BLOCK G

PRIVACY & SECURITY CONSULTING

The BC Services Card:

Drivers, Architectures, and Risks

This page has been intentionally left blank

CONTENTS

About the Authors 3

Executive Summary 5

Introduction 9

Section One - A Survey of Existing International Identity Systems 10
- International 11
- Common International Themes 15

Section Two - The BC Services Card Initiative 16
- A Brief History of the Services Card Initiative 17
- Drivers and Inhibitors in BC 19
- Situating the BC Services Card 24

Section Three - BC Technical Infrastructure 25
- The Smart Card's Attributes 26
- BC Government Database Architecture 29
  - SSL/TLS/SSH 32

Section Four - An Overview of Risks and Vulnerabilities 33
- Enrollment 34
- Physical Card Protections 35
- Data Management and Security 37
- NFC Chips 41
- Function Creep 45
- So, What Does It All Mean? 46

Section 5 - Further Securing the Services Card 49

Conclusion 53

Appendix A - Acronyms 55

Legal Information 57

About the Authors

This report was researched and written by Christopher Parsons and Adam Molnar. They are the principals of Block G Privacy and Security Consulting.

Christopher Parsons is a Privacy by Design ambassador. He has over a decade's experience working with challenging privacy issues that are linked to digital technologies. He specializes in how Canadian privacy law intersects with digital systems, and the implications of such law on the development and deployment of novel projects and practices. Christopher is presently completing his PhD in the Department of Political Science at the University of Victoria, where he is a fellow at the Centre for Global Studies. He has published in the Canadian Journal of Law and Society, European Journal of Law and Technology, Canadian Privacy Law Review, CTheory, and has book chapters in a series of academic and popular books and reports.

Adam Molnar has spent over a decade researching, teaching, and consulting on developments in security and privacy, particularly in the areas of policing, national security, and public safety. He specializes in how collaborative governmental initiatives are arranged, and the privacy and security benefits and challenges that follow. Adam is presently completing his PhD in the Department of Political Science at the University of Victoria, and he is a forthcoming Postdoctoral Fellow at the Surveillance Studies Centre at Queen's University. He has published book chapters and policy reports, and he regularly presents his research domestically and further abroad.

Executive Summary

This report was written in 2012-13 for the British Columbia Civil Liberties Association. In it, we focus on the BC Services Card, which is part of the BC government's e-government initiatives. The Services Card is a smartcard enabled identity document that is designed to interoperate across BC government services, with the intent of providing superior access to services than existing delivery mechanisms. The goal of this report is to contextualize the politics and technology behind the new BC Services Card and, in the process, understand prospective security-and privacy-related issues that are linked with the initiative. A core aspect of our report consists of a technical survey of the Services Card and its associated infrastructure. As part of our survey we evaluate possible vulnerabilities that could be exploited by a hostile third-party intent on undermining, disrupting, or otherwise compromising Services Cards or the trust BC residents are expected to place in them as technically sophisticated and reliable identity tokens.

Our report is divided into five sections. **Section One** examines the drivers behind identity cards in the United States, United Kingdom, and the European Health Insurance Card; this provides a framework against which we evaluate the drivers of the BC Services Card. In the **Section Two** we annotate the history of the Services Card initiative, to understand drivers and constraints of its progress. We then contrast drivers in BC against those internationally and find that unlike in other jurisdictions, political and social opposition in BC has not sufficiently manifested to delay implementation of the cards. Nor have the technological innovations associated with the card led to public opposition. Absent these inhibiting factors, only government delays have significantly slowed the deployment of the BC Services Card.

Our third and fourth sections investigate the technologies and infrastructure of the BC Services Card. **Section Three** outlines the technical infrastructure. This includes accounting for the standards, data processing framework, and responsibilities of government and non-government actors in enabling the Services Card. **Section Four** conducts a holistic evaluation of the risks and vulnerabilities associated with this infrastructure. We focus on how enrolment processes and physical card protections could be attacked, as well as how data management and security processes might have points of weakness. We also examine the significance of the smart chip that is embedded in the card and how the purposes and uses of the card could 'creep' beyond currently stated intentions and applications.

Highlights from our section on risks and vulnerabilities includes:

- The importance of ensuring that government actors responsible for issuing the cards are trustworthy; failure to do so could undermine many of the government's identity assurance processes that underlie the entire card system.
- The assertion that the Services Card's physical security characteristics are positive, though the inclusion of biometric facial images does not necessarily lead to the security enhancements suggested by the government.
- The near field communication (NFC) chips embedded in the cards are a point of significant vulnerability, insofar as they could be read at a distance, compromised by a malicious actor, or tampered with to intrude into the computers and mobile phones reading the chips.
- The potential for 'function creep', or the expanded use of the Services Card for purposes beyond the current scope of the card. This might include use of the card by private parties or the card ultimately being integrated with the federal government's planned pan-Canadian identity card.

