish and maintain connection with the federation. Furthermore, implementing change on a federation-wide scale is slow as each institution must comply individually.

6.5.3 Hybrid Topology

Despite the focus on Hub-and-Spoke and Full-Mesh topologies, many of the interviewees mentioned a middle ground, or a hybrid topology.

> *"Oh and also it's a spectrum. It's not an either-or kind of thing."* (Interviewee 3)

While each interviewee spoke about which side of the spectrum their federation began at, either Hub-and-Spoke or Full-Mesh, many interviewees added that their federation has begun to incorporate aspects of the other.

> *"So, the first thing that you need to understand is that every federation worldwide is becoming a Hybrid federation. All the Full-Mesh federations are introducing Hub-and-Spoke elements, and all the Hub-and-Spoke federations are becoming more Full-Mesh like."* (Interviewee 7)

The decision to start a federation with a Hub-and-Spoke or Full-Mesh topology is an important one that requires research and understanding of the local environment. However, as Federated Identity Management progresses and new breakthroughs are being made, the line between the two topologies is fading.

A federation is unlikely to remain the topology it originally began as. As the barrier to entry decreases and the maturity of the federation members increases, a Hub-and-Spoke federation may incorporate aspects of a Full-Mesh federation.

Similarly, a Full-Mesh federation may incorporate aspects of a Hub-and-Spoke topology as the federation matures and becomes more established and self-sufficient.

> "We've got a hybrid topology, so we got primarily a mesh sitting in the middle [...] Uhm, we've gone beyond that that we've attached a thing called rapid connect which is a bit of a spoke type thing for Hub-and-Spoke which sort of sits off on one side." (Interviewee 1)

> *"We call that the hybrid so that we, from the outside we look like a Mesh but on the inside, we're able to work either as a Mesh or as a Hub-and-Spoke federation."* (Interviewee 4)

Interviewee 7 summarizes the discussion of topologies as follows:

> *"So, the obvious way of looking at this is it's really which side of the equation you start on. Do you start as a Full-Mesh or do you start as a Hub-and-Spoke , knowing that ultimately everyone is becoming a Hybrid?"* (Interviewee 7)

As Federated Identity Management evolves and underlying aspects such as topology improve, the research and education sector is moving towards a mix of both Hub-and-Spoke and Full-Mesh topologies.

6.6 Topic Area 5 - Success and Failure

The previous four topic areas find their origins in Federated Identity Management literature and input from stakeholders. However, as mentioned throughout earlier parts of this research, literature is incomplete, especially concerning the research and education sector. To learn additional lessons from successful or unsuccessful ventures, interviewees were asked to discuss any additional factors that positively or negatively influenced their federations at some point.

6.6.1 Maturity and Trust

In Topic Area 3, encouraging an environment of co-operation and mutual support was shown to be beneficial to the speedy and successful handling of incidents as they arise. Similarly, an environment that treats each member institution as separate from the federation can have a negative impact on the growth of the federation. Encouraging institutions to think at the federation level will create an environment that promotes mutual growth and increased trust amongst members of the federation.

> *"Just recently we've started to notice the maturity in the thinking of the universities in the federation and how they deal with the federation [...] It's the observation that they're starting to think federation wide as opposed to just thinking enterprise wide when it comes to these things."* (Interviewee 1)

Smith (2008) states that trust is the backbone of Federated Identity Management. Even in the research and education sector, continuously developing trust amongst institutions and the federation will have positive ripple effects. Interviewee 2 recommended introducing a lightweight set of baseline practices that increase over time.

This will improve the standardization of processes throughout the federation and will reduce risk. This leads to a safer and more trusted federation environment.

> *"I would have a baseline set of practices that are very very lightweight. That everybody can adhere to and put a place and an expectation that those will raise over time."*

> *"A lot of them will have a unique identifier, but it's not persistent and they reassign it. Make sure they don't reassign it."* (Interviewee 2)

The interviewee put a clear emphasis on the fact that any baseline standardized practices should be extremely lightweight, especially in the beginning. Interviewee 5 too, emphasizes this point.

> *"We can either mandate these rules, which mean every member in every federation has to participate, and if they don't that means we have to cut the whole federation. So our minimum rules have to be quite low."* (Interviewee 5)

Introducing and enforcing baseline practices with high requirements will raise the barrier to entry and may exclude smaller institutions that cannot fulfil them. This may do more harm to the federation than good, by reducing the overall adoption.

6.6.2 Industry Standards

There are many ways in which Federated Identity Management can be implemented. Over the past decade, a select few have stood out from others. Shibboleth is an example of an implementation of Federated Identity Management that has been much more successful than any other implementation within the research and education sector, as discussed in Chapter 4. SimpleSAMLphp is an example of an alternative to Shibboleth that has been used within the research and education sector.

> *"one thing I guess we've made wrong from the start was that we went with SimpleSAMLphp and it has a lot of non-standard configuration options. So what we have learnt is, keep, use the standards of meta-data and everything else actually. And we've been kind of moving in that direction now."* (Interviewee 4)

Thanks to the standardization of many aspects of Federated Identity Management within the research and education sector, new federations have

the advantage of being able to adopt the most common standards and methods of implementations. This reduces the learning curve for federation operators as well as for federation members and increases the initial trust in the federation. Cost and risk is also reduced.

> *"Standing on the shoulders of giants basically is really easy. Now like you said the land scape has matured and we know what kind of policies we need and what we need for security and technologies."* (Interviewee 6)

New and future federations have the advantage of skipping the stage of trial and error and benefiting from the standards mapped out by the initial federations within the research and education sector.

> *"A brand new federation doesn't have that legacy baggage [...] because they come to it with fresh eyes."* (Interviewee 5)

Established standards of implementing and maintaining Federated Identity Management within the research and education sector have the potential to reduce technical and financial burdens for new federations. Neglecting the accepted standards is a decision that must be made with caution.

