1. Problem Definition

In light of the recent tragedies of September 11, 2001, America has felt the immediate need for a system that could positively identify individuals who pose a threat to national security. Suicide attackers have added a new dimension to potential threats the country might face. It is absolutely critical that we keep these potential terrorists out of sensitive areas that could be a target for a terrorist act. However, America's long-standing tradition of freedom may be one of the greatest assets to potential terrorists. The American spirit for privacy and freedom has led to a weak system of authentication when compared to other nations. For the security of America and her citizens, it is time to create a strong national identification system that can expose those who exploit our free system.

Before the attacks of September 11, most of society was opposed to any form of national identification due to privacy concerns. However, this sentiment is beginning to change. According to a New York Times/CBS News poll on September 27, 2001, fifty-six percent of the people said that they would accept a mandatory national electronic identification system [22]. In a Pew Research Center for the People & the Press survey, seventy percent of the U.S. public supported a system of national ID cards [23].

The prospect of carrying a national identification card still raises concerns among the public. Many claim that the recent proposal will constitute a breach of civil liberties because it may allow authorities to track the movements of individuals throughout the nation [24]. Another criticism being raised is that the ID card system could become a powerful tool for ethnic profiling. Many feel that the authorities would be more likely to stop Arab-Americans for an ID check. Other opponents argue that the information provided by the card system would strengthen the power of the bureaucracy who could potentially use it for their own gains [25]. There is also a major concern that such a system would provide a false sense of security among the public. Any national ID system will always have the human factor, making it susceptible to forgeries no matter how secure the implementation. For example, no matter how well card making machine operators are screened, it is still possible for them to abuse their power to make fake cards. Because of increased levels of security, anyone who found a way to get a forged

card would actually have an easier time breaking through the security measures. The fact that the immigration laws would be enforced using these cards, finding ways around them would also become an immediate priority for counterfeiters.

Also, many people still do not believe that a national ID system would provide any added security against terrorism. The following story refutes those claims. In 1999, a man named Khalid Al-Midhar was spotted by Malaysian security meeting with some of Osama bin Laden's top aides. The Malaysian authorities immediately reported this information to the United States where the FBI put Al-Midhar's name on the Immigration watch list. In August 2001, Immigration finally realized that Al-Midhar was already in the United States, and ironically, he had used his real name and identification to do so. Immediately, the FBI sent agents across the nation to find Al-Midhar. Unfortunately, they did not find him until they scanned the flight manifest of American Airlines Flight 77 on the day of America's worst tragedy [21]. A national identification system hopefully would have stopped Al-Midhar from entering the nation, and it certainly would have stopped him from boarding a plane on that fateful day. The system proposed in this document will provide a way for America to recognize terrorists, criminals, and identity falsification with minimal effects on the privacy of ordinary citizens.

2. Related Work

A. Other Countries

The United States is one of a handful of industrialized countries without a standard national identification card. This is attributed to the fact that the U.S. puts such a high value on personal liberties, freedom, and privacy. After the recent attacks on America devastated our sense of security, many are calling for the U.S. to join the hundreds of other nations with a national identification system.

Of the countries that have national ID systems, there are two extremes and many that fall in the middle. Some of the oppressive Asian nations like Korea, Malaysia, Singapore, Hong Kong, and Thailand all have national ID systems. Most of these Asian systems fall on the overly restrictive end. Singapore assigns each citizen a serial number at birth and then requires all citizens to carry their national ID card at all times. Cameras are located throughout the town at intersections, playgrounds, and even office buildings, and citizens are constantly monitored and tracked using this system of national identification [20]. Malaysia also has a similar smart card system where all citizens are tracked and forced to swipe their ID card at places like shopping malls and office buildings. This system holds fingerprint data and must be carried by all citizens over the age of twelve [16].

On the more liberal end, the Dutch system is relatively open and used mainly for tax and identification purposes [15]. Much of the rest of Europe and South America fall somewhere between the Asian systems and the Dutch system. Countries like Argentina, Belgium, Brazil, Finland, France, Greece, The Netherlands, Portugal, and Spain all have national ID systems as well as nearly a hundred other countries [12]. Many of these countries are not overly restrictive, but those citizens who do not keep their card in their possession could wind up in jail [16]. Of the European countries, the United Kingdom is one of the only other major countries that currently does not have a national ID, but after the recent attacks, it too is considering ways to implement a national ID system [10]. Interestingly, most common law countries have rejected national ID attempts, and Australia and New Zealand both do not have national ID cards [16].