Section Five covers suggestions to ameliorate security risks linked with the Services Card and associated infrastructure. Core suggestions include:

- Penetration tests should conducted to 'attack' the system, in order to understand where vulnerabilities exist, how they could be exploited, and how to subsequently rectify them. Given the magnitude of the government's proposed data linking infrastructure associated with the Services Card this kind of analysis is critical. Testers should be given a wide permit in testing the system and not be artificially limited in what they can do to identify vulnerabilities.
- Public consultations with security experts should occur and consultations findings summarized and subsequently made public. These consultations should attend to how security of the cards and BC residents' privacy can be maximized.
- Public audits should be routinely conducted on the systems and infrastructure surrounding the BC Services Card. This should include auditing private vendors who are contracted to provide service.

In essence, this report calls for a careful appreciation of the technical constraints associated with the proposed BC Services Card initiative. A failure to carefully consider the risks and vulnerabilities associated with the provincial - and potentially national - identity system could lead to increased costs and risks if the design suffers catastrophic collapse or if core facets of the design can be successfully - and reliably - made vulnerable to attackers. Core drivers for this system revolve around efficiency of service

delivery and the reduction of government costs: it is imperative that, if an e-credential initiative is to be implemented, that the province ensures it can actually meet its stated objectives and project drivers.

Security systems are meant to impose costs that are high enough to preclude, or delay, attackers. The BC Services Card system is slated to bloom into a broad provincial identity schema and, as such, the incentive to establish fraudulent identities or otherwise disrupt the system will grow as the system expands. Moreover, BC cannot ignore that their proposed system may ultimately turn into the core of a national identity scheme: in light of this, BC officials must consider the range of actors who are interested in disrupting a Canadian identity system and establish security measures that are sufficient to limit such attacks. To date, we have not seen provincial or federal officials publicly comment or address the effectiveness of the BC system in defraying highly interested attacks on a proto-national system: it is time to publicly engage in these discussions if we are to adequately, and functionally, secure BC's proto-pan-Canadian identity institution.

Introduction

Identity documents have historically been used to monitor the movement of individuals both across, and within, national borders. Monitoring and controlling movement has been justified on grounds of military service, taxes, labor, facilitation of law enforcement, to protect people from harm, for ethnic and religious reasons, on medical grounds, and to supervise the 'space' that individuals inhabit.[1] In the past, these justifications have turned identity cards into 'detecting' tools, insofar as they operated as "a set of tools for examination, inspection, monitoring, watching and detecting, tools which must be applicable to a wide range of objects."[2] These cards have transformed into 'effecting' tools, or ones that let government impact the outside world: there is a degree of state agency associated with contemporary cards that was absent in prior decades.[3] This shift correlates with movements from crude paper documents and fixed policing checkpoints to digital systems that can increase the rapidity of government examinations, evaluations, and actions taken on the basis of card-mediated identities. In effect, "digital technologies allow government to use its organization more precisely and discriminatingly than ever before"[4] and, with the advent of contactless smart chips and radio frequency identification (RFID) tags, combined with a gross decline in the cost-per-unit of such chips and tags, identity documents that Western citizens carry on a routine basis are being 'modernized' to facilitate more 'transparent' and frictionless state surveillance.[5]

In this report, we focus on the BC Services Card, which is part of the BC government's e-government initiatives. Our goal is to contextualize the politics and technology behind the new BC Services Card and, in the process, understand prospective security- and privacy-related issues linked with the initiative. Throughout the report we rely on primary and secondary documents, as well as limited interviews. A comparativist

[1] J. Torpey. (2000). *The Invention of the Passport: Surveillance, Citizenship and the State*. New York: The Cambridge University Press. Pp. 7.
[2] C. Hood. (1983). *The Tools of Government: Public Policy and Politics*. New Jersey: Chatham House. Pp. 91.
[3] D. Lyon and C. J. Bennett. (2008). "Playing the ID card: Understanding the significance of identity card systems," in C. J. Bennett and D. Lyon (eds.). *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. New York: Routledge. Pp. 13.
[4] C. C. Hood and H. Z. Margetts. (2007). *The Tools of Government in the Digital Age*. New York: Palgrave. Pp. 120.
[5] We use the term 'surveillance' to refer to systems that monitor for particular stimuli and react when those stimuli are present in order to effect some change in environmental conditions. The term is not used pejoratively, and should not be understood as suggesting a normative stance towards surveillance itself.

approach is adopted to ascertain common/dissonant drivers and inhibitors of identity card systems, and to draw tentative conclusions about the political viability of the BC card. In reviewing how BC's Services Card system might be compromised we rely on published research that reveals how the technology underlying the initiative has been, and is being, targeted in other scenarios. In light of our primary source documents lacking comprehensive information about the Services Card's security characteristics many of the concerns we raise are theoretical, yet salient. Our final findings, which address how to ameliorate risks, discuss how to better secure the identity system itself.

