Security Using Digital Identification Methods for Use within "Federated, Secure Trust Networks for Distributed Healthcare IT Services"

A Thesis
In TCC 402

Presented to

The Faculty of the
School of Engineering and Applied Science
University of Virginia

In Partial Fulfillment

Of the Requirements for the Degree

Bachelor of Science in **Computer Science**

By

Vincent Noël

March 23rd, 2004

On my honor as a University student, on this assignment I have neither given nor received unauthorized aid as defined by the Honor Guidelines for Papers in TCC Courses.

Signed _____

Approved _____ Date _____
Technical Advisor – Alfred Weaver

Approved _____ Date _____
TCC Advisor – Patricia Click

PREFACE

I would like most importantly to thank Professor Weaver for his help and guidance throughout every stage of this piece. Also, my TCC advisor, Professor Click, for her repeated guidance and suggestions. The members of my research group: Jim, Andrew, Chen and James all played important roles getting this project to where it is today.

TABLE OF CONTENTS

GLOSSARY

Authentication: The process by which a computer system attempts to verify the identity of second party user or computer. (Wikipedia)

Authorization: The process in which a computer system decides if a particular user has permission to access a certain resource. (Wikipedia)

Biometric Identification: The class of identification methods that rely on physical or biological features in order to authenticate a user (e.g. fingerprint scanner or handwriting recognition)

Digital Identification: The class of identification methods that rely of the storage and processing (usually encryption) of digital data in order to authenticate a user (e.g. smartcard)

eToken: A digital identification device produced by Aladdin Knowledge Systems. The eToken is a USB electronic token.

False Rejection Rate (FRR): The FRR of a particular identification technology is rate at which users that should be authenticated are rejected.

Federation: The sharing of trust among disparate networks, usually when an explicit trust relationship has not been specified between the two parties.

HIPAA: The Health Insurance Portability and Accountability act is a piece of legislation first introduced in 1996 which, among other acts, mandates that medical data be stored and transmitted in a secure manner.

SDK: A Software Development Kit is a software bundle provided by a vendor which allows their product to be used by other developers.

Token: In the context of this paper, a token is a device which allows for authentication within computer systems.

Web Services: Web services are the result of a series of protocols and standards which allow for the sharing of program functionality over a network (usually, the Internet). (Wikipedia)

ABSTRACT

Recent federal regulation mandates strict new standards for medical data privacy, which is a topic that is so important in the rapidly modernizing medical sector. This is the motivating factor that prompted Professor Alfred Weaver to initiate a project entitled Federated, Secure Trust Networks for Distributed Healthcare IT Services.

My research focused on the identification techniques that our architecture uses to authenticate users. I studied the digital class of these techniques, doing a broad review of the field and narrowing the choices to those best suited to the medical context. Finally, I implemented the technique most suitable for our needs as a web service.

During my initial research, five promising techniques emerged: Key fobs, USB electronic tokens, traditional keys, smart cards and RFID wristbands. By assessing these technologies using criteria such as cost, usability and security, I was able to choose one technology for implementation: a USB electronic token. The token, produced by Aladdin Knowledge Systems as the eToken, was strong in all areas of assessment, especially cost, practicality, security and availability.

In order to integrate the eToken into our system, I followed a series of steps that led to the creation of a wrapper interface to communicate with the token, a client to allow the user to interact with the wrapper and a web service with could accept data from the wrapper and issue authentication decisions based on this information.

This project made important contributions on two levels. The first contribution is the tool I have created, which allows a new authentication technique to be used within a web services architecture. More importantly, the roadmap I have laid out will allow new other identification techniques to be similarly implemented.

1 INTRODUCTION

1.1 Purpose Statement

This paper will present research performed with the aim of enabling certain digital identification techniques for a web services architecture. This work was done as a component of a larger research project, led by Professor Alfred Weaver of the Computer Science department, working toward securing and distributing healthcare data through web services.

1.2 Problem Statement

This research project is motivated by a fundamental concern for the safeguarding of patient data in all medical dealings. As might be expected in a fast moving, rapidly modernizing field, medicine has not perfectly anticipated its need for data security. In reaction, recent federal leislation requires new systems to ensure the correct handling of patient information (e.g. HIPAA, the Health Insurance Portability and Accountability Act).