6.7 Concluding Remarks

The previous sections organized and discussed the information provided by the interviews. This section concludes the main points summarized from each section.

Initial Adoption

- There is a barrier to the adoption of Federated Identity Management within the research and education sector
- The customers of Federated Identity Management are often not the users
- Make users aware of the value of Federated Identity Management
- Early adopters act as an example for other potential adopters

- Making popular services available exclusively through the federation attracts potential adopters

Complexity and Understanding

- Institutions within the research and education sector perceive Federated Identity Management as complex
- The lack of understanding of Federated Identity Management contributes to perceived complexity
- There is no viable alternative to Federated Identity Management within the highly collaborative environment of the research and education sector
- The participation of potential adopters in the development and improvement of the federation has a positive effect on the awareness and understanding of Federated Identity Management

Incidents

- The federation operator has the ability to act as a trusted third party in the resolving of incidents
- Creating a friendly environment has a positive effect on the turnaround time of incidents
- Establishing and maintaining good relationships with federation members aids in resolving incidents quickly

Topology

- A Hub-and-Spoke topology lowers the barrier of entry for federation members
- A Hub-and-Spoke topology places more responsibility on the federation operator
- The technical responsibility of a Full-Mesh topology is spread more evenly throughout the federation

- The underlying federation topology is a spectrum between Hub-and-Spoke and Full-Mesh
- A federation's local environment plays a primary role in which topology best suits it

Success and Failure

- Encouraging unity amongst federation members aids in the maturity of the federation
- Baseline practices assist in developing trust within the federation

This chapter organized and discussed the practices of federations that are responsible for the relative success of Federated Identity Management within the research and education sector. Chapter 7, Lessons, compiles and discusses the final lessons learnt from implementing Federated Identity Management within the research and education sector.

Chapter 7

Lessons

The position of Federated Identity Management literature has changed from one of optimism at the adoption of Federated Identity Management to a state of concern, when it became clear that industry did not share literature's enthusiasm for Federated Identity Management. Industry has taken a conservative approach to the adoption of Federated Identity Management. As a result, literature has identified a number of factors that hinder the adoption of Federated Identity Management.

Chapter 5 describes the process of interviews that took place with established federations around the globe within the research and education sector. The aim of the interviews was to learn how similar or different the implementation of Federated Identity Management has been within this sector of industry. Chapter 6 displays an analysis of the data collected from the interviews. Together with previous literature from Chapter 3 and 4, a number of practices used within the research and education sector have been extracted. This chapter, Lessons, contains the final version of the lessons learnt from implementing Federated Identity Management within the research and education sector.

7.1 Lesson 1: Cooperation with Early Adopters

Literature has identified a barrier to the adoption of Federated Identity Management that exists throughout industry. Chapter 3 discusses a number of factors and challenges that are responsible for this barrier, such as low awareness aw well as a general lack of understanding.

This barrier to the adoption of Federated Identity Management is also present within the research and education sector.

> *"I would say our rate of adoption was also relatively slow."* (Interviewee 2)

Despite this, Federated Identity Management has been relatively successful within the research and education sector (Landau & Moore, 2012; Smith, 2008). Literature does not explain, however, how this sector has addressed the adoption barrier. Interviewee 1 made mention of the effort involved in addressing the barrier.

> *"So it was a lot of work involved. It wasn't just, it's there now people will come."* (Interviewee 1)

Interviewee 2 described their approach to increasing the awareness and general understanding of their federation.

> *"So I would say part of this is identifying those individuals at those campuses that get it and really reaching out to them and engaging them in terms of case studies."* (Interviewee 2)

Therefore, the purpose of the first lesson is to overcome the initial adoption barrier by using the example of early adopters.

> ***Lesson 1: Use the successful integration of early adopters as an example for other potential members of the federation.***

Assigning more resources to early members ensures a smooth and successful integration into the federation. Weary and more conservative potential members will look to the example of early adopters to gauge the reliability of the federation. Providing a good example for the other potential members of the federation will have a positive effect on the widespread adoption of the federation.

7.2 Lesson 2: Customers and Users

Interviewee 7 pointed out that there is a difference between customers and users of Federated Identity Management. Users of Federated Identity Management include students, researchers and library departments, etc. The IT department is often the customer on behalf of any particular institution and is responsible for implementation and maintenance.

> *"So, for me an interesting problem is how to get into those departments without talking to the IT departments."* (Interviewee 7)

Neglecting to address the users about the value of Federated Identity Management effectively invalidates half of its value. The definition of value, according to ITIL is: Value = Utility + Warranty (Rudd, Lloyd, & Hunneback, 2011). Utility is the desirability of Federated Identity Management for the user (Fewer passwords, access to more services) and warranty describes the benefit of Federated Identity Management for the customer (Increased security and privacy protection). This definition makes it clear that, in order for a potential adopter to see the value of Federated Identity Management, both customer and user must be made aware.

> *".. So, I'm going to the library conference later this year for this very reason, to talk to librarians, not to talk to IT people."* (Interviewee 7)

Therefore the purpose of this lesson is to raise awareness amongst all the beneficiaries of Federated Identity Management.

> ***Lesson 2: Propagate the value of Federated Identity Management both to potential users and to potential customers.***

Successfully demonstrating the value of Federated Identity Management to users will, in turn, place pressure on the customer to consider the adoption of Federated Identity Management seriously.

7.3 Lesson 3: User Demand

Chapter 3 discusses new security and privacy risks associated with Federated Identity Management, together with initial investment costs. Owing to perceptions of high complexity and low understanding of Federated Identity Management, some institutions may place a low priority on joining a federation.

Interviewee 6 experienced a similar barrier to adoption. Despite the recognized value of Federated Identity Management, many potential members placed a low priority on the adoption of Federated Identity Management.

> *"So, there was awareness in parts of our community that this is the right thing to do, but you still need the carrot that makes people jump through the hoops."*(Interviewee 6)

In an attempt to increase the immediate value of Federated Identity Management, a number of federations within the research and education sector have made exclusive partnerships with service providers, to offer services of high demand through the federation.