In summary, our report begins by contrasting international drivers and inhibitors of identity documents against the drivers and inhibitors in BC. As a result of this contrast we can understand why some efforts to introduce such documents have been stymied or stopped, and why advocacy may be less successful in the BC situation. From there, we speak to core architectural elements of the new Services Card system - examining the cards' physical, database, and future technical designs - to establish how the system may be vulnerable to third-party attackers. We conclude by outlining ways of ameliorating prospective data security - and, to some extent, privacy - risks linked to the Services Card initiative.

Section One - A Survey of Existing International Identity Systems

In this section, we explore some of the pressures that are driving, or have driven, the adoption of identity card-based monitoring systems outside of Canada. We look at the United States' REAL ID Act, efforts to deploy identity cards in Britain, and the successful deployment of the European Health Insurance Card (EHIC). Cases were chosen based on common policy drivers, as well as because the US and UK share common histories - like Canada - of opposing what are seen as national identity systems.[6] The EHIC was chosen in the interests of identifying how a relatively minimalistic set of card requirements, when introduced to a population that is generally used to carrying national identity documents, might limit or stymie resistance to the new card. Ultimately, our evaluation of international initiatives will provide a qualitative frame against which we can contrast drivers and inhibitors related to British Columbia's recently introduced 'smart' Services Card.

[6] See: M. Froomkin. (2009). "Identity Cards and Identity Romanticism," in I. Kerr, V. Steeves, and C. Lucock (eds.). *Lessons From The Identity Trail*. Toronto: Oxford University Press. Pp. 245-263.

International

Identity systems are meant to render societies, and individuals, "legible" to administrative and bureaucratic aspects of the state.[7] For an identity document to 'properly' function it must enable "the reliable identification of each member of the population to which it is issued."[8] What these identifiers enable or signify can change, especially in the digital era, where a number can be used to query existing databases or, subsequent to being issued, integrated with new and unfolding data records. In effect, these documents' static identifiers can potentially operate as a nexus for more and more data; the very presence of the unique number can facilitate surveillance creep by operating as a hub for data integration and transmission. To be fully effective, however, identity documents must successfully and reliably do two things; they must "provide a reliable or trusted link back to the issuing authority" as well as "authenticate a specific individual within the political body of that authority."[9] In what follows, we briefly examine how identity cards have been issues in the United States and Britain, and also examine the (relative) lack of controversy around the European Health Insurance Card (EHIC). Our survey is meant to ascertain, principally, what drives and inhibits the adoption of the identity systems, so as to derive a model for contrasting the BC case.

The United States' (US) REAL ID Act requires that citizens possess identity documents that meet federal security and authentication requirements; generally, the federal law required that state drivers licenses (and associated identity documents) meet federal requirements. The law also establishes data sharing requirements amongst state Department of Motor Vehicle (DMV) offices. While the REAL ID Act itself does not mandate the use of facial recognition technologies it does "indicate that states must refuse to issue a driver's license to anyone holding [a license] from another state; thus the policy may be read as anticipating the use of facial recognition technology."[10] Cards also must be machine readable. This characteristic is meant to facilitate communication with digital networks for data collection and processing requirements, as well as to better verify cards' authenticity. As such, the cards are intended to better

[7] J. C. Scott. (1998). *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: New York University Press.
[8] F. Stadler and D. Lyon. (2003). ""Electronic identity cards and social classification." In *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination.* D. Lyon (ed.). New York: Routledge. Pp. 83).
[9] B. McPhail, C. Parsons, J. Ferenbok, K. Smith, and A. Clement. (Forthcoming). "Identifying Canadians at the Border: ePassports and the 9/11 legacy," *Canadian Journal of Law and Society*.
[10] K. Gates. (2008). "The United States REAL ID Act and the securitization of identity," in C. J. Bennett and D. Lyon (eds.). *Playing the Identity Card: Surveillance, security and identification in global perspective*. New York: Routledge. Pp. 226.

secure "the process of determining the legitimacy of an individual's claim to identity represented on an identification document"[11] than present, non-automatic, verification processes.

One of the primary problems with the federal requirements stems from requiring DMVs to check license applications against other states' databanks. At the time that the REAL ID Act was passed, this requirement was functionally impossible to implement because state DMVs lacked common record systems. Moreover, to comply with federal requirements, states are responsible for collecting 'breeder' documents - such as birth certificates and other primary identification documents that are prerequisites to receiving a 'second order' identity document like a drivers license - and thus establish *de facto* national ID documents by virtue of all citizens having to carry federally-backed documents, which just happen to be state-controlled. Biometric identifiers are perceived as guaranteeing ongoing authentication of ID card holders' identity, and machine readable zones as a technique to call information to verify biographical histories.