HIPAA, first introduced in 1996 and later revised in 2002, mandates that all "individually identifiable health information" (Summary of the HIPAA, 2003) be subject to "stringent privacy regulations" regarding its disclosure, usage and transfer (Weaver et al., 2003). HIPAA places careful limits a patient's rights to see his or her own medical data as well as healthcare provider's rights to share and use the data for any purpose.

These new requirements motivated Professor Alfred Weaver to form a research group seeking to implement a prototype system to serve as a testbed for the new technologies and methodologies called for by the updated regulations. This overall system will rely heavily on an emerging technology known as web services and will seek

to simulate the varied environments in which medical data is accessed, for example: in a hospital, in a doctor's home, or in a pharmacy (Weaver et al., 2003).

The project title, *Federated, Secure Trust Networks for Distributed Healthcare IT Services*, summarizes the content of the project nicely. The core of the project is "Healthcare IT services," which simply refers to the systems by which medical data is shared among users for use in a wide range of applications. The "Federated" aspect of the project reflects the pool of networks which seek access to the data. These networks are referred to as "Trust Networks" because security measures, such as user identification that is done on a primary network, should be trusted by any subsequent networks the user attempts to access. Federations are groups of networks which already have trust established between them, such as pharmacy networks or the networks within a hospital. The key to this project is the "Secure" aspect of these networks, in accordance with the mandated regulations.

Another important concept that distinguishes this prototype from currently available solutions is that it introduces the concept of associating a "trust level" with authentication methods, which is how a computer system verifies a user's identity. This term is used to define how much trust the particular authentication method of a user is given. For example, if we issue a trust level of 1 for a username/password combination, a trust level of 10 might be associated with a retinal scanner, which is far more secure. These trust levels are then used as access constraints upon certain requests. Take for example a doctor who initially logs on to the system using his/her username to authenticate. If this doctor later requests a patients medical history, he/she will be prompted to provide better proof of identity in order to raise his/her trust level.

Identification techniques work in conjunction with trust sharing and access devices to establish the trust levels of users. These methods include various biometric, digital, and physical means. Incorporating digital identification methods within our larger framework was the focus of my research.

1.3 Scope and Method

The correct and secure verification of a particular user's identity is crucial to satisfying the federal regulations guiding this project. Without trustworthy identification methods, all trust sharing and data encryption becomes compromised. Anyone with the proper tools to fool our team's techniques will be able to access the most private medical records.

Identification techniques can generally be broken down into two broad categories: biometric and digital. Biometric methods are those that use biological features to determine identity. Examples include fingerprint scanners, iris scanners, signature recognition and keystroke dynamics.

1.3.1 Digital Identification Methods

Digital methods rely on data to identify a person. After investigating five principle methods identified in preliminary research, I chose one that was actually implemented as a web service. In order to rule out technologies, I used a series of criteria: usability in a hospital environment (operating room, emergency room), cost, frequency of false negatives, overall security and compatibility with other methods. The best solution could have been a combination of methods.

My initial research dealt with the five following digital identification techniques:

1. Key fob: A hardware token with built-in AES (Advanced Encryption Standard) encryption generating a constantly changing number sequence (PIN) that is required, in addition to a password, for a user to identify himself. The user would have a physical token, probably an attachment to his or her keychain (hence the name Key Fob), that contains a small display showing their current PIN. The PIN is generated algorithmically every 60 seconds.
2. RFID wristband: A wristband containing an embedded RFID (Radio Frequency Identification) chip that broadcasts encrypted identification information, used to confirm the user's identity.
3. Traditional keys: In certain circumstances it may be appropriate to lock IT systems with a physical key, requiring users to have a copy. This allows tight control over system access, especially if the user group for a particular system is small.
4. USB Electronic Token: This device plugs directly into a computer's USB port and conveys a user's ID information to software already running on the system. These devices are the size of a key and could be kept on a user's keychain for easy access (USB Token Authentication Device, n. d.).
5. Smart Card: A plastic card with an embedded chip that contains various pieces of ID information; a smart card provides not only memory capacity but also processing power, which enables encryption of its data (Fadely, 1998).

The power of these techniques comes from the fact that in order for a system to authenticate a user of one of these hardware tokens, the user must prove that he/she can correctly answer two questions: "What do you have?" and "What do you know?"

The first question is answered with the physical device, the second with a pin or password. The advantage gained through this property is that if the answer to either question is compromised, the security of the system has not been put in jeopardy. If a password is hacked, it is useless when not used in conjunction with the token and, conversely, if a token is stolen, it is powerless without a password.