B. History of the United States national ID

With the creation of Social Security during the Great Depression, all Americans were given their national identification number without really knowing it. Today that number is used for all purposes of identification, but the validation procedures are relatively weak. For example, anyone who knows a person's name, Social Security number, and address can steal that person's identity for the purposes of opening financial accounts, a credit card, or even applying for a job. If the imposter can produce false documents that have a matching picture with the stolen identity, it is relatively difficult to prove that the imposter is using a stolen identity.

Because of the ease of identity theft, the idea of a national ID card has been kicked around for decades. National ID's first came up in 1971 when a Social Security task force proposed the creation of a complex national identification card to complement the Social Security number [12]. Later in 1973, the Health, Education, and Welfare Advisory committee concluded that a national ID card would not be beneficial to America [12]. In 1976, the Federal Advisory Committee on False Identification also rejected the idea. A year later, the Carter administration reiterated that the Social Security number was not to become a national identifier, and in 1981, the Reagan administration said that it too was opposed to a national identifier [12]. Members of the Clinton administration also denounced the idea of a national identity card.

However, in 1996 Clinton signed an important bill called the Illegal Immigration Reform and Immigration Responsibility Act. This bill was mostly focused on controlling immigration, but tacked on as a rider, a provision essentially created a standard national identification card [13]. The bill stated that all forms of state identification must comply with a certain Federal standard or they would not be accepted as valid identification by the Federal Government. This also mandated the use of the Social Security number as the identification number on all state ID cards. After this act, states not only included the Social Security number on cards, but some acted even more aggressively. Georgia passed laws that required the fingerprint to be on all drivers' licenses, and Oregon licenses held digitized information about the cardholder in a magnetic stripe [13]. After considerable criticism from civil liberties organizations, Congress repealed the identification portion of the Act in 1999 [12].

After that bill, the national ID debate appeared to quiet down - until September 11. Since then, Larry Ellison has publicly come forward calling for a national ID card that used Oracle's software to run the database infrastructure, and Harvard professor Alan Dershowitz has also released plans that call for a national ID [14].

The idea has also been bounced around Congress. Senator Diane Feinstien, who also called for national ID's various times throughout the 1990's, is leading a new effort to explore a national identification card [8]. In early November, she released an immigration reform bill that would make new immigrant visas tamperproof through the use of smart cards. This system would also provide for a database that would allow the government to track immigrants [8]. Feinstien also supports the creation of a standard national ID card for all Americans.

Most recently on November 16, the House Committee for Government Reform organized up discussions of the feasibility of implementing a national ID and potential ramifications of such a system [18]. However, Congress has been slow to accept the security gains of such a system when compared to the potential infringements on personal privacy, and the White House has publicly rejected the idea of a national ID card. The next few months will be important to find out how much support a national ID actually has, and if any concrete proposals will materialize.

Although the national ID idea has bounced around for decades, it is difficult to give detailed information about the implementation of any of these previous proposals. Nearly every one of these proposals was rejected before the projects made it to an implementation stage. Because of recent attacks on America, these proposals are now being revisited, and the same privacy issues that hindered them may no longer apply. The system designed in this report will offer a viable start to the complete implementation of a national ID system.

C. Implementation

When discussing how to actually implement such a system, we first focused on the feasibility of storing encrypted information on the Smart Card. We wished to store the basic information on the front of the card (the cardholder's name, address, DOB, identification number, etc.) as well as in the memory of the Smart Card. However, since

the Smart Card would be used for high-security applications, we also wanted to include a photo, thumbprint, and voiceprint. Information in text form such as the identification on the front of the card would take up a trivial amount of storage space, but including images and voiceprint information could take more storage than the Smart Card has available if not compressed. Surprisingly, a fingerprint only requires about 256 bytes of memory if not stored as an image, so they too have a negligible amount of storage [4]. We found that voiceprint verifiers can store enough information to identify a voice in about 20 kilobytes [2] and a 200 by 200 pixel image compressed with medium JPEG compression should only require about 4 to 8 kilobytes [3]. The Smart Card must therefore be able to store about 30 kilobytes of information. A typical Smart Card has 64 to 128 kilobytes of ROM, so the card should have enough storage to hold all of the information necessary to verify the cardholder [1]. The Smart Card also has a microprocessor, but our implementation of the National ID card has no use for it. However a future implementation of the National ID card could require the use of a processor, so it should be left in for potential use.