The REAL ID Act was, in part, driven by efforts to 'securitize' services in the United States following the 9/11 terror attacks; the federal government saw value in establishing 'guaranteed' identity documents to correctly identify individuals, to limit the issuance and circulation of fraudulent documents, and to prevent individuals from receiving multiple licenses from different states. Vendors associated with Information Technology Association of America also advocated for REAL ID; this association's members stood to benefit from states adopting uniform identity standards given their commercial involvement with DMVs across the United States.[12] States, however, would have been left to pay for the majority of the costs, costs imposed by federal law. In response to this cost download, many states passed legislation to preclude meeting the REAL ID standards. Privacy advocates and civil libertarians also oppose the cards, on the basis that the cards would facilitate data sharing and matching - and thus operate as a natural space for function creep - as well as because the federal government was inappropriately trying to intrude on states' responsibilities. Other experts also oppose the cards based on concerns related to the security of databases associated with such cards; they are not just concerned about DMV systems being compromised, but that

[11] K. Gates. (2008). "The United States REAL ID Act and the securitization of identity," in C. J. Bennett and D. Lyon (eds.). *Playing the Identity Card: Surveillance, security and identification in global perspective*. New York: Routledge. Pp. 227.

[12] ACLU North. (2007). "Who Loves REAL ID? The Companies Do," *ACLU North* (website). Published September 28, 2008. Last accessed November 25, 2012. Available at: https://www.aclunc.org/issues/technology/blog/who_loves_real_id_the_companies_do.shtml

any *other* system that uses the license for authentication/verification purposes (e.g. travel-linked databases, pharmaceutical databases, etc.) could be vulnerable to attack.[13] The risk, specifically, is that without fully securing these databases there is the potential for significant new amounts of personal information to be disclosed to unauthorized third parties.

Similar to the United States, the British government has been unsuccessful in establishing a long-term cross-national identity system.[14] In the past decades identity cards were proposed by the Conservative government in 1996 in response to Irish Republican Army terror attacks, though curtailed after the 1997 election of the Labour government. Subsequently, Asylum Registration Cards were proposed following 9/11, though these were (effectively) unable to certifiably authenticate individuals. In 2002 the government proposed introducing 'Entitlement Cards' that individuals on government benefits would receive, and be forced to use prior to receiving benefits, but the media generally declared this an identity card by stealth. While a draft bill was proposed in 2004 it was suspended in 2005 prior to a general election.[15]

Arguably the closest the British government has come to imposing national ID cards followed the passage of the Identity Cards Act 2006. David Wills identifies a series of core drivers of the Act.[16] Internationally, travel to the US demanded International Civil Aviation Organization (ICAO) standardized documents, which was interpreted as requiring updated e-passports. The ID card was to be integrated with the passport and, as such, would simultaneously meet US entry requirements and ICAO general travel standards. The government of the day also argued that other European nations used national ID cards without significant civil liberties issues or concerns. In addition to these international drivers, there were (effectively) four domestic drivers: immigration and illegal working, a personalized and 'joined-up' e-government system, national security and crime, and securing identity. Symbolically, the card would merge an increasingly multicultural Britain though shared legal and card-denoted identities while, simultaneously, functioning as the 'glue' binding citizens to various government

[13] S. Egelman and L. Faith Cranor. (2006). "The Real ID Act: Fixing Identity Documents with Duct Tape." *I/S: A Journal of Law and Policy for the Information Society* 2(1). Pp. 149-183.
[14] It is significant to note that, in times of national crisis (e.g. world wars) the British government has successfully issued national identity cards, though such cards have been repealed following the crises.
[15] D. Wills. (2008). "The United Kingdom identity card scheme: Shifting motivations, static technologies," in C. J. Bennett and D. Lyon (eds.). *Playing the Identity Card: Surveillance, security and identification in global perspective*. New York: Routledge.
[16] D. Wills. (2008). "The United Kingdom identity card scheme: Shifting motivations, static technologies," in C. J. Bennett and D. Lyon (eds.). *Playing the Identity Card: Surveillance, security and identification in global perspective*. New York: Routledge.

services. This would facilitate engagement with the government and, by extension, lead the cards to become part of the so-called 'great British institution.' The cards would also functionally combat identity-fraud by establishing common breeder requirements and heightened card-based security standards, which would be directly linked to streamlining existing identity-document dissemination processes.

