Secure ID Report:
*Meeting the Needs of Governments and Citizens*

Balancing security, privacy, cost effectiveness and convenience in a world where data breaches and fraud are commonplace, requires the use of Secure ID.

Catherine Johnston, President & CEO
ACT Canada: stakeholders driving secure payment evolution and digital identity
2015/01/12
Secure ID Report: Meeting the Needs of Government and Citizens

Contents

Executive Summary ............................................................................................................................................ 5

1 Defining the Issue ........................................................................................................................................... 7
  1.1 Overview .................................................................................................................................................. 7
  1.2 What is a secure identity? .......................................................................................................................... 7
    1.2.1 Strong Authentication – Are you the person to whom the ID was originally issued? ..................... 8
    1.2.2 Tamper and counterfeit resistance: Can I trust the ID you are presenting? ................................. 8
  1.3 Who are the Secure ID stakeholders & what do they want? ................................................................. 9
    1.3.1 Taxpayers .......................................................................................................................................... 9
    1.3.2 Government of Ontario .................................................................................................................. 10
    1.3.3 Ministry of Health .......................................................................................................................... 10
    1.3.4 Doctors, Nurses and all other Healthcare Providers ....................................................................... 11
    1.3.5 Criminals ........................................................................................................................................ 11
    1.3.6 Law Enforcement ............................................................................................................................ 11
    1.3.7 Suppliers .......................................................................................................................................... 11
  1.4 What are the consequences of having unsecured identity? .................................................................... 12
  1.5 What does this have to do with Secure ID? What are the advantages of raising the bar on ID security? .............................................................................................................................. 12
  1.6 Why isn’t the status quo good enough? ................................................................................................. 13
    1.6.1 How many health records do you have? ......................................................................................... 13
    1.6.2 Quality of Healthcare ..................................................................................................................... 13
    1.6.3 Technology ....................................................................................................................................... 14
  1.7 Who says we have a problem...? ............................................................................................................ 14

2 Defining the Solution .................................................................................................................................... 17
  2.1 Overview ................................................................................................................................................ 17
  2.2 How do we solve the access problem? .................................................................................................... 17
  2.3 How does a Secure Identity differ between the physical and digital identity? .................................... 18
  2.4 Applying the principles and securing our digital identity ..................................................................... 18
  2.5 What is the state-of-the-art in secure ID ............................................................................................... 19

3 Secure ID in other Jurisdictions .................................................................................................................. 21
  3.1 Overview ................................................................................................................................................ 21
  3.2 Governments with Secure ID initiatives ................................................................................................ 21
    3.2.1 British Columbia ............................................................................................................................ 21
    3.2.2 France ............................................................................................................................................. 22
4 Implementing a Secure ID Solution in Ontario

4.1 Determine cut-off date for red and white health cards

4.2 Decide on multi-application cards

4.3 Determine privacy implications

4.4 Determine authentication requirements

4.5 Request for proposals

4.6 Budget

4.7 Legislative changes

4.8 Select vendors

4.9 Re-enrollment strategy – schedule and criteria

4.10 Rollout schedule

4.11 Public communication strategy

4.12 Public consultation

4.13 Stakeholder engagement

4.14 Build the system and cards

4.15 Rollout secure chip cards and infrastructure

5 Summary of Net Gains for Ontario

5.1 Overview

5.2 Improved health outcomes /Renaissance of the Ontario Health Care system

5.3 More accurate health information for research, operational, policy and funding decisions

5.4 Reduced cost of fraud

5.5 Proactive treatment for patients

5.6 Reduced administrative time and reduced errors in keyed data

6 Recommendations

6.1 Upgrade security on health cards

6.2 Implement strong authentication

6.3 Issue multi-application cards

6.4 Review all government issued ID
APPENDIX A......................................................................................................................................................41
Glossary............................................................................................................................................................43
Bibliography ....................................................................................................................................................47
EXECUTIVE SUMMARY

About this report

This report provides an analysis of the need for secure ID for all levels of government that issue either physical or digital IDs, using the Province of Ontario’s Ministry of Health as an example.

It looks at other jurisdictions that have already made the move, their objectives and the results. It also reports on a similar move by the global financial sector. The report outlines major milestones and best practices for the implementation of secure ID. Although it uses Health ID as an example, the steps would be similar for any government department or organization.

Findings

Both the public and private sectors are being compelled to raise the bar on security for cards that link people to specific rights or privileges. This is to protect people from identity theft and to reduce fraud in government funded programs. Organizations want citizens and clients to interact with them online because it is cost effective, so there are similar needs for increased online security.

An analysis is provided for the savings that the Province of Ontario could realize if the current magnetic stripe OHIP (health) card was upgraded to a secure chip card. This was based on comparing published figures from British Columbia when they implemented their secure CareCard and the 2011 Ontario payment to doctors for healthcare services. Although a conservative approach was taken in this analysis, there was still over $3.5 billion annual savings identified for the Ministry of Health budget.

The move to secure ID for the Ontario Ministry of Health also comes with a bonus, in that new cards could be leveraged to provide the secure access process needed to implement a full e-health system. This in turn would support more savings and better health outcomes for citizens.

Conclusions

- Magnetic stripe technology cannot meet the criteria for secure ID and is being phased out by ID issuers around the world in both the public and private sectors.
- Secure access to e-health data requires secure ID for the patient, all healthcare providers and all other administrative resources.
- Ontario is trailing behind the Province of British Columbia, Passport Canada, Canadian banks and credit unions in upgrading to secure ID.
- A viable business case exists for secure ID in health and other government issued ID.
Recommendations

Adopting best practices from other jurisdictions and sectors:

- **Upgrade security on health cards**
  This would involve adding a secure chip to meet two objectives. The first is to enable the card to be used as secure access to e-health records. The second is to make the cards both counterfeit and tamper resistant to effectively combat fraud.

- **Implement strong authentication**
  Strong authentication will be required for secure access to e-health. It will also meet the need of reducing user fraud that involves one person loaning their card to another.

- **Issue multi-Application cards**
  Either offer citizens the ability to carry more than one provincial government ID application on a card or mandate this. Citizens are comfortable with multi-applications on smart phones, computers and other devices. This will reduce government costs.

- **Review all ID policies and processes**

  Governments at all levels should review the risks to their citizens, as well as to their own costs and reputations of not using Secure ID and strong authentication.
1 DEFINING THE ISSUE

1.1 OVERVIEW

In this chapter we will look at:

- what makes identity secure
- who are the stakeholders and what do they want
- what problems could be solved with secure ID
- what opportunities could be facilitated
- why is the status quo no longer supportable

- and who says it’s a problem...

1.2 WHAT IS A SECURE IDENTITY?

In a general sense, security is basically the protection of something valuable to ensure that it is not stolen, lost, or altered. This applies to our physical and digital worlds. Both the public and private sectors want to make an increasing number of services available online, but that requires new levels of security.

Secure identity is the verifiable and exclusive right to use the identity information being presented by an individual, to access a set of privileges. In other words, it is my ability to prove to you that I am the person who is entitled to do or have something. It could be my driver’s licence, health card, office access badge or my computer logon credentials. Each of these is secure if it is both sufficiently tamper and counterfeit resistant and the person presenting it can prove they are the person to whom it was originally issued.

At a time when identity theft is at an all-time high and reports of data breaches are increasingly frequent, secure identity is the tool that companies and governments are turning to in order to protect their reputations, revenue and clients. This was inevitable because of the increasing public reliance on computer and mobile applications that touch everyone’s daily life, from parking meters to national defense.
Let’s look at the two underlying principles of secure ID.

1.2.1 STRONG AUTHENTICATION – ARE YOU THE PERSON TO WHOM THE ID WAS ORIGINALLY ISSUED?

Authentication is the process of establishing that the authorized user is the person who is making the transaction. There are several well established definitions. The European Central Bank’s definition has wide acceptance especially with payment networks such as American Express, MasterCard and Visa. They define Strong Authentication as “a procedure based on the use of two or more of the following elements – categorized as knowledge, ownership and inherence”:

✓ something only the user knows, e.g. static password, code, personal identification number
✓ something only the user possesses, e.g. token, smart card, mobile phone
✓ something the user is, e.g. biometric characteristic, such as a fingerprint

In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the Internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data and either biometrics or knowledge based information to authenticate the presenter.