1.3.2 Roadmap

In order to implement these technologies within our framework, I followed a roadmap laid out by several technical papers, beginning with "From CPP to Com" by Markus Horstmann of Microsoft, which details how to turn a normal header file (in this case a file which gives access to the functionality of the identification product) into a COM compliant DLL. In other words, I provided a standard interface for this product that I eventually converted to a web services compatible implementation (Horstmann, 1995). Next, with some guidance from "Beyond (COM) Add Reference: Has Anyone Seen the Bridge?" by Sam Gentile of Microsoft, I turned the COM object into a web services compatible component (Gentile, 2003). Finally, I created a web service that recognized authentication tokens generated by an eToken.

1.4 Overview of Remainder of Report

The rest of this technical report will present the procedures followed to meet my research goals and my results.

In chapter 2, I will discuss the relevant literature and the role it played in my research. Following this, in chapter 3, I will discuss the materials used and methods followed over the course of this research. Chapter 4 will present my results and their

analysis. The final chapter, chapter 5, will provide recommendations for future research in this area.

2 REVIEW OF RELEVANT LITERATURE

2.1 Medical Data Privacy

The medical profession has always been controversial. From its beginnings, it has faced, and still faces, challenges from religious authorities, governments, various cultural beliefs, and now more than ever, privacy advocates. The building block of all modern medical philosophies and ethical thinking is the Hippocratic Oath. Even when Hippocrates wrote it, in the 3rd or 4th century B.C., it dealt with patient privacy: "Whatever, in connection with my professional practice or not, in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret" (The Hippocratic Oath, 1998).

Further complicating this process has been the onset of the digital age, which makes information flow more fluid. This prompted the Institute of Medicine, part of the National Academy of Sciences and a non-profit organization, to publish a report entitled "The Computer-Based Patient Record" in 1991, which speaks at length on the critical importance of safeguarding patient data. In fact, the digital age progressed so rapidly in the 1990's that, in 1997, a revised edition of the report was published to highlight advances in CPR's (Computer-based patient records), in which confidentiality is re-stressed (Dick, Steen & Detmer, 1997). The importance of this issue prompted the Institute of Medicine to go one step further in 2000, publishing a report entitled "Protecting Data Privacy in Health Services Research." In this report, the Institute makes recommendations to the various entities in the healthcare industry about their treatment of sensitive data. One example is recommendation 3-6, which states that healthcare

organizations “that disclose or use personally identifiable health information for any purpose … should have comprehensive policies, procedures and other structures to protect the confidentiality of health information” (p. 12).

With all the concern pertaining to privacy, the ability to reliably recognize a user’s identity has been the focus of much research, not just in the medical field but many others as well.

2.2 Identification Technologies

There is a wide range of technologies applicable to this problem that are available today. I will focus on those that are classified as digital. A common feature in today’s state-of-the-art devices in this class are that they have an integrated microprocessor which has the capability to encrypt the data stored within them.

The prototypical example is the so-called smart card, which Hendry (1997) defined as a bank card sized piece of plastic which “incorporat[es] one or more IC [integrated circuit] within its thickness” (p. 4). According to Chen (2000), this technology was first introduced in 1968 by Jürgen Dethloff and Helmut Grörupp, who later filed a patent for their early work (p. 3). The first success of smart cards, wrote Rankl and Effing (1997), came in 1984 when “French PTT (Postal and Telecommunications services) successfully carried out a field trial with telephone [smart] cards” (p. 3). A more recent report, written by Michael Fadely in 1998, lists dozens of real-world applications of smart cards in more than 12 fields, including electronic commerce, banking, security, and healthcare.

Recently, many of these smart cards have been implemented in a new form: a USB token. This is, according to Kolodgy (2003), simply a "cryptographic algorithm … embedded in a plug that is inserted into the USB port" of a PC. According to a 2003 whitepaper sponsored by a USB token producer (USB Token Authentication Device, n. d.), this form factor has an advantage over traditional plastic smart cards because they require no extra hardware to be used in any modern PC (and laptop) with a USB port (Kolodgy, 2003).

2.3 My Contribution

I intend to make progress on several fronts. My research will contribute both to medical data privacy and identification technologies by expanding on what authentication systems are currently available.

