# *Auctorizo ergo sum:*
# The Lure, Perils, Privacy and Liability Implications of Authentication, Identification and Key Management Systems (AIKM)

**Authors:**

**Limor Fried** *ladyada@mit.edu*

**Tzer Hung Low** *low@mit.edu*

**Sina Kevin Nazemi** *nazemi@mit.edu*

**Faisal Reza (edit.)** *faisal@mit.edu*

**Advisors:**

**Hal Abelson** **Joe Pato** **Danny Weitzner**

**Massachusetts Institute of Technology**
**6.805/STS.085: Ethics and Law on the Electronic Frontier**

**May 17, 2001**

# Contents

**1 Executive Summary 4**

**2 Introduction to and Justification for Today's and Tomorrow's Authentication, Identification and Key Management (AIKM) Systems 5**

**3 Policy Criteria for Information Exchange Between Parties 7**

3.1 Privacy . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

3.2 Versatility . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

3.3 Accessibility and Ease of Use . . . . . . . . . . . . . . . . . . . . . . . . . 9

3.4 Freedom and Applicability without an Undue Burden . . . . . . . . . . . . . . . 9

3.5 Cost . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10

3.6 Degree of Distribution and Security . . . . . . . . . . . . . . . . . . . . . . 10

3.7 Trust and Confidence in AIKM system . . . . . . . . . . . . . . . . . . . . . 11

**4 Privacy and Liability of an Information Exchange 12**

4.1 What Privacy and Liability Issues are Involved Before, During and After an Information Exchange? . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 12

4.2 What Privacy and Liability Implications Exist for the Information Gathered? . . . . . 13

**5 Evaluation of AIKM Systems 14**

5.1 State Issued Identification . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

5.1.1 Trust Model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15

5.1.2 Analysis based on policy criteria . . . . . . . . . . . . . . . . . . . . . . . 15

5.2 Credit Cards . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 16

5.2.1 Trust Model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 17

5.2.2 Policy Analysis Based on Criteria . . . . . . . . . . . . . . . . . . . . . . 18

5.3 Social Security . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 21
5.3.1 Trust Model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 22
5.3.2 Policy Analysis Based on Criteria . . . . . . . . . . . . . . . . . . . . 22
5.4 Public Key Cryptography . . . . . . . . . . . . . . . . . . . . . . . . . . 26
5.4.1 PGP . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 26
5.4.2 PGP in Practice . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27
5.4.3 Trust Model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 28
5.4.4 Policy Analysis Based on Criteria . . . . . . . . . . . . . . . . . . . . 28
5.5 SDSI . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 29
5.5.1 SDSI in Practice . . . . . . . . . . . . . . . . . . . . . . . . . . . . 30
5.5.2 Trust model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 32
5.5.3 Policy Analysis Based on Criteria . . . . . . . . . . . . . . . . . . . . 32
5.6 X.509 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34
5.6.1 X.509 in Practice . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34
5.6.2 Trust Model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36
5.6.3 Policy Analysis Based on Criteria . . . . . . . . . . . . . . . . . . . . 37

**6 Private Credentials 40**

6.1 Why Private Credentials? . . . . . . . . . . . . . . . . . . . . . . . . . . 40
6.1.1 Current Privacy Threats . . . . . . . . . . . . . . . . . . . . . . . . 41
6.1.2 Current Security Threats . . . . . . . . . . . . . . . . . . . . . . . . 42
6.1.3 Imposing Threats . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43
6.2 Technical Overview of Relevant Cryptography . . . . . . . . . . . . . . . 43
6.2.1 Elements of Public Key Cryptography . . . . . . . . . . . . . . . . . 44
6.2.2 Privacy Concerns . . . . . . . . . . . . . . . . . . . . . . . . . . . . 44
6.3 Chaum's Digital Cash . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45
6.3.1 Technical Overview . . . . . . . . . . . . . . . . . . . . . . . . . . . 45
6.3.2 Evaluation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 46
6.4 Private Credentials . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47
6.4.1 Improving Un-Linkability . . . . . . . . . . . . . . . . . . . . . . . . 48
6.4.2 Desired Technical Elements of a Private Credentials Protocol . . . . . . . . . . 48
6.4.3 Criteria Overview . . . . . . . . . . . . . . . . . . . . . . . . . . . . 51
6.5 Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 52

**7 The Lure of Single Sign On 54**

7.1 Why do companies want a single sign-on? . . . . . . . . . . . . . . . . . . . . . . . . . . 54

7.2 Why do individuals want a single sign-on? . . . . . . . . . . . . . . . . . . . . . . . . . . 54

7.3 Case Study: CompanyX . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55

7.3.1 Description of the business . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55

7.3.2 Potential Concerns and possible solutions . . . . . . . . . . . . . . . . . . . . . . . 55

7.4 Case study: Yodlee . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 57

7.4.1 Description of the business . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 57

7.4.2 Potential Problems . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 58

7.4.3 Proposed Solution . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 59

**8 Conclusions and Recommendations 60**

**9 Acknowledgements 64**

# Chapter 1

# Executive Summary

In today's world of pervasive information flow, authentication, identification and key management (AIKM) systems play a key role in facilitating these exchanges. As AIKM systems are designed from a technical perspective and protected by legal policy, we have noticed that the paradigms of thought among these two camps leads to AIKM systems that are less ideal than thought. In evaluating current AIKM systems as well as new and proposed AIKM technologies, such as single sign on and private credentials, we established a policy criteria composed of privacy, versatility, accessibility and ease of use, freedom and applicability without an undue burden, cost, degree of distribution and security, and trust and confidence in the system. In concluding, we have proposed a novel policy structure that attempts to preserve privacy concerns and offered recommendations on future courses of action.

# Chapter 2

# Introduction to and Justification for Today's and Tomorrow's Authentication, Identification and Key Management (AIKM) Systems

Today's authentication systems are largely the product of two distinct paradigms of thought. Not surprisingly, they are held by the two key players in the design of AIKMs, namely the technical engineers and the policy makers. As a generalization, technical engineers plan AIKMs with an almost paranoid sense of security, designing for every flaw that might occur and attempting to predict every contingency. They deal largely with the here-and-now, concentrating on "how" a process can be accomplished. In contrast, policy makers cover AIKMs with almost absolute confidence, making assurances and guarantees against invasions of privacy through policies and laws meant to deter AIKM misuse. They deal largely with the future implications, focusing on "what" to do when something in the AIKM goes wrong and then who to hold liable. Thus while the need for rigorous and well-thought out AIKMs exists in our society, and even relied upon to maintain the daily lifestyle of individuals and communities, we believe that the status quo of AIKMs can be improved upon.

In examining the current state of AIKMs, we have chosen three real-world (state issued identification, credit card, and Social Security cards) and three cyberspace technology-based (PGP, SDSI and X.509) AIKM systems. While the nature, purpose and needs of these AIKM systems vary widely, we believe each will elucidate some characteristic benefits and disadvantages that we can improve upon. We have also arrived at a policy criteria to be used to judge these systems and bring their strengths and weaknesses to bear. In showing that there is a loss of privacy due to a failure in one or more of our policy criteria, we offer two novel approaches (private credentials and single sign on) to AIKM systems that may offer better privacy protections. This discussion leads us to conclude and justify the need for further work in the technical and policy arena to ensure a greater concern and further protection of an individual's privacy from a world of relentless information exchange.

# Chapter 3

# Policy Criteria for Information Exchange Between Parties

In order to discuss the privacy implications of current and prospective AIKM systems, we established a policy criteria that was used to evaluate the current real-world and cyberspace AIKM systems. The threats to each of these AIKM systems differ in approach and frequency, but as a general assumption, if a system is tailored to be used in real-world or cyberspace settings, it can also be misused. We then examined how current AIKMs fail to meet our criteria standards and use this information along with novel AIKM theses to propose ways to improve upon the AIKMs used today. We hope that the new technologies will meet or exceed our policy criteria, and in doing so, limit invasions into one's private information to only what is necessary to complete a task.

## 3.1 Privacy

We feel that privacy is a two-fold criteria, dealing firstly with what information is collected and then what happens to that information. In one sense, the amount and type of information that is requested by a service in order them to identify and authenticate you is a measure of the privacy granted to the user by the service. If the user chooses to use the service, they must surrender this information. Thus, the service attempts to control the collection of sensitive personal information and maintain such information according to the service's privacy policy. Such a privacy policy usually includes the principles of notice, choice, access and security but there are no clear laws or even guidelines on how, where and to what degree each should be implemented.

Furthermore, once this information is collected, the privacy implications of using this information toward tasks not intended in the original exchange (i.e. selling mailing lists from an online e-tailor) without the knowledge or consent of the user are raised. In fact, according to Robert Ellis Smith of the Privacy Journal, "Privacy in this context means the attempt by individuals to control the collection and disclosure of sensitive personal information and to be assured that personal information is maintained safely and accurately."[1] These implied possible and unseen invasions into one's privacy now raises legal issues of who is liable for what actions. For example, if AIKM mechanisms are compromised such that a user's personal among a large group of trusted component, it may not be all that clear exactly where the burden of responsibility lies. Even if the compromised party could be isolated, according to our discussions with Joe Pato, there are few legal precedents or laws to protect the individual, at least online from such reckless use of their identities.

Thus, we evaluate the privacy implications of our AIKM systems by the degree of access to the information, the ability to correct the erroneous information, to know the purpose for which that information is collected, to minimize the information collected in an attempt to maximize privacy concerns, to ensure that once the information is collected that it remain secure and if it is compromised that there are parties that can be held accountable and liable for such invasions of privacy.

## 3.2 Versatility

We also felt that an AIKM system must be versatile, in largely a social but also technical context. In terms of social versatility, the AIKM should be easy to implement in a host of socioeconomic settings and be able to perform under a variable set of conditions that will be present in the given setting. The system should not be awkward, and should largely be intuitive and more helpful rather than burdensome to the user. It should not drastically change the socially accepted means and practices of authenticating and identifying without an appreciably higher benefit to changing these modalities of society. (i.e. use AIKM, which are not current used at supermarkets, just like credit card to make a grocery purchase intuitively and without a steep learning curve.) In examining the social versatility of an AIKM system, we also concluded this largely depends on the technical versatility and longetivity of the system. An AIKM system must not be limited by an unreasonable degree by the hardware/software infrastructure so that it cannot support the social loads for which it was designed. Thus, to a large extend, the system must have clear levels of abstraction and modularity, such that it can grow and scale to serve the needs of the populace while limiting the potential ways

[1] email correspondence from Robert Ellis Smith, 05/15/2001 10:23am

to infringe upon an individual's privacy.

## 3.3 Accessibility and Ease of Use

We also felt that an AIKM system is only useful if the individual not only has access to such a system but also is able to determine the access or fate of the private information about him that resides on this system. The usage of such an AIKM system not only should afford him accurate and reasonable identification and subsequent information exchange, it should limit the spread of such information to parties with a critical need-to-know in order to complete the exchange.

This rigorous selective accessibility need is balanced by the reasonable ease of use of the AIKM system. Not only should an AIKM system limit access to private information as a function of exchanges between users and the other necessary parties but also while doing so, it should remain relatively simple and easy to implement and use. If an AIKM system is so intricate and difficult to use because of the accessibility barriers, and thus places heavy burdens upon one's ability to use the system, they will most likely resort to other means to accomplish the same task.

## 3.4 Freedom and Applicability without an Undue Burden

The freedom and applicability without an undue burden criteria element is largely a two-fold policy matter with possible constitutional and state law underpinnings. Basically, an AIKM system should be designed, examined and be able to be used without the significant probability (note, probability not possibility, as there is always some degree of uncertainty that we cannot design for) of violating someone's legal rights through an obscure technical process. For example, technical loopholes that may stop someone, who really is the authentic user of their AIKM device, from exercising their rights to exchange credit card information as legal tender for a purchase, should be minimized. Put another way, while the Fourth Amendment does not explicitly mention privacy, an AIKM in our criteria should not ask more than what is imminently necessary for an AIKM transaction. Perhaps one can think of this as the "freedom to exchange necessary information for an expected return" clause of our criteria.

Furthermore, on the applicability without undue burden, an AIKM should not impose any undue process or series of actions that are not imminently necessary for a person to get a desired transaction. Notice, that this is different from the ease of use clause, which deals more with the limited and valid access and use of an individual's private information on an AIKM designed for that use, while applicability deals with the ability of the AIKM system as an instrument of exchange to be physically applied in different contexts. We find there is a precedent to a need for freedom without undue burden in Reno, where "no case has ever held that a speaker has a right to have no burden imposed at all to advance a compelling state need; the only requirement of Reno is that the burden the be least restrictive burden."[2] While this was applied to First Amendment issues, we believe the same limitations on burden can be applied to the preservation of privacy.

## 3.5 Cost

Cost is a very broad criteria element that encompasses both the technical costs associated with establishing and maintaining an AIKM systems and the social costs of entrusting one's personal information to these systems. While the technical costs, can be further examined and be shown to be key on the types of AIKMs implemented in a given situation, this does not form the bulk of our cost criteria. Rather, we believe that the technical features or limitations allow us to gleam the privacy costs and implications of a given technology. The information we provide for a service or transaction inherently has a commercial value associated with it, though this value is largely dependent what the owner plans on doing with such information. For example, while many individuals would not find their own home mailing addresses to be of much value, retailers and sweepstakes organizers with the goal of selling these addresses as part of a mailing list often collect these addresses. Not only is there an up-front cost in privacy as one exchanges personal information in return for a good or service, but also there is also the long-term and often unpredictable implied privacy costs when such personal information gets distributed beyond the scope of the original exchange.

## 3.6 Degree of Distribution and Security

As we believe that large, centralized repositories of information are wonderful targets for compromising private information collected by AIKM systems, our degree of distribution criteria is based on the premise that if information is distributed throughout the parties involved in the AIKM exchange, it will present less of a worthwhile target for compromise. While many trusted parties in AIKM system can claim high levels of security, we feel that is keeping everyone's private crown jewels of information

[2] p. 21, Lessig, "The Law of the Horse"

behind one closed door begs for an attack. In raising the number of sites and effort needed to get to a given set of personal information, we raise the costs associated with getting to the benefits of such private information. This information is distributed and kept isolated until explicitly and imminently requested from valid AIKM instruments. (e.g. confirm one's birth date by getting her name and biometric from one data source and e-birth records from another) Thus, we believe that the privacy of an individual both initially and also in the future will be held to a higher level of security, as those who wish to infiltrate an AIKM system would have to invest more time and effort toward multiple targets. Ideally, if done rigorously and with notice, distribution of information should raise technical security at a reasonable cost but also raise benefits at a hopefully greater than or equal to amount.