Core opposition could be arranged alongside either pragmatic or principled positions; the former explored the technical problems associated with the proposed cards (e.g. issues with biometric and baseline document authentication, information security flaws in government services) whereas the latter considered whether it was right to facilitate broader government surveillance of the population. The issue of cost was also raised in a London School of Economics (LSE) study, which argued that the proposed program would cost up to £20 billion over ten years.[17] Ultimately, the enabling Identity Cards Act 2006 was transformed into an election issue in the 2010 election. The Conservative-Liberal Democrat coalition, which took control of government from Labour, introduced a draft Identity Documents Act 2010 in May and it ultimately received Royal Assent by the end of the year. As a result of the 2010 Act, the existing National Identity Register that had been developed subsequent to the 2006 Act was destroyed in February 2011, marking a conclusion to the UK government's most recent efforts to establish a national identity card system.

In both the US and British situations, we see that there are common drivers behind the identity card systems. Federal governments are the principal advocates and cost, efficiency, fraud, and security have been offered as reasons to impose identity cards. In the British case, e-government was also highlighted as a motivation. Before turning to the British Columbia situation we conclude by looking at the European Union's (EU) proposed European Health Insurance Card. As with the UK card, the symbolism of the EHIC was significant; the card was seen as placing "another piece of Europe in your pocket."[18]

The EU advocated for the card for a series of reasons:

1. It would ease daily life for EU citizens by enabling movement throughout the union;
2. It would ensure EU citizens received health care when travelling through the EU;

[17] The Identity Projects. (2005). *The Identity Project: An assessment of the UK Identity Cards Bill and its implications. Version 1.09*. London: LSE Department of Information Systems.
[18] European Commission. (2003). "Communication from the Commission to the Council, the European Health Insurance Card," *COM*: 73.

3. It would facilitate convenience in protecting the safety of EU citizens;
4. It could help prevent harm linked with inappropriate medical care, such as those linked with patient diseases or allergies;
5. It would fulfill the Union's commitment to ensuring high degrees of health protection;
6. It could reduce costs by increasing efficiency though the card should never become a surveillance tool for public authorities.[19]

Significantly, the EHIC does not contain *any* medical information; it instead displays "the cardholder's surname and first name, personal identification number and date of birth."[20] There are two variants; the first has a common front to the card with the back used by member nations. The second puts the common design on the back of the card of existing national or regional identity cards. The ultimate aim is to include an electronic chip on the card to "greatly facilitate exchange of information between Member States and reduce risk of error, fraud and abuse." However, when the EHIC was established no clear date to 'chip' the card was included,[21] and proposals to adopt an e-EHIC continue.[22]

Common International Themes

Together, these cases underscore some of the core characteristics surrounding state reification of citizens' identities. It is on the basis of how identities are constructed, disclosed, and accepted or rejected that most concerns related to identity card projects arise: who establishes a person's identity, under what conditions is an identity recorded or used to authenticate a person or their action, and what are the terms of 'failing' to properly authenticate. Across our cases, we can detect common themes; typically a federal body introduces identity schemes based on efficiency, security, or e-government reasons. Vendors often strongly advocate for these systems, on the basis that long-term business can follow from states adoption of such projects. Taken

[19] W. Maas. (2008). "Another piece of Europe in your pocket: The European Health Insurance Card," in C. J. Bennett and D. Lyon (eds.). *Playing the Identity Card: Surveillance, security and identification in global perspective*. New York: Routledge.
[20] W. Maas. (2008). "Another piece of Europe in your pocket: The European Health Insurance Card," in C. J. Bennett and D. Lyon (eds.). *Playing the Identity Card: Surveillance, security and identification in global perspective*. New York: Routledge.
[21] EUROPA. (2004). "European Health Insurance Card: Frequently Asked Questions," Published March 26, 2004. Last accessed November 21, 2012. Available at: http://europa.eu/rapid/press-release_MEMO-04-75_en.htm?locale=en
[22] A. Grode. (2010). "Patient Identification in Europe - From EHIC to eEHIC," Health Conference 2010. Last accessed November 19, 2012. Available at: http://www.worldofhealthit.org/sessionhandouts/documents/PS14-1-Grode.pdf

together, states and vendors, along with standards bodies, are sometimes said to compose a "card cartel."[23] This cartel establishes the terms of what constitutes an identity, terms of evidence underlying the token - the card - denoting identity, and the administrative and technical processes that are needed to mobilize citizens' token-instantiated identities.

Opposition to cards and their support infrastructure typically emerges on both practical and principled fields. For the former, security, cost, efficiency, and effectiveness arguments are used to argue against the card system, on the basis that the stated 'benefits' of these cards are actually misleading. Function creep is also invoked, insofar as the card system may facilitate broader sharing of citizens' information over time. Critiques from principle tend to focus on the 'correctness' of the schema, identifying how identity card systems facilitate increased state surveillance or offend constitutional or moral dignities.[24] As evidenced in the US and UK, opponents can successfully 'block' cards even after legislation is passed, though civil society advocacy alone is insufficient: other political partners must be found and, in the US and UK, pragmatic grounds appear to be key to supporting a principled anti-card coalition. The EHIC, on the other hand, speaks to the ability to propagate cards *if and only if* they are introduced as being relatively non-invasive, minimally involved in data collection, and have a low barrier of entry; together these features limit advocacy concerns, though still do serve as a potential 'stealth' means of introducing more detailed or invasive data card schema infrastructures.