Much of today’s identification does not use strong authentication, leaving it open to fraud. For example, paper or plastic health cards that only have the user’s name, but no photo. Better cards have the user’s photo, but that is only good if the card can’t be tampered with and you can be sure that the photo is the one originally put on the card.

1.2.2 TAMPER AND COUNTERFEIT RESISTANCE: CAN I TRUST THE ID YOU ARE PRESENTING?

Billions of secure smart devices are shipped annually and many of these are used for secure ID. In fact, in 2010, 100 million secure chips were shipped for government use and this number has grown every year. In 2014 it is expected to be 240 million.¹ The devices could use any number of form factors, but they all contain a secure chip. The form factors could be cards, fobs, sim cards for use in mobile phones, even jewellery can contain secure chips.

The chips are similar to other computer chips in that they can store information and compute, but they have additional security features that make them counterfeit and

¹ Eurosmart
tamper resistant. For security reasons, this report will not go into details, but here are publically known features.

The chip is an active computing device. It can be programmed to perform many security functions. For example, it can require the chip reader to identify itself as a trusted device before conducting a transaction. It can encrypt data before transmission and decrypt incoming data. It can store biometric data for security usage. It can hold a set of rules that dictate what the card owner is entitled to do, including reference to when and where they can perform certain functions. This can be valuable if your application is for physical access. The chip can be programmed with a range of authentication rules. For example, it may require a simple PIN (personal identification number) to logon to certain computer applications, but a biometric for high security programs. The same could be true if it is a health card being used at a doctor’s office, versus being used to provide consent for an operation. All rules are determined by the ID issuer, even the choice to require no authentication if desired.

Let’s look at this in the context of healthcare stakeholders.

1.3 WHO ARE THE SECURE ID STAKEHOLDERS & WHAT DO THEY WANT?

1.3.1 TAXPAYERS

Healthcare has always been a priority for Canadians. Not only do they want better and more efficient healthcare but they want a system in which the abuse is reduced. To ensure efficient and fraud free healthcare, Canadians since the 1990’s have expressed their desire to support secure ID cards if they addressed the ongoing fraud and abuse in the system.

In 1994, the Toronto Star asked a question related to ID cards in their popular “You Asked Us” column. They asked whether citizens would be willing to carry a national ID card. Although more than half who responded said they would, there were several comments about police states and similar concerns. A second question was asked several months later. This time more information was provided as to the reason why such a card would be issued. The question was, “Do you think all Canadians should carry an identity card to crack down on welfare and medicare abuses?” Of 1,535 calls 89% said yes on February 24th 1994. As individuals we constantly assess the risks that we face in the world and make decisions related to minimizing those risks.

Recently, a poll commissioned by the Ontario Medical Association found that health care remains an important issue to Ontarians personally. Further, more than two thirds of Ontarians (67.6%) say that a provincial party with a strong platform on health care would have an impact on their likely vote for a party.

The survey was commissioned by the Ontario Medical Association. This random telephone survey of 500 Ontarians was conducted between May 22nd and 26th, 2014,
as part of an Ontario omnibus survey by Nanos Research. The dual frame sample included both land and cell-lines across Ontario. The results were statistically checked and weighted by age and gender using the latest Census information and the sample is geographically stratified to be representative of the population of Ontario. Individuals randomly called using random digit dialing with a maximum of five call backs. The margin of error for a random survey of 500 Ontarians is ±4.4 percentage points, 19 times out of 20. (https://www.oma.org/Resources/Documents/NanosPoll.pdf)

For Ontario citizens there are several objectives. If asked, the likely answer would be that more funding for healthcare should be available and yet 42% of every government dollar spent goes to healthcare. We have children, aging parents and our own health to protect and are aware that an aging population is likely going to require more healthcare funding.

The other side of the coin is taxation. It is not acceptable that tax dollars be spent on healthcare for persons who are not entitled to government funding, particularly not at the expense of our own health care funding. Nor is it acceptable that our current system is susceptible to fraud at a time when other jurisdictions and other service sectors have proven that there is a better way. We know that our financial institutions have had to replace magnetic stripe cards with secure chip cards to protect our bank accounts and payment cards and we would expect the government to follow suit.

### 1.3.2 GOVERNMENT OF ONTARIO

A primary duty of any provincial government is the health and well-being of its citizens. This transcends any and all political ideologies. It is reasonable to assume that governments are obligated and seek to ensure that the best means available are used to guarantee that healthcare funds are spent wisely. While all persons should have access to healthcare, government funds should only pay for eligible citizens.

The government will also want to leverage any investment in secure ID infrastructure. This would include using any new cards to enable controlled access to e-health records. The investment could also be leveraged by reducing existing costs through allowing citizens to use the security and privacy capabilities of the chip to carry multiple ID “apps” or one digital credential to let a back-end system handle the authentication.

The government will also benefit by the ability to fund as much of the cost as possible through the fraud reduction and once the fraud has been minimized, those funds can be earmarked for other government projects.

### 1.3.3 MINISTRY OF HEALTH

As administrator of the healthcare budget, the Ministry of Health wants to ensure that the healthcare system is responsive, efficient, fair and honest; and seen to be so. A key
step in improving efficiency both administratively and medically is e-health. When e-health becomes an effective operational reality, the use of tele-health can be maximized. Both of these programs are core to increasing the long term efficiency of our system.

The Ministry will also want to use e-health data to better allocate resources and proactively manage services.

1.3.4 **DOCTORS, NURSES AND ALL OTHER HEALTHCARE PROVIDERS**

Doctors, nurses and first responders, as the frontline healthcare providers, are acutely aware of the stress and inefficiencies of our current system. Reducing fraud would be a direct net financial gain to the entire system. In turn, that benefits healthcare professionals by making more resources available to them with the same allocated budget.

Today, it is the Healthcare professional who has to determine whether an OHIP card is authentic. If they fail, they do not get paid. While this is less of a problem when the Doctor knows the patient, it is a real issue where that relationship does not exist. For example, walk-in clinics, emergency wards and doctors taking new patients are all at risk.

Having patients’ medical records available online would reduce paperwork and the opportunity for data entry mistakes. Also, having instant online access to a patient’s complete health history benefits everyone from first responders at an accident scene, to hospital staff and doctors at their offices. The desired result is better healthcare outcomes.

1.3.5 **CRIMINALS**

A secure health ID that cannot be counterfeited thwarts organized crime. Secure chip cards are counterfeit resistant as other jurisdictions and sectors have proven. Secure ID practices effectively reduce Medical Identity Theft. This is one stakeholder group that would like to maintain the status quo.

1.3.6 **LAW ENFORCEMENT**

The corollary for the reduced crime is the reduced need for law enforcement resources to be allocated to monitoring and seeking out fraud and the perpetrators.

1.3.7 **SUPPLIERS**

New business opportunities for traditional and non-traditional government ID suppliers could be opened up, as seen in other jurisdictions.
1.4 WHAT ARE THE CONSEQUENCES OF HAVING UNSECURED IDENTITY?

Ontario spends 42 cents of each budget dollar on healthcare, which was $51 billion in 2013 – 2014. This is 11.5% of the provincial gross domestic product (GDP), up from 7.5% in 1982. The increase is publically attributed to an aging population, decrease in health transfer funds from the federal government and inflation, but there is another factor. That is a lack of secure ID related to health care. The current magnetic stripe technology used on OHIP cards cannot adequately protect against counterfeit cards or fraudulent use of authentic cards. It facilitates Medical Identity Theft and cannot facilitate secure access of e-health records.

The population in the Toronto area alone is projected to increase 23.6%, a total of 3.45 million, by 2030, and Ontario expecting a total growth of about 29%, or 17.1 million people by 2036 (Ontario Population Projections, 2013). Furthermore, the senior demographic aged 65 or older could reach 4.2 million, or 24.0% of the population by the same year (Ontario Population Projections, 2013). These demographic trends will severely affect our healthcare system.

Our healthcare system is under stress. It suffers from increasing costs and administrative inefficiencies and is challenged to provide a security infrastructure to enable e-health. Currently, without investing more money in the system, there are limited means to improve patient outcomes and enhance physician and patient relations.