## 3.7 Trust and Confidence in AIKM system

Our last policy criteria deals with the perception of AIKM systems through the eyes of the system creators (e.g. the policy makers and the technical designers) and through the eyes of the public (i.e. services and end users). As an AIKM system is designed, the technical designers and policy makers attempt to build confidence in the system via engineering and legal guidelines respectively. These AIKM creators ask whether this AIKM can be trusted by those who use it because of the technical infrastructure and multiple redundancies and cross-checks in place? Do the privacy and security policies surrounding the AIKM install a sense of confidence in the system?

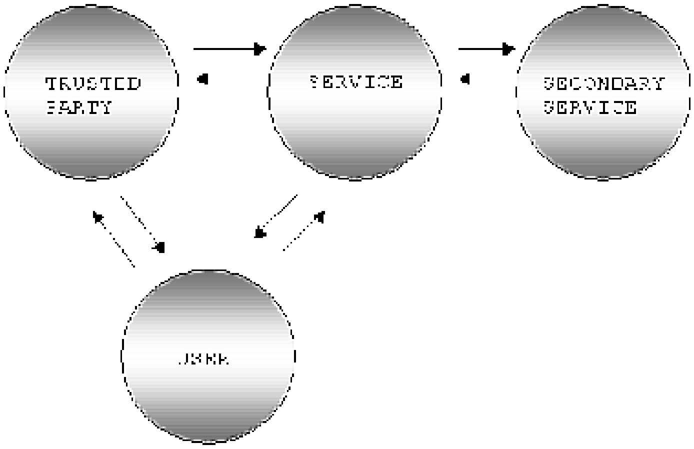
Once a system has been designed and implement, the public, who deem whether this AIKM system is worthy of holding and manipulating their private information, answers the proof of principle. For example, in filling out a U.S. Department of Justice Employment Eligibility Verification Form (I-9), the federal government lists the documents that they place confidence in establishing only identity (such as a driver's license or school id card with a photograph), documents that establish only employment eligibility (such as a social security cart), and documents that do both (such as a U.S. Passport). The privacy implications of trust are inherent in the policies set by the AIKM service provider, who is given private information because the public feels that they will safeguard it with some reason. This criteria seeks to qualitatively gauge whether the public would use such an AIKM under given circumstances with relative confidence.

# Chapter 4

# Privacy and Liability of an Information Exchange

## 4.1 What Privacy and Liability Issues are Involved Before, During and After an Information Exchange?

In an attempt to analyze a broad range of AIKM systems, both real-world and cyberspace, we abstract the systems to some basic necessary parts. In the simplest sense, authentication and identification of a stranger by a service requires a party is trusted by the service and who can vouch for the stranger.



When a request is made by the user for a particular service, if needed, the service will ask the individual for key identification information. Once this information is gathered the service matches it with the trusted party to authenticate the identity of the user. Once authenticated, a confident exchange of information can occur between the service and user.

The privacy implications play a largely two-fold role in this picture. First, when an initial exchange of information takes place, the information that is requested at that time is subject to the privacy rights of an individual. Is the information requested explicitly necessary to authenticate the user with the trusted party? Can other less invasive means or pieces of information be used and still make a valid authentication? The second fold role deals with secondary parties and accessors of information who may at some point receive the identification and authentication information. When this happens, what protection does the user have that his privacy is not violated? If it is violated, on whom does the liability fall? Do privacy concerns travel with the private information or do they stop at the door once revealed to the whole world?

## 4.2 What Privacy and Liability Implications Exist for the Information Gathered?

Once private information about an individual is gathered and resides in the hands of another parties, another series of privacy concerns come into play. Now, the issue is not whether certain personal information is necessary for a valid authentication but rather what is the future of such information? If the information resides on a service's database but deals with the personal information of an individual, who owns this information? More importantly, who is liable for this information should it be compromised and misused in some way? If a third party asks for this information, should they ask the service provider who collected the information or track down the user for their permission? In some cases, private information passing through third party hands is part of the AIKM infrastructure. (such as private information passing through routers to their desination) While these parties may not be able to read the information contained in the data packets, would the still be liable for making sure these packets cross their juncture point safely and securely? Currently, there are few laws or guidelines in place that clearly state what kinds of information sharing is permissable with or without the end user's knowledge. Much of this is due to a lack of precedent or model by which privacy policy makers can base new laws upon. However, due to the rising concern among the public about the information gathered about them, as well as the realization by companies and institutions that their reputations can be damaged and they can be held liable for releasing private information, many have instituted privacy policies to protect themselves and their end users from immediate and future invasions of privacy without their knowledge. Albeit, it should be noted that these policies are by no means are uniform throughout industries or technologies and in many cases not subject to legal review and litigation  they are merely a statement of reassurance and good faith.

# Chapter 5

# Evaluation of AIKM Systems

## 5.1 State Issued Identification

State issued identification cards are arguably the most widely used form of identification in the United States. These cards are usually issued in the form of driver's licenses to those who pass a driving test, though cards used solely for identification are also issued. Each state issues a card with a standardized appearance and basic security features like a distinct hologram. The identification cards generally contain a person's name, a picture, a birth date and other identifying information (height, eye color etc.).

Though the specifics on how a state resident obtains an identification card varies from state to state, we employ the example of Washington State to illustrate how one generally receives a card. To receive an identification card in Washington State, one must visit the local Department of Motor Vehicles office and present valid federal, military, or state identification. If the person does not have a government or military issued identification card or document, he can either present a certified birth certificate or two documents that contain identifying information (e.g. Social security card, marriage certificate, IRS document, bank statements etc). Those under the age of 21 can receive an identification card provided that they present a signed affidavit by their parent or legal guardian confirming their identity. [1]

Today, state issued identification cards are both used as a credential and for identification. To illustrate this point, we employ the example of purchasing cigarettes. When Alice wants to buy cigarettes at her local supermarket, she shows the clerk her identification card. The clerk checks to see if the card is real, if the picture on the card matches Alice's appearance, and if the card indicates

[1] http://www.wa.gove/dol/drivers/dl.htm

that Alice is over the age of 18. Based on his analysis, the clerk either allows Alice to purchase cigarettes or does not allow her to purchase cigarettes.

### 5.1.1 Trust Model

The state agencies that issue identification cards serve as authorities that certify one's identity and other information and bind it to a unique card that is not easy to tamper with. Each person or entity that requires the card for either verification of one's identification or verification of a characteristic like height certifies the validity of the card being presented using his or her knowledge of what a state issued card should look like.

### 5.1.2 Analysis based on policy criteria

- Privacy When analyzing privacy in this section, we mean to analyze the privacy concerns a user might have to apply for a State Identification Card. The State may store information about a user, but that is a separate topic.

  **Access to information** All the information that is stored is on the card itself, so the user has access to the information.

  **Ability to correct erroneous information** The user can change erroneous information, such as his height or address, as it changes. **Know the purpose that the information is collected** The purpose is for identification of an individual, and possibly to prove his age or any other attribute that is on his card, and to prove his current residential address. It may also allow him to drive, in the case of a driver's license. Minimize the information collected The information collected is minimal. In the past, Massachusetts required that the card number be the social security number. This has now been changed.

  **Security of the information collected** The information collected is secured within the States facility, and the card is as secure as the user protects the card.

  **Accountability** The user is accountable for his privacy loss if the card was stolen.

- Versatility State issued identification cards are quit versatile. The cards can be used in nearly all settings where personal interaction takes place since the uniform appearance of the cards and the abundance of the cards makes them easily recognizable.

- Accessibility and Ease of Use As our Washington state example points out, any state resident that can prove his identity to state is eligible to receive an identification card. Using the card is quite easy, one merely has to take the card, which fits in ones pocket, and present it.

- Freedom and Applicability without an Undue Burden When one uses a state identification card for any transaction, he is sharing all the information that is on his card, regardless of whether it is relevant. In our example, even though the clerk only wants to verify that Alice is at least 18 years old, he sees all the information that is on Alice's card. The clerk sees Alice's name, her address, her birth date, her picture, her weight, her height, and a description of her eye color. Just by looking at Alice, the clerk would have a good approximation of Alice's age, height, weight and eye color. Alice needs to only worry about the misuse of her name and address. While the identification card system requires that one give up more information than is absolutely necessary, the fact that most uses of state identification cards occur in person and take no more than a few seconds makes it difficult for information to be recorded.

- Cost State identification cards are generally inexpensive. A Washington state photo identification card costs $4.00, with additional costs for driving permits.

- Degree of Information Distribution and Security The information that is put on state identification cards is usually placed on a central server that is accessible by all of the branch offices that distribute cards. Since there are multiple points of entry, the system is somewhat vulnerable to attack.

- Trust and Confidence In the System Nearly everyone trusts state identification cards. From grocery stores to banks, an array of companies and organizations accept state identification cards. It is hard to find people who do not have state identification cards that they use on a regular basis.

## 5.2 Credit Cards

Millions of American's use credit cards everyday. Corporations like Visa and American Express issue credit cards either directly to customers or through banks that they authorize to issue cards on their behalf. To apply for a card, one must provide the credit card company or authorized bank enough information for the bank to conduct a credit check on the applicant. At a very minimum the applicant's name, address, birth date, and social security number are required. If the credit card company or authorized bank finds that the applicant meets its credit requirements, it issues a unique card to the applicant with a limit on how much can be charged to the account.

The front of the card usually bears a name, an account number, and an expiration date, along with the hologram and logo of the credit card company. There is sometimes a unique code imprinted above the account number on the front of the card. On the back of the card, there is usually a magnetic strip that has the account number encoded in it, a blank strip for the cardholder to sign when he initially receives the card and information about how to get in contact with the credit card company. The credit card companies establish accounts with merchants around the world, enabling them to accept cards through credit cards through credit card terminals that connect the merchant to the credit card company.

Credit cards generally serve as credentials in transactions that require money. To illustrate this point, we employ the example of an in person credit card transaction, the most common type of credit card transaction. In this example, Alice wants to purchase a latte from her favorite coffee shop, Starbucks, using her Visa card. Since Starbucks accepts Visa, Alice presents her card to the Starbucks employee who swipes the card's magnetic strip through her terminal to charge Alice for her latte. The Starbucks terminal reads the magnetic strip and sends the corresponding account number with the request to charge the $3.00 for the latte to the credit card company. The credit card company verifies the validity of the card number and sees if the account has $3.00 of available credit. If there is $3.00 in available credit, the card company sends an authorization code to the merchant's terminal that activates the printing of a receipt showing the amount that is charged to Alice's account. Alice signs this receipt and the merchant checks to see if Alice's signature on the receipt matches her signature on the card. If the signatures match, Alice walks away with a latte in hand, the merchant places the signed receipt in his register, and $3.00 is transferred into Starbuck's account. If the signatures do not match, the merchant does not give Alice her latte and notifies Visa of the discrepancy.

### 5.2.1 Trust Model

The credit cards companies or the banks that the credit card companies authorize to act on their behalf bind one's name to a card with a specific account number and a credit limit associated with that account number. Each time that there is an attempt to use the card for a purchase, the credit card company verifies that the account exists, is valid and that it has sufficient available funds. Each merchant is in charge of verifying that the identity of the card user matches that of the person that the card was issued to by verifying the signature of the card user with the signature on the back of the card.

### 5.2.2 Policy Analysis Based on Criteria

- Privacy issues with obtaining a credit card When analyzing privacy in this section, we will analyze the privacy concerns a user might have to apply for a credit card.

  **Access to information** Credit card companies allow users to have access to transactional information stored about them. For example, billing statements sent to the user include a name, address, account number, all the transactions made during that month and whether the user is late at paying.

  There may be other information stored about the user, such as information obtained from a credit bureau. Other information may be obtained from affiliates, or from the user's employer. Citibank, for example, controls a number of financial services, and the information obtained from their experience with a user for a mortgage, could possible be shared with the credit card division. Such information is not necessarily revealed to the user.

  **Ability to correct erroneous information** For information that is reported to the user, the user will have the ability to correct it within a reasonable time. For example, users can very easily change their phone number or address on record. They can also dispute transactions, possibly with a signed affidavit.

  Some information that is not reported to the user cannot be corrected. However, for information obtained from third parties such as a credit bureau, the user can correct the information by going to the source.

  **Know the purpose that the information is collected** The user has one clear understanding on the purpose the information is collected for in the case of credit cards, namely to evaluate the granting of credit and to set the rates. Depending on the credit card company, however, there could be other purposes for the information collected. This is usually disclosed to the user in an unexpected section of the cardholder's agreement in vague terms.

  Let's consider Citibank[2] as one example. While Citibank never directly claim that they will use information collected about the customer for telemarketing decisions on what the customer is likely to buy or pay, they reserve the right to do so in the section describing how they intend

[2] Please refer to "Citibank's Privacy Disclosure Notice"

to provide superior service. They will use collected information to improve their services which will include "advising our customers about our products, services and other opportunities."

While the customer cannot directly opt out of such uses of this information, he can effectively do so by opting out from receiving promotional offers from Citibank. As an exception, marketing offers that are packaged in the same envelope as the monthly account statement cannot be opted out of. Therefore, the customer will still have information collected to study his purchasing habits on a database at Citibank. It is just not used as often.

**Minimize the information collected** While there is nothing to stop a credit card company for collecting as much information as they wished, many reputable companies will actually promise to minimize the information collected, and a user can choose to do business with only these companies.

For example, according to their privacy promises, Citibank will "limit the collection and use of customer information to the minimum that they require to deliver superior service to our customers." However, as noted before, their broad range of "services" leave much to be questioned about the minimization process.

**Security of the information collected** Most credit card companies claim to take precautions on a user's information. Citibank as an example Citibank, for example, promises to "safeguard, according to strict standards of security and confidentiality any information our customers share with us" and "will only permit only authorized employees ... to have access to that information." Furthermore, companies that wish to market to the user "are not permitted to retain any customer information", and companies that work for Citibank must "conform to their privacy standards."