Section Two - The BC Services Card Initiative

So, having briefly surveyed a handful of identity systems abroad, what can be said about the proposed BC Services Card? In this section we first provide some of the history around the card and then identify how the government has justified the card, core drivers for the system, as well as some of the inhibitors. We conclude by contrasting these drivers and inhibitors against what we learned from examining identity systems that have been introduced abroad. Awareness of the political drivers of the Services Card does more than just clarify political alliances: it also reveals the relative degrees of concern that different actors have displayed towards privacy and security related issues that are linked to the BC Services Card.

---

[23] D. Lyon. (2009). *Identifying Citizens: ID Cards as Surveillance*, Cambridge: Polity Press. See also B. McPhail, C. Parsons, J. Ferenbok, K. Smith, and A. Clement. (Forthcoming). "Identifying Canadians at the Border: ePassports and the 9/11 legacy," *Canadian Journal of Law and Society*.

[24] For a discussion of the dimensions of constitutional dignities, see N. Rao. (2011). "Three Concepts of Dignity in Constitutional Law," *Notre Dame Law Review*, Vol. 86(1). Pp. 183-271.

A Brief History of the Services Card Initiative

In early 2010 a governmental working group began evaluating the merits of a photo Services Card for British Columbian government services. Dubbed the "Care Card initiative," the group involved a number of ministries and private sector corporations. Together they establish a foundation for British Columbia's move toward electronic service delivery models.[25] The BC Ministry of Health (MoH) initiated a CareCard replacement project, which evolved into the broader BC Services Card initiative. This latter project drew together the Ministry of Citizen Services and Open Government, and the Insurance Corporation of British Columbia, as partners with MoH. The development of the Services Card is now seen as developing core infrastructure for a larger BC Identity Management/Information Technology (IM/IT) government project, the Information Access Layer, which is a project intended to facilitate sharing residents' personal information across Ministry information silos to "better achieve outcomes."[26] BC's move to an ID Card initiative echoes those seen in the US, UK and Europe, with the stated goal of "transform[ing] the way [the Province of BC] does business" and with an insistence on "leveraging technological solutions and innovation" in the move towards digital record keeping and increased electronic service delivery.[27] The Services Card is seen as the foundation for British Columbia's move towards electronic delivery models.

In May 2011, BC Ministry of Health (MoH) publicly announced the rollout of the new electronically enhanced CareCard. Over a span of the next five years (coinciding with the expiry of residents' BC driver licenses) the MoH will phase out the current magnetic-stripe MSP CareCard with a new mandatory Services Card that will feature contactless smart chips.[28] Under the current Services Card initiative, BC citizens will have the option of visiting Insurance Corporation of British Columbia (ICBC) branches to obtain a new photo Services Card and to combine the it with a driver's license. Alternatively, BC citizens will be able to keep a stand-alone driver's license and receive a Services Card that will expire five years after being issued. After the five years has

[25] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 19, 2010 (Version 2.4). Pp. 1

[26] I. Bailey. (Office of the Chief Information Officer, Architecture and Standards Branch). (2009). "Identity Information Management Architecture Summary," Last Updated March 23, 2009, Version 0.7, Pp. 7.

[27] Office of the Chief Information Officer. (2010). "IM/IT Enablers Strategy for Citizens @ The Centre: B.C. Government 2.0". Pp. i

[28] Seniors and those under 19 years of age will be exempt from mandatory adoption of the new Services Card.

expired, many citizens of BC will be rolled into the new multifunctional (drivers license/ Services Card) BC Services Card.[29]

The new BC Services Card is ostensibly meant to ameliorate identity fraud and theft. Cards will be designed with more robust card-based identification and anti-fraud features, including biometric images, holographs, and a chip that will facilitate rapid access to citizen health records. ICBC is a core partner in the Services Card initiative because of the institution's experience in producing high-quality identity documents (i.e. drivers licenses). Specifically however, the new Services Card fits within the province's "Smart Card initiative", insofar as it establishes multi-purpose identity cards that incorporate e-Health service delivery as well as drivers license certifications. The ultimate goal of these cards is to integrate them with a wide range of provincial and federal services.[30]

Integrating the new Services Card with drivers licenses stems from the recent introduction of more secure drivers licenses in BC; the new Services Card will leverage ICBC's existing physical, business, and facial recognition processes while simultaneously employing a smartchip where the BC resident lacks an enhanced drivers license.[31] The current stage of the government's IM/IT plan calls for integrating the Services Card and drivers license, though this is just a first step: as part of our research interviews, a member of the Office of the Chief Information Officer (OCIO) stated that other government ministries, such as the Ministry of Education (MoE), and the Ministry of Children and Family Development (MCFD) could also use this integrated card;[32] in essence, the Ministry of Citizen Services will assist any Ministry decide how, when, and whether to integrate their systems with the Services Card. Having provided some background on the Services Card initiative, primarily in the context health care service