More funding is not a viable option. Other means to improve healthcare outcomes must be taken. We are reaching the limits of what can be accommodated by taxpayers, and no one wants to see service cuts, patient co-pay schemes, increased wait times or higher taxes, so other savings must be identified.

Other jurisdictions have invested in secure ID to improve their healthcare, such as in France and other countries of Europe and closer to home, in British Columbia. Other industries have also raised the security bar on cards, such as the financial sector.

1.5 WHAT DOES THIS HAVE TO DO WITH SECURE ID? WHAT ARE THE ADVANTAGES OF RAISING THE BAR ON ID SECURITY?

The current OHIP cards, both the red and white and the green versions, are billing cards, not true healthcare cards that can link authorized parties to health data. Both existing cards use magnetic-stripe technology which is vulnerable to fraud.

One of the key challenges with the current OHIP card is the inability to know whether it is genuine or counterfeit when it is presented, and if the person presenting it is the one to whom the government issued the card. The green card carries a photo and uses a number of secure printing techniques, making it more secure than the red and white, but neither is as secure as other health or payment cards.

---

2 Institute for Competitiveness and Prosperity, Building Better Health Care: Policy Opportunities for Ontario, April 2014
Secure ID would overcome these issues. It is both counterfeit and tamper resistant. It can be a partner in enforcing your program’s security design and would be robust enough to enable secure access to e-health records.

When information is stored on a secure chip, it can be trusted. That means that information about the cardholder, which is often keyed into a computer at the hospital, could be retrieved from the chip. This could reduce wait times and reduce keying errors and it could provide another benefit. Currently a sheet of labels containing patient information is printed when a person is admitted to the emergency ward. It travels with the patient and labels are used for various procedures. Those left over are thrown out. In addition to the cost of the labels, it is possible that an identity thief could salvage the labels from the garbage. All this could be eliminated if the same information was read from the card when needed and printed on the appropriate form.

Done properly, implementing a health card, as opposed to a billing card, is an opportunity to improve the healthcare system in Ontario. Other countries, as we illustrate below and credit and debit networks such as American Express, Interac, MasterCard and Visa are implementing cards with secure digital identities linked to secure networks. Since implementing these programs, they have seen significant drops in the occurrences of fraud. In systems still using magnetic stripe technology, such as the United States where chip technology is just beginning to be implemented, fraud rates remain high. (see 3.3 for more details)

1.6 WHY ISN’T THE STATUS QUO GOOD ENOUGH?

1.6.1 HOW MANY HEALTH RECORDS DO YOU HAVE?

Any given patient or family can have multiple medical records. Your family doctor has a chart for you. Every specialist you see also has a chart. So does every walk-in clinic and every hospital where you have been treated. Over a lifetime, that can be many charts that represent your overall medical history. Keeping track of information through our paper system is awkward, prone to mistakes and expensive. Although family doctors often get information from other health care providers, they don’t get all the information that is on those charts, and the others (ERs, specialists and walk-in clinics) do not have access to those additional charts. You can see where access to your complete health information would be beneficial to anyone treating you. E-health is needed to deal with this problem.

1.6.2 QUALITY OF HEALTHCARE

The underlying premise of e-health is that healthcare improves when timely and accurate information is available to healthcare providers. It is also believed that access by patients to their health information may increase their steps to proactively maintain good health, reducing long term costs to the system. In order to reach these goals, all parties need secure ID capable of not only granting access to specific records, but
providing and enforcing rules as to what they can do with each data field. None of the existing OHIP cards are capable of this.

1.6.3 TECHNOLOGY

Whereas conventional magnetic stripe technology has a preloaded set of information which can be skimmed (read and copied) and duplicated (counterfeited), a secure chip card is built on microprocessor technology. The counterfeit vulnerability has been exploited by organized crime resulting in a move away from the use of magnetic stripe technology by both the public and private sectors.

The secure chip, however, can store information that dictates what the cardholder can do and then can make the cardholder prove they are the person entitled to use that card. For example, keying in a PIN, as we do when we use our credit and debit cards, helps authenticate the person presenting the card. Then, if we were accessing our e-health record, the chip will be programmed to know whether we can view, add, modify or delete information on a field by field basis. This same process is used to ensure that authorized doctors, hospitals, and medical staff can access the health network and patient records and dictates their data privileges.

Secure chips also support digital signatures which can be used to determine that the card was issued by a valid organization and that the data on the card has not been fraudulently altered since issuance. This technology is, by design, highly counterfeit and tamper resistant. Unfortunately, magnetic stripe cards are not.

Further, magnetic stripes are vulnerable to interference from external magnetic sources. Indeed ‘demagnetization’ can occur through regular wear and use. Chip technology is not damaged through this process, which greatly increases the lifespan of individual cards.

1.7 WHO SAYS WE HAVE A PROBLEM...?


For example, the Ontario Provincial Police (OPP) have 28 dedicated officers to investigate health fraud. The Auditor-General identified the limited scope of permitted investigation tools that this investigation unit has, as a hindrance to identifying and preventing fraud. This of course also hinders the ability to understand the scope of the problem in Ontario.

An idea of the true scope of the problem can be gleaned from British Columbia’s experience and Canada’s banking sector. In British Columbia, when they converted to a Secure Chip Service Card, there was a population of 4.5 million, but there were around 9.1 million
magnetic striped Health Care cards in circulation. This card was similar to Ontario’s OHIP card.

In the Canada’s financial sector, domestic counterfeit card fraud has been reduced significantly. The Interac Association reported that Interac debit card fraud losses as a result of skimming (counterfeiting) are at a record low – decreasing to $29.5 million in 2013 from a high of $142 million in 2009. Only 25 percent of losses in 2013, or $7.3 million, are the result of fraud exploitation within Canada. Total losses in 2013 represent 0.0093 percent of domestic Interac debit card volume (0.93 basis points) and the lowest volume of recorded fraud losses. As a result of this significant decline in fraud exploitation, the number of cardholders reimbursed by financial institutions fell to 72,200 in 2013 from 238,000 in 2009. Cardholders are protected from losses under the Interac Zero Liability Policy.

“The combination of sound policies, investments in technology - such as chip and fraud detection - and outstanding collaboration with financial institutions, acquirers, merchants and law enforcement makes the Interac system a world-class payment network,” said Caroline Hubberstey, Head of External Affairs for Interac Association and Acxsys Corporation. “Debit products are about accessing people’s money in their bank accounts and need to offer stronger protections. Debit is our expertise, and when we have control over the payments environment, our leadership in fraud prevention is evident.”

Chip technology is another key part of the Interac fraud prevention strategy. This smart technology also enables advancements like Interac Flash®, which is currently being rolled out across the country.

While not all contactless technologies are created equally, the Interac Flash solution is secure because it leverages secure chip processing, not magnetic stripe data type processing. This, along with the policies outlined above, protects Interac Flash against counterfeiting and transaction replay types of fraud, including electronic pick-pocketing.

While mag stripe technology served us well for many years, it cannot withstand the types of attacks that are commonplace today and cannot effectively be used where security is an issue.
2 DEFINING THE SOLUTION

2.1 OVERVIEW

In this chapter we will look at:

- How to enable secure access to e-health records
- How secure identity differs between the physical and digital worlds
- The state-of-the-art in secure ID

2.2 HOW DO WE SOLVE THE ACCESS PROBLEM?

We are well on our way to making e-health access happen. The first, and hardest step, was to determine how to access information when much of it is in different formats. Because information has been recorded over the years and there was no “standard” format in place, a lot of work was necessary to make it possible for information from one computer system to be made readable by another. Much of that has been done.

What is still outstanding is the work to build a secure, privacy protective mechanism that would allow each of us, as well as all our healthcare providers, to work with the information. That could be facilitated by a secure chip health card. Other jurisdictions and sectors use secure chips to control access.

Think of accessing health records as being similar to your bank account. Your secure chip bank card allows you to do certain things at an ATM, once you have proven to the system that you are the “owner” of the account. You do that by using your card and providing your personal identification number (PIN). Then you can deposit money, take money out of your account, transfer funds and do other things. Bank employees can only do those things for you if you present your card. Without your card and PIN, they can’t prove that they are entitled to do them. On the other hand, those employees can prove to the system that they have the right to do other things. For example, they can withdraw funds from your account to pay utility bills if you have set up a pre-authorized debit.