**Accountability** The credit card is accountable for misuses. Since they are corporations with considerable assets, there is in fact a reason for class-action suits against a credit card company that has misled consumers or is negligent to consumers.

- Privacy issues with using a credit card **Online Usage of Credit Cards** According to consulting and auditing firm Ernst & Young, the number of U.S. consumers who shopped online in 1999 more than doubled compared to a year ago. The study reported that U.S. consumers made an average of 13 purchases online in 1999, and spent $1,205, while in 1998, U.S. shoppers averaged six purchases and spent $280.

  Unfortunately, the Internet is a place where credit card theft is most likely to occur. For example, hackers have been reported to have infiltrated the credit card database of health products supplier, Global Health Trax, Inc and Connecticut-based CDUniverse. There are several other incidents, and many more that may be unreported or unnoticed.

The most obvious danger of credit card theft is unwanted charges. Traditionally, the user is liable for the first $50 in a credit card theft, or even more if he was negligent in reporting the loss immediately. The thief can call the user's credit card issuer and, pretending to be him, and change the mailing address on his credit card account. If the theft was from an online merchant, the chances are that the thief will have information on the user's zip code and birthdate. This information may be sufficient for the credit card company to trust the thief. Then, the imposter runs up charges on the account. Since the bills are not being sent to the user but to the new address, the user will not report fraudulent usage until a substantial bill has been run up.

- Versatility Credit cards are both socially and technically versatile. Credit cards can be used for an array of transactions, regardless of the of the dollar amount of the transaction. Cards are often used to make purchases, place safety deposits, receive credits, and receive cash. With the growth of e-commerce, credit cards easily adapted to this new frontier, and are accepted at nearly all online stores. Credit cards are versatile enough to suite small stores as well as large corporations. There is not one standard terminal that all merchant must use, rather some stand-alone terminals are used while some terminals are integrated into a companies existing system.

- Accessibility and Ease of Use Nearly all large retail stores and most small stores take credit cards. Nineteen million merchants accept the Visa credit card[3]. Using a card is very simple. For transactions like the one in our example that take place in person, one merely has to hand their card to the store clerk and sign a receipt. For transactions that take place over the phone or online, one has to speak or type in their credit card number and its expiration date.

- Freedom and Applicability without an Undue Burden As a result of the required verification process, one must give up more information than just their account number to partake in a transaction. As our example points out, one must sign a receipt that the merchant keeps a copy of. Since one's name usually appears on a credit card and also on the transaction receipt, there is potential for misuse. To counter this problem, credit card companies have begun to introduce smart chips, which require a pin number for verification instead of a signature.

[3] http://www-s2.visa.com/pd/consumers/us/main.html

- Cost Credit cards are generally free to use for consumers, though merchants are charged a transaction fee, which is arguably passed on to consumers.

- Degree of Information Distribution and Security The information that is put on credit cards and additional identifying information (address etc) is on a secure database that is accessible only by the credit card companies. Merchants are only told if the transaction that is being requested is approved or not. The target of attack is undoubtedly the credit card companies' database.

- Trust and Confidence in the system Most people are not hesitant about using credit cards. To alleviate the fears of those who have any hesitations towards using a credit card, most companies place a limit or eliminate the cardholder's liability in cases of misuse. For example, Visa has introduced its 'Zero Liability" policy, which frees cardholders from any liability in cases of unauthorized use. [4]

## 5.3 Social Security

In 1935, the federal government created a federal pension program, called Social Security[5]. The government distributed Social Security cards, which had a name and a distinct number on them, to workers and used the Social Security numbers (SSNs) to track contributions to the pension fund and to distribute pensions proportional to the contributions. Since "no one wanted to miss out on a government pension, of course, and there was no need to show any proof of identity in order to register' nearly everyone signed up for card.[6]

Over the years, the use of Social Security Numbers has greatly expanded. In 1943, President Franklin D. Roosevelt signed Executive Order 9397 requiring federal agencies to use the Social Security Numbers for identifying individuals in any new "system of accounts."[7] Within thirty years of the signing of Executive Order 9397 by Roosevelt, the IRS, state tax authorities, the Medicare and Medicaid programs, the military, and financial organizations were all using SSNs as unique identifiers. Today, it is quite difficult to function in America without the use of a SSN. From applying for a job to receiving welfare benefits, from creating an account to checking one's credit, SSNs are

[4] http://www-s2.visa.com/pd/consumers/us/main.html

[5] http://www.ssa.gov/history/history.html

[6] p. 287, Smith, Robert E., "Ben Franklin's Web Site"

[7] pgs. 289-290, Smith, Robert E., "Ben Franklin's Web Site"

used as identifiers in every aspect of life. In many cases, even though Social Security cards have been distributed without proof of identification, they are used for proof of identification.([8]

To illustrate this point, we employ the common example of receiving one's medical records. In this example Alice wants to obtain her medical records. Alice calls up her hospital to inquire about the results of her throat culture. As a security measure, the receptionist at the hospital asks for Alice's Social Security Number. Alice, having provided this information, is told that her throat is not infected.

### 5.3.1 Trust Model

The Social Security Administration (SSA), through 12 units that are organized by geographical regions, issues cards and stores records in a single universal index. [9] The SSA credits Social Security taxes that it receives to the account associated to the SSN designated by the person who sends in the Social Security taxes. At the appropriate time, the SSA sends pensions to the person and address assigned to a specific SSN.

### 5.3.2 Policy Analysis Based on Criteria

- Privacy: Intended uses

  When analyzing privacy in this section, we mean to analyze the privacy concerns a user might have to apply for a social security card, and when he only uses it as it was intended to. However, in the next section, we will discuss the privacy concerns about the misuse of social security numbers.

  **Access to information** The user has access to the information reported to social security, since his company reports to him at least through pay stubs.

  **Ability to correct erroneous information**

  The user is able to correct the earnings reported if he discovers an error with the pay stub. He is also able to change information about name, if he had legally changed his name.

  **Know the purpose that the information is collected** The declared purpose of the Social Security number is used to keep a record of a user's earnings, and this is made clear to the user.

[8] pgs. 289-293, Smith, Robert E., "Ben Franklin's Web Site"

[9] pg. 289, Smith, Robert E., Ben Franklin's Web Site

**Minimize the information collected** The information collected about the individual during this process is already minimal. Security of the information collected The privacy of your records is guaranteed by the social security administration.

They will not be disclosed unless law requires the disclosure to another government agency, or the information is needed to conduct Social Security or other government health or welfare programs.

**Accountability** The social security administration guarantees the privacy of their records, and should be held responsible if there is a security breech.[10][11]

- Privacy: Misusing Social Security Numbers **Information that is in a social security number alone** The nine-digit Social Security number is divided into three parts. The first three digits are the area numbers. These digits originally indicated the state where you applied for your first card. Now it is derived from the ZIP code in the mailing address on your application for a card. The middle two digits are the group numbers. They have no special geographic or data significance but merely serve to break the number into conveniently sized blocks for orderly issuance. The last four digits are the serial numbers. They represent a straight numerical sequence of numbers within the group.

  Therefore, by revealing the social security number alone, the user is at least giving a clue about the state or zip code he is from.

  **Information that is in a social security number using databases** A social security number is often used as a method of identification. Therefore, through a social security number, companies can merge databases and potentially share a wide variety of information about the user. As a simple example, credit bureaus often share information with one another, and they could use the social security number and some other information as a means of identifying the user whose information is shared.

  As another example, landlords often request social security numbers from prospective tenants. They have two reasons for doing this. Firstly, they may want to do a credit check to make sure that the tenant can pay the rent. Secondly, they may want to check a database of ”bad tenants” as reported by other landlords. In some areas, it is hard to evict a tenant without a lengthy legal process, and so the landlords do have an interest to do this. There is probably no

[10] Social Security Administration FAQ: http://www.ssa.gov/pubs/10002.html

[11] CPSR FAQ: http://www.cpsr.org/cpsr/privacy/ssn/ssn.faq.html

law that restricts the use of such a database.

However, there are some consequences for a tenant. For example, a prior tenant might give an incorrect social number, or a landlord could report an incorrect "bad" number. This could affect an innocent person trying to find a place to stay. There is no way that person could have access to the information because he does not know which database the landlord will use. For that reason, he will not be able to correct erroneous information. Even if he discovers a database which erroneous information, it is not clear if he can easily correct such information. That would depend on the policy of the database provider.

**Problems with not providing social security numbers** The obvious solution to such privacy concerns is not to provide social security numbers except for legitimate uses.

In fact, government Agencies that ask for a social security number is bound by the Privacy Act of 1974[12]. A government agency that asks for a social security number is required to provide a Privacy Act Disclosure Note. This will disclose what the law allows them to ask, whether the provision of the number is mandatory and the consequences of not providing the number.

Unfortunately, there is a lack of legislation to provide the same protection for the private sector. Individuals or companies that ask for a social security number Private companies are not affect by the Privacy Act, and the user can only look for some one else to do business with.

For the landlord example, the applicant can refuse to supply the number, but in a seller's market such as in Boston, the landlord can choose from many other applications and is not affected or compelled to change his policy. On the other hand, the applicant may be in trouble if it becomes a norm that all landlords in Boston want to check through the database of "bad tenants" which is filed by social security number.

Furthermore, the choice of not dealing with a company or individual that insists on a social security number is not sufficient. There are gray areas, such as when a tenant is willing to provide the social security number for a credit check, but is unwilling or does not know that the same number will be used for other purposes. Ideally, laws should be passed to at least make it madatory for commercial requests for a social security number to be followed by a disclosure of what the number will be used for. In this way, the tenant will at least be aware of database checks other than a credit check.

**Relevant Bills proposed** Representative Bob Franks has introduced HR 1287, the Social

[12] Privacy Act of 1974 and Amendments

Security On-line Privacy Protection Act, which prohibits ”interactive computer services” (such as Lexis-Nexis) from disclosing social security numbers or using them as a method to identify a user to disclose personal information. We will be watching this with great interest.

- Versatility The versatility of Social Security Numbers has greatly outgrown the intended uses. Social Security Numbers, in some cases, as our example points out, are used to authenticate one's identity.

- Accessibility and Ease of Use Anyone who is eligible to work can receive a Social Security card with a Social Security Number. Those who are not eligible to work in the United States can still receive a social Security Card with a SSN but there is a stamp on the card that indicates they are ineligible to work.

- Freedom and Applicability without an Undue Burden When a card is used for authentication or as an identifier, only one's Social Security number is usually needed. There are very few instances when the Social Security Card must be shown in person. In these instances, the information that is required is usually at least the information that is on the Social Security card. For example, one usually has to show a valid social security card to prove that he or she is eligible to work when applying for a job. One's employer will need to know your name, your social security number, and will need your signature on the employment contract, so seeing it on your card will not make that much of a difference.

- Cost There is no cost to the consumer to get a card though there are substantial administrative costs that are paid for using tax monies.

- Degree of Information Distribution and Security The Social Security program is administered through 12 units, which house data about the cards they distribute. This data is compiled in a universal index. The twelve units and the universal index are vulnerable to attack. More importantly, since the SSNs are used in thousands of databases, there are thousands of potential points of attack.

- Trust and Confidence in system Since the use of Social Security Numbers is so vast, one must gauge the public's trust and confidence of the use of SSNs on a case-by-case basis. People are generally confident that when they pay their Social Security taxes using their number that they will be credited for the contributions that they make. The public is reluctant, however, to use SSNs as identifiers and tools of authentication in other settings like hospitals or banks because of recent high profile cases of identity theft, where using stolen Social Security numbers criminals have been able to set up fake accounts and access the medical records of individuals that have had their SSNs stolen.

## 5.4 Public Key Cryptography

There are several Public Key Infrastructures in use today. We present the three most prevalent infrastructures: Pretty Good Privacy (PGP), and Simple Distributed Security Structure/Simple Public Key Infrastructure (SDSI/SPKI) and X.509, evaluate each infrastructure based on the defined policy criteria, and highlight some of the technical deficiencies that are present.

### 5.4.1 PGP

Pretty Good Privacy, a public key cryptography program developed in early 1990s for use with email, is used to encrypt and sign messages[13]. Today, people primarily use PGP for secure email communication. To use PGP, each user maintains a key ring, a list of public keys of people the key ring holder corresponds with. Each user (key ring holder) signs his key ring with his own private key to reduce the risk of tampering. Users have the ability to exchange key rings to increase the number of public keys on their key ring and the numbers of people they can securely correspond with[14].

Since PGP is mainly used for email, users typically exchange an email address, a public key value, and a degree-of-trust attribute. For example, when placing Bob's public key on her key ring, Alice assigns of one of four degree-of-trust attributes to Bob's public key[15]:

- Completely Trusted: Anyone that Bob trusts, Alice trusts (If a key is signed by Bob, Alice trusts it).
- Marginally Trusted: Anyone that is trusted by Bob and another marginally trusted individual, Alice trusts (If a key is signed by Bob and another marginally trusted person, Alice trusts it).
- Untrusted: Alice does not trust Bob (If a key is signed by Bob, it does not make the key any more credible).

[13] http://www.cypherspace.org/ adam/timeline

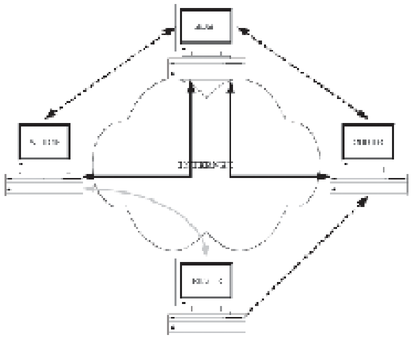
[14] Branchaud, M. "A Survey of Public-Key Infrastructures", http://home.xcert.com/ marcnarc/PKI/thesis/title.html

[15] Branchaud, M. "A Survey of Public-Key Infrastructures", http://home.xcert.com/ marcnarc/PKI/thesis/title.html

- Unknown: Alice does not know Bob well enough to make a trust judgment (If a key is signed by Bob, it does not make it any more credible).