In effect, this means that I will seek to adapt current identification technologies to make them suitable for the healthcare environment mandated by HIPAA. I will also contribute by implementing these technologies as web services, enabling them to be used as web applications from remote locations, thus increasing their potential.

3 MATERIALS AND METHODS

3.1 Materials Used for Overall Project

The main source of funding for this project is Microsoft, which contributed the hardware and software necessary to construct a research group laboratory containing desktop PCs, Tablet PCs and Toshiba Pocket PCs. All of these came with the latest software in terms of operating systems, server software, productivity suites and development environments.

3.2 Materials Used Within the Scope of the Personal Project

To move forward with the goals of my project, I obtained several pieces of hardware and software from two companies: Aladdin Knowledge Systems and RSA Security. Both of these supplied samples of their digital identification tokens (eTokens and key fobs, respectively) and appropriate SDK's at reduced educational rates. SDKs, or Software Development Kits, are pieces of software supplied by vendors which allow other developers to interact with their product.

3.3 Method

Background research

The initial stage of this research project consisted of researching the state-of-the-art in digital identification. This work was aimed toward discovering what techniques are most likely to be suitable for out projects needs.

The primary criteria for assessing techniques were reliability and resistance to attacks. However, due to the specific medical context of our project, other properties

needed to be taken into account: ease of use, false rejection rate, suitability in different medical environments (e.g. ambulance, hospital, ER, research lab) and cost.

The vulnerability to attack of a technique was the governing factor in our choice as the central goal of this project is ensuring the privacy of patient medical data. Were our project to employ techniques that did not give this assurance of privacy, it would expose patients to any number of vulnerabilities, including insurance companies accessing information in order to decide whether to insure, employers basing hiring decisions on illegally acquired data or political opponents using this information against one another. Obviously, such a scenario must be avoided in any proposed implementation.

The ease of use was critical because patient medical records are sometimes needed in emergency situations, for example, in an ambulance on its way to a hospital. This means that we need to provide a way for emergency medical technicians (EMTs) to authenticate rapidly to reach crucial information, such as drug allergies and a patient's medical history. Other ease of use concerns are in regards to the specific constraints under which this data might be accessed. An example of this would be a surgeon needing to review an X-ray in the middle of surgery while he already has his gloves and mask on. In this situation, authentication using such methods as fingerprint or voice recognition would not be feasible.

The false rejection rate (FRR) of an authentication technology is defined as the rate at which the technology will reject an access attempt by an authorized user (Computer Security Dictionary, 2003). While this rate is not as important as concerns over vulnerability to attack, a high FRR would nonetheless render a technique impractical

for our purposes. If a doctor had to attempt to log in an average of five times before being given access to data records, this would drastically lower the value and usability of our system.

Selecting Technologies for Implementation

With these factors in mind, I selected five general identification techniques. Next, specific implementations of these techniques were chosen for evaluation. As stated in the introduction, the five selected technologies were, with the companies whose implementations were investigated in parentheses: Key fob (RSA Security), RFID wristband (Precision Dynamics Corporation), Traditional keys (no companies found), USB electronic token (Aladdin Knowledge Systems) and a smart card (Aladdin Knowledge Systems).

Next, I further refined my search in order to find two final candidates for implementation.

The first technology to be discarded was traditional keys, since no companies could be found currently selling an implementation. Although this method is mentioned in literature, and implementations exist in other contexts (to lock computer tower cases, for example), none were readily available for use as a web service authentication solution.

Next, RFID wristbands were discarded for a combination of reasons. The first is that while RFID's are a valid authentication tool in certain circumstances, they are not secure enough for many of our target situations. For example, because of their broadcast nature, an experienced user may relatively easily intercept and analyze data traffic from the emitter to the detector. Also, since they constantly broadcast their identification

tokens over a certain range, a malicious user could use this information simply by attempting to log on from a station that is within range of a doctor or other privileged user.

The first selected technology was the Key fob, as implemented by RSA Security. These provided a robust solution in a product that was already trusted by many large companies, such as AOL and Sprint. These credentials aided in our evaluation that this solution met our criteria for security, ease of use and usability in the medical context.

The next decision was to choose between the two smart card form factors (traditional smart card and USB token) offered by Aladdin Knowledge Systems. After comparing the two implementations and finding that they did not differ significantly in terms of security, the USB token (known as the eToken) was selected for its portability and ease of use. The decision was largely based on the fact that, while a traditional smart card required a customized reader, a USB token could be used by nearly any computer with a USB port and the proper software installation.