How does that equate to your health information? With an e-health system:

- You could be authorized to view the data on your record(s), and to change your address. You could be blocked from adding any other information or either changing or deleting existing information. Each of these “rules” would be defined on the chip on your card.
- The receptionist at a doctor’s office or the administrative staff at the hospital might be allowed to view some, or all, of the data and add or change your weight and height. Once again, the rules would be written on their chips.
- Your doctor would be authorized to view all data, add data, but not modify or delete anything.
All this would be defined by the Ministry of Health and stored on your health card or the healthcare provider’s access card.

Globally, secure access to digital records is widespread and effective with proven track records, as will be discussed in Chapter 3.

2.3 HOW DOES A SECURE IDENTITY DIFFER BETWEEN THE PHYSICAL AND DIGITAL IDENTITY?

If shopping in person, we provide a secure credit or debit card with our name on it. Even though we have possession of this identifying item (aka the “token”), we still need something which only we know to identify us as the rightful owner of the card. In Canada, we use a PIN to identify us as the unique individual who is authorized to use that payment card. You have a token (your card) and you know the password (unique knowledge of the user).

When online, we can’t use the physical token (our card), as one of the elements of proving that we are who we say we are – the person to whom the card was issued. We may have the account number of that card, but the card itself is not in the presence of the merchant or government department. This means that we need something else to prove that we are authorized to do whatever we are trying to do online.

For online transactions we need a secure “digital identity”. It must be capable of establishing that the party asking for access to information or seeking to buy goods or services is entitled to do so.

There are other options. One is to use the physical card with a reader, or USB fob, attached to a smart device. Another is to “accept” the secure ID credential that was issued by another source.

2.4 APPLYING THE PRINCIPLES AND SECURING OUR DIGITAL IDENTITY

To use secure chip technology to implement a true Health card is not reinventing the wheel as we will see in Chapter 3. Furthermore, in chapter 4, we will outline the critical path to implementing the solution by utilizing the well-established principles of secure identity.

- determine how to authenticate who is authorized to receive government funded healthcare
- re-enroll authorized healthcare users only (ie citizens)
- decide how to verify that the card presenter is the person to whom you issued the card
- introduce counterfeit, tamper resistant cards, secure chip cards
- deploy the necessary infrastructure (ie. card readers)
- change legacy computer systems
- potentially introduce enabling legislation
2.5 WHAT IS THE STATE-OF-THE-ART IN SECURE ID

Technology has enabled different jurisdictions and industries to evolve highly secure digital identities. These include secure chip technology, biometrics, dynamic password generators and cryptographic algorithms. Facial recognition, iris and fingerprint are the 3 most used biometrics

Today they are used for e-passports, payment cards, health and other government ID.

Secure chip cards are embedded with microprocessors that can encrypt and securely store information. They allow access to that stored information only to authorized users. The data access rules can be enforced by the secure chip, even when used offline.

Secure chip cards can support personal identification numbers and biometrics (e.g., a retina scan) to further protect access. They also can support digital signatures, which can be used to determine that the card was issued by a valid organization and that the data on the card has not been fraudulently altered since issuance. Their chip technology, encryption and other cryptography measures makes it extremely difficult for unauthorized users to access or use information on a secure chip card or to create duplicate cards.

Biometrics is the adoption of inherent aspects of a person into the authentication process of the token. Finger prints or retina scans are two of the more common. As noted above, secure chip cards can be adapted to use biometrics. Nexus, the border crossing program for Canada-USA, uses biometrics.

E-passports use a combination of biometric and chip technology to authenticate the passport holder and prevent duplication or fabrication of false documents. Both Nexus and E-passports are discussed in Chapter 3.

These advances are not only technological. We are seeing changes in acceptance of third party authentication. This happens when someone’s identity is ‘vouched for’ by a third party who already has an established relationship with the person. It is the digital equivalent of a reference for the person seeking authentication. In Canada, there are more than twenty federal government programs where online access can be granted through the use of the person’s online banking credentials.

Third party authentication is the use of the authentication credentials from a third site (site B) for authentication to access another site (site A). The third party who verifies the user’s credentials are considered secure by the first site, site A and are pre-approved. For example, to access a government site one would use one’s online banking credentials. The bank’s system authenticates you but privacy is assured in the sense that the bank does not know what institution is seeking authentication.
The need for strong digital identities will grow as people use their computers, tablets and mobile phones to interact with the public and private sectors. From the government’s point of view, the cost to interact with a citizen is less expensive online than in person, so digital identity is important.

Chip cards are an investment in our future. They are able to adapt to new and expanded purposes. Chip cards are inherently future proofed unlike magnetic striped cards.
3  SECURE ID IN OTHER JURISDICTIONS

3.1  OVERVIEW

Secure ID around the world is subject to attacks and both the public and private sectors monitor these so that they can increase security as needed. One of the upgrades has been to move from magnetic stripe technology on cards to the use of secure chips. This has been instrumental in reducing counterfeit ID, and depending upon the cardholder verification method (e.g. PINs, biometrics etc.), has also reduced fraudulent use of authentic IDs.

3.2  GOVERNMENTS WITH SECURE ID INITIATIVES

3.2.1  BRITISH COLUMBIA

Why Secure Chip ID?
British Columbia had 9.1 million magnetic stripe “CareCards” in circulation for a population of approximately 4.5 million residents; more than two cards for every person. A need was identified in British Columbia by the public administration, elected officials, and taxpayer stakeholders that upgrades were necessary to the aging card infrastructure to deal with this problem.

How?
As of February 15, 2013, British Columbia started phasing out the magnetic stripe CareCard replacing them with the secure chip “BC Services Card”, designed to transform the way BC does business and “leverage technological solutions and innovation”. Residents of BC have until 2018 to update their cards to the Services Card and may continue to use their CareCard during a grace period.

Under the new system citizens have the option to obtain an alternate driver’s license card, or combine the two. Those who choose to combine their cards are protected by a firewall that protects the information in each application. Police are not able to access medical records, and healthcare providers cannot access the driver’s data.

The government dealt with security, privacy, public communication and other issues. Many private sector organizations that deal with these issues in the financial sector were consulted.

The Result
British Columbia’s implementation of its secure chip card continues with wide support and provides a made-in-Canada approach for the implementation of a government secure chip ID Card. Note: secure cards can use one certificate for authorization or multiple certificates where appropriate for multiple card applications.
Secure ID Report: Meeting the Needs of Government and Citizens

See Appendix A for the June 2014 press release from the Government of British Columbia.

3.2.2 FRANCE

**Why Secure Chip ID?**
Implementation of secure chip technology in France was a logical step towards efficiency and cost control within their health network. France needed a way to control a large volume of paperwork associated with tremendous healthcare spending (second in the world in 1997 at the time of launch).

**How?**
Originally conceived as early as 1978, France launched their Sesame Vitale Smart Card program in 1997 and the successor, Sesame Vitale-2, in 2007. In the Sesame Vitale system, what previously took two months to process and reimburse to citizens, can now be accomplished in a few days. The program is managed by the state controlled social security organization, known by its French acronym (CNAM). Information on treatment and cost is processed at the doctor’s office and is immediately transmitted to the health insurer. Both the service provider and the patient have secure chip cards to access the system. The Sesame Vitale system is managed by the government and was initially met with resistance by professionals who perceived interference with their practice. Through information and cooperation by the government, practitioner objections were resolved and there are now over 60 million combined users between Sesame Vitale and Vitale-2.

**The Result**
Widely viewed as one of the best healthcare systems in the world, France combined private and public sector services to produce extremely satisfied consumers and healthy outpatients. Furthermore, through a variety of public policies and initiatives ensures universal coverage to the population. Patient choice is maintained throughout the process.

Since implementing the smart (chip) card system, France’s healthcare system has seen an annual saving exceeding 1 billion euros, reduced expenditures, increased patient privacy, and record turnaround time for settlements as fast as a few days. The power of the system lies in its non-contestable ability to document identity.