The database that we will be implementing must be easy to query, highly secure, and easily manageable. The Center for Database Research at the University of Illinois has been doing a great deal of in depth research into these types of databases. They have even developed an extension to SQL that allows for the querying of multi-level secure databases [5]. This research coupled with the already present methods of creating secure databases discussed in Oracle Security by Theriault and Heney provide a good step towards the creation of a fast and easily manageable secure database [6]. We must also not forget that Larry Ellison has promised us that Oracle can provide such a database for the exact purpose that we will need it [14]. Overall, we will assume that there is enough research and resources available in industry currently to create a sufficient database that would meet our requirements.

The secure channel, however, may be the most important area to maintain security. When developing the secure channel, there are a number of possibilities. The following will describe some of the protocols we considered and how each works. The three possibilities we considered for the implementation of the secure channel are:

1. A dial-up connection service similar to current credit card transactions
2. A private government network
3. A secure tunneling system over the existing Internet network

A dial-up service would be beneficial because of ease of access and low costs. Phone lines are widely used across the nation and no existing infrastructure would have to be built to support such a system. It would be relatively simple to connect to an authentication network that uses some form of encryption to ensure the security of sensitive data. The main problems with this method, however, are that the technology is somewhat primitive, less reliable, and much slower than a computer network implementation.

Another solution would be to use a private government network that has been recently been proposed. The proposed Govnet would consist of a private computer network that only government systems would have access to utilize [19]. This network would be completely separate from the Internet so that connected computers will not be vulnerable to viruses or denial of service attacks. Govnet is currently designed to simply replace the Internet connection at current government agencies for applications like file transfer, voice-over-IP, and video [11]. This design would scale easily to include card readers for the national ID system because of the nature of the transactions with a central database. This solution would be much more secure than an Internet based solution, but it would also be much more costly. A similar solution would be to create a separate, specialized network, like an ATM network, that only the national ID system would be able to access. This solution has similar benefits as the Govnet solution.

The third solution would be to utilize current Virtual Private Network (VPN) technology over the existing Internet. This VPN technology is what the government currently uses for security on its computer network [19]. VPN's create secure tunnels over existing network connections to create a low-cost secure connection over a normally insecure channel [17]. When compared to the creation of wide area networks, VPN's are much less expensive while still offering a high level of security. VPN's use traditional symmetric and asymmetric encryption methods to bundle up packets and send them over traditional network connections where they can be unwrapped by the receiver [7]. A

traditional VPN will use Diffie-Hellman key exchange to create a session key and then use a symmetric encryption technique to transfer data. However, typically any security method like public-private keys, digital signatures, and symmetric cryptography can all be used to assure the security of the tunnel. The main problem associated with this network is that all the systems, especially a centralized database, will be located on a public network. This makes the system vulnerable to denial of service attacks and viruses, and it makes the entire network available to general Internet hackers.

3. Solution

A. Overview

This project delves into designing a National Identification Card system for the United States, which would be specifically used to provide high-level security at strategically vulnerable locations such as airports, banks, military installations, and research laboratories. It will also be used to facilitate the task of the Immigration & Naturalization Services (INS) to watch over the immigration system of the country.

The issue of introducing an ID card is sensitive because it raises the scenario of the security of the country being pitted against the privacy of the people. The motivation of this project is drawn from this concern. Also, the fact the immigration laws would be enforced using these secure cards, hacking them would become an immediate priority for counterfeiters. Therefore, our design not only aims at providing a system in which the dissemination of information about a person is highly limited and controlled, but also at providing a system that is robust against attacks by hackers.

The current American authentication system relies on multiple official documents provided by different government agencies to verify credentials. However, these documents can be easily falsified or destroyed. Having a digital system would be a quick and efficient way of sufficiently deterring would-be attackers and evildoers. A model of our design is shown below in Figure 1.