After narrowing the field to two suitable, and comparably secure, technologies, the eToken was chosen for implementation simply because its cost was significantly lower than the key fob's, making it a more practical tool for users of our system.

Implementing the eToken

Implementing the eToken as a web service within our medical portal architecture began with creating a suitable interface to the eToken hardware. This meant that I had to provide a standard way for programs written for our architecture to access the on board functionality of the eToken. The functionality exposed by this "wrapper" interface included reading and writing files, encrypting and decrypting data and examining the

properties of an eToken (see Figure 1, next page). As stated in the introduction, this process was accomplished with the guidance of papers by Horstmann and Gentile of Microsoft.

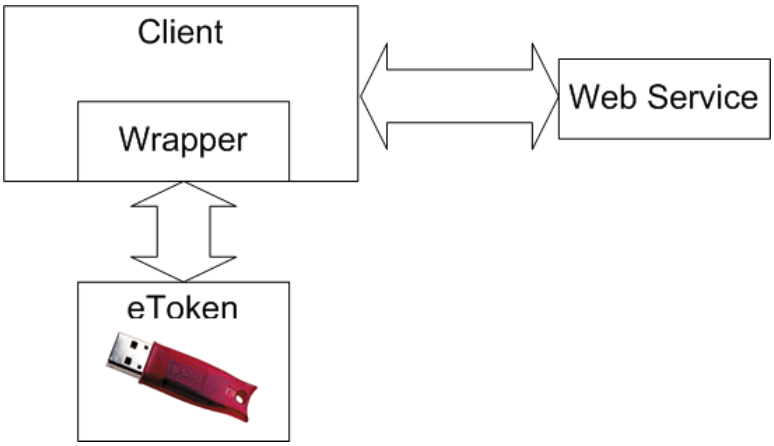

Figure 1: Schematic representation of eToken implementation.

The next step in the implementation phase for this technology was deciding the exact mechanisms by which authentication would take place. I decided that in order to ensure the user was providing the exact same UB token as was registered to his/her name within our system, I would use the unique chip ID which is hardwired onto each eToken. In accordance with this decision, I modified the systems database to store and verify a user's identity using this chip ID number.

These modifications led to the construction of one of the two central pieces of this project, a web service that could serve to authenticate a user based on his or her eToken credentials (see Figure 1). This service compares the registered eToken chip ID with the one being provided to it as well as the username and password of the user in order to make its authentication decision.

The next major component, as seen in Figure 1, was the client that provides the link between the "wrapper" I had created for the eToken and the web service I produced.

This client is an ASP.net web application and can be viewed as a webpage with an embedded program. The program embedded in the page was built to provide a user interface to the wrapper application that would allow the user to select his or her eToken. The program would then pass this information on to the webpage. The webpage component of the client is responsible for interaction with the web service that I described previously, and hence a user could now use an eToken to log onto our system and gain access to needed medical data.

4 RESULTS AND DISCUSSION

4.1 Results

As discussed above, the final deliverable for my particular project is a web application that utilizes several components I developed: the wrapper interface for the eToken, the web service that relies on this hardware for authentication and the client that provides a web page to utilize these. As shown in Figure 2, all of these components interact seamlessly using the Microsoft .NET architecture for ASP web applications.