### 5.4.2 PGP in Practice

To show PGP in practice, a simple example of PGP trust network based off of Marc Braunchaud's example in his 1997 thesis entitled *A Survey of Public-Key Infrastructures* is provided (Figure 1):



In this example and all other PGP interactions, some offline transactions, known as *out of bound transactions*, must take place (these transactions are represented by dashed arrows in Figure 1). In our example, such a transaction takes place when Bob and Alice physically meet and exchange their public keys. At another time Bob and Chris also meet offline and they exchange their public keys. And at yet another time, Chris and Elvis meet offline and Elvis gives his public key to Chris. At this point, Alice has Bob's public key, Bob has Chris' public key and Alice's public key, Chris has Bob's public key and Elvis' public key, and Elvis has no one else's public key.

In order to obtain more public keys to securely communicate with more people, users of PGP exchange their key rings using online transactions (these transactions are represented by solid black in figure 1) Such a transaction takes place when Bob and Chris exchange their key rings online. Since Bob and Chris previously met offline and exchanged public keys, they can securely exchange their key rings using RSA encryption. At some point after Bob and Chris' exchange, Bob and Alice exchange their key rings. Since Bob and Alice previously meet offline and exchanged public keys, they can also securely exchange key rings. At this point, Alice's key ring has Bob, Chris and Elvis' public keys on it, Bob's key ring has Alice, Chris and Elvis' public keys on it, Chris' key ring has Elvis and Bob's public keys on it and Elvis' key ring has no one else's public key on it.

Alice can now securely communicate with Bob, Chris and Elvis, since she has all of their public keys. We use a thick gray arrow to show one such communication occurring between Alice and Elvis (Figure 1)

### 5.4.3 Trust Model

As more and more users trade key rings, they obtain more and more public keys that are passed to them from different sources, creating what is called a "Web of Trust" Since each user assigns a degree-of-trust attributes to other users, each user is in effect his own root Certification Authority[16].

### 5.4.4 Policy Analysis Based on Criteria

- Privacy PGP can be used as a tool to protect the privacy of a communication. Such communication can be messages such as in Electronic Mail, or it can even be phone conversations through PGP Phone. [17]

  PGP's intent is to link a cyber-identity with the actual person in real life. Therefore, the standard framework of whether the user has access to the information does not apply. The receiver of the communication already knows the individual or traits of the individual, and is not only trying to ensure that the sender of the communication is from that person himself.

  The privacy of the communication is protected by encryption schemes, such as RSA. Furthermore, since the code is open-sourced, it can be argued to be fairly robust. However, the later sections will describe some privacy pitfalls.

- Versatility PGP's versatility is somewhat limited. Looking at our example, when Alice communicates with Elvis, she is relying on the word of Chris, someone who she has never met. As the number of people in the PGP network increases, so do the number of interactions with people Alice does not know or necessarily trust.

- Accessibility and Ease of Use PGP is quite simple to use. A freeware copy of the PGP software is available for download at http://www.pgpi.org/. Though the software is simple to use, it's size(7MB) and the necessity to download it burdensome for dial up users to have access to.

- Freedom and Applicability without an Undue Burden In a PGP based system, one decides whether or not he wants to distribute his own private key. A determination of what information, if any, to distribute through email correspondence can be made on a case-by-case basis.

[16] Branchaud, M. "A Survey of Public-Key Infrastructures", http://home.xcert.com/ marcnarc/PKI/thesis/title.html

[17] Available at http://web.mit.edu/network/pgpfone

- Cost There is no cost to the consumer to get the basic version of PGP, though more advanced versions need to be purchased. Since there is no controlling entity, there are no costs for the administration of the system.

- Degree of Information Distribution and Security Individual users safeguard their own private keys that are associated to the public key that they distribute. Every individual user of PGP is vulnerable to attack. Going back to our example, if Elvis' private key was somehow comprised, someone could pretend to be Elvis when communicating with Alice, Chris, or Bob.

- Trust and Confidence in systemMany people use PGP since its free, and open source

## 5.5 SDSI

Simple Distributed Security Infrastructure (SDSI) is a credential based Public Key Infrastructure developed to create a system based on credentials rather than identity. Instead of attaching a key to an identity, a SDSI entity is a key itself. The SDSI entities (known as principals) are defined as digital signature verification keys. The SDSI principal issues verifiable signed statements for the individual controlling its associated private key. The use SDSI, principals issue statements in the form of one of three types of certificates:[18]

- Name-binding certificate: A name is bound to some value (typically the principal)

- Group-membership certificates: A group association is bound to the principal

- Identity certificates: An identity is bound to the principal

When a principal creates a name-binding certificate, the "name is said to exist in the principal's *local name space*"[19] Each principal has the ability to create his own names in referring to other principals since local names spaces can be linked together. For example, Alice and Elvis may both have two completely different principals that they refer to as Chris in their local names spaces. Alice can refer to a principal in her local name space as Chris and Elvis can refer to a different principal in his local name space as Chris. To Alice, the Chris is Elvis' local name is Elvis' Chris while to

[18] Branchaud, M. "A Survey of Public-Key Infrastructures", http://home.xcert.com/ marcnarc/PKI/thesis/title.html

[19] Branchaud, M. "A Survey of Public-Key Infrastructures", http://home.xcert.com/ marcnarc/PKI/thesis/title.html

Elvis the Chris in Alice's local name space is Alice's Chris. This chain of reference can been further extended. For example, Elvis may define a principal as Alice's Chris's Joe.[20]

"SDSI achieves this name linking because it has an 'online' orientation. Principals that issue certificates are assumed to be able to provide an on-line Internet server to distribute those certificate upon request."[21] For Elvis to find out which principal is behind Alice's Chris, he can connect to Alice's server and request from Alice's server the name-binding certificate that defines the name Chris.

Each principal can also define groups. To create a group, a principal must give the group a name and a set of members. This set of members can either be other principals or other groups that have been created by other principals that are referred to using a system similar to the local name space linking system described above.

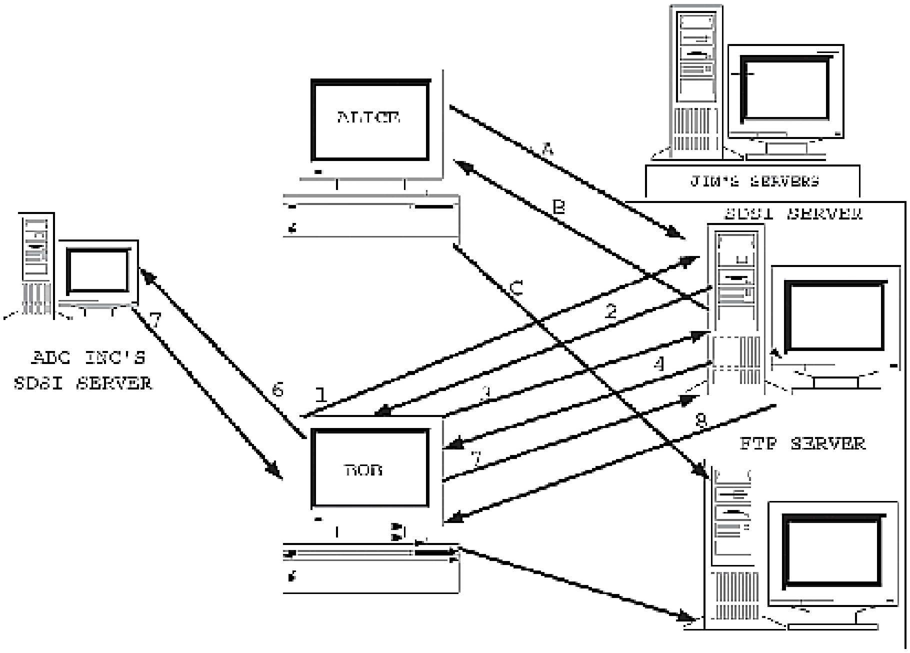
### 5.5.1 SDSI in Practice

In 1999, an Internet working group created a standard for the Internet called Simple Public Key Infrastructure (SPKI) by which the SDSI standard for attaching credentials to public key values could be implemented on the Internet.[22] To illustrate such an implementation, a SDSI/SPKI taken from Marc Braunchaud's 1997 thesis entitled *A Survey of Public-Key Infrastructures* is provided (Figure 2).

[20] Branchaud, M. "A Survey of Public-Key Infrastructures", http://home.xcert.com/ marcnarc/PKI/thesis/title.html

[21] Branchaud, M. "A Survey of Public-Key Infrastructures", http://home.xcert.com/ marcnarc/PKI/thesis/title.html

[22] ftp://ftp.isi.edu/in-notes/rfc2693.txt



In this example, Jim has an FTP server that he wants to give his friends and fellow employees at ABC Inc. access to. Jim creates two groups in his SDSI server: friends and ftp-users. ABC Inc. creates one group in its SDSI server named employees and places the principals Bob and Jim in the group. Jim places three principals in his friends group: Alice, Hal, and Danny. In his ftp-users group, Jim places his friends group and ABC Inc.'s employees group. For one to be an ftp-user that is able to access Jim's server he must be a member of Jim's friends group, ABC Inc.'s employees group, or both. The SDSI/SPKI system uses protocols in which messages are exchanged. In this example, Alice and Bob will be using the Membership and Get protocols to access Jim's Ftp server[23].

- Alice, Jim's friend, accessing Jim's server: For Alice to gain access to Jim's server, Alice sends a Membership.Query message (Arrow A) to Jim's SDSI server specifying her principal and the group name ftp-users. By sending this message, Alice is requesting a certificate stating the status of her membership in the group ftp-users. Jim's SDSI server now replies either with a status of true (Alice is a member), false(Alice is not a member) or fail(Alice might be a member, but the computer needs more credentials to determine her membership).

  In Alice's case, since Jim has a principal named Alice that matches the principal in the Membership.Query message and is a member of Jim's friends group, Jim's SDSI server replies with a true certificate for Alice's principal (Arrow B). Alice then uses this true certificate to access Jim's ftp-server (Arrow C)

[23] Branchaud, M. "A Survey of Public-Key Infrastructures", http://home.xcert.com/ marcnarc/PKI/thesis/title.html

- Bob (an employee of ABC) accessing Jim's server: Like Alice, Bob sends a Membership.Query message to Jim's ftp-server, yet since Bob is not in Jim's friends group, Jim's SDSI server replies with a fail membership certificate along with a message stating that if Bob can show that he is a member of the ABC's employees group, he will be considered a member of the ftp-user group(Arrow 1). To find out which principal Jim has named ABC, Bob sends a Get.Query message to Jim's SDSI server(arrow 3) which requests all of the name binding certificates on Jim's SDSI server that specify the local name ABC. Jim's SDSI server sends Bob a certificate stating that Jim's local name ABC refers to ABC Inc.'s principal. (Arrow 4)

  Bob now sends a Membership.Query to ABC Inc.'s SDSI server specifying his principal and the group employees (Arrow 5). ABC Inc.'s SDSI server now replies with true membership certificate, since ABC Inc has a principal matching Bob's principal (Arrow 6). Bob next sends this certificate, along with a Membership.Query message, to Jim's ftp-server (Arrow 6). Jim's server returns a true certificate (Arrow7) which bob uses to access the Jim's ftp-server (Arrow 9).

### 5.5.2 Trust model

Since users decide which groups to allow into their system, each principal acts as their own Certification Authority. There is no CA hierarchy placing one CA over the other, each principal is equal in authority. Like a PGP system, a principal defines groups in terms of other principles (e.g. ABC's employees) developing the previously defined "Web of Trust".

### 5.5.3 Policy Analysis Based on Criteria

- Privacy In this section, we assume that SDSI is used by companies and individuals to authenticate one another, and to prove attributes such as age or membership to an organization.

  **Access to information** The user has access to information stored on the SDSI certificate, which he can clearly read from one principal before submitting it.

  **Ability to correct erroneous information** The ability to correct erroneous information is not within this framework. The user will have to contact the principal issuing the certificate itself to do this.

  **Know the purpose that the information is collected** The purpose is usually clear, and can be described in the descriptive format of the certificate.

**Minimize the information collected** Unlike X.509, a person can have many certificates from the point of view of many principals. Therefore, in that sense, information provided can be minimized. When Alice wants to access Bob's FTP server, for example, she only has to obtain a certificate from MIT to prove that she is in fact a student at MIT. That certificate will not reveal other information about her. For example, she could be a member of the Middle Eastern Belly Dancing Group, but that attribute will not be on the MIT certificate. When going to clubs, she can show a membership certificate from the Middle Eastern Belly Dancing Group to get a free drink, but no one at the club will be able to know she is actually an MIT student (and think of her as a nerd). Security of the information collected The privacy of the communication is protected by encryption schemes, such as RSA. The technical pitfalls are discussed later.

**Accountability** Accountability is present, but may be a little complicated. Since the certificate may go through a series of principals, it takes some effort to find out who in the chain made a mistake. However, it is still possible.

The responsibility may be unclear. The receiving party relies on the issuing party, but the issuing party may not have a formal contract with the receiving party, nor may it be a reputable company with enough assets to pay damages. The receiving party can therefore be partly to blame if it accepts a certificate with a dubious link in the chain of claims.

- Versatility In terms of versatility SDSI/SPKI passes with flying colors because it is a very descriptive AIKM system. SDSI/SPKI has many customizable fields where you can put information so adept in various settings. The semantics in SDSI/SPKI are more descriptive than in X.509.

- Accessibility and Ease of Use SDSI/SPKI is not as easy to use as X.509. In order to obtain authentication, SDSI/SPKI requires many network connections to be set up in the web of trust. This causes the performance to be much slower than X.509 where the certificates of each CA does not need to be checked every time.

  Next, the multiple perceptions of SDSI/SPKI is potentially confusing. In X.509, the user may be asked to accept Microsoft's software. In SDSI/SPKI, the same user will be asked to accept XYZ's Microsoft, and then have to understand that XYZ may not be a trusted CA. The user can therefore be misled into accepting code easily, if a malicious XYZ recognizes a malicious entity that pretrends to be Microsoft.

- Freedom and Applicability without an Undue Burden SDSI/SPKI is a credential-based system; one does not need to reveal his identity to be authenticated. While identities can be tied to principals, they do not have to be and usually are not. As long as your principal matches the principal that is authorized to take the action you want to take, you are granted what you request. Since the user is not required to reveal more than is needed, there is little undue burden to the user.

- Cost The technical cost of SDSI/SPKI is low because issuing certificates is free; No one has to pay a CA for them.

- Degree of Information Distribution and Security The information in SDSI/SPKI is distributed over many principals. For this reason, it is secure because it is hard for a hacker to accumulate a lot of information about each user from all the different principals.