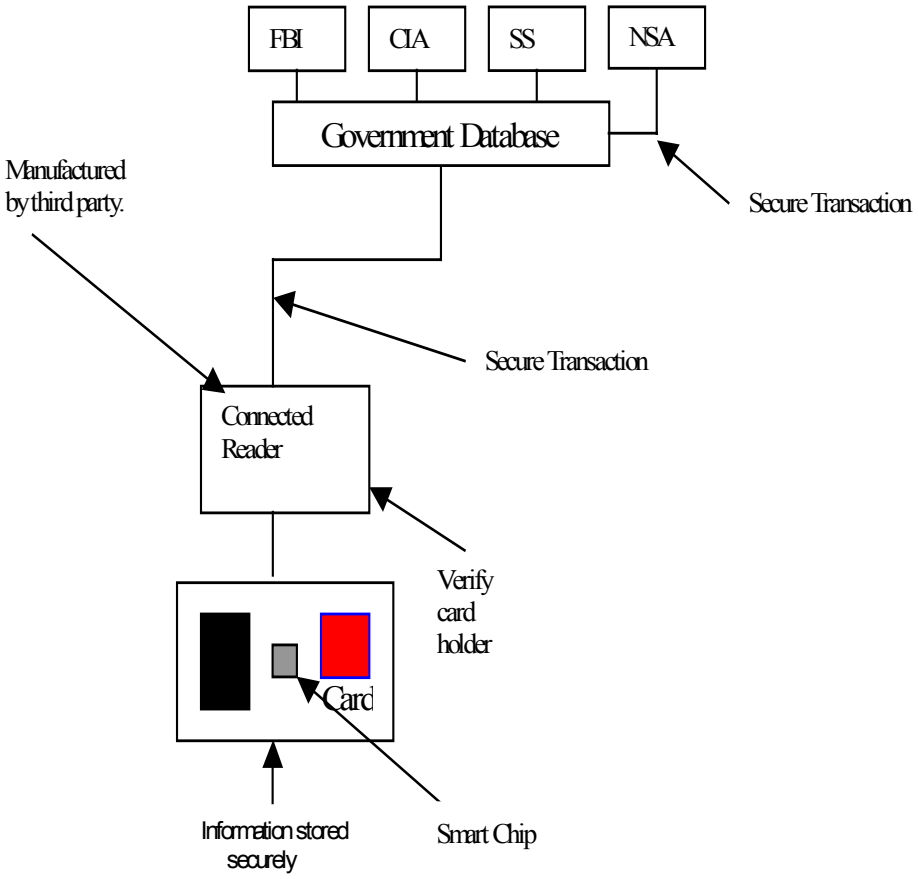

Figure 1. A national ID system

The design we are proposing would include an ID card that would store the digitalized fingerprint and the personal identification number of the person. All citizens and non-visitor immigrants will be required to hold a national ID card. The card would also show a photograph of the person and other basic information such as an individual's Social Security number and date of birth. The information on the chip would be encrypted to ensure its integrity. The system would include a reader that would read the information on the card without allowing any loopholes for the information on it to be leaked or logged. We will address issues like storing personal information on the reader and make sure that proper measures are taken to make the reader resistant to counterfeiting or being stolen. Also, the reader would be designed such that it would not

be able to read any card without the cardholder's permission by requiring the cardholder to have his or her thumbprint scanned on the reader for verification.

A database, maintained by the Office of Homeland Security, will hold the flags deemed necessary by the various government agencies to do a background check on a person. We will use the database provided by Oracle, which has been proclaimed secure for a national ID application by CEO Larry Ellison [28]. Also, the uploading of information onto the database by the government agencies is also assumed to be secure and resistant to any information leaks. The database would be connected to the card readers by a secure channel so that the holder of the card can be authorized. The user will swipe the card through the reader and scan their thumbprint to verify that individual is the actual owner of the card. Then the data from the smart chip is transferred through the secure channel to the database for a cross check, and the result transmitted back to the reader. The dynamics of the different components of this system including the card itself, the secure channel and the database are discussed below.

B. The ID Card

The center of the national ID system is found in the identification card. We have decided on two levels of security for the card itself and the information that is stored on it via the smart card. The low security section resides on the face of the card, while the high security section uses the cryptographic powers of the newer smart card processors.

Low Security

The card will have printed information on the outside much like a driver's license, since most Americans use their driver's license for positive identification. Most merchants will accept a driver's license as identification because to obtain a driver's license, a person must present both a Social Security card and a birth certificate [Foley]. We will follow this scheme because it works for our current identification system, and we do not wish to radically change the country's predominant verification system for day-to-day activities. The front of the card will display information such as name, date of birth, address, phone number, and a unique identification number, much like a driver's license.

A person's Social Security number will suffice for the identification number, and a new number will be assigned to people who do not wish to use this number on their card. The card will also feature a photograph and will include the standard tamper-proofing tools used in current driver's licenses. This card can be used anywhere that a driver's license worked before (buying alcohol, verifying identity for checks and credit cards, driving a car, etc.). Our aim in the low-security aspect of the card is to make the card virtually the same as a current driver's license in terms of use and ease.