3.2.3 GERMANY

**Why Secure Chip ID?**
Germany’s healthcare system is one of the oldest. It was enacted in the late 19th century. The system uses little of the public coffer to function. Instead, they rely on mutual investment by the workforce into non-profit insurance companies. The investment is scaled at about 8 percent of their income. There are no deductibles in German healthcare. For-profit insurance is available to those who are self-employed.
Enrollment into healthcare is mandatory for all citizens including working professionals, students, and elderly into either non-profit insurance coverage or for-profit private payment. The government itself does not provide healthcare, but strictly regulates and enforces the non-profit, compulsory service. It’s an individual’s choice to pay for private insurance.

To reduce fraud and increase efficiency, especially communication amongst multiple healthcare providers for any given patient, secure individual records was the logical next step for this system. To have secure digital records, a secure chip health card was needed.

**How?**

Germany launched their Gesundheitskarte (eGK) program in 2006 with 71 million legal customers, and it has since grown to 80 million cards of which 375,000 are professional class cards. This represents one of the largest IT systems worldwide, at a cost of 1.6 billion euros. A professional class card is for a service provider, such as a practitioner or a pharmacist. Such a card allows that service provider to access patient data stored on regional databases. As of 2011, refinements of this system are expected to save as much as 500 million euros annually, and prevent accidental patient death by advance-detecting reactions from mixed medication.

Germany’s network uses the internet as a communication backbone channel, allowing access to the Electronic Health Network (HER) anywhere in the world. The key to the system is the use of smart (secure) chip cards that enable authentication, authorization, and secure access to data storage for both patients and service providers.

**The Result**

Patient information is readily available to service providers increasing the standard of care and unnecessary paperwork has been reduced resulting in hundreds of millions of euros in savings.

### 3.2.4 AUSTRIA

**Why Secure Chip ID?**

The Main Association of Austrian Social Insurance Institutions developed their secure chip e-card system, the “Electronic Administration System,” to provide a connection between the health sectors insured patients, insurers, employers, doctors, and the hospital Health Information Network, expediting information access and ensuring control of it.
How?
The e-card replaced the paper-based system allowing tracking of health claims electronically. The card contains an electronic signature, which allows citizens to use it as an identity card.

Austria is an example of an efficient healthcare system that provides a high standard of care to its citizens, even those living in remote mountain regions. Like other nations, Austrian citizens must make health insurance contributions which constitute part of the social security system. Dental care and simple treatments are covered under Austria’s healthcare network. The system is managed by a board of directors representing the insured and their employers.

There are approximately 11 million patients and 24,000 professionals on the network, which launched in 2005 (Healthcare CFO’s Guide, 2009).

The Result
Bureaucratic barriers that existed were eliminated, substantially improving the turnaround time on care and reducing waiting times.

3.2.5 ESTONIA

Why Secure Chip ID?
The implementation of secure chip card technology to track patient care records was implemented through the Estonian Hospital Network Development Plan 2015. This is a fifteen year plan to concentrate technology and care to provide a higher standard of care.

How?
Estonia has a mandatory National Identity Card. This is a secure chip card. It is used by citizens to access all government electronic or digital resources including voting, health records and health billing. Their secure chip card uses a 2048-bit public key encryption to serve as a mandatory proof of ID for secure e-services. Approximately 90% of the Estonian population carries an e-card.

Specifically, the Estonia healthcare system has been undergoing reform since the early 1990s to improve the use of healthcare resources, restructure the funding system, and make care more accessible for patients. Healthcare is predominantly funded by the general public, followed by public coffers. Estonian healthcare relies on the principle of solidarity so accessible medical data is essential to the functioning of the system.

Estonia has agreed that the cardholder’s name and national ID code are public by nature, and can be accessed in public databases. This data cannot be accessed online, and a cardholder must present themselves in person with their ID to authorize database
use. Furthermore, citizens of Estonia receive a lifetime email address issued by the government that is unique to them and supersedes the life cycle of an individual card.

The Result
By using the secure chip card technology, Estonia has been able to provide more accessible care across a consolidated network and continue to enhance service and efficiencies in their collaborative healthcare model. Their Health Care model is integrated into a broader secure, digital government service network which includes voting.

3.3 THE FINANCIAL SECTOR

Why Secure Chip ID?
For financial institutions around the world, the cost of counterfeit cards was a growing problem that needed to be stopped.

How?
In 1994, Europay International SA, MasterCard, and Visa developed the EMV standards so that payment (credit and debit) cards could be upgraded from magnetic stripe to secure chip. These cards needed to be interoperable everywhere payment is accepted. Since then, most regions have started or completed their conversion.

Conceived by the Plastics Fraud Prevention Forum and implemented in 2002, the United Kingdom migrated from signature authorization to chip-and-PIN transaction verification. By the end of 2006, they saw an increase to 99.8% of transactions being PIN-verified, leading to a significant decline in card fraud of over 34%. Furthermore, face-to-face card fraud has declined 69% since migration in 2004. Some increases were seen in ‘cross-border fraud losses,’ due to many EMV cards still containing a magnetic stripe to
be backwards compatible with out-of-date merchant systems, usually in other countries. As of 2010, lost or stolen cards have declined 61% since the migration in 2004; however Card Not Present (CNP) fraud increased after migration.

Canada’s migration to chip-and-PIN technology has been very successful in reducing fraud. All Interac branded ATMs now require EMV chip cards (for Canadian issued cards) and the same will be true of merchant point-of-sale by the end of 2015. As noted already the Interac Association reported in June 2014 that Interac debit card fraud losses as a result of skimming are at a record low – decreasing to $29.5 million in 2013 from a high of $142 million in 2009. Only 25 percent of losses in 2013, or $7.3 million, are the result of fraud exploitation within Canada. Total losses in 2013 represent 0.0093 percent of domestic Interac debit card volume (0.93 basis points) and the lowest volume of recorded fraud losses. As a result of this significant decline in fraud exploitation, the number of cardholders reimbursed by financial institutions fell to 72,200 in 2013 from 238,000 in 2009. This is in large part due to chip technology. What little remains is attributed to the use of cards in foreign jurisdiction that have not adopted chip technology yet.

Fraud levels in the United States are trending upwards. The United States does not have a single body mandated to collect fraud data, but there are trends that can be noted about the almost exclusive usage of magstripe technology. Between 2004 and 2009 there was a 70% increase of bank card fraud and in 2010 the US exceeded the UK fraud rate for the first time. This trend is followed by debit cards issued in the United States, which also use magstripe technology.\(^3\) EMV is now anticipated in the US, where fraud liability will shift in October 2015. A liability shift means that the cost of fraud that could have been prevented by chip (principally counterfeit) will shift to the party that cannot transact on chip. That means that either the card issuer did not employ chip, or the merchant cannot read the chip, or the acquirer/processor cannot accept chip data from the merchant.

Again in the United States, physical tampering and card skimming increased 30% in 2010, second only to Malware threats online.

China will also convert to EMV chip by 2015.

**The Result**

In Canada, the decrease in fraud is dramatic since Interac has adopted secure chip cards. Fraud has been reduced by 95%, from $159.3 million in fraud to $7.3 million.

\(^3\) Douglas King, Federal Reserve Bank of Atlanta, Chip-and-PIN: Success and Challenges in Reducing Fraud
3.4 E-PASSPORTS

**Why Secure Chip ID?**
Passport fraud is a challenging problem with consequences to financial risk, physical securities, and border control.

**How?**
Passport fraud is historically committed by supplying false documentation, or the documentation of another person, in the country of origin. As of April 10th, 2014, the Chief of Interpol has identified passport fraud as the biggest threat facing travelers internationally, with as many as 11 million bogus passports in circulation at the present time. Lack of a simple mechanism for intelligence sharing between countries was identified as an obstacle to comparing documentation to database records. Although chip does not solve the problem of false applications, it has been proven to deal effectively with counterfeit identification.

Conventional passport technology, Machine Readable Passports (MRP) uses a ‘machine readable zone’ in compliance with International Civil Aviation Organization standards, allowing it to be read manually or with a machine. It contains technology that can be reproduced by determined attackers. MRPs are vulnerable to tampering and reproduction.