> *So we tried a number of uhm, bringing in compute and storage to researches [...], and to use those services, universities had to be part of the federation, so that also helped. So that was our sort of character if you like.* Interviewee 1

Therefore, the purpose of this lesson is to reduce further the barrier to the adoption of Federated Identity Management by creating an immediate desire to join a federation through the demand for popular services.

> ***Lesson 3: Make popular services available through the federation by means of partnerships with service providers.***

This approach adds a more simplistic argument for the adoption of Federated Identity Management, one that benefits the customer and users.

7.4 Lesson 4: Community Participation

Literature has identified complexity as a barrier to the adoption of Federated Identity Management. Smith (2008) aptly states that Federated Identity Management is not rocket science, but that there is confusion about what it delivers and the complexity involved. Interviews revealed a similar challenge within the research and education sector. Interviewee 2 agrees that potential adopters may perceive Federated Identity Management as complex.

> *"I think identity management in general is difficult to understand, and uh, federated identity management uhm, is even more difficult in some ways because people jump right to the risks."* (Interviewee 2)

Perceived complexity and a lack of awareness results in a high level of perceived risk. Both literature and the interviews revealed complexity as a challenge to the adoption of Federated Identity Management, making it an important concern for new federations.

However, Federated Identity Management was created as a solution to an ever growing problem within highly collaborative environments such as the research and education sector, namely the secure management and cost of identity management. Interviewee 4 and others point out that within the research and education sector, there is no alternative to Federated Identity Management.

> *"So the risk might be kind of higher but there's no economically viable alternative to doing that, because everyone's accessing so many systems today. So it would be impossible for a user to maintain a lot of accounts of different systems without the federated identity"* (Interviewee 4)

Therefore, the purpose of this lesson is to reduce the perceived risk and complexity of Federated Identity Management.

> ***Lesson 4: Involve potential adopters in the development and improvement of the federation.***

By including potential adopters in the development of the federation, institutions become a part of the development process and have the opportunity to influence the federation. This involvement reduces perceived complexity as well as increasing awareness of the federation.

7.5 Lesson 5: Problem Solving

Liability is the state of being legally obliged or responsible (Jensen, 2012). Landau and Moore (2012) list liability as a major point of contention between members of a federation. A number of interviewees addressed the topic of resolving incidents between identity providers and service providers.

The research and education sector has opted for a peaceful approach to resolving incidents.

> *"It's just a matter of us joining the dots between the service provider and the identity provider, understanding what the issue was and getting it resolved."* (Interviewee 1)

By intervening as a third party and facilitating co-operative discussions and resolutions to incidents, a number of the interviewees have mentioned how they managed to solve problems simply and quickly. Interviewee 5 suggests maintaining longevity of the front-line help desk staff, in an attempt to create a friendly relationship between the help desk and federation members.

Therefore, the purpose of this lesson to is reduce the impact of incidents on the relationship between the federation and its members.

> ***Lesson 5: Facilitate and broker a co-operative and problem solving environment***

The correct environment will give members the peace of mind and confidence to approach the federation operator to help resolve incidents as they occur.

7.6 Lesson 6: Federation Topology

There is a gap within literature with regard to the underlying topology of a federation, especially within the research and education sector. However,

talks with stakeholders have revealed the importance and potential impact that the network topology has on the federation and its local environment.

The two most common federation topologies used within the research and education sector are Hub-and-Spoke and Full-Mesh. However, interviewees have described it in reality, as existing on a spectrum.

> *"Oh and also it's a spectrum. It's not an either-or kind of thing."* (Interviewee 3)

The benefits of each side of the spectrum are discussed in Chapter 6. From the discussion, it is clear that the benefits of each topology, favour particular environments over others. The Hub-and-Spoke topology lowers the technical and monitory barrier to entry for federation members while the Full-Mesh federation simplifies the initial set up of the federation and places more responsibility on the federation members.

Therefore, the purpose of this lesson is to emphasise the potential impact the underlying network topology can have on the adoption and success of a federation, depending on its unique local environment.

> ***Lesson 6: When making topology decisions, the state of the local environment and community must be a primary consideration.***

Interviews have also revealed that the future of federation topologies is a hybrid between Full-Mesh and Hub-and-Spoke.

> *"So, the obvious way of looking at this is it's really which side of the equation you start on [...] knowing that ultimately everyone is becoming a Hybrid?"* (Interviewee 7)

Although the underlying topologies of Federated Identity Management are moving to a common hybrid, the decision of which side of the spectrum to start at is still a primary consideration to insuring the successful adoption of a federation.

7.7 Lesson 7: Baseline Practices

Interviewee 1 spoke of the benefits of a federation community that has matured and incorporates a collective view rather than a isolated, self-serving one.

> *Just recently we've started to notice the maturity in the thinking of the universities in the federation and how they deal with the federation [...] It's the observation that they're starting to think federation wide as opposed to just thinking enterprise wide when it comes to these things.* (Interviewee 1)

As a federation matures, initial challenges are solved and new opportunities arise. Interviewee 1 mentions the collective thinking of the community, which is only possible if there is a strong underlying fabric of trust. Although literature praises the research and education sector for its environment of trust, in order for the federation to mature, so too must the trust between the federation and federation members increase.

Interviewee 2 has suggested the introduction of lightweight baseline practises to standardize the collective growth and maturity of all federation members, new and old.

> *"I would have a baseline set of practises, that are very very light weight. That everybody can adhere to and put a place and an expectation that those will raise over time."* (Interviewee 2)

Therefore the purpose of this lesson is to standardize the baseline practises of the federation members with the aim of increasing trust between institutions and facilitating the progressive maturity of the federation.