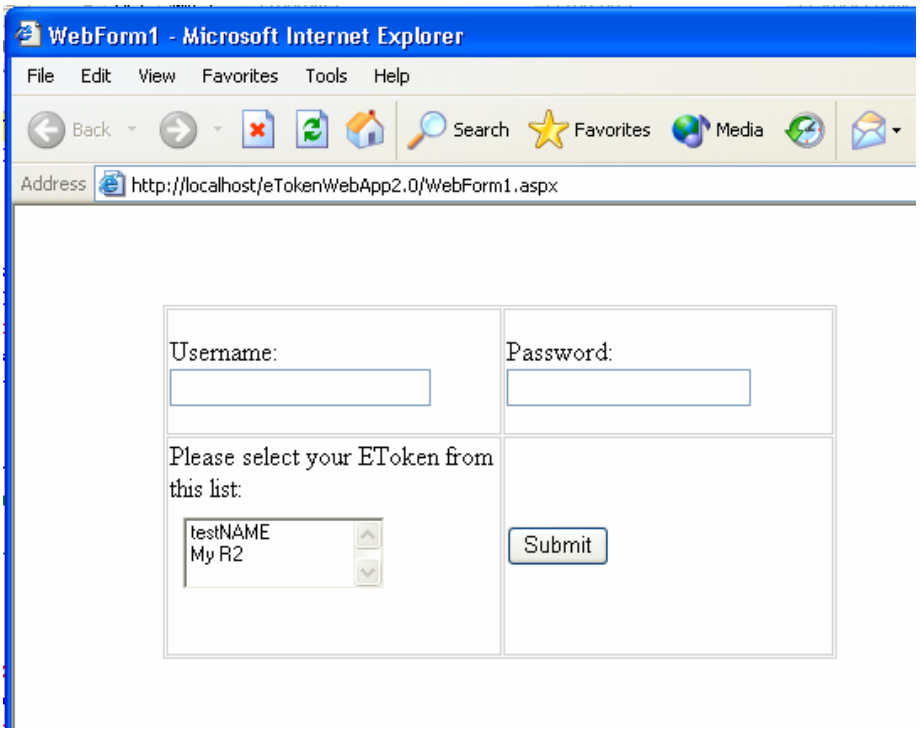

Figure 2: The client web form is the visible interface to this project. It allows a user to be authenticated by selecting his/her eToken and passing relevant information about it to the web service.

The particular implementation shown in Figure 2 allows a user to enter a username/password combination and exposes the eToken via a listbox which lists all of the eTokens currently plugged into a computer ("testNAME" and "My R2" in Figure 2).

In addition, the wrapper interface provides status information related to errors in the eToken functions to the user.

This particular interface is of use when a user has not been authenticated at all within our system. However, since our system introduces the concept of trust levels, a second interface exists which provides for authentication with an eToken in a session after a username and password have already been verified. This interface is also a webpage but simply has the control which prompts for the user to select an eToken for authentication without requiring any further data inputs.

While this deliverable is both important and practical, the more significant aspect of this work is the roadmap which enables other digital identification techniques to be integrated in a similar architecture. This aspect will be crucial when migrating this prototype into a production system, which will need to be equipped to deal with any identification techniques a medical institution wishes to use.

4.2 Discussion

The outcome of this work will be a valuable tool for improving the privacy of medical records as well as providing a method to increase the efficiency of available resources in certain situations.

While there exist a host of identification techniques, a significant subset of which will be in place within our research group's testbed system, the push into digital techniques represented by this work is significant in that it addresses medical data privacy for a space which is in some cases distinct from that in which biometric techniques are a viable solution. This distinction comes from the nature of biometric identification techniques, which rely of characteristics of a person to verify his identity,

and therefore rely on the duplication and constancy of these traits. However, any trait can at times change for a given person. For example, a cold could foil the algorithm within a voice recognizer, a cut or burn could result in an authentication failure in a fingerprint scanner and a jammed finger could effectively lock out a user who relies on handwriting recognition. On the other hand, barring the loss of a device, a digital token will be consistent in its interactions with authentication engines, ensuring that a user will always be given access to the vital information within.

The differences between biometrics and digital identification mean that, because of the introduction of the former by this work, we have allowed for the safe and secure access to medical data in time sensitive medical situations independent of the factors that limit biometric usability. If a tablet PC is used in an ambulance which is driving over unpaved roads where there is a high probability that neither handwriting, nor iris, nor retinal recognition will succeed, a digital technology becomes a crucial tool for providing medical care.

Within a larger scope, this structure for utilizing digital identification technologies provides a service that has applicability in other areas. The addition of eToken security into online shopping websites would provide an additional layer of security by ensuring that the user not only knew the right information, but also possessed a certain piece of equipment. Presently, if a credit card number or password is stolen, the user will not know of the theft until his/her credit card bill arrives at the end of the month. However, in this new scheme, the loss of a physical device would be noticed sooner, and therefore identity theft could be prevented.

This work makes a further contribution to these fields by opening the way for other authentication technologies, both those introduced in chapter 1 and other future inventions to be included in such an architecture, both within and external to the medical data context. Also, the modularity of this system allows this technology to be used in any web services enabled design.

5 CONCLUSION

5.1 Summary

This project's contributions are a practical tool for digital authentication through web services and a roadmap for implementing other technologies in a similar fashion in the future.

The practical tool that came of my work is a module that authenticates users of any web services architecture using a particular digital identification technology, an eToken provided by Aladdin Knowledge Systems.