  However, on the other hand, since the information is distributed over many principles, more entities are given the information than X.509. As an analogy, X.509 is a system where all your information is given to an omnipotent “tiger”, while in SDSI/SPKI your information is broken into pieces and sent to a “pack of wolves”.

- Trust and Confidence in System In SDSI/SPKI the distributed information leads to web of distributed trust. If something gets compromised, there are ways to track down the individual. Due to the distributed nature, not all principals are created equal. Companies are afraid because there is no one person to sue. Furthermore, because unlike a major CA, which has the capital and standing to be sued, the individual users in a shared web are not well funded and thus it is difficult to collect large, class-action compensations for privacy violations.

## 5.6 X.509

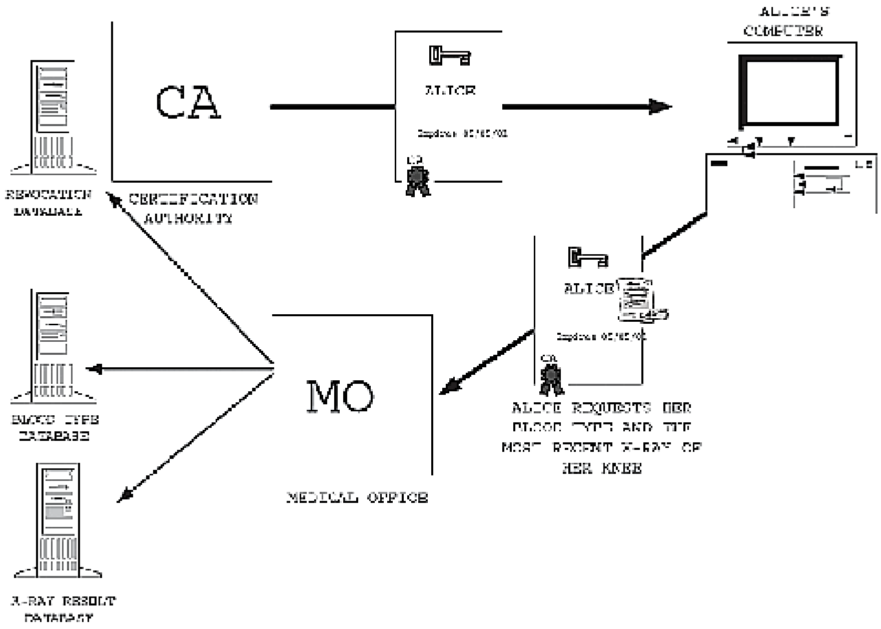
### 5.6.1 X.509 in Practice

X.509 is a Public Key Infrastructure designed originally for use with the X.500 directory, a directory similar to a telephone directory where using a persons name; one can find other information about that person. X.509 was originally created to authenticate entries in an X.500 directory, but is used today primarily to authenticate identities. In an X.509 system, an entity called a Certification Authority (CA) binds a public-key to a subject’s identity and issues a certificate. To obtain a certificate, the subject must usually visit the offices of the CA in person with a valid form of identification. The subject holds the associated private key. The holder of a certificate can use the certificate to communicate securely with any relying party (CA or user) who trusts the certificate issuing CA. A certificate that is issued by a CA typically contains:

- Key policy and information: The CA can include the information about the specific policies that were followed when the certificate was created (This information typically gives the potential relying party enough information to determine whether the certificate is suitable for a particular purpose).
- Certificate Revocation Lists with reason codes: This is a list of certificates that have been revoked by the CA and the reasoning behind why they have been revoked (e.g. associated private key has been compromised, certificate was wrongly issued).
- Alternative Name: The CA can attach alternative names for both the subject and the CA to the certificate.
  - Version
  - CA's Name
  - Issuer's
  - Serial Number
  - Validity Period
  - unique identifier
  - CA Signature Algorithm
  - Subjects Public-key
  - Subject unique identifier

To best illustrate the role of a CA and the certificates it issues in an X.509 based example, we present an example based off of an example from a white paper entitled *Private Credentials* by Zero Knowledge Systems[24] (Figure 3):

[24] www.zks.net

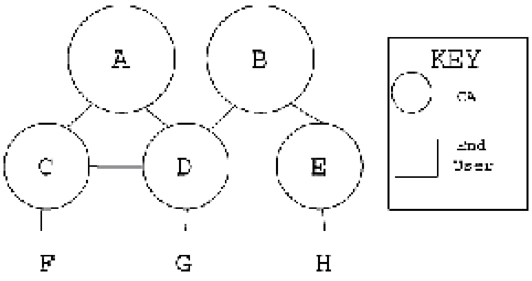


In this example, Alice visits a Certification Authority where she is issued a certificate that binds a public key to his identity. Alice keeps this certificate along with the private key corresponding to the public key bound to Alice's public key by the CA on his computer. Alice signs this certificate using his private key and uses the certificate to send an encrypted request to the Medical Office. The medical office needs to verify one's identity before giving out any information. The Medical Office looks at the certificate and realizes a CA that it trusts has issued that certificate. The Medical Office then turns to the CA and checks to see if Alice's Certificate is on the CA's Certificate Revocation List (CRL). Seeing that Alice's certificate has not been revoked, the Medical Office provides Alice the information that she requests in her encrypted message, her blood type and the most recent X-Ray of her knee.

### 5.6.2 Trust Model

In 1995, an Internet working group created a standard for the Internet call PKIX by which the X.509 PKI basic infrastructure was expanded for use on the Internet[25]. Since it is unrealistic for there to be one CA governing the whole Internet, X.509 systems using multiple CAs have been set up. An example of one such possible hierarchy is presented below (Figure 4)

[25] http://www.ietf.org/html.charters/pkix-charter.html



In this example, there is a basic hierarchy present, with 2 CAs at the top of the hierarchy. The end users are represented by squares, while circles represent the CAs. In general, each node on the chart relies on the node(s) above it to verify its identity. In our example, there is one exception to the general hierarchical model: the CAs C and D can verify each other's identities even though they are on the same level. This action is generally referred to as cross-certification. As a result, if end user F wants to communicate with end user G, he can either follow the certification path F-C-D-G or F-C-A-D-G. When more than one CA is present an additional feature is added to the certificate issued by the CA called a certification path constraint. The certificate path restraints details any restrictions that certificate issuing CA has placed on the authorization path. For example a CA might restrict a path to a given domain and allow certification along the path by CAs who follow a particular set of policies. In this way, the relying party is aware of the boundaries and policies of the path within which a subject was authorized[26]. Overall, the trust model is hierarchical. One has to rely an authority (CA) to authenticate users.

### 5.6.3 Policy Analysis Based on Criteria

- Privacy There are many different implementations of X.509. For fault, there can be modifications to prevent the fault. In this discussion, we will focus on the current privacy concerns with current implementations of X.509. There is no doubt that changes for the better are always possible.

  **Access to information** The user has access to the information, since the information is detailed in the certificate.

  **Ability to correct erroneous information** The ability to correct erroneous information is not within this framework. The user will have to contact the CA issuing the certificate itself

[26] Branchaud, M. “A Survey of Public-Key Infrastructures”, http://home.xcert.com/ marc-narc/PKI/thesis/title.html

to do this. However, there is a good framework to revoke certificates that has been issued.

**Know the purpose that the information is collected** The user knows this, since the information is detailed in the certificate.

**Minimize the information collected**

This is not always possible with X.509. Since each certificate has a unique name, a CA will often be required to putmuch information about the person on the certificate. For example, they may put a person's age and address on a certificate.

In accessing a porn site on the Internet, all that is really required is proof of age. However, in giving the certificate, the user will have to give information about his address, as well as age, and this exposes the user to obtain unwanted mail for example.

The solution is to have certificates for each attribute. A better solution can be found in Brands' thesis, where he detailed how certificates can have attributes blanked out.

**Security of the information collected** The privacy of the communication is protected by encryption schemes, such as RSA. The technical pitfalls are discussed later.

**Accountability** The CA can be held liable for mistakes. However, the liability is capped by agreements that the CA made, and is categorized into different classes of liability.

- Versatility In terms of versatility, x.509 seems, at first glance to be less versatile than SDSI/SPKI. However, while it is less descriptive. However, the counter argument is that a large amount of information can be place in the x.509 fields, and that information can even include the semantics of SDSI.

- Accessibility and Ease of Use The information contained in an x.509 certificate is shared with only 1 CA, rather than a web of trust as in SDSI. In this respect, each pair in x.509 can be seen as a client-server relationship, whereas in SDSI/SPKI it is more of a peer-to-peer relationship. The privacy of an individual is entrusted only to to the CA who signed his certificate, and to the entities that he choses to present to certificate to.

  In this sense, x.509 is easier to use than SDSI. The user does not need to be confused with multiple certificates. He does not need to make opinions on whose opinions are trustworthy, since he can always find a superior authority that can should trust.

- Freedom and Applicability without an Undue Burden This ease of use is obviously a compromise with the lack of privacy with all a user's attributes being placed on a single certificate. This causes a lot of undue burden for a user that does not want to pass around a wide spectrum of information. He will need to get a certificate for each set of information that he wants to give out, and he will have to solve the restriction of unique names in x.509. We will discuss a better solution in the Private Credentials section.

- Cost Out of all the infrastructures analyzed, those using an X.509 based hierarchy appear to be the most costly since Certification Authorities are required to bind information to a public key in the form of certificate, to verify the authenticity of certificates, and to maintain and distribute Certification Revocation Lists. There are currently a number of private Certification Authorities, like Verisign Inc., that charge the general public, corporations, and the government for their services.

- Degree of Information Distribution and Security As mentioned earlier, information is only distributed to a CA and those parties are entrusted with your private information. However, the information itself is centralized in one certificate and there is much liability upon this select chain to preserve your privacy concerns. Even if they did not request certain information, the certificate certainly contains that information for the taking.

- Trust and Confidence in system While trust in the X.509 system is debatable, companies tend to instill trust and confidence in X.509 on the grounds that there is a specific chain of trust and moneyed parties involved. Thus, if a confidence is compromised, there is some financial backing and the ability to hold someone liable for privacy violations, sue and collect reasonable sums of money. On the other hand, there are individuals who despise such companies having so much power with one's information.

  Therefore, there seems to be a disparity between what individuals prefer and what companies prefer. As a thesis, we propose that individuals socialize in groups with no hierarchy. The web of trust is a better model of how they interact, and SDSI will be the system they choose for authentication amongst each other. On the other hand, companies are hierarchical. They are used to have a superior entity at every stage, and therefore will naturally chose x.509.

# Chapter 6

# Private Credentials

In this section we will introduce the private credentials approach to identification and authentication. Private credentials are still a subject of active research so there are no concrete examples of deployed systems to analyze. However, the cryptographic foundations of private credentials, which are independent of any particular implementation, can be examined from a privacy standpoint.

The implementation of on-line authentication and identification has created new opportunities for identity/credentials theft and privacy violations. For example, online databases are easy to access, computers are more likely to leak information, and the ease of logging means that often entire credentials transactions are stored in an easy to re-play format. However, many of these transactions can be improved upon from a privacy standpoint by using privacy enhancing technology such as private credentials. There are some cases in which private credentials not only improve upon the authentication method currently used on-line, but may improve upon the authentication methods we use in day-to-day life, like passports, credit-cards and written signatures.

## 6.1 Why Private Credentials?

Many of the commonly-used authentication systems we have examined so far in this report, such as PGP, SPKI, and X.509 rely primarily on identity to perform credentials transactions. For example, the PGP introduction system involves known or trusted users signing the keys of unknown or untrusted users, essentially saying “this key really does belong to this person.” X.509 works in a similar manner, using a more strict hierarchy for trusted signatures. However, in both systems, no other information is exchanged. Assuming that private keys remain private, an observer can identify an unknown person by asking them to prove that they possess the private key that is uniquely tied

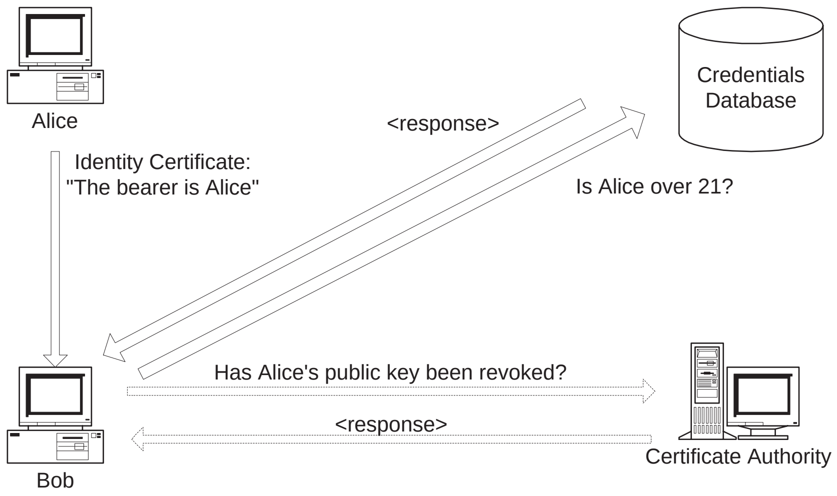


Figure 6.1: This diagram shows a typical identity-based credentials-proving transaction. Bob is interested in determining Alice's age. First, he acquires her public key. Then he makes Alice prove that she is the owner of the matching private key. (Bob may contact a CRL, in the case of X.509, to determine if Alice's key is known to be abused.) Lastly, he contacts a database, perhaps with Alice's permission, to find out her age.

to the public key that is tied to their identity. These systems do not allow us to prove any other property about the individual. To prove other credentials, both parties must depend on some trusted database that contains that data. Unfortunately, reliance on databases or their querying, even their very existence presents disheartening technical and privacy risks. Among the technical risks is the problem that the data in the database could be incorrect. Even if the user were to find out about the error, it may be difficult to amend or correct. There is no guarantee that these databases are reliable or available; they may also be outdated or require payment for access. Privacy concerns include risks of database hacking, data "leaking," mergers (i.e. ToySmart) or database linkage (i.e. DoubleClick and Abacus).

### 6.1.1 Current Privacy Threats

There are many privacy risks that are taken on by both parties in the transaction shown by Figure 6.1.