More than 100 countries are using chip-based passports. The advantage of chip-based passports with biometrics is that they help the border agents to authenticate the traveler. This is also used increasingly at automated border gates to securely expedite legitimate travelers.

An enhancement for border Canada-USA border crossing is Nexus. It is a Canada-USA biometric security travel ID. Nexus, or “neXus,” is cryptographic ‘middleware.’ When the card is used a series of steps occur to verify the user’s identity. Nexus is designed to provide secure and timely international border crossing at a time of exponentially increased security due to ongoing terrorist threats. Secure and quick border crossings for those using the Nexus.

**The Result**
Canada has been issuing ePassports since July 1, 2013. Over 100 countries worldwide are also using ePassports built on chip technology. Canadians are able to learn what information is stored on their passport by visiting a Passport Canada service location. Passports are even deemed valid in the event of a chip malfunction. However at this time there have been no reported chip failures.
4 IMPLEMENTING A SECURE ID SOLUTION IN ONTARIO

Multiple jurisdictions and industries have migrated from magnetic stripe card technology to highly secure chip card technology, including British Columbia in Canada. That government has done so recently, as discussed in the prior chapter. We have clear and concise precedents on how to do that.

To design, build and implement a secure ID program, many decisions must be made, but there are ample best practices.

Most of the following milestones will be reached before public announcements are made. This is so that the government is in a position to prepare for questions that will come from the public. Privacy, security, costs and benefits all need to be determined before public consultations start. There may be changes as a result of the public consultation process.

Major milestones for implementation of a secure chip card for Ontario would be:

1. Determine cut-off date for red and white health cards
2. Decide on multi-application cards
3. Determine privacy implications
4. Determine authentication requirements
5. Request for proposals
6. Budget
7. Legislative Changes
8. Select vendors
9. Re-enrollment strategy - schedule and criteria
10. Rollout schedule
11. Public communication strategy
12. Public consultation
13. Stakeholder engagement
14. Build the system and cards
15. Rollout secure chip cards and infrastructure
4.1. DETERMINE CUT-OFF DATE FOR RED AND WHITE HEALTH CARDS

Red and white cards are easily counterfeited, which is why photo ID and security printing features were added to the “green” cards in 2007. Because the old red and whites can still be used to trigger a government payment, the counterfeit vulnerability remains in the billing system.

While it is important to establish a date when red and whites can no longer be used, it is equally important to keep that date confidential, on a need to know basis. This will prevent counterfeiters from stepping up their production to take advantage of the remaining time.

Establishing a cut off is important, because other milestones will be set in relationship to this date.

4.2. DECIDE ON MULTI APPLICATION CARDS

Simply put, will the new card have more than one use or not? In British Columbia, citizens may choose to combine their driver’s license and health card. This decision is made in the early stage because it impacts choice of chip operating system, privacy and security designs and the public communications plan. Consideration must be given to using the card to provide secure access to e-health records. Legislative changes may also be required.

4.8 DETERMINE PRIVACY IMPLICATIONS

At this stage, a Privacy Impact Assessment should be done. Specialized PIAs for chip cards are available from the office of the Ontario Privacy Commissioner and ACT Canada. There are both single and multiple application PIAs.

With both single and multiple application cards, access to data is rule driven. The PIA is designed to help identify what data will be stored on the chip, who is authorized to access it and what they can do with each piece of data. Can they read it, change it, delete it or add to it? The PIA then extends this to the data outside of the chip. That is to say, it is the data when on any other device (mainframe, desktop pc, tablet, USB key etc.) and the data at the point of collection, e.g. on a paper form.

These PIAs go beyond many currently used and take a considerable effort to complete, but there are several benefits:

- this process helps identify security gaps
- you have proof that privacy protection has been both planned and implemented
- your PIA plan facilitates both the building and the testing of the new card, and changes to legacy systems
4.4. **DETERMINE AUTHENTICATION REQUIREMENTS**

Secure chip cards are both tamper and counterfeit resistant, but one still needs to ensure that the person presenting the card is the person to whom it was issued. In the Canadian financial sector, this is usually accomplished by the cardholder entering a PIN (personal identification number) into a PINpad. This way you have a 2 factor authentication; something they have (the card) and something they know (the PIN). There are a number of options available and they need to be decided upon at this point so that you can build your decision into your RFP. One issue to consider is people who are incapable of remembering a PIN. Again, there are several options to deal with this.

4.5. **REQUEST FOR PROPOSALS**

Before the RFP is issued, a review of potential bidders should be conducted. There are many organizations that traditionally provide the required products and services for other sectors, but have not done so for governments. Including them would be beneficial for the government. There is a proven network of efficient and cost effective suppliers both domestically and internationally.

4.6 **BUDGET**

Based on the RFP’s, a realistic budget would be presented to the Ontario Cabinet’s Board of Management with implementation timelines.

4.7 **LEGISLATIVE CHANGES**

The legislative and regulatory framework would be designed. A legislative omnibus bill would then drafted and co-ordinated with the legislative calendar. Regulatory rules are also drafted. Any anticipated administrative regulations needing changes would be drafted as well, especially any accompanying medical professional amendments for stakeholder engagement strategy and support.

4.9 **SELECT VENDORS**

Vendors and sub-vendors will be determined. Due diligence investigations will be conducted. All will be bound by the established security and confidentiality protocols. There will be established contractual parameters and timelines for each of them. At this point, there must be provision for changes that could result from public consultation.
4.10 RE-ENROLLMENT STRATEGY – SCHEDULE AND CRITERIA

A strategy would be devised to ensure that people with counterfeit cards, or those who have legitimate cards under false pretenses, cannot exchange their old cards for new ones. Decisions would need to be made as to what documents or credentials will be accepted. Other decisions would be made as to when and where re-enrollment would take place. This would be influenced by where new cards are first put into effect (see 4.10). The government also would have the opportunity to replace both red and white and green cards at the same time. A decision about this would be influenced by whether rollout is geographically based.

4.10 ROLLOUT SCHEDULE

The ideal rollout schedule would be based on reducing counterfeit card fraud, so that those savings can be leveraged to pay for the balance of the project. Most fraud takes place where the card presenter is not known to the care provider. Traditionally, this would be walk-in clinics and emergency wards because the card holder may be new to the staff who have little time or expertise to determine whether or not the card is counterfeit. For this reason, the initial areas for roll out would be cities with large airports and border locations. Following that would be cottage country, where cards might be government issued, but the cardholder, not necessarily entitled to government paid medical care. The cost savings of decreased fraud will finance the completion of the roll out to the remainder of province.

Infrastructure must also be deployed and installed. Training may be required. In Canada we have a timing advantage, in that cards, devices and processes will likely mirror those we already use with credit and debit cards.

*It would be recommended that this preliminary planning be done in confidence, ensuring that criminal elements do not manipulate the migration to secure chip card.*

4.11 PUBLIC COMMUNICATION STRATEGY

At this point the communication strategy would be designed to ensure that Ontario knows what is happening, when it will happen and why. In particular, the public would want to know:

- that the new card is coming and how they will benefit from the change
- costs
- what data is tied to the card and who can access it to view, change, delete or add data
- who else has taken a similar step
- how and when the change will occur and what they will need to do
The policy should also determine who may speak on behalf of the government. Information channels and specific messages need to be identified at this stage.

### 4.12 PUBLIC CONSULTATION

Public outreach would commence to ensure “public ownership” of the process. Through this process, it is anticipated that the public would come to understand the full potential of the secure chip card. The full scope of communication tools should be considered; ranging from town halls, focus groups, interactive web sites and social media.

### 4.13 STAKEHOLDER ENGAGEMENT

Some stakeholder engagement will need to be done confidentiality and in the earlier stages to anticipate and address any legislatives or regulatory needs. During this stage, the engagement would be to facilitate implementation of the new card within the healthcare stakeholders, such as with hospital and clinic staff, pharmacists, doctors, nurses, long term care facility staff and others. Best practises of other jurisdictions should be shared and implemented.

### 4.14 BUILD THE SYSTEM AND CARDS

Design of the actual card would commence. The “artwork” of any card could be a Public Engagement opportunity. Legacy systems would need to be updated for all the chosen applications (health, driver’s licence, e-health data access etc.). Although many steps must be taken during this stage, similar projects are common, not only within government, but across other sectors. One example would be the conversion of Canadian credit and debit cards between 2007 and 2011. The expertise to do this work is commercially available.