[29] Based on interviews with government officials in January 2013

[30] Province of British Columbia. (2012). "Notice of Intent (Notice of Internet #SATP-290)," Published 2012. Last accessed November 26, 2012. Available at: http://bccla.org/wp-content/uploads/2012/10/20120101-BC-Services-Card-notice-of-intent.pdf. See also: V. Gogolek. (2012). "Is B.C.'s New CareCard Another Technological Quagmire For Province?" *Huffpost British Columbia.* Published October 31, 2012. Last accessed November 25, 2012. Available at: http://www.huffingtonpost.ca/vincent-gogolek/bc-new-carecard_b_2041307.html

[31] Such licenses already contain an RFID chip and, as such, cannot integrate the smartchip required for the new integrated license/care card. See: S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 19, 2010 (Version 2.4).

[32] Using the new cards, employees in social services, who have access to educational databases through the intermediary of the OCIO, can evaluate the academic standing of social services clients and integrate that information into social services delivery. Example is from an interview with a representative of the Office of the Chief Information Officer on November 13, 2012.

delivery, we turn to explicitly address what is driving - and inhibiting - deployment of the new Services Card.

Drivers and Inhibitors in BC

The Ministry of Health (MoH) is - seemingly - a primary driver of the new Services Card along with the Office of the Chief Information Officer, with core backend infrastructure residing within the Ministry of Citizen Services and Open Government. The Services Card is aligned with the province's e-Health initiative, which is guided by five business objectives:

- Reduce fraud and identity theft resulting from CareCard misuse
- Ensure the delivery of health services to the right person and enhanced accuracy of health record information
- Enable secure online client access to health and other government information and services
- Enhance privacy protection
- Leverage existing ICBC and MoH systems[33]

The Office of the Chief Information Officer (OCIO) is responsible for implementing the province wide IM/IT architectural plan to securely connect "systems and people, identifying evidence-based outcomes and making sound investment decisions." As a result, they are motivated to support government services with "a next generation information structure."[34] Per the IM/IT plan, the OCIO will operate the information hub (termed the Provincial Identity Information Services Provider) and ensure that data is not directly copied/pasted between different ministries under the proposed e-Health and Services Card initiatives; instead of a government employee from ministry A *copying* data from Ministry B, that employee would only *view* records from Ministry B after being authenticated through the OCIO's integrated system. Consequently, in addition to stated motivations of encouraging 'e-government' services, the OCIO has a political motivation to drive this program, insofar as it enhances their relative stature amongst public institutions.

The OCIO exists within the Ministry of Citizen Services and Open Government. The Ministry stands to be broadly responsible for the functioning of the identity

[33] S. van der Merwe (Insurance Corporation of British Columbia). (2011). "BC Services Card Project - HCCP BT - Insurance/Marketing/Licensing C.LI.10.HCCP Interim Project Charter," Drafted February 28, 2011. Pp. 6.
[34] Office of the Chief Information Officer. (2009). "Identity Information Management Architecture Summary," Version 0.7, Last Updated March 23, 2009. Pp.1

infrastructure associated these enhanced identity documents and, as such, has (successfully) sought to change BC privacy laws to implement the identity assurance program linked to the Services Card.[35] These laws had to be modified because, prior to being changed, the e-government project was operating under a research clause in the privacy law.[36] Specifically, the clause was being used to permit government data sharing between ICBC and other government departments to trial e-Health and Services Card initiatives; while early documents from ICBC simply note that this clause was being used, in subsequent communications the manager of privacy and freedom of information at the Insurance Corporation of British Columbia worried that the clause was being used inappropriately.[37]

There have been some actors that have inhibited, or are perceived as inhibiting, the Services Card program. Almost all of the inhibitors have been related to privacy concerns, under the guise of data security, collection, retention, and storage challenges. ICBC has been at the forefront of identifying these problems. This is not surprising given the institution's core role in the Services Card initiative; the decision to 'partner' with ICBC is based on their possession of administrative, technical, and business process resources required to massively deploy the new card.[38] Given ICBC's own operational requirements - to issue standards compliant drivers licenses - they have required MoH to conform to ICBC's data formatting processes[39] and explicitly wrote that "ICBC will not conform to the Office of the Chief Information Officer (OCIO) identity standards; ICBC will continue to conform to AAMVA and Canadian Council of Motor Transport Administrators (CCMTA) standards."[40] In addition to such standards issues, ICBC has previously identified business process, financial risk, and privacy and data sharing concerns as potentially stymying the initiative.[41] It has also raised an 'institutional sovereignty' flag, insofar as ICBC has raised concerns that 'its' data would