High Security

The real change in the system from our current identification and verification standards will be the high-security aspect of the card. The card will have a smart chip to hold encrypted information about the user's identity. This encrypted data will hold all of the person's information listed on the front of the card, and also a digitized thumbprint and voiceprint.

To further understand how this process works, we will now explain how the card is made. A person can get a national ID card at certain governmental offices (most commonly, at the local DMV). The person presents valid credentials (a birth certificate, Social Security card, etc) to the officer. The individual then scans his or her thumb on the DMV's scanner and has his or her picture taken via digital camera. The person then speaks a simple pass phrase into a microphone to obtain a voiceprint. When all of this information has been collected, a computer generates a key pair using the RSA algorithm. The information is encrypted with the private key of the generated key pair and the private key is destroyed. The computer then stores the new encrypted information onto a smart card that has been created with a unique processor ID and sends the public key, processor ID, and person's ID to the government database. The information is then printed onto the card, and the standard tamper-resistant items are applied to the card.

The high-security aspect is reliant on public key cryptography. We are assuming that people can fake smart cards, but it will not matter since the database holds the public key of each card. Even if a person can make a fake card, it would be impossible to put information on the card that the reader can decrypt without knowing the private key, which is thrown away when the card is made. Note that it is possible for a person to

make a fake card that does not have the proper encrypted information. The person could use the card for low-security purposes (which do not check the encrypted information on the smart card) but due to the tamper-resistant measures on the card itself, the card would be difficult to manufacture for anyone but the most determined criminals, who undoubtedly can manufacture driver's licenses and passports already.

The government will identify high security areas that will strictly be the only places allowed to use a reader to access the centralized database. Many of these places already require identification checks for authorization, so using a national ID card should be a minimal privacy infringement. A few of the many applications for high security are:

- Airports
- Gun purchases
- Explosives purchases
- Employment background checks
- Research laboratories
- Nuclear facilities
- Military installations

C. The Database

An essential piece of our project is the database system. The database needs to be a secure place to store pertinent information pertaining to whether an individual poses a security threat or not. The card readers will be connected to the database using a secure unique connection, and upon inserting the card, the database will send back the public key, which unlocks the data on the card for the reader to verify. The following section will discuss in more detail the role and features of the database.

Due to the already large scope of our project, the actual implementation of the database will not be discussed. For analysis purposes, we will assume that it is possible to create a highly secure database although this is clearly not a trivial task. The database will contain a mapping between reader serial numbers and reader locations on the network. It will also contain a mapping between reader location and the access permissions for each reader. The access permissions are set so that each reader will only

have permission to see a given subset of flags that are relevant to its particular location. There will also be a separate table for the cards that will contain the personal ID numbers versus card ID numbers. These numbers will be mapped to a public key that can be sent when needed. Each record will also include a table of flags that can be set, such as suspected terrorist, fugitive, illegal immigrant, convicted felon, etc. These flags may contain various data from the government agencies, but will appear to be simply binary flags to the card readers. With the mentioned design completely and securely integrated together, the database should be able to meet the necessary requirements.

The newly created Office of Homeland Security will maintain the database. It will be able to be updated by a variety of government offices. These offices, FBI, CIA, NSA, IRS etc, will be able to put a flag on an individual along with fields explaining the reason for the flag. The design will not allow these agencies to see any other flags that may have been placed on the same person without the proper permissions or warrants, and the information along with the flag will not be sent to the readers during card authentication.

In the end, the database will need to be quite fast, highly secure, and easily manageable. This is a challenge in itself, but we believe it is feasible with current technology.

D. The Secure Channel

A secure channel for communications is critical to the security of this system. Each of the three potential solutions discussed in Section 2 of this report have distinct positive and negative tradeoffs. Each of these implementations pits cost versus speed and security. The dial-up service like the one used for credit card transactions is probably the cheapest option, but it is also the slowest and possibly the least reliable. On the other end, constructing a private network to house the data transfer for this identification system would be much more secure and reliable, but also incredibly more expensive. The other solution, use of a public network like the Internet, would be relatively inexpensive, relatively quick, but some security problems may be introduced. To narrow the scope of this project we will assume that the identification card system is on a private network. The communications protocol that we have developed could still be used over

the Internet in a secure fashion. A private network, however, allows us to reduce the risk of various network attacks like denial of service and database attacks. This also makes it easier for the central database to be assured of the location of the reader on the network, and it decreases the risk of having spoofed readers on the network.