Bob loses privacy because she is revealing to the database the sort of information he is looking up and that he is interacting with Alice. If Bob contacts the CRL to inquire about the validity of Alice's key, the CRL can also find out that he is talking to Alice. Alice has an even greater privacy loss, as she must to reveal his identity and public key to Bob. Granted, she needs to give Bob some sort of information (her age), but that is not related to her name. The database must know her age, so that it can tell Bob, and also knows that she is trying to prove her age to Bob. Of course, once this information has been released, it may be stored forever, linked with other data or handed off to other parties. Often there are privacy policies in place that protect our data, but this is not always true. Even worse, the policies that do exist may not cover the cases we desire or the data is leaked unintentionally.

From a purely theoretical and technical point of view, there is a lot of unnecessary/excess information that is being released in this transaction. It may be that Bob is only interested in learning Alice's age, a credential that he may want authenticated by a trusted authority. Certificates in the form of X.509 and PGP can therefore be classified as 'identity-proving.' Private credentials do not rely on identity but instead are purely 'credential-proving' where by credential we may mean a trait, feature, characteristic, etc. By using a private credential, Alice may prove her age to Bob without having to prove her identity and without leaking information about the transaction to other parties.

### 6.1.2 Current Security Threats

The use of identity certificates for credentials-proving has many security threats as well, stemming from the overuse of identity as a stepping stone for credentials. That is to say, because every credentials-proving transaction undertaken hinges on the authenticity and ownership of a single private key, the owner of that key ends up placing all his eggs in one basket. If that key is ever lost or stolen, the proper owner ends up losing all of his credentials at once.Even though this is a clearly risky behavior, it has proven to be extremely popular because of its ease of use.

We can categorize identity certificates as a skeletal single sign-on authentication mechanism. By this we mean that once a user has proven their identity via a single 'identity credentials' transaction, they no longer have to formally prove any other credentials; all of that information is harvested from databases Single sign-on systems have low costs and are very flexible. They are easy to implement and use because there is only one point at which a user is actually authenticated. However that also means that there is a single point of failure. For example, users of Microsoft's *Passport* log into a server with one password which allows them to download a cookie that then identifies them to any Passport partner web-site. But now any user who can get that cookie can perform a complete identity theft within the Passport realm.

Identity theft is a criminal act resulting in privacy loss. One way in which a criminal can commit identity theft in the real world is by learning the name and social security number of his victim. Since these two pieces of data are often used as unique identifiers and authenticators, the criminal can apply for fraudulent credit cards, access bank accounts, etc. In analogy to our example of credential-proving using X.509, we can think of the victims name as the identity, the SSN as the key-pair (both the public and private key) and the Federal directory of SSNs as the certification authority. True, the given SSN matches to the name, but there is no check to see if the person making bank-transfer requests is really the identified person. For these reasons, social security numbers are clearly a poor authentication method.

It is impossible to completely defend against identity theft, but using credentials instead of single sign-on will cut the losses on any particular case of theft.

### 6.1.3 Imposing Threats

Of course, the use of SSNs is an overly simplistic identification method. Americans use many other identification methods with greater assurance of authenticity, such as drivers licenses and passports. Say Alice is trying to prove her age to Bob, who works in a liquor store. She will likely present one of these pieces of identification, which have her picture, age and name imprinted on them. If Alice ends up revealing all this information just to make a simple purchase, why isn't this considered a privacy risk? Well, if Alice just flashes her ID, she doesn't leave any evidence of the credentials transactions. If Alice were to dictate to Bob all of the information on her card who typed it into a computer, she might be less comfortable with the privacy loss (which is even less than that of our identity certificate scenario above). Of course, one doesn't actually do this now, but the creation of smart card IDs and the prevalence of magstripes may result in allowing Bob to quickly capture all of Alice's information. The research done on private credentials may end up branching out of on-line only authentication protocols and become a common ingredient in day-to-day real-life credentials proving.

## 6.2 Technical Overview of Relevant Cryptography

We claimed that we can actually design systems that are privacy enhancing. This claim relies on the data control technology that is afforded to us by recently developed data-management algorithms. These algorithms are cryptographic in nature. Here we provide a general introduction to the cryptographic algorithms used in private credential systems in the hope that it will make these systems easier to understand. Those interested in a more thorough text are referred to *Applied Cryptography*[1] and *Rethinking public key infrastructures*[2].

### 6.2.1 Elements of Public Key Cryptography

The discovery that makes all of this cryptography viable is outlined in *New Directions in Cryptography*[3]. In this paper, the authors describe *asymmetric key cryptography* often referred to as public-key cryptography. The most important properties of public-key cryptography are as follows:

1. A party can distribute a key which can be used to encrypt data in a manner so that only the original party can decrypt the ciphertext.
2. Two parties can exchange secret information without requiring a secret channel.
3. A piece of data can be digitally "signed" by one party so that the signature is unforgeable yet verifiable by any other party. Also, the data cannot be modified without voiding the signature

There are some basic protocols we can design using public-key cryptography to perform authentication, almost all of them rely on all the parties having a private key that they keep secret and a public key that all other parties know. A simple example is one party encrypting a random number with the other party's public key and sending it to them. To authenticate their identity the other party decrypts the message to get the random number, then re-encrypts it with the first party's public key and sends it back. Both parties are assured of that they are talking to the owner of the private key that is tied to the public key they know. (Of course, this means very little; it is more important that we know the "identity" of the public key, a problem undertaken by PKI.)

### 6.2.2 Privacy Concerns

To prove a credential using a trusted authenticator, we simply concatenate the desired credential with the identity of the person we are trying to authenticate and then sign the message with the private key of the authenticator. Assuming private keys are kept private, this system is cryptographically secure: there is no way to forge a credential.[4]

[1] Schneier, B., "Applied Cryptography", John Wiley and Sons, NY, NY, 2nd edition, 1996.

[2] Brands, Stefan A., "Rethinking public key instrastructures and digital certificates", The MIT Press, 2000.

[3] Diffie, W. and Hellman M., "New Directions in Crypt

[4] The assumption that private keys are truly private is often unaddressed by public-key cryptographic systems because of the human factors involved.

However, there are privacy concerns such as linkability and tracability, possible because in current PKI systems, each user has one public key tied to each identity; the unique public key or identity can then be used to index data about the individual. Re-identification is just one of the possible results that can occur when we have traceable/linkable data.

## 6.3 Chaum's Digital Cash

We can start picking away at many of our privacy concerns with the introduction of some cryptographic methods developed after the release of *New directions in cryptography*[5]. For example, Chaum's paper on digital cash[6] is filled with interesting and relevant new concepts in cryptography, such as blind signatures and limited show certificates (related to an earlier work on threshold secret sharing[7]).

### 6.3.1 Technical Overview

A "blind" public-key signature has the same properties as non-blinded ones with an additional benefit: it makes it possible to have data signed without the signer knowing what it is being signed. That means there is no worry about the retention of that data. Basically, blind signatures work by having the party who wants some data signed (traditionally called Alice) "blinding" the data by multiplying it with a large random number $R$ and then presenting it to the signer (traditionally called Bob). Bob signs the file and returns it to Alice who then divides out $R$.

To prove a credential using this system we have to create an analogue to the digital cash protocol. Bob, this time, has a key pair for each credential he wishes to prove. For example, one pair for "Is a US citizen," one pair for "Possesses a drivers license," etc. For example, Alice wants to prove that she is a US citizen: she proves her citizenship to to Bob who is a trusted authenticator. She then presents her public key, which has been blinded, to Bob who will sign it with the private key that bestows "citizenship." Bob returns the signed, blinded message to Alice who then unblinds to reveal her public key signed with Bob's "citizenship" key. Figure 6.3.1 demonstrates how (possibly) off-line communication with a notary has replaced the online database.

[5] New directions in cryptography, 1976.

[6] Chaum, D. "Achieving electronic privacy", Scientific American, Intl. ed. 76-81, August 1992.

[7] Shamir, A. "How to Share a Secret.", Communiates of the ACM, 612-613, November 1979.

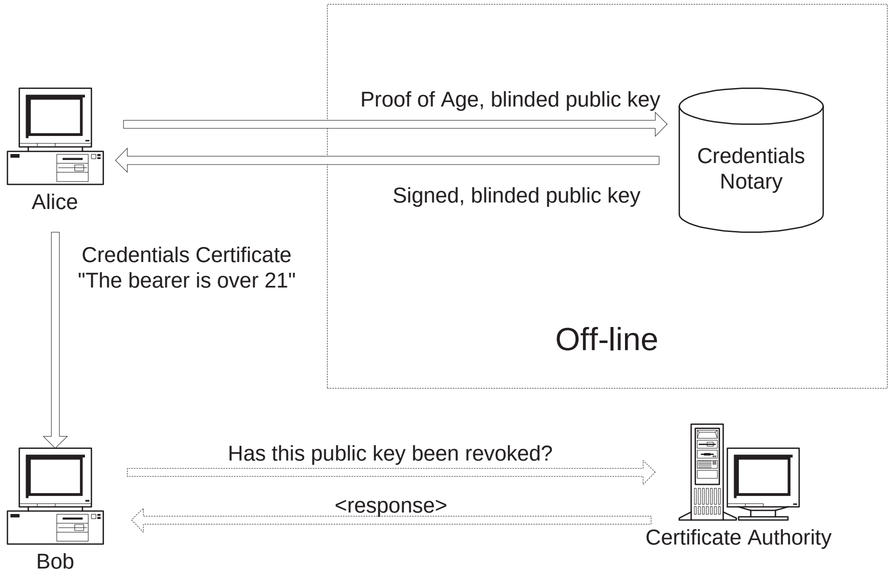


Figure 6.2: This diagram shows a typical anonymous credentials-proving transaction. Alice sends a blinded copy of her public key signed by an off-line notary after proving her age. The notary signs the key and returns it to Alice who unblinds it. Whenever Bob asks Alice to prove her age she presents the certificate and proves her ownership.

### 6.3.2 Evaluation

In this protocol, Bob does not learn the public key of Alice, which reduces her privacy risk. In this example, Alice probably has to reveal her identity because her birth certificate has her name on it, but say we are dealing with a non-identity tied credential. For example, say Alice is buying a ticket to a concert. If she makes her payment in anonymous digital cash or with a service like PayPal, she can receive an anonymous "ticket" from Bob. Also, even if she does have to reveal her identity, her public key can't be tracked around if it shows up elsewhere (linking). More importantly, we've gotten rid of the 3rd party database that keeps all of Alice's credentials tracked with her name or public key. Now we only have a single trusted party, the authenticator.

Unfortunately, in exchange for this increased privacy, we've given up a lot of flexibility. Our credentials have to be descretized so that they may be encoded by a single key. For example, "citizenship" or "allow this person into a concert hall" works well but a date of birth, or name is a lot more difficult. The aforementioned credentials are boolean in nature, either someone has citizenship or they do not. It is not as useful for us to say someone was "either born on Nov. 3rd, 1965" or not when what we really want to convey is the actual date of birth. What we want to say is "this person was born on: MONTH-DAY-YEAR" which is a 'string' credential. Otherwise, just to authenticate date of birth the CA would need tens of thousands of key pairs. The situation becomes even more complicated when dealing with names, which can vary immensely. However, we are definitely improving our situation privacy-wise.

- **Privacy:** As we have already shown, Chaum's digital cash protocol affords us extra privacy against linking and tracking by the Authenticator. We have also removed one party from the equation. However, the party that sees the credential in the end will still be able to track Alice through her public key.
- **Versatility:** We lose some versatility as compared to PKI-styled systems because the sort of data we are encoding in the signature is easiest to handle when it is in a simple boolean format.
- **Accessibility/Ease-of-use:** The system is as easy to use as a non-blinded asymmetric key-pair system and the blinding algorithm is easy to program.
- **Cost:** The cost of this system is basically equivalent as that of a basic PKI system. The authenticator has to create and use many more keys which may or may not be a revocation problem (depending on how they are stored). Of course, the cost of having a third party database is now unnecessary.
- **Security:** We have increased security because we no longer have a third party database.
- **Trust and Confidence in System** The verifier doesn't even realize the message was blinded so there is no less confidence. There is no security gained by having the authenticator knowing Alice's public key.

## 6.4 Private Credentials

There is much ongoing work in the field of private credentials and the research results are very promising. Using private credentials algorithms and techniques we can increase the privacy-retention of the user much more than with Chaum's work alone. Private credentials in real life are often completely anonymous, private, untraceable and unlinkable. A subway token is the ideal lendable private credential: there is no way to tie it to the original purchaser, even if it was purchased with a credit card. There is also no way to tell if it was lent out, and there is no reason to care. It is reasonably unforgeable and thus is forced to be "single show." A Tyvek bracelet, like those given for admission to nightclubs, is close to an ideal non-lendable private credential.

In designing digital private credentials systems we should keep these examples in mind and strive to achieve the same levels of privacy and security.

### 6.4.1 Improving Un-Linkability

One of the great insights that catalyzed the creation of private credentials protocols is that, compared to physical documents such as cards, papers and tokens, there is no cost associated with computation. Computer cycles and network traffic are a renewed resource, and secondary storage (such as magnetic-disk) is becoming smaller and cheaper at exponential rates. For example, many international tourists end up owning more than one passport so that they minimize privacy risks: showing up at the Israeli border with an Iranian stamp may make one liable for harassment, interrogation or detainment because any observer can see the countries previously visited.

Of course the optimal solution would be to have one passport for each visit to a country, but the costs of manufacture and processing passports are prohibitive, on the order of $60 per. Fortunately, or digital credentials systems face no such constraints, allowing us to do things like create hand out and store a thousand one-time-use certificates at once.

One of the privacy issues that we are looking to resolve is linkability and tracability. Identity certificates are traceable because there is a name being used as an intermediate lookup. Chaum-style signature credentials are linkable, despite being anonymous, because even though direct identity is not used, the public key can be used to track the owner's actions. We will add one more ingredient to make these credentials private; the ownership of many 'disposable' credentials.

Say for example Alice has a blind-signature credential that says only that she is over 21. Since proving this credential to the notary needs to only be done once she can have thousands of randomly generated public keys signed one after the other and use them only once apiece. The verifier doesn't care and can't tell that she is only using the key once, so we lose no confidence in the system. The certificate authority's computational time and Alice's disk storage is cheap so there is no added cost. Overall, we see a benefit in privacy over Chaum without any tradeoffs. In fact, we are starting to see how private credentials can perhaps even be preferable to paper credentials.