> ***Lesson 7: Introduce baseline practises that scale with the maturity of the federation***

As emphasised by interviewee 2, the initial baseline practises must be very lightweight with the goal of progressively increasing them as the federation members mature. Interviewee 5 warns that enforcing practises that are too high will effectively restrict the size of the federation, increase the barrier to entry and negatively affect the adoption of the federation.

7.8 Lesson 8: Industry standards

There are a number of ways to implement Federated Identity Management throughout industry. Each implementation has unique benefits and challenges associated with it. Chapter 4 has discussed the state of Federated Identity Management within the research and education sector, with emphasis on Shibboleth. As the dominant standard of implementing Federated Identity Management, Shibboleth is well supported and well understood throughout this part of industry.

Implementing Federated Identity Management using alternative software reduces the amount of community support usually available. Interviewee 4 describes the experience their federation has had with alternative methods of implementing Federated Identity Management.

> *"one thing I guess we've made wrong from the start was that we went with simple saml php and it has a lot of non-standard configuration options. So what we have learnt is, keep, use the standards of meta-data and everything else actually."* (Interviewee 4)

Therefore the purpose of this lesson is to encourage the use of industry standards and to avoid potential challenges that accompany alternative implementations.

> ***Lesson 8: Follow standardized practises of the research and education sector.***

Following the established practises of the research and education sector increases the understanding of Federated Identity Management by both the federation operators and federation clients. Similarly, the barrier of adoption is lower as a result of the familiar technical and non-technical processes that must take place.

Chapter 8

Conclusion

The previous chapter revealed eight lessons learnt from implementing Federated Identity Management within the research and education sector. These lessons are the main contribution of this research study.

This chapter will revisit the objectives and problem statement defined at the beginning of this study and summarize the progress made throughout the research process. The contribution of this research study together with the limitations and recommendations for future studies are also discussed. The chapter ends off with an epilogue.

8.1 Revisiting the Objectives and Research Layout

The primary objective of this research was to identity lessons learnt from implementing Federated Identity Management within the research and education sector. To complete this objective, five sub-objectives were fulfilled. The layout of this study was designed to address and complete these objectives. The layout of the study was discussed in Chapter 2 and is repeated here for convenience in Figure 8.1.

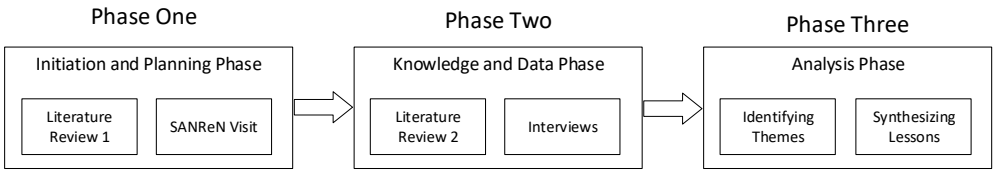

Figure 8.1: Research Layout

Phase One

Phase one was the initiation and planning phase. This phase and its two sub components were covered in Chapter 3. This chapter introduced and discussed Federated Identity Management from the perspective of literature. The focus was on Federated Identity Management within industry, of which the research and education sector forms part of. Input from stakeholders was also included in Chapter 3. The majority of stakeholder input came in the form of direction, drawing attention to more relevant parts of Federated Identity Management. Additionally, stakeholders provided input where literature could not, which can be primarily seen in section 3.2.3, Architecture. A focus of Chapter 3 was the identification and discussion of the benefits and challenges of Federated Identity Management throughout industry.

Altogether, phase one fulfilled the following sub-objectives:

- Discuss the state of Federated Identity Management within industry
- Identify and discuss the benefits and challenges of Federated Identity Management

Phase Two

Phase two of the research was the knowledge and data phase. This phase has two sub-components, a literature review and interviews.

Chapter 4 contains the extended literature review. This literature review focused on the research and education sector specifically. It is included in the knowledge and data phase as it forms part of gathering data about the research and education sector from literature and stakeholders as well as setting the scene for the interviews to come.

Chapter 5 discussed the structure and format of the interviews. The bulk of the chapter discussed and validated the five topic areas on which all interviews were based. The purpose of the interviews was to learn from the real-world experiences of federations within the research and education sector and to identify factors that influence the adoption and growth of Federated Identity Management within this sector.

Together, Chapter 4 and 5 fulfilled phase two of this study and the following sub-objectives:

- Determine the current state of Federated Identity Management within the research and education sector
- Collect the experiences of implementing Federated Identity Management throughout the global research and education sector

Together, phase one and phase two fulfil all four of the sub-objectives defined in Chapter 1, Introduction.

Phase Three

Phase three is the final phase of the research and includes the analysis and final output of the study. This phase has two sub-components, the identification of themes and the synthesis of the final lessons.

Chapter 6 covers the primary analysis of the interviews. Literature and stakeholder input from previous chapters were used to order and understand the feedback from the interviewees. The output of the analysis produced a number of concluding remarks found in section 6.7. These remarks summarize the output of the second phase of the research, knowledge and data phase.

Chapter 7 synthesized the final output of this study, lessons learnt from implementing Federated Identity Management within the research and education sector. The concluding remarks from Chapter 6 and literature from Chapter 3 and 4 were used to identify, validate and discuss the final lessons.

Together, Chapter 6 and Chapter 7 use the output of the four sub-objectives with the addition of argumentation to fulfil the primary objective of the study, to identify lessons learnt from the implementation of Federated Identity Management within the research and education sector.

Chapter 7 presents the eight lessons learnt from implementing Federated Identity Management within the research and education sector.

8.2 Addressing the Problem Statement

Literature has extensively covered various aspects, benefits and challenges of Federated Identity Management throughout industry. The research and education sector has been praised for implementing Federated Identity Management relatively successfully compared to the situation in the majority of industry. However, Federated Identity Management literature has not covered the reasons for this relative success. Literature has not examined the unique challenges of implementing Federated Identity Management within this sector, nor has literature documented the practises of the research and education sector in this regard.