In order to ensure the security of this channel, we will use techniques similar to Secure Shell (SSH) that we have discussed in class. The entire connection process is shown in the figure below. The handshake process will authenticate the reader and encrypt all of the sensitive information. The reader will initiate the connection by sending a connection request to the database along the reader's unique serial number encrypted with the database's public key. The database will decrypt the message and then look up the reader's serial number and authenticate that it resides in the proper location on the network. The database will then send back a large random bit string encrypted with the reader's public key. After decoding the string, the reader will send back the string encrypted with the database's public key. Once the database verifies the string, the handshake will be complete, and the string will be used as the session key. All future communications can be encrypted using this session key and the new Advanced Encryption Standard (AES).

When a user enters a card in the reader, the reader will immediately create the unique session key with the database. The reader will then send the person's identification number and the card serial number using AES symmetric encryption. The database will check for a match in the database, and send back the cardholder's public key and any associated flags. The public key can then be used to decrypt the information on the card, and the cardholder can be verified.

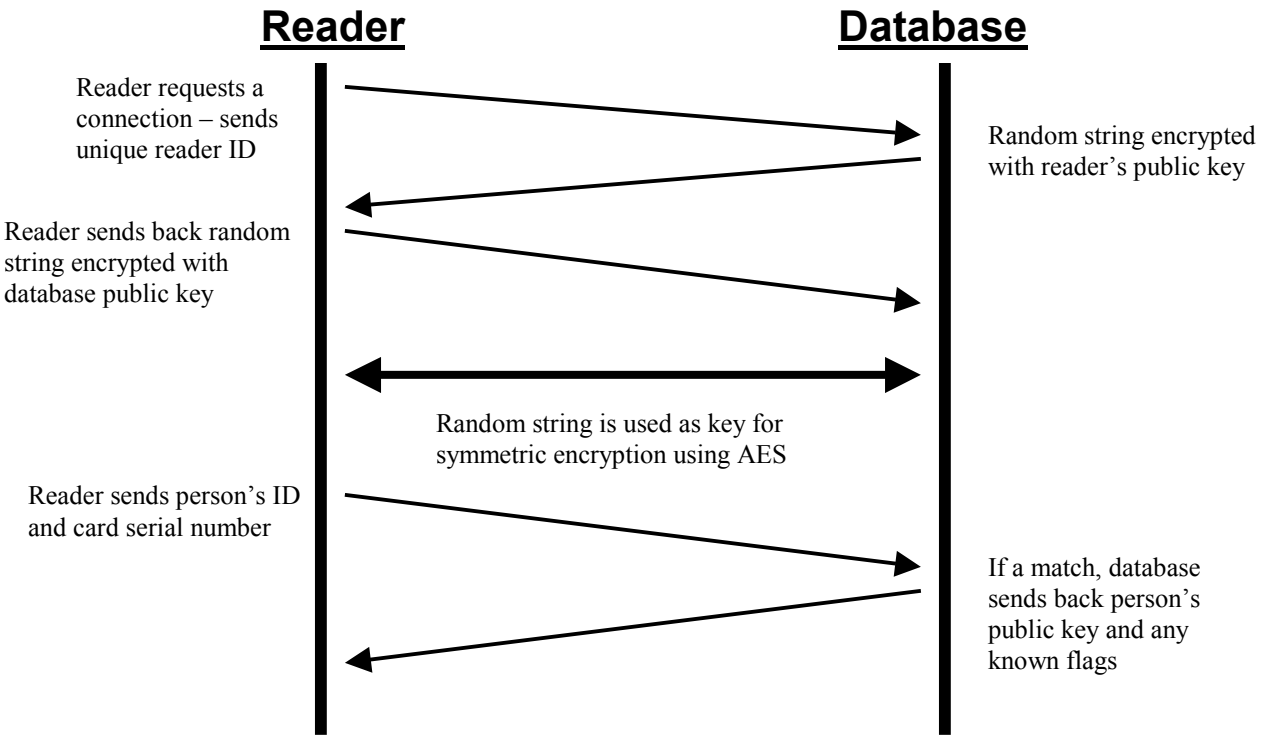

Figure 2. Secure Channel Communication

4. Evaluation

A. Overview

Reviewing the feasibility of our system from a security and functionality standpoint, our system proves to be robust, efficient, and secure. It is an efficient system because it provides a centralized system to the government for keeping a record of any individual located within the boundaries of the United States, hence reducing the time and error in tracking down potential criminals. Another benefit of our system is the minimal loss of privacy compared to great gains in security. This will be discussed in more detail in Part C of this section. Its robustness comes from the mechanism it proves for maintaining and transferring the data with the highest level of security, at each functional stage of the system. These stages include the storage of the data on the card, the transmission of the data through the secure channel and the storage of the data in the database. The robustness of our system to security flaws can be reflected by the resilience of our system to potential attacks.