### 6.4.2 Desired Technical Elements of a Private Credentials Protocol

We are still left with the problem of how to encode non-boolean credentials, which is a side-effect from the "all-or-nothing" blind signature algorithm. On one hand, the anonymity and privacy gains are enjoyable but if they are not flexible, then users and deployers may forgo privacy for usability

(an incredibly common trade-off in computer privacy and security: where usability and privacy are in conflict, privacy almost always loses.)

A key desirable technical element of a private credentials system is the ability to have flexible credentials with the same unlinkability and untraceable we've already seen with Chaum. On that note, we will present an private credentials system that has been designed but not yet engineered. Brands first published his design in his Ph.D. thesis[8] and was recently hired by Zero Knowledge Systems, a Canadian company famous for their thorough implementations of privacy enhancing technology. We hope to soon see his patents come to light ad replace the current identity certificates infrastructure.

In his thesis, Brands lays out what he believes to be the desirable criteria of digital credentials, both privacy-related and technical, of a system:

- **Limited Show** By this we mean that the credential can only be presented a limited number of times. Chaum shows how to implement one-show digital-cash (i.e. no double-spending). When the credential is shown too many times, some data is released, such as the private key or the identity of the user. Limited show allows verifiers to accept credentials and then check the validity of them at a later point, lowering cost and infrastructure requirements. However, use of limited-show presents a privacy risk to the user: if the credential or private key is stolen there may be a way to extract the real name of the user or some other secret information.

- **Lending Discouragement** Although some credentials should be lendable, there are some that should stay attached to one entity. With the previous systems, there was nothing stopping a user from giving away a private key and credential. Brands recommends either making the credential limited show (so that there is a risk of the other party over using the credential), forcing the private key to contain some private information, like a credit card number or some other secret data. Adding lending discouragement is a risk to users but may be attractive to clients of the system. For example, airlines would prefer that tickets don't pass from hand to hand because they can garner a $75 fee for the service. (On the other hand, using unlendable credentials instead of presenting identification at the airport may be a preferable tradeoff).

- **Discard Discouragement** Some credentials may be considered 'undesirable' for example, a bad credit history, and since they are just data, the user can just throw them out. Brands suggests that by binding desirable and non desirable information we can keep users from discarding

[8] Brands, Stefan A., "Rethinking public key instrastructures and digital certificates", The MIT Press, 2000.

unwanted credentials. In the real world we often use lookup databases and service bureaus to find out this sort of information, but that brings us back to our original credentials transaction system system. There is a tradeoff between the user distaste of revealing undesirable credentials vs. the gained privacy of not having a third party vs. the verifiers desire to gain information about clients.

- **Anonymous Re-issuance** Re-issuance comes into play when we have limited-show certificates or certificates that have an expiration. Say Alice has a refillable prescription credential that she can only show 20 times before she needs to have the prescription refilled. With anonymous re-issuance, Alice can get her prescription refilled without having to admit what drug it is. Hence, anonymous re-issuance definitely increases Alice's privacy.

- **No Self-Authenticating Records** A self-authenticating record is a transaction log that has a digital signature and a public key tied together so that, even a dozen years later, the record can be self authenticated. For example, a name and public key signed the corresponding private key is a a self-authenticating record. Brands believes this to be a liability risk because it makes repudiation difficult.

- **Control** We have already mentioned control, and it is a oft used privacy-concerns yardstick. A good system should allow the user to have complete control over his or her data. That is, they can choose who to release data to and when. Having a third-party database act as an infomediary is an example of a low-control situation.

- **Anonymity** By anonymity we mean that there is no identifying tied to these credentials unless they are meant be proof of identity. For example, a credential for proof of age should not have the presenters name attached as well.

- **Un-Linkability** Even though we may have anonymity, we may not have un-linkability. Chaum's design, for example, allows data-miners to correlate the many credentials attached to a public key and create a 'dossier' of that individual. Re-identification techniques may then unearth the true name of the key-holder.

Some of these, such as un-linkability, anonymity, control and limited show have already been achieved in cryptosystems predating Brands' work However, the others are not possible using the pre-Brands cryptography. Hence we require Brands' mathematics and cryptography. The algorithms are cryptographic in nature and we will cover some of the more relevant capabilities without inclusion of the proofs.

- Control Chaum gives us all-or-nothing control of our credentials: we can either hand over a signed credential or not. Brands, on the other hand, makes it possible to have parts of a message 'blinded' and other parts not. So now we can blind the public key encoded into the credential but not the credential itself, then have the entire credential signed by the certificate authority. Although the level of control is the same from a privacy standpoint, we can now encode variable-format credentials. We can also have many credentials in one message and blind certain ones depending on the transaction. However, there is the risk of linkability because the public key is still the same between transactions.

- Discouraging Discarding Some credentials only make sense when tied to other credentials. For example, knowing that someone has a drivers license is meaningless unless they also have insurance so a car-rental store will probably demand to see both credential. However, say that tied with the drivers license is also a history of serious car-accidents. If we used Chaum's protocols, the shower could just shrug and claim he had no history of accidents (discarding the negative credential). What we need to do is have the digital signature of the CA cover both credentials, now possible with partial blinding. Brands also includes a method by which the CA can keep the shower from hiding the undesirable traits.

- Selective Disclosure We already mentioned partial message blinding, but selective disclosure is much more powerful. Brands elaborates in his thesis a method by which boolean operations can be applied to blinded credentials and respond truthfully without revealing the actual credential. For example, one can apply a test for whether a user is either a minor or a senior without knowing which one.

These properties are very powerful and allow us to have many different kinds of credentials: lendable, renewable, bound, selectively disclosed, partially hidden. We have regained the flexibility of X.509 credentials without sacrificing any of the privacy gains we have made with Chaum style credentials.

### 6.4.3 Criteria Overview

- **Privacy:** By using private credentials, we gain even a lot of privacy for parties involved. The end user gains privacy because she now has better control over her data and how much information she wants to disclose. With selective disclosure, she can even prove a function of her credentials without revealing them. As we have already mentioned, there is an increased risk of an identity disclosure when using (or misusing) non-lendable or limited-show credentials.

- **Versatility:** We have as good if not better versatility over X.509-type certificates. Limited-show certificates may prove to be very useful. We also now have lendable and non-lendable credentials, whereas X.509 credentials are strictly non-lendable.

- **Accessibility/Ease-of-use:** There are some complaints that the mathematics behind private credentials are unwieldy because all of the parties have to share cryptographic-seed data. ("[An] inconvenience of these and the other discrete-logarithm-based schemes mentioned above is that all the users and the certification authorities in these schemes need to share the same discrete logarithm group" [9])

- **Cost:** There are no additional costs involved as computational power and storage is cheap or free.

- **Security:** The addition of lendable and non-lendable credentials may create some mistrust of the system; there is really no way to absolutely prove that a credential was not lent out. The ability to create hundreds of key-pairs means that lending out one may be not compromise the others.

- **Trust and Confidence in System** Private credentials, like public key cryptography, rely on the assumption that there are certain processes that are easy to verify but difficult to compute. There should be no loss of confidence due to inclusion of new algorithms.

## 6.5 Conclusion

Right now, on-line credentials are based on identity certificates, a simple infrastructure that relies on third party databases for information lookup. These systems build out of two dated technologies: X.500 directories and PGP key-signing. X.509 certificates were appropriate for phone-book systems like X.500 where identity is the look-up "key" and people were only interested in proving digitally signed message authenticity. However, a true credentials system is what is really needed. More

[9] Lysyanskaya, A. "An efficient system for non-transferable anonymous credentials with optional anonymity revocation." Advances in Cryptology, 2001.

importantly, a credentials system that puts people in power of their data, one that provides privacy protection. Granted, there are hundreds of privacy-concern bills being introduced to the senate, and web sites are being pushed to create privacy policies and these are an important ingredient to preserving user privacy. However, we would like to avoid ex post facto solutions and minimize the trust put in others. Technologies such as P3P are a good example of control being pushed farther away from the untrusted party and closer to the owner of the data. Private credentials, such as those developed by Brands, Chaum and Lysyanska bring that control even closer, allowing the user to explicitly choose what data he or she chooses to reveal.

# Chapter 7

# The Lure of Single Sign On

Lure of a single sign-on This paper will describe the balance between privacy and security on the one hand, with ease of use on the other hand. In this section, we will describe how some have chosen ease of use in terms of having just one sign-on procedure to access a wide variety of information. We will also weight the advantages of a single sign-on, with the disadvantages.

## 7.1 Why do companies want a single sign-on?

CompanyX estimates that companies spend $300-400$ a year per employee to manage problems with password resets. [1] Also, with numerous passwords, employees are more likely to forget them, leading to high cost of password maintenance. Furthermore, they are more likely to write them on the computer screen or in some way make fraud easier rather than more difficult. In an effort to reduce cost, companies are also eager to outsource password management to biometrics authentication companies that use biometrics as a single sign-on. All these factors play a role in the current trend.

## 7.2 Why do individuals want a single sign-on?

Individuals want a single sign-on for ease of use. They want to be able to access information without having to be bothered with sending password information. Some even want their content to be aggregated from various institutions all in interest of convenience.

[1] Due to confidential, non-disclosure agreements, we are not at liberty to disclose the identity of CompanyX

## 7.3 Case Study: CompanyX

### 7.3.1 Description of the business

[2]

CompanyX is a company which helps other companies outsource their sign-on problems using a single sign-on with biometrics information received via face and fingerprint images.

For a monthly per-user fee, CompanyX supplies all the required on-site hardware (cameras and fingerprint readers), provides support for integrating the customers' applications with the CompanyX system (which runs on computers owned and operated by CompanyX), and manages a Security Operations Center which monitors system activity and handles situations where the system has failed to authenticate a user. The free hardware and monthly fee per user cost structure means that companies can install and use biometric identification without any capital expenditure. Managers' wanting to use CompanyX can pay for it out of their operating budgets.

In analyzing CompanyX's system, we came up with several concerns with the model of using biometrics as a single sign-on. We also recommend solutions.

### 7.3.2 Potential Concerns and possible solutions

Here are our concerns:

- **1.** The communications between the fingerprint reader and the computer may not be encrypted depending on what kind of fingerprint reader is used. Some versions of the Verdicom reader, for example, do not have encryption. This leaves it prone to a repeat attack, where the fingerprint data stream is collected and sent again.

  A solution will be to time stamp and device stamp the data, and then encrypt the data.

- **2.** The data is sent from the browser to the CompanyX server through a browser using SSL encryption. Therefore, the encryption could be as weak as 56 bits or up to 1024 bits with a certificate. This may still be insufficient for biometrics data for which you only have one set.

  A solution will be to add another layer of stronger encryption preferably with another encryption technique.

[2] Please visit http://www.CompanyX.com/solutions/download/CompanyX.pdf

- **3.** The face recognition tool gives a false sense of security, since it is a 2D algorithm and may be fooled by a good picture. While fingerprint recognition is more foolproof, the software may have been set to accept a fingerprint match or a face match, in an effort to reduce call center costs.

  A solution to this problem is not to use face recognition software, or to use a 3D face recognition software (which is at least more difficult to fool).

- **4.** Procedure for the setup of the one-time password is dubious. There is a written list of one-time registration passwords that can only be used once per registration. In the interest of reducing costs, CompanyX does not verify the employee, but lets the company management distribute these one-time passwords for user registration securely. Therefore, a hacker with the access to the list can sign himself up and access the network.

  A solution will be to use a more robust method of user registration. For example, the employee can go personally to CompanyX and show 3 types of identification.

- **5.** There is also no backup mode of sign-on in the event of a failure. For example, a denial of service attack can prevent communication between CompanyX and the company. Alternatively, CompanyX may be financially strained to support the system. For whatever reason, a failure could mean that the company not only loses the service, but also comes to a computing halt. Such a risk is not acceptable.

  A solution will be to place the authentication server in the company site. This will be more troublesome for CompanyX since they will have to travel to each company to maintain the server.

- **6.** There is a loss of privacy. CompanyX stores the triplet of a username (which is usually chosen to be fairly similar to a person's real name), the face of the person, and the fingerprint of the person. Therefore, a security analyst at CompanyX can know this set of information about the person registered, and perhaps know which company he is working for based on the location the triplet set is stored. The analyst will also know when the person logs in, which gives information about her location and work cycle. The solution is to firstly remove the username from the triplet set. This is a sacrifice, since CompanyX will now require a one-to-many instead of a one-to-one matching algorithm. This is more expensive, slower and more prone to errors. Secondly, CompanyX should store template information in such a manner that it minimizes the information available to the naked eye. That is, instead of storing the picture of the user, store some coded data that is required to identify him, such as distance information between facial features.

- **7.** There is a privacy concern that the company will be able to trace employees whereabouts even outside the workplace, through close-circuit cameras around the world. Also, an employee who leaves the company is not really guaranteed that copies of the biometrics information are destroyed.

  On a separate note, there is concern that should the CompanyX server be hacked, the hacker will be able to use the biometrics data collected to sign-on as the user in future circumstances for the rest of the user's life.

  The solution is cancellable biometrics,[3] developed in the IBM Research Laboratories. In this solution, the picture of the face or fingerprint is warped with a given seed. (This seed can be at a third party server or a smart card that is in the control of the user.) The image is always warped in a certain fashion and CompanyX can only identify the warped image. Therefore, destroying the seed effectively cancels the possibility of identifying the user.

- **8.** Non-repudiation problems may also occur. In some states and in Singapore, a person cannot repudiate a digital signature easily. If CompanyX's service is used to sign timecards, all that is really said is that the person placed his finger at a certain time, but it does not directly verifies what was on the screen that the user intended to sign.

## 7.4 Case study: Yodlee

### 7.4.1 Description of the business

Yodlee is a provider of account aggregation services, with partnerships with reputable companies such as Chase. The user is expected to provide username and password information to various services, and will, in return, receive the convenience of having content aggregated on one page. Furthermore, the user can also track his account balances over time, and do other statistical analysis for forecasting his budget and finances.

[3] Reference: N. Ratha, J. Connell, R. Bolle. Cancelable Biometrics. 2000 Biometrics Consortium Workshop, September 2000.