> ***There is little insight into the challenges of implementing Federated Identity Management within the research and education sector. Similarly, there is also little insight into the solutions deployed to overcome the aforementioned challenges.***

The research layout shown in the previous section was designed to address the primary research objective and hence, this research problem. By consulting literature and stakeholders together with interviewing federations within the research and education sector globally, this research produced eight lessons learnt from implementing Federated Identity Management within the research and education sector.

These eight lessons provide increased insight into the challenges of implementing Federated Identity Management within the research and education sector as well as the solutions deployed to overcome those challenges.

8.3 Summary of Contributions

This research study has addressed a problem present in literature and experienced by stakeholders. The primary contribution of this research study is eight lessons learnt from implementing Federated Identity Management

within the research and education sector. These lessons provide increased visibility into the challenges of implementing Federated Identity Management within the research and education sector as well as the solutions deployed to overcome them.

Lesson 1: Cooperation with Early Adopters

Use the successful integration of early adopters as an example for other potential members of the federation.

The purpose of the first lesson is to overcome the initial adoption barrier by using the success of early adopters as an example for other potential adopters.

Lesson 2: Customers and Users

Propagate the value of Federated Identity Management both to potential users and to potential customers.

The purpose of the second lesson is to increase the awareness of Federated Identity Management amongst both customers and users, thereby exposing potential federation members to the full value of Federated Identity Management.

Lesson 3: User Demand

Make popular services available through the federation by means of partnerships with service providers.

The purpose of the third lesson is to reduce further the barriers to the adoption of Federated Identity Management by creating an immediate desire to join a federation through the demand for popular services.

Lesson 4: Community Participation

Involve potential adopters in the development and improvement of the federation.

The purpose of the fourth lesson is to reduce potential adopter's perceived complexity and risk of joining a federation by integrating them in the development and improvement of the federation.

Lesson 5: Problem Solving

Facilitate and broker a co-operative and problem solving environment

The purpose of the fifth lesson to is reduce the impact that incidents have on the success of the federation and the relationship between the federation and its members.

Lesson 6: Federation Topology

When making topology decisions, the state of the local environment and community must be a primary consideration.

The purpose of the sixth lesson is to emphasise the potential impact that underlying network topology can have on the adoption and success of a federation, depending on its unique local environment.

Lesson 7: Baseline Practices

Introduce baseline practises that scale with the maturity of the federation

The purpose of the seventh lesson is to standardize the baseline practises of the federation members with the aim of increasing trust between institutions and facilitating the progressive maturity of the federation.

Lesson 8: Industry standards

Follow standardized practises of the research and education sector.

The purpose of the eighth lesson is to encourage the use of industry standards and avoid potential challenges that accompany alternative implementations.

8.4 Limitations and Future Research

Every notable researcher understands that there are limitations to their research that may have had an effect on the process or outcome of their research. Similarly, one should realize that the word 'Research' is also a verb.

Research is a continuous process that takes into consideration and changes with new discoveries and progress.

8.4.1 Limitations

Interviews were chosen as the primary method of data collection for this research study. The interviews were based on literature and stakeholder input as described in Chapter 2 and 5. However, literature and stakeholder input can only provide a certain level of guidance. To gain additional, detailed insight into the challenges and accompanying solutions of implementing Federated Identity Management within the research and education sector, more data is required at the outset. Preliminary interviews or case studies would have provided valuable direction for the construction of primary interviews. Time, resource and limited research experience prevented this course of action from being taken.

In total, seven federations were interviewed. However, not all seven interviewees were equally quoted throughout the writing up of this research study. While all interviewees played a part in the researcher's interpretation of the research output, owing to limitations in communication during the interview and transcription processes, some interviewees were referenced more often than others. Communication issues include language barriers which had an effect on the understanding and interpretation of interview questions and replies. Additional limitations in the communication between the interviewer and interviewees arose as a result of spontaneous changes in the quality of the internet connection, on both ends. Ultimately, this resulted in minor gaps in the transcription of the interviews. While the impact of this on the understanding of the researcher was negligible, incomplete sentences could not be quoted in the writing up of this research.

8.4.2 Future Research

Moving on from this research study, to further increase insight into the challenges of implementing Federated Identity Management within the research and education sector as well as the solutions deployed to overcome them, different research methods can be used.

With a focus on interviews as a qualitative method of research, this re-

search made use of a semi-structured approach. Chapter 2 describes interviews as existing a spectrum between structured and unstructured approaches.

Moving on from this research study, future research can gain detailed insight into how federations within the research and education sector have implemented or made use of the eight lessons provided, by means of more structured interviews. Structured interviews allow for the direct comparison of interviewees and a narrowed focus on specific questions.

On the other side of the spectrum, unstructured interviews provide the setting to learning and discussing a number of new practises used by federations throughout the research and education sector. By using this research together with other research in the field, and with the help of case studies, well planned and constructed interviews can reveal the practises of this sector in greater detail.

The federation operators were the subjects of this study. However, as stated in Chapter 2, federation operators entail only one of four actors in Federated Identity Management. Users and the federation members (identity and service providers) have an important role to play in the success of any federation.

Future research focusing on the perspectives of established federation members as opposed to new federation members, could reveal the similarities or differences between reasons for the adoption of and the concerns regarding the adoption of Federated Identity Management.

Comparing the perspectives of federation members and federation operators will also reveal points of interest and points of weakness. Identifying and addressing these points will increase the trust within the federation.

This study has shown that the users of Federated Identity Management have a role to play in the adoption rate of a federation. Research focusing on the awareness of Federated Identity Management users and its value together with the expectations and concerns of users will aid federation members and operators in the diffusion of Federated Identity Management to users.

8.5 Epilogue

This research study began with the intention of helping new federations within the research and education sector to establish themselves by following the success and learning from the failure of other federations in this sector. The result is eight lessons learnt from implementing Federated Identity Management within the research and education sector. Each lesson, derived from literature, stakeholders and interviews, provide insight into the success and failure of the research and education sector.