As a whole, we feel that our scheme provides a viable design for a national ID system. Because the scope of this problem is incredibly large, there is no way we could take all implementation issues into account. We have focused on assuring that the main design is extremely secure from attacks while minimizing any losses of privacy or freedom.

B. Anticipated Attacks

This section will review a subset of some of the potential attacks we have considered when designing our system. Because of the large scope of this project and Larry Ellison's promise that Oracle can come through with a national ID database, we will assume that the database is completely secure. This is a broad assumption that should not be ignored in an actual implementation for obvious security reasons.

Attacks on the Card:

1) The attacker could forge the face of the ID card. This would not compromise the

high security mechanism of the card. In such a case, the individual can only misuse the fake card for low security identification. Tamper-resistant measures are also applied to the card to minimize this risk.

2) The attacker might be able to obtain the encrypted data from a card and forge the card using this data. In such a case the system will not function, as the attacker's fingerprint will not match the data on the card. Secondly, the new card serial number will not match up with the one in the database, so there will be no valid record for the attacker's forged card. Finally, if the attacker got past the previous two problems, the attacker would not have the private key that was used to encrypt the card whose identity was stolen. When the public key is returned from the database, it will not properly decrypt the card information and the attacker will not be authorized.
3) The attacker can try to obtain a card-creating machine, which encrypts the data on the card with a private key and discards the private key. To make sure that an attacker does not use such a card creator, a code will be required to be entered into the card creator each time a new card has to be created and this code would be updated at fixed intervals of time. The operator of the card creator would only know the code. Also, since the system knows the location of each reader, the attacker would have to be in an official card making facility to forge a card.

Attacks on reader:

1) The attacker could enable the card reader to store the card information and later use this information to forge a card. Such attacks cannot work in this system because the readers are only deployed at designated locations and each reader has its own identification number. Under the supervision of law enforcement authorities these readers can be kept under check. If stolen, using its identification number, it can de denied access to the database.

2) An attacker cannot make a reader because it would be impossible to register it with the database. The reader will not have its corresponding public key stored in

the database. Also, the reader will not have a designated location in the database records and so it will be denied access to the database.

3) Another possible attack by someone who would want to invade on another's privacy would be to enable the reader to store unencrypted information on it. The attacker would then try to obtain a log of all data that passed through the system. This would not be possible in our system because the readers are manufactured by a number of third party companies. If a company were to build logging capabilities into the reader, the other companies would publicly expose this practice.

Attacks on Communication Channel:

1) Assuming a private network is being used for communication in the system, the system is secure from most attacks. Denial of service attacks are possible if an attacker can gain access to the network, and there is no immediate solution to this problem.

Active eavesdroppers in the communication channel would not be able to spoof a card reader because it would be difficult to simulate the proper network location of a reader. Even if they could simulate another reader's location, they still do not know the private key for the reader to decrypt communications from the database. They could not create a new network location because there would be no valid entry in the database. A passive eavesdropper would not have the reader's private key, the database's private key, or the session key used for symmetric encryption. Under current technology and assuming random session keys, this scheme effectively thwarts passive eavesdroppers.

C. Security vs. Privacy Tradeoffs

In order for a national ID card to be widely adapted, Americans have to feel comfortable using them. As mentioned earlier, we spent a great deal of time and paid close attention to our method of providing a high level of security while still not infringing on the individual's privacy. We all know the fate of previous attempts at

national ID cards, and one of the main causes of failure was due to this infringement of personal privacy. In our design we have not taken away any additional rights than what is currently in place. Our low security level, is not only disconnected to any traceable government office, but also provides even more state of the art security than the current drivers' license. With our selection of locations, which involve the use of card readers, we feel that either Americans are willing to give up their personal privacy, or already have been currently. At airports, for example, most people would be willing to have their information be accessed from a government verifier in order to thwart the intentions of the fraudulent criminals. Our card will also be used to purchase guns, or to qualify for certain employment opportunities. In both of these cases the individual already submits to a background check. This heightened security level, with minimal affect on privacy, is exactly what this country needs to adopt a national ID card that would protect our society from many potential dangers.