In our analysis, we have some concerns that we will list in the next section. Finally, we will propose a new more secure model.

### 7.4.2 Potential Problems

We are concerned about the following:

- **1.** There is a security flaw in having a single password. A hacker that breaks the system will be able to access all of a user's accounts. Therefore, the damage can be enormous, rather than localized. The user may have to have bad trades placed with his stockbroker, or have his money in the bank wired away.

- **2.** The valued added services of financial monitoring imply that the content aggregated is stored locally at Yodlee. Such information about what you purchased with your credit card, may remain on Yodlee for a long time, even after you "destroyed" it by canceling your credit card account. There is a loss of privacy and a danger of misuse by Yodlee employees or hackers that gain access to Yodlee. Furthermore, such illegal access may no be known to you. Certainly, Yodlee does not have the incentive to report if there is a compromise in the system.

- **3.** A user will also have to trust in Yodlee's "good faith" to do things correctly. Content Aggregation may be done in a crude manner. Yodlee may not use the high level of SSL encryption as the user would normally do. Yodlee may enter HTTP Post and Get commands based on a fixed program. It is likely that sending the "command=B" could mean obtaining the account balance on one day, and buying stock on another day. In the event of such errors, neither Yodlee nor the stock broker can be held responsible.

- **4.** Finally, using Yodlee may be illegal. In the Yodlee agreement, it is stated that:

  *"You agree that Account Providing Institutions shall be entitled to rely on the foregoing authorization, agency and power of attorney granted by you."*

  However, as an example, Datek Online, a stock broker, requires the following agreement to be signed before an account can be opened:

  *"Any order entered using your password is yours or your duly authorized designee... You ... warrant that you ... are the only authorized user of such password ..."*

Therefore, in using Yodlee, the user has breech the agreement both with Yodlee and with Datek Online.

### 7.4.3 Proposed Solution

We will only outline a possible solution for some of Yodlee's problems, since the actual implementation could be the work of another paper.

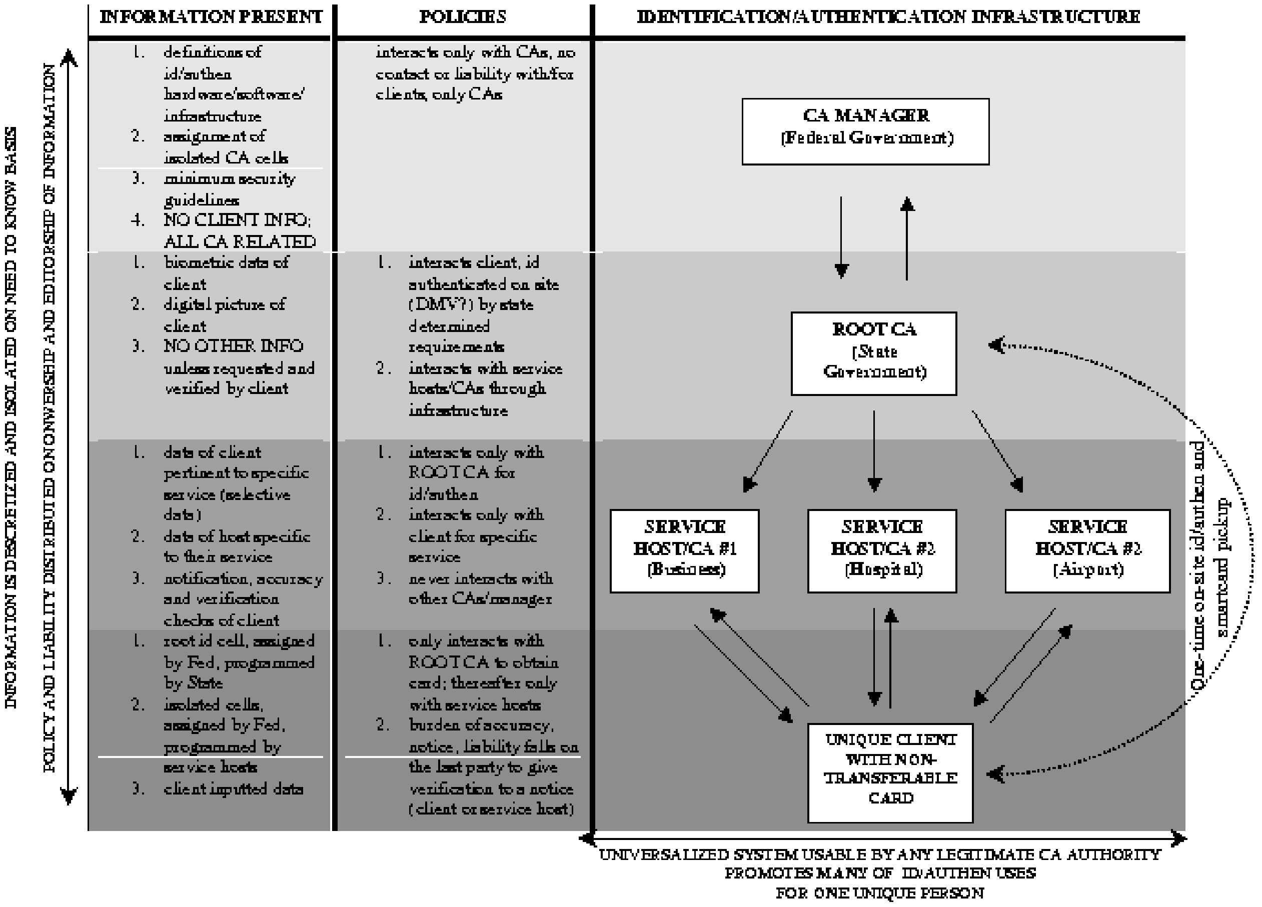
- **1.** Yodlee will develop an application that can be installed on the user's computer. Alternatively, Yodlee can use a Java Applet that is set with security settings such that access to the hard drive is possible.
- **2.** The application will first check the user is authorized to use the program getting the user's password, which is required to decrypt the file on the hard drive that has been previously loaded with account sign-on information of various websites.
- **3.** The application will download updated templates on how to handle and parse foreign WebPages to aggregate content.
- **4.** The application will then do the actual content retrieval, and store any required information on the hard drive, preferably encrypted.
- **5.** The application can then display the relevant information.

This proposed solution is an improvement since the password, account information and retrieved information is in the direct control of the user. The user still maintains the ease (and dangers) of a single-sign on. In fact, more functionality can be added with a local application, or at least the speed will be better. Finally, the user is not breeching any contracts since he is the entity actually signing on to various websites.

# Chapter 8

# Conclusions and Recommendations

In conclusion, we have learned that there are three truths of information: persistence, loss of control, and linkability. By evaluating three real-world and three cyberspace AIKMs using our agreed upon policy criteria, we have shown that each has its own unique strengths and vulnerabilities. The current AIKM systems leave room for mismanagement and misidentification from a technological standpoint, for example the accidentally signed Microsoft certificates by Verisign. Furthermore, we cannot rely solely on the policy or legal infrastructure to protect our privacy concerns as there are few legal precedents or laws currently in place to combat invasions of privacy. If an AIKM system is accessible by a user, in most cases they are vulnerable to attack by an intruder, whether that individual uses a technical attack or legal loophole is another matter. Thus we recommend that new AIKM technologies be developed as a joint venture among policy makers and technical engineers. As policy makers have full faith that their laws and policies will be adhered to and technical engineers design with the mindset of creating for every flaw and contingency, the synergy of these two dichotic viewpoints, evaluated with our criteria and a costs of criteria element vs. benefits resulting in criteria element, may result in a much improved AIKM system. The new concepts of cancellable biometrics for a single sign-on, or new methods of private credentials presented show great promise. However, until these theses are engineered, put into practice and tested against our privacy concerns and policy criteria, there must be privacy and AIKM policy protection laws on the books. We have already begun to discuss hybrid policy structures that are more apt to meet our policy criteria, such as those based on X.509 but with a more rigorous examination of the privacy and liability concerns involved.



| INFORMATION PRESENT | POLICIES |
|---|---|
| 1. definitions of id/authen hardware/software/ infrastructure<br>2. assignment of isolated CA cells<br>3. minimum security guidelines<br>4. NO CLIENT INFO; ALL CA RELATED | interacts only with CAs, no contact or liability with/for clients, only CAs |
| 1. biometric data of client<br>2. digital picture of client<br>3. NO OTHER INFO unless requested and verified by client | 1. interacts client, id authenticated on site (DMV?) by state determined requirements<br>2. interacts with service hosts/CAs through infrastructure |
| 1. data of client pertinent to specific service (selective data)<br>2. data of host specific to their service<br>3. notification, accuracy and verification checks of client | 1. interacts only with ROOT CA for id/authen<br>2. interacts only with client for specific service<br>3. never interacts with other CAs/manager |
| 1. root id cell, assigned by Fed, programmed by State<br>2. isolated cells, assigned by Fed, programmed by service hosts<br>3. client inputted data | 1. only interacts with ROOT CA to obtain card; thereafter only with service hosts<br>2. burden of accuracy, notice, liability falls on the last party to give verification to a notice (client or service host) |

INFORMATION IS DESCRETIZED AND ISOLATED ON NEED TO KNOW BASIS
POLICY AND LIABILITY DISTRIBUTED ON ONWERSHIP AND EDITORSHIP OF INFORMATION
IDENTIFICATION/AUTHENTICATION INFRASTRUCTURE
CA MANAGER (Federal Government)
ROOT CA (State Government)
SERVICE HOST/CA #1 (Business)
SERVICE HOST/CA #2 (Hospital)
SERVICE HOST/CA #2 (Airport)
UNIQUE CLIENT WITH NON-TRANSFERABLE CARD
One-time on-site id/authen and smartcard pickup
UNIVERSALIZED SYSTEM USABLE BY ANY LEGITIMATE CA AUTHORITY
PROMOTES MANY OF ID/AUTHEN USES
FOR ONE UNIQUE PERSON

In this proposed policy structure, we ask that an initial identification be made by physically being present at the notarizing root certificate authority (CA), in this case the state government. As not to bias against certain individuals as well as limit the information gathered by this root CA, we ask that the state CA only record minimal information to make a positive identification, such as a name (initially authenticated by a birth certificate), a photo of the individual and a biometric signature. No other information should be recorded by the root CA. Once identified and authenticated, the user is given an identical copy of this root CA record on a storage and input medium with a secure, tamper-proof hardware/software lock, such as a verifiable timestamp. With this device, the user may go to other service CAs, to load information specific to that CA into isolated data cells that have no linkage to neighboring cells owned by other CAs. This permits selective giving of information and thus enhances the privacy afforded to the individual. (e.g. if the user uses this AIKM hardware to carry both his insurance info and his health records, the insurance company cannot access his records)

In terms of liability, the owner of a cluster of isolated cells (such as the hospital CA) determines the information gathered, privacy policy and security implementations for those cells and makes the user aware of this policy when he makes a first, on-site identification and is authenticated at the service's place of establishment. For on-line services, a trusted physical notary can be used. Now, exchanges between the user and service CAs are authenticated by the root CA, yet since the cells of different CAs are isolated, and not accessable across CAs, it is as though a user carries multiple customized certificates for a variety of exchange situations. The only information that is common and accessable to all the CAs is the name, biometric data and photo of the user found at the root CA. Liability for violations in privacy due to failures in notice, access to personal information, opportunity to correct errors, purpose for information request, security and accountability will fall on either the user or service CAs, as they exist in an almost peer-to-peer relationship and thus must keep the other informed. As most service CAs have financial standing, they are weill suited to handle this liability, in case they are sued for misuse of private information. However, the federal CA (which simply establishes the guidelines for the policy) and the state CA (which implements the guidelines) are merely liable for this new AIKM infrastructure, but not the information contained therein. Since most of the privacy violation suits would arise due to a failure to secure the information, rather than follow the AIKM infrastructure policy, It is reasonable to argue that the service CAs would be more prone to privacy liability suits than the federal and state root CAs, since most of the privacy violation suits would arise due to a failure to secure the information, rather than follow the AIKM infrastructure policy. Furthermore, upon speaking with Danny Weitzner, we learned that it is quite difficult to sue the federal or state governments unless there are significant violations at play, that could result in a class-action scale suit.

In evaluating this proposed policy against our policy criteria, we notice that it aptly meets many of our requirements. It affords us the privacy to control the information we carry and provide. Due to the ability to custom-tailor each cluster of isolated cells to the service CA's needs, this policy is versatile and can be used in a variety of situations, from obtaining an immigration visa in your passport cells, to paying for groceries from your credit cells, to giving ER doctors life-saving information from your medical record cells. Apart from the name, biometric and photo information, which is hard-coded into the device, the other information on the cells is accessible by the user and the service CAs who together can agree upon the pertinent information necessary for an exchange. Similarly, since the attributes and characteristics of a cluster of cells is mutually determined by the user and CA owner of the cells, the user should be free to use those cells without being burdened by revealing information from other cells. We cannot speculate on the cost of the technical infrastructure at this time, but believe that the social costs of handing over private information can also be limited, as the user will be notified of the purpose of the request and can select to have this exchange terminate at the service

CA and not proceed to secondary parties. Note, that this policy distributes information both along its infrastructure as well as isolates information in clusters of data cells held by the user. Thus, levels of security can be customized to the needs of the given CA and user, as well as the level of privacy needed for the information involved. For example, while a video rental CA would not bother encrypting and securing their cells' information (perhaps so that rental credits can be transferred among users), a medical institution may heavily encrypt a users medical history. At this time, we can only speculate if society can place trust and confidence in such a universally applicable system, but perhaps the convenience of having all one's identification records in one modular, customizable yet private and secure device may turn the public eye in our favor.

It is in good faith that we recommend to both the engineering and legal communities to reach a compromise that promises a high tolerance against technical failure as well as a clear protection of privacy and policy concerns.

# Chapter 9

# Acknowledgements

We would like to acknowledge and thank Joe Pato, Hal Abelson and Danny Weitzner for the generous advice, time and experience they shared with us in examining the legal and technical topics discussed in this white paper. We would also like to convey our gratitute to the helpful individuals at the MIT Student Information Processing Board (SIPB) for helping us typeset this document in LaTeX. This white paper is the culmination of an MIT academic term's worth of learning, understanding and ultimately tackling the legal and ethical implications of technology on the digital frontier.