### 4.15 ROLLOUT SECURE CHIP CARDS AND INFRASTRUCTURE

Citizens would need to know how to use their new cards, but they likely already use secure chip payment (credit and debit) cards so any education campaigns would be minimal. The same is true of healthcare stakeholders. As well, the card readers have prompts to lead the user through the transaction.
5 SUMMARY OF NET GAINS FOR ONTARIO

5.1 OVERVIEW

There are five significant gains for the province, its citizens and healthcare providers. At a time when government budgets are tight, these five warrants the investment needed to upgrade ID.

5.2 IMPROVED HEALTH OUTCOMES /RENAISSANCE OF THE ONTARIO HEALTH CARE SYSTEM

This all leads to a province with an improved health system and individuals who are both empowered to and able to better manage their own healthcare needs. Reduced fraud, a more efficient and responsive system because of more accessible individual health records can usher in A Renaissance of the Ontario Health Care system.

5.3 MORE ACCURATE HEALTH INFORMATION FOR RESEARCH, OPERATIONAL, POLICY AND FUNDING DECISIONS

More reliable individual medical data will mean more accurate medical data for policy decisions. Policy makers will know, on an aggregated basis, who is using what medical resources, where and when they are using them. This is not to say that policy makers will know what an individual had for treatment since privacy protections are already legislated for data collection. However, they will know how many patients went to ABC hospital for lung cancer or hip replacement, for example. This information will support better decisions about funding and resource allocation.

5.4 REDUCED COST OF FRAUD

With an open, transparent medical record and billing enabled by a secure chip health card, the opportunity for billing fraud is markedly reduced. Doctors charging for services not given, or charges of pharmacists for medicines not dispensed, will be reduced because the potential patient could be required by the government to verify and approve the service or sale through the use of their own card. Even conservative estimates put the savings at 5 to 10% of the healthcare budget of $51 billion.

The costs driven by the use of counterfeit cards could be significantly higher than billing fraud, but this can be substantially reduced through the use of secure ID. (see Fraud Savings chart)
Using British Columbia as an example, there were 2.02 cards in use for every eligible citizen prior to the introduction of the secure chip card. It can be assumed that the additional cards were a combination of counterfeit cards used by people not entitled to government paid health care in British Columbia and cards issued by the Ministry of Health to people who submitted false applications.

The chart above is based on a more favourable comparison of 1.5 cards per Ontario citizen. It then looks at the potential savings if the 1.5 could be reduced to 1.25, and then to the state where there is only one card in use for each Ontarian. When compared to the 2013 fees paid to doctors which is only 16% of the total healthcare spend, we see annual savings of ranging from $3.38 billion to $6.57 billion. There are additional related savings in the categories of drugs, hospitals and other health care areas.

It should be noted that the cost per counterfeit card is potentially higher than the average cost per legitimate card. This assumption is made on the basis that counterfeit cards are usually
purchased from criminals and it is reasonable to assume that the purchase is not made unless the medical treatment is pressing. They are also used in scenarios where the physician doesn’t know the patient, such as walk-in clinics and emergency rooms. Under other circumstances, the unauthorized patient may seek out a doctor and provide additional false identification documents when a longer term relationship and care is desired.

5.5 PROACTIVE TREATMENT FOR PATIENTS
A secure chip health card which enables access to e-health records, will allow patients to have accessible complete and reliable medical records. With a complete picture of a patient and the medical resources available to them, healthcare professionals will be able to better anticipate the medical needs and treatments for patients. As resources are freed up from ‘crisis’ medical care, there will be savings from dramatically less fraud and from more efficient allocation of resources. With these savings relatively more affordable preventive medicine can be practised.

5.6 REDUCED ADMINISTRATIVE TIME AND REDUCED ERRORS IN KEYED DATA
A secure chip health card will do away with some repetitive administrative work. Currently, we always need to update our ‘medical information’ upon arrival at any type of medical office. This will no longer be needed. This creates administrative savings. With less inputting of data, there is less opportunity for data entry errors.

With less administrative work, actual time for a patient to get to see a doctor or nurse could be reduced.
6 RECOMMENDATIONS

Based on the net gains for Ontario, this report recommends that the Province of Ontario:

6.1 UPGRADE SECURITY ON HEALTH CARDS

This would involve adding a secure chip to meet two objectives. The first is to enable the card to be used as secure access to e-health records. The second is to make the cards both counterfeit and tamper resistant to combat fraud.

6.2 IMPLEMENT STRONG AUTHENTICATION

Strong authentication will be required for secure access to e-health. It will also meet the need of reducing user fraud that involves one person loaning their card to another.

6.3 ISSUE MULTI-APPLICATION CARDS

Either offer citizens the ability to carry more than one provincial government ID application on a card or mandate this. Citizens are comfortable with multi-applications on smart phones and this will reduce government costs.

6.4 REVIEW ALL GOVERNMENT ISSUED ID

Governments at all levels should review the risks to their citizens, as well as to their own costs and reputations of not using secure ID and strong authentication.
APPENDIX A

BRITISH COLUMBIA ISSUES COMBINED ID FOR DRIVER LICENSE, HEALTH, ONLINE USE - CONTACTLESS EMV TO ENABLE NON-PAYMENT FUNCTIONS
Source: SecureID News (06/05)

The Province of British Columbia was in a bind. It had a health ID card that was more than 20-years-old with practically no security features and little identity vetting on the backend.

The province is home to 4.5 million residents, yet had issued 9.2 million BC Care Cards. While some were justifiable duplicates, there were still too many cards floating around in the system. "Basically there were a lot of cards and suspected misuse of the health card," says Kevena Bamford, executive director for the Provincial Identity Information Management Program in British Columbia. "The Ministry of Health was challenged to replace the Care Cards, strengthen the process of getting the card and incorporate more security features."

While this was happening, the Ministry of Technology, Innovation and Citizens' Services was looking to expand the functionality of their BCeID service, Bamford says. The BCeID is an online credential that citizens can use to access government services. Typically it was a low-level, self-asserted credential that takes the form of a username and password combination that was federated for use across provincial online services. The citizen could conduct in-person vetting to raise the level of assurance underlying the username and password login. Unfortunately, few citizens opted for this in-person vetting. Like the BCeID, the Care Card was typically a low security, level one credential. So the Ministry of Technology, whose primary function is supporting other agencies with the delivery of their technology solutions, started to work with Ministry of Health. The goal was to improve the security of the BC Care Card while also increasing the usability and identity assurance behind their eID service.

Enter the ICBC Driver Licensing Services. Every half-decade a license expires and the citizen must show up to renew the credential and provide foundational documentation. Thus, this is the one government agency that has both in-person contact with citizens and has access to the documents that prove citizen identity.

The ministry saw a chance to kill three birds with one stone. When citizens came to renew their driver license, the same foundational documents could be used to receive a health ID card and increase the assurance level of the eID, Bamford says.

Then came another idea. What if one card was used for all three functions? Thus was born the BC Services Card: driver license, health ID and electronic ID all rolled into one contactless smart card that serves as an extremely strong, level three credential.
By the close of 2013, the province had issued 800,000 BC Services Cards, Bamford says. Residents can choose to combine their driver license and Services Card, or have a standalone Services Card. All Services Cards replace the prior Care Card with improved identity proofing and security features and also enroll citizens in the digital identity program. The contactless smart card has an EMV application stored on it that will eventually be used to authenticate an identity.

Uptake on combination cards has been a little slower than expected, Bamford says. There are businesses around British Columbia that require two forms of identification and two of the most common pieces are the driver license and health ID card. Spreading the word to businesses regarding acceptance of the new combination card has been slow. British Columbia is working with SecureKey to enable the BC Services Card to be used for access to online provincial services. SecureKey also has a contract with the Canadian federal government to enable contactless bank EMV cards to be used for access to federal services, and there is potential to enable the BC Services Card for access to federal resources as well, Bamford says.

The province is working to build authentication service functionality and business cases so the card can be used to digitally access online services, she explains. At the moment, however, the chip is yet to be used. Still, significant value has been gained based on the fact that all 800,000 eID holders have undergone the stronger in-person identity vetting.