5. Conclusion

The proposed card system provides a highly security scheme that also minimizes the invasion on privacy of an ordinary innocent individual. This privacy is ensured by not implementing any mechanism that could be used to track the movements of a person. We also use a safe database so that the government cannot gain access to the information that they not to see under Federal law. Finally, a secure data transmission, storage and reading scheme allows for secure exchange of information about the individual. While this privacy is ensured, we also make great strides in the area of security and authentication. A digitally encrypted card will be many times more secure than simple print cards that are in existence today. This will allow law-abiding citizens to enter critical areas with the confidence that they are safe from criminals and terrorists.

The main goal of our project was to show that a national ID system is feasible to implement in a secure fashion. The major concern going forward will shift from the feasibility of implementation to the level of public support for the added security these cards will offer. Before September 11, it would have been impossible to find nearly enough support to start a national ID effort. But with the security of our nation shattered by cowardly terrorists, many Americans are now willing to sacrifice some precious privacy. In the coming months, it will be interesting to see just how much privacy Americans are willing to give up in order to support a national ID card that may help maintain that precious feeling of security.

Works Cited

[1] http://www.litronic.com/solutions/pkicard.html

[2] http://www.nuance.com/pdf/verifier3_techds.pdf

[3] http://www.faqs.org/faqs/jpeg-faq/part1/

[4] http://www.autostar.com.sg/pollexfamily.html

[5] http://drl.cs.uiuc.edu/security/

[6] Marlene Theriault & William Heney. Oracle Security. O'Reilly, 1998.

[7] Cartwright, D. *Setting up a Virtual Private Network*. Internet Magazine. Feb. 2001, 123.

[8] Feinstein, D. *Senator Feinstein introduces bill*. http://www.senate.gov/~feinstein/releases01/r-visas1.htm

[9] Greene, T. *Virtual private network market coming of age*. Network World. May 14, 2001, 14.

[10] *ID cards opposition grows*. BBC News. Sept 24, 2001. http://news.bbc.co.uk/hi/uk_politics/newsid_1559000/1559245.stm

[11] Lemos, R. *Should the government get its own Net?* ZDNet News. http://news.excite.com/printstory/news/zd/011011/07/should-the-government.

[12] *National ID Cards*. Electronic Privacy Information Center. http://www.epic.org/privacy/id_cards

[13] *National ID Card*. The Winds. http://www.thewinds.org/1997/06/id_card.html

[14] Rogers, P and Elise Ackerman. *Oracle boss urges National ID cards, offers free software.* Sept. 22, 2001. http://www.siliconvalley.com/docs/news/svfront/ellsn092301.htm

[15] Rossant, J. *Should the U.S. Follow Europe's Lead?* BusinessWeek Nov 5 2001. http://www.businessweek.com/magazine/content/01_45/b3756010.htm

[16] Scheeres, J. *ID Cards are de Rigueur Worldwide*. Wired News. Sept. 25, 2001. http://www.wired.com/news/print/0,1294,47073,00.html

[17] Shein, Esther. *Full Steam Ahead (virtual private network technology).* PC Week Jan. 18, 1999, 69.

[18] *Testimony of ACLU Legislative Counsel Katie Corrigan*. ACLU. http://www.aclu.org/congress/l111601a.html

[19] Williams, K. *U.S. Seeks to Build Secure Online Network*. http://www.washtech.com/news/govtit/13066-1.html.

[20] *You Want Security? They've Got Security*. BusinessWeek Nov 5 2001. http://www.businessweek.com/magazine/content/01_45/b3756009.htm

[21] *Privacy in an Age of Terror*. BusinessWeek Nov 5, 2001. http://www.businessweek.com/magazine/content/01_45/b3756001.htm

[22] *Risks of National Identity Cards* by Peter G. Neumann and Lauren Weinstein. http://www.csl.sri.com/users/neumann/insiderisks.htm, November 11,2001.

[23] *Americans mull national ID cards*. http://www.cnn.com, October 31, 2001.

[24] *A question of Identity*. http://www.bbc.co.uk, September 25, 2001.

[25] *National ID cards: One size fits all.* by Daniel J. Walkin. The New York Times, October 7, 2001.

[26] *National ID cards: New technologies, Same Bad Idea* by Adam Thierer. Techknowledge, September 28, 2001.

[27] *Is a National ID card the answer?* The New York Times October 16, 2001.

[28] *Why fear National ID Cards* by Alan M. Dershowitz. The New York Times October 13,2001