The roadmap I provide is for future researchers who wish to expand on the authentication options currently usable through web services. Following a path similar to mine, a developer should be able to integrate almost any technology in such an environment, using a set of steps similar to the ones I discuss in this technical report.

5.2 Interpretation

While this project fulfilled its major objectives, some other goals were not met. For example, I originally intended to implement two identification technologies, but instead have only one fully functional implementation. Meanwhile, the most valuable component of this research, setting the web services precedent for digital identification, is complete.

During the course of the research for this project, many unforeseen obstacles interfered with my progress. One main issue that slowed progress was that this work depended on establishing relationships with outside companies in order to acquire the hardware and software (SDK's) on which the research depended. I found that this step was more difficult than anticipated because the salespeople were sometimes difficult to

contact and were not technical experts on the products that they were selling. For a product to be a worthwhile investment for our research group, I needed to ensure that it had the proper characteristics to allow its interface to be raised to a web service standard, and therefore needed such technical information from salespeople.

Despite these setbacks, the final result of this work was still substantial in its contributions. The implementation of the eToken will aid in securing and flexibly accessing private medical information. This goal is important both for medical practitioners who need quick access to reliable data to better perform their duties and for patients who need to trust that their sensitive information is well guarded. Furthermore, the blueprint that I have presented will be valuable as this system moves toward more practical implementations.

5.3 Recommendations

Looking past the research done for this paper, the immediate steps that need to be taken to pursue this line of work are clear.

The first step is to perform both empirical and case tests to verify the reliability of this technology. According to Aladdin Knowledge Systems and the limited testing during implementation, the reliability of this product seems to be acceptable. However, this technology has still not been tested for it's resistance to a malicious attack and FRR numbers are not available. This means that, before any real life usage, a thorough and careful evaluation is critically necessary.

The second recommendation for future work is to extend this methodology beyond the eToken into different USB tokens and the other technologies presented earlier in this work (Key Fobs, RFID wristband, traditional keys and smart cards). This

extension will provide the flexibility of choice that a production system would need to deal with the variety of real world technologies.

REFERENCES

Computer Security Dictionary: False Rejection Rate. (2003) Retrieved March 19, 2003 from http://www.itsecurity.com/dictionary/frr.htm

Chen, Z. (2000). *Java Card Technology for smart Cards.* Boston: Addison-Wesley.

Dick, R. S., Steen, E. B., Detmer, D. E. (Eds.). (1997). *The Computer-Based Patient Record.* Washington, D.C.: National Academy Press

Fadely, M (1998). *An examination of Today's and Tomorrow's Smart Card Technology.* Unpublished undergraduate thesis, University of Virginia, Charlottesville, VA

Gentile, S (2003) *Beyond (COM) Add Reference: Has Anyone Seen the Bridge?* Retrieved January 20, 2004 from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndotnet/html/bridge.asp

Hendry, M. (1997). *Smart Card Security and Applications.* Boston: Artech House

Horstmann, M. (1995) *From CPP to COM.* Retrieved January 20, 2004 from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncomg/html/msdn_cpptocom.asp

Institute of Medicine. (2000). *Protecting Data privacy in Health services research.* Washington, D.C.: National Academy Press.

Kolodgy, C. J. (2003). *Identity Management in a Virtual World.* Unpublished whitepaper.

Marshall, A. (2003). *COM Compliance and Type Libraries for the KnoWho SDK.* Unpublished whitepaper, University of Virginia, Charlottesville, VA.

Rankl, W., & Effing, W. (1997). *Smart Card Handbook.* Chichester: John Wiley & Sons.

Summary of the HIPAA Privacy Rule. (n.d.). Retrieved October 17, 2003 from http://www.hhs.gov/ocr/privacysummary.pdf

The Hippocratic Oath. (1998).Retrieved October 17, 2003 from http://members.tripod.com/nktiuro/hippocra.htm

USB Token Authentication Device. (n.d.).Retrieved September 12, 2003, from http://www.ealaddin.com/etoken/

Weaver, A. C., Dwyer, S. J., Snyder, A. M., Van Dyke, J., Hu, J, Chen, X., Mulholland, T., Marshall, A. (2003, August). *Federated, Secure Trust Networks for Distributed Healthcare IT Services.* Paper presented at EEE International Conference on Industrial Informatics, Banff, Alberta, Canada.