The goal is for citizens to have NFC readers attached to their computers where they could tap the card, enter a passcode and then gain access to online government services. One day, citizens might do the same thing at a doctor's office to authenticate their identity in order to receive health services.

Government officials are working on the authentication services and business requirements that will enable the smart card's use, Bamford says. Citizens are being asked how they expect the services to work and what services they would like to see offered.

The results are mixed, particularly around the area of usage history, Bamford says. "Many people in the early focus groups said they would expect to access usage history, similar to a bank account's transaction history," she explains. "Others refuse this concept outright, claiming it's a compromise of privacy and personal security."

Over the course of 2014, the province plans to work with programs and begin to roll out some digital services that can leverage the authentication service, Bamford says. "Citizens of British Columbia are very interested in using the card," she adds. "There are many years ahead of us in building the system as well as dialogue around using the credential."
## GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Apps</strong></td>
<td>Apps is an abbreviation for application. An app is a piece of software. It can run on the Internet, on your computer, or on your phone or other electronic device. The word &quot;app&quot; is a more modern usage, but this is really the same thing as a program.</td>
</tr>
<tr>
<td><strong>Biometrics</strong></td>
<td>The term “Biometrics” has also been used to refer to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition.</td>
</tr>
<tr>
<td><strong>Chip Card</strong></td>
<td>Also known as a smart card or memory card. A chip card is a plastic card that has a secure computer chip implanted into it that enables the card to perform certain functions. These could include the enablement of financial transactions, security system or physical access, storage of biometric data, medical or other records. These cards are highly tamper and counterfeit resistant using the security features of the chip.</td>
</tr>
</tbody>
</table>
| **Cryptographic algorithms** | 1. The science or study of the techniques of secret writing, especially code and cipher systems, methods, and the like.  
2. The procedures, processes, methods, etc., of making and using secret writing, as codes or ciphers.  
3. Anything written in a secret code, cipher, or the like.  
A cryptographic algorithm is a mathematical algorithm, used in conjunction with a secret key that transforms original input into a form that is unintelligible without special knowledge of the secret information and the algorithm. Such algorithms are also the basis for digital signatures and key exchange. | Source: [dictionary.reference.com](http://dictionary.reference.com) & [www.itlaw.wikia.com](http://www.itlaw.wikia.com) |
| **Debit card**        | A card used to make transactions that is linked to the cardholder’s direct deposit account | Source: ACT Canada |
| **Digital signatures** | A technique used to prevent denial of a transaction or message by the sender. A technique used to authenticate a transaction or message by the sender. The digital signature is generated using a cryptographic algorithm and information that identifies the user, including a cryptographic key. Digital signatures do not, by themselves, prevent the sender from repudiating the message. The sender | Source: ACT Canada |
**Secure ID Report: Meeting the Needs of Government and Citizens**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic password generators</td>
<td>A random password generator is software program or hardware device that takes input from a random or pseudo-random number generator and automatically generates a password. Random passwords can be generated manually, using simple sources of randomness such as dice or coins, or they can be generated using a computer.</td>
</tr>
<tr>
<td>Source: <a href="http://www.en.wikipedia.org">www.en.wikipedia.org</a></td>
<td></td>
</tr>
<tr>
<td>E health</td>
<td>eHealth (also written e-health) is a relatively recent term for healthcare practice supported by electronic processes and communication, dating back to at least 1999.</td>
</tr>
<tr>
<td>EMV</td>
<td>EMV stands for Europay, MasterCard and Visa, a global standard for inter-operation of integrated circuit cards (IC cards or &quot;chip cards&quot;) and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.</td>
</tr>
<tr>
<td>Source: <a href="http://www.en.wikipedia.org">www.en.wikipedia.org</a></td>
<td></td>
</tr>
<tr>
<td>Eurosmart</td>
<td>EUROSMART is an international association located in Brussels representing the Voice of the Smart Security Industry for multi-sector applications</td>
</tr>
<tr>
<td>Source: Eurosmart</td>
<td></td>
</tr>
<tr>
<td>First responder</td>
<td>A person (such as a police officer or an Emergency Medical Technician) who is among those responsible for going immediately to the scene of an accident or emergency to provide assistance</td>
</tr>
<tr>
<td>Source: Miriam Webster</td>
<td></td>
</tr>
<tr>
<td>Gesundheitskarte</td>
<td>Germany’s Personal identification health card, the insured entitles the holder to medical and dental treatment.</td>
</tr>
<tr>
<td>Source: <a href="http://www.versicherungsmagazin.de/Definition/32911/elektronische-gesundheitskarte.html">www.versicherungsmagazin.de/Definition/32911/elektronische-gesundheitskarte.html</a></td>
<td></td>
</tr>
<tr>
<td>Identity Card</td>
<td>A card bearing identifying information about and often a photograph of the person whose name appears on it</td>
</tr>
<tr>
<td>Source: Miriam Webster</td>
<td></td>
</tr>
<tr>
<td>Magnetic stripe card</td>
<td>A card with one or more magnetic stripes, containing data necessary to complete a transaction</td>
</tr>
<tr>
<td>Source: ACT Canada</td>
<td></td>
</tr>
<tr>
<td>MasterCard</td>
<td>MasterCard Worldwide advances global commerce by providing a critical link between financial institutions and millions of businesses, cardholders and merchants worldwide.</td>
</tr>
<tr>
<td>Source: <a href="http://www.mastercard.com">www.mastercard.com</a></td>
<td></td>
</tr>
<tr>
<td>OHIP</td>
<td>The Ontario Health Insurance Plan is the government-run health insurance plan for the Canadian province of Ontario. OHIP is funded by taxes paid by the residents and businesses of Ontario and by transfer payments from the federal</td>
</tr>
</tbody>
</table>
## Secure ID Report: Meeting the Needs of Government and Citizens

<table>
<thead>
<tr>
<th><strong>Services Card</strong></th>
<th>In British Columbia, the new BC “Services Card” will provide secure access to provincial government services. New cards are now being issued with the goal of eventually replacing all existing Care Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source:</td>
<td>www2.gov.bc.ca/gov/topic.page?id=87EEAD6D19974459950AA7FF7F60AD54&amp;WT.mc_id=Offsite_BC_Service_Card</td>
</tr>
<tr>
<td><strong>Sesame Vitale</strong></td>
<td>The SESAM-Vitale program is a paperless care sheets for health insurance in France, based on the Carte Vitale.</td>
</tr>
<tr>
<td>Source:</td>
<td><a href="http://www.fr.wikipedia.org/wiki/SESAM-Vitale">www.fr.wikipedia.org/wiki/SESAM-Vitale</a></td>
</tr>
<tr>
<td><strong>Smart Card Alliance</strong></td>
<td>The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.</td>
</tr>
<tr>
<td>Source:</td>
<td><a href="http://www.smartcardalliance.org/pages/alliance">www.smartcardalliance.org/pages/alliance</a></td>
</tr>
<tr>
<td><strong>Smart card</strong></td>
<td>An integrated circuit card with a microprocessor, i.e. capable of calculation, also known as a chip card.</td>
</tr>
<tr>
<td>Source:</td>
<td>ACT Canada</td>
</tr>
<tr>
<td><strong>Third party authentication</strong></td>
<td>A component of the SGD server that trusts authentication information supplied by a third party and uses that information to automatically authenticate the user as an SGD user, allocating a user identity and a user profile</td>
</tr>
<tr>
<td>Source:</td>
<td>download.oracle.com/docs/cd/E19351-01/821-1926/z400030a6457.html</td>
</tr>
<tr>
<td><strong>VISA</strong></td>
<td>Visa Inc. is an American multinational financial services corporation.</td>
</tr>
<tr>
<td>Source:</td>
<td>Visa Inc.</td>
</tr>
</tbody>
</table>
BIBLIOGRAPHY

2. Ontario Budget 2013
10. The Austrian E-card System.  
11. The Digital Society.  
12. The Estonian ID Card and Digital Signature Concept. 
This report was made possible by our:

**PRINCIPAL SPONSOR**

[Logo: ingenico GROUP]

And the support of:

[Logo: Canada Post]

[Logo: infineon]