References

Ahn, G.-J., & Lam, J. (2005). Managing Privacy Preferences for Federated Identity Management. In *Proceedings of the 2005 Workshop on Digital Identity Management - DIM '05* (pp. 28–36). ACM. doi: 10.1145/1102486.1102492

Arias-Cabarcos, P., Almenarez-Mendoza, F., Marin-Lopez, A., & Diaz-Sanchez, D. (2009). Enabling SAML for Dynamic Identity Federation Management. In *Wireless and Mobile Networking* (Vol. 308, pp. 173–184). Springer. doi: 10.1007/978-3-642-03841-9

Baldwin, A., Casassa Mont, M., Beres, Y., & Shiu, S. (2010). Assurance for Federated Identity Management. *Journal of Computer Security*, *18*(4), 541–572. doi: 10.3233/JCS-2009-0380

Bhargav-Spantzel, A., Squicciarini, A. C., & Bertino, E. (2006). Establishing and Protecting Digital Identity in Federation Systems. *Journal of Computer Security*, *14*(3), 269–300. doi: 10.1145/1102486.1102489

Bhatti, R., Bertino, E., & Ghafoor, A. (2007, feb). An Integrated Approach to Federated Identity and Privilege Management in Open Systems. *Communications of the ACM - Spam and the Ongoing Battle for the Inbox*, *50*(2), 81–87.

Birrell, E., & Schneider, F. B. (2013). Federated Identity Management Systems: A Privacy-Based Characterization. *IEEE Security and Privacy*, *11*(5), 36–48. doi: 10.1109/MSP.2013.114

Broeder, D., Jones, B., Kelsey, D., Kershaw, P., Luders, S., Lyall, A., ... Weyer, H. J. (2013). Federated Identity Management for Research Collaborations. (August). Retrieved from `http://cds.cern.ch/record/1442597`

Brown, I., Hoppe, R., Mugera, P., Newman, P., & Stander, A. (2004). The Impact of National Environment on the Adoption of Internet Banking: Comparing Singapore and South Africa. *Journal of Global Information Management*, *12*(2), 1–26. doi: 10.4018/978-1-59140-468-2.ch014

Catuogno, L., & Galdi, C. (2014). Achieving Interoperability Between Federated Identity Management Systems: A Case of Study. *Journal of High Speed Networks*, *20*(4), 209–221. doi: 10.3233/JHS-140499

Chadwick, D. W. (2009). Federated Identity Management. In *Foundations*

of Security Analysis and Design V (FOSAD 2007/2008/2009 Tutorial Lectures) (Vol. 5705, pp. 96–120). Springer. doi: 10.1007/978-3-642-03829-7_3

De Clercq, J. (2002). Single Sign-On Architectures. In G. Davida, Y. Frankel, & O. Rees (Eds.), *Infrastructure Security: International Conference, InfraSec 2002 Bristol, UK, October 1–3, 2002 Proceedings* (Vol. 2437, pp. 40–58). Springer. doi: 10.1007/3-540-45831-X_4

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage Handbook of Qualitative Research*. Thousand Oaks : Sage.

Dhamija, R., & Dusseault, L. (2008). The Seven Flaws of Identity Management. *IEEE Security and Privacy*, *6*(2), 24 – 29. doi: 10.1109/MSP.2008.49

Ferdous, M. S., & Poet, R. (2013). Dynamic Identity Federation Using Security Assertion Markup Language (SAML). In S. Fischer-Hubner, E. de Leeuw, & C. Mitchell (Eds.), *Policies and Research in Identity Management: Third IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013. Proceedings* (pp. 131–146). Springer Berlin Heidelberg. doi: 10.1007/978-3-642-37282-7_13

Gefen, D., Rose, G. M., Warkentin, M., & Pavlou, P. a. (2005). Cultural Diversity and Trust in IT Adoption: A Comparison of Potential e-Voters in the USA and South Africa. *Journal of Global Information Management*, *13*(1), 54–78. doi: 10.4018/jgim.2005010103

Gross, T. (2003, dec). Security Analysis of the SAML Single Sign-on Browser / Artifact Profile. In *19th Annual Computer Security Applications Conference, 2003. Proceedings.* (pp. 298–307). doi: 10.1109/CSAC.2003.1254334

Han, J., Mu, Y., Susilo, W., & Yan, J. (2010). A Generic Construction of Dynamic Single Sign-On with Strong Security. In *Security and Privacy in Communication Networks* (pp. 181–198). doi: 10.1007/978-3-642-16161-2_11

Horbe, R., & Hotzendorfer, W. (2015). Privacy by Design in Federated Identity Management. *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 167–174. doi: 10.1109/SPW.2015.24

Hove, S. E., & Anda, B. (2005). Experiences from Conducting Semi-Structured Interviews in Empirical Software Engineering Research.

International Software Metrics Symposium(Metrics), 203–212. doi: 10.1109/METRICS.2005.24

Hughes, J., Maler, E., Microsystems, S., & Lockhart, H. (2005). SAML v2.0 Technical Overview. *Language*(September), 1–51. Retrieved from `http://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf`

Hühnlein, D., Roßnagel, H., & Zibuschka, J. (2010). Diffusion of Federated Identity Management. In *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)* (Vol. P-170, pp. 25–36). Retrieved from `http://www.scopus.com/inward/record.url?eid=2-s2.0-84874258383{\&}partnerID=tZOtx3y1`

Jensen, J. (2011). Benefits of federated identity management - A survey from an integrated operations viewpoint. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6908 LNCS*, 1–12. doi: 10.1007/978-3-642-23300-5_1

Jensen, J. (2012). Federated Identity Management Challenges. *2012 Seventh International Conference on Availability, Reliability and Security*, 230–235. doi: 10.1109/ARES.2012.68

Jensen, J. (2013). Identity Management Lifecycle - Exemplifying the Need for Holistic Identity Assurance Frameworks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7804 LNCS*, 343–352. doi: 10.1007/978-3-642-36818-9_38

Jensen, J. (2014). *Jostein Jensen Federated Identity Management in the Norwegian Oil and Gas Industry* (Unpublished doctoral dissertation).

Jensen, J., & Jaatun, M. G. (2013). Federated Identity Management-We Built It; Why Won't They Come? *IEEE Security and Privacy*, *11*(2), 34–41. doi: 10.1109/MSP.2012.135

Jensen, J., & Nyre, A. A. (2013). Federated Identity Management and Usage Control - Obstacles to Industry Adoption. *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, 31–41. doi: 10.1109/ARES.2013.10

Josang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S. (2005). Trust requirements in Identity Management. *Conferences in Research and Practice*

in Information Technology Series, *44*, 99–108.

Josang, A., & Pope, S. (2005, may). User Centric Identity Management. In *AusCERT Asia Pacific Information Technology Security Conference* (p. 77). doi: 10.1109/MSP.2007.99

Khattak, Z. A., Sulaiman, S., & Manan, J. L. A. (2010). A Study on Threat Model for Federated Identities in Federated Identity Management System. In *2010 International Symposium on Information Technology* (Vol. 2, pp. 618–623). Kuala Lumpur: IEEE. doi: 10.1109/ITSIM.2010.5561611

Kylau, U., Thomas, I., Menzel, M., & Meinel, C. (2009). Trust Requirements in Identity Federation Topologies. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 137–145. doi: 10.1109/AINA.2009.80

Landau, S., Gong, H. L. V., & Wilton, R. (2009). Achieving Privacy in a Federated Identity Management System. In *Financial Cryptography and Data Security 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers* (pp. 51–70).

Landau, S., & Moore, T. (2012). Economic Tussles in Federated Identity Management. *First Monday*, *17*(10), 1–29. doi: 10.1016/j.physletb.2008.11.040

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2978–2987. doi: 10.1109/HICSS.2013.192

Maler, E., & Reed, D. (2008). The Venn of identity. *IEEE Security and Privacy*, *6*(2), 16 – 23. doi: 10.1109/MSP.2008.50

Malik, A. A., Anwar, H., & Shibli, M. A. (2016). Federated Identity Management (FIM): Challenges and Opportunities. *Proceedings - 2015 Conference on Information Assurance and Cyber Security, CIACS 2015*(1), 75–82. doi: 10.1109/CIACS.2015.7395570

Mcknight, D. H., & Chervany, N. L. (1996). *The Meanings of Trust* (Tech. Rep.). University of Minnesota. doi: 10.1117/12.304574

Morgan, R. L. B., Cantor, S., Carmody, S., Hoehn, W., & Klingenstein, K. (2004). Federated Security: The Shibboleth Approach. *EDUCAUSE Quarterly*, *27*(4), 12–17. Re-

trieved from https://pdfs.semanticscholar.org/c1cf/205c99d2b92ff63a0a83497869592a43012d.pdf

Pashalidis, A., & Mitchell, C. J. (2003). A Taxonomy of Single Sign-On Systems. In R. Safavi-Naini & J. Seberry (Eds.), *Information Security and Privacy 8th Australasian Conference, ACISP 2003 Wollongong, Australia, July 911, 2003 Proceedings* (Vol. 2727, pp. 249–264). doi: 10.1007/3-540-45067-X_22

Qu, S. Q., & Dumay, J. (2011). The Qualitative Research Interview. *Qualitative Research in Accounting & Management*, *8*(3), 238–264. doi: 10.1108/11766091111162070

Ravitch, S. M., & Carl, N. M. (2015). *Qualitative Research: Bridging the Conceptual, Theoretical, and Methodological*. SAGE Publications.

Ritchie, J., & Lewis, J. (Eds.). (2003). *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. SAGE Publications.

Rogers, E. M. (1995). *Diffusion of Innovations* (Third Edit ed.). New York: The Free Press.

Rubin, H. J., & Rubin, I. S. (2011). *Qualitative Interviewing: The Art of Hearing Data* (second ed.). SAGE Publications.

Rudd, C., Lloyd, V., & Hunneback, L. (2011). *ITIL Service Design*. TSO.

SAFIRE. (2017). *SAFIRE joins eduGAIN*. Retrieved 2017-08-20, from https://safire.ac.za/safire/news/safire-joins-edugain-20170220/

Satchell, C., Shanks, G., Howard, S., & Murphy, J. (2011). Identity Crisis: User Perspectives on Multiplicity and Control in Federated Identity Management. *Behaviour Information Technology*, *30*(1), 51–62. doi: 10.1080/01449290801987292

Scott, C., Wynne, D., & Boonthum-denecke, C. (2016). Examining the Privacy of Login Credentials Using Web-Based Single Sign-On: Are We Giving up Security and Privacy for Convenience? In *Cybersecurity Symposium (CYBERSEC)* (pp. 75–80). IEEE. doi: 10.1109/CYBERSEC.2016.19

Scudder, J., & Jøsang, A. (2010). Personal Federation Control with the Identity Dashboard. *IFIP Advances in Information and Communication Technology*, *343 AICT*, 85–99. doi: 10.1007/978-3-642-17303-5_7

Shin, D., Ahn, G.-J., & Shenoy, P. (2004). Ensuring Information Assurance in Federated Identity Management. *IEEE International Conference on Performance, Computing, and Communications, 2004*, 821–826. doi: 10.1109/PCCC.2004.1395193

Silverman, D. (2013). *Doing Qualitative Research: A Practical Handbook*. SAGE Publications.

Smedinghoff, T. J. (2012). Solving the Legal Challenges of Trustworthy Online Identity. *Computer Law and Security Review*, *28*(5), 532–541. doi: 10.1016/j.clsr.2012.07.001

Smith, D. (2008). The Challenge of Federated Identity Management. *Network Security*(4), 7–9. doi: 10.1016/S1353-4858(08)70051-5

Struwig, F. W., & Stead, G. B. (2001). *Planning, Designing and Reporting Research* (V. Nattrass, Ed.). Cape Town: Pearson Education South Africa.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), 13–23. doi: 10.1.1.104.6570

Appendix A

Transcription and Coding

Transcription and coding is first introduced in Chapter 2, Research Methodology and then again later in Chapter 5, Interviews. The benefits of transcription is also presented in earlier chapters and it is clear that to have a deep link with the interview data, transcribing of the recorded interviews was necessary. Coding was the next logical step after transcribing the recorded interviews. Coding of the interview data is the processes of grouping segments of the data into logical groups. Atlas.ti 7 was used to transcribe and code the recorded interviews.

The process of transcribing the recorded interviews began as soon as the first interview was completed, and continued in parallel with the rest of the interviews. Using Atlas.ti 7, a recording was placed next to a transcription sheet and transcribed at most, one sentence at a time. In situations where the interviewee's speech was not properly audible, I logically filled in the missing words according to memory and context. However, in situations where the meaning and context of what was being said was lost, a note was made in the transcription. Throughout the entire process of transcription, time stamps were places at regular intervals and after points of interest, for easy reference.

After the completion of the transcription, the process of coding began. Instead of using pre-determined codes, I created codes as needed, building the list of codes seen in Figure A.1 after the final transcript was coded. Thereafter, I analysed each transcript a second time with the complete list of codes available. With the transcripts broken up and coded into the initial groups, the second, more general process of grouping the codes into family

codes took place. Family codes reduces the number of organizational groups to be analysed and assist in prioritising more important codes from less important codes. The list of Family codes produces is shown here again in Figure A.2 for convenience.

The family codes were then used in conjunction with literature to derive eight lessons learnt from implementing Federated Identity Management within the research and education sector, contained in Chapter 7.

Name	Grounded	Created	Modified
Enforcing rules	2	04/12/20...	04/12/20...
Federated Incident Response Plan	1	04/12/20...	04/12/20...
General Security	2	05/01/20...	05/01/20...
Cost savings	2	04/11/20...	05/15/20...
Customer vs User	3	05/01/20...	05/15/20...
Encryption	1	04/10/20...	05/15/20...
IdP and SP test	1	04/10/20...	05/15/20...
IdP software upgrade	1	04/10/20...	04/10/20...
Import EduGAIN meta data	4	04/10/20...	05/12/20...
Guidelines/practises	1	04/11/20...	04/11/20...
Hub and Spoke	14	04/11/20...	05/15/20...
Hub vs Mesh	3	05/01/20...	05/12/20...
Attribute release	2	04/10/20...	04/11/20...
Baseline set of practises	4	04/12/20...	05/01/20...
Benefit of adopting Identity Federation today	1	05/01/20...	05/01/20...
Adoption Strategy	4	04/11/20...	05/01/20...
Affecting Change in the federation	2	04/10/20...	05/01/20...
Association to NREN	2	04/10/20...	05/01/20...
Conflict intervension	2	04/10/20...	04/11/20...
Conflict resolution	5	04/10/20...	05/15/20...
Corporate SPs	2	04/11/20...	05/12/20...
Central Discovery Service	1	04/10/20...	05/12/20...
Communicating Identity federation	3	05/01/20...	05/01/20...
Community effort	4	04/11/20...	05/01/20...
Scalability	1	04/10/20...	04/10/20...
Shibboleth	1	04/10/20...	04/11/20...
South African institution maturity	1	05/01/20...	05/01/20...
Risk is the lowest Risk option when collaborating glo...	2	04/11/20...	05/15/20...
SAML	2	04/10/20...	04/10/20...
SAML security	1	04/10/20...	04/10/20...
Use Identity Federation for internal (unsafe) services	1	05/01/20...	05/01/20...
Value proposition	7	04/11/20...	05/15/20...
Weakness of identity federation	4	05/01/20...	05/15/20...
Trust	1	04/11/20...	04/11/20...
Trust establishment	3	04/12/20...	05/15/20...
Unique success and hardships	2	04/10/20...	05/15/20...
Legal agreements	7	04/11/20...	05/12/20...
Maturity	1	05/01/20...	05/01/20...
Mesh Federation	5	04/10/20...	05/15/20...
Initial adoption	3	04/11/20...	05/12/20...
Interested in results	1	04/11/20...	04/11/20...
Lack of functional IdM	2	05/01/20...	05/01/20...
phasing out full mesh	1	05/01/20...	05/01/20...
Privacy	6	04/10/20...	05/12/20...
Risk	4	04/11/20...	05/15/20...
Multi factor authentication	2	04/12/20...	05/15/20...
Mush/Hub Hybrid	6	04/11/20...	05/15/20...
Persistant unique identifier	1	04/12/20...	04/12/20...

Figure A.1: Atlas.ti Codes

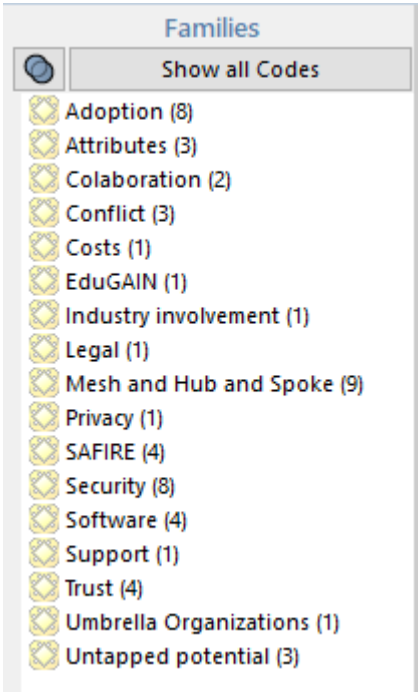

Figure A.2: Atlas.ti Families