[35] S. van der Merwe. (2011). "Business Transformation Meeting Minutes: HCCP Weekly Team Meetings for May 18, 2011."
[36] C. Ulveteg. (2010). "Mini Privacy Impact Assessment for Research request from the BC Vital Statistics Agency, Ministry of Health," Drafted May 19, 2010. Pp. 1-6.
[37] Correspondence between ICBC Employees, May 29, 2010.
[38] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 31, 2010 (Version 2.6). Pp. 6.
[39] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 19, 2010 (Version 2.4). Pp. 11.
[40] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 31, 2010 (Version 2.6). Pp. 15.
[41] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 31, 2010 (Version 2.6). Pp. 34.

be held by the OCIO after ICBC had collected it:[42] this would move control - and thus power - over ICBC's data to another government institution and, in effect, constitute a degradation of ICBC's sphere of influence and power. Ultimately, this migration of data does not seem to have occurred.[43]

In terms of privacy, a 2011 document from ICBC recognized that the "Privacy Commissioner has not been involved in Government decisions. Unresolved privacy issues could impact the project scope, schedule, and budget."[44] Indeed, ICBC was explicitly prohibited from communicating with the provincial privacy commissioner about data sharing with MoH, and internally raised worries about putting "a chip on the [driver's license] that will store a bunch of information that will be irrelevant to a driver license" and that "people have to see their personal health number so it will be on some part of this driver license and that to me is a privacy issue."[45]

So, while ICBC is seen as a potential inhibitor, the Privacy Commissioner is seen as another. MoH drafted a 'conceptual privacy impact assessment' and provided it to the commissioner. Internal ICBC documents state that the "concept of a "conceptual PIA" seems to be exploited to mean that they don't think they need to provide much detail"[46] with a further suggestion that "the document is really an overview of the BC Services Card Project since no assessment from a [Freedom of Information and Protection of Privacy Act] perspective has been done."[47] After presenting the conceptual document to the Commissioner, the Ministry of Health purported to have had the document 'approved' by the OIPC and,[48] subsequently, released press releases about the project.[49] As of when this report was drafted in December 2012, documents had not been provided by MoH or OCIO under access to information laws; this means that a full

[42] Correspondence between ICBC Employees, Ministry of Health Employees, and Office of the Chief Informaton Officer Employees, dated February 7, 2011. It is significant to note that this account of how data would be stored by the OCIO stands in variance with information disclosed to us in an interview with a member of the OCIO on November 13, 2012.
[43] Based on communications with government officials, December 2012.
[44] S. van der Merwe (Insurance Corporation of British Columbia). (2011). "BC Services Card Project - HCCP BT - Insurance/Marketing/Licensing C.LI.10.HCCP Interim Project Charter," Drafted February 28, 2011 (Updated September 8, 2011). Pp. 17.
[45] Correspondence between representatives in Ministry of Health and ICBC, July 18, 2010.
[46] Correspondence between representatives in Ministry of Health and ICBC, April 19, 2011.
[47] Correspondence between representatives in Ministry of Health and ICBC, April 21, 2011.
[48] Correspondence between representatives in Ministry of Health and ICBC, April 27, 2011.
[49] It is worth noting that the OIPC does not 'approve' any privacy impact assessments, but only offers feedback on assessments that they review.

accounting of how these institutions perceive privacy and security concerns related to the Services Card initiative are almost entirely non-existent.[50]

Other inhibitors are around legislation that had to be changed; such legislative amendments were proposed - and passed - before anything the MoH had developed more than a 'conceptual PIA'. Privacy advocates are only indirectly referenced as inhibiting the Services Card; specifically, there is a recognition that prior Canadian advocacy against the introduction of Enhanced Drivers Licenses (EDLs) was largely unsuccessful and, thus, a chip-configured Services Card platform is unlikely to meet appreciable public resistance. This said, ICBC correspondence does reveal that Passport Canada has encountered "a lot of resistance to having chips in cards or passports"[51] and so opposition to the Services Card initiative could become more significant than that towards the EDLs. Furthermore, while the vendors that have been chosen haven't themselves inhibited the program, IBM has previously warned that the BC government's plans may be imprudent. Specifically, the company wrote, that

> [t]here's strong pressure to save citizen's tax monies by using technology to create multi-tenant/use credentials. While technically feasible, it's our opinion that for the foreseeable future it's not a good idea. Continuing the current approach of discrete credentials for travel, health care, driving, etc., promotes resiliency and limits damage if a specific credential's information or technology is compromised.[52]

Despite IBM's previous concerns, they are now a core corporate partner in developing and issuing the BC Service's Card.

In addition to a lead vendor previously warning about the appropriateness of the current identity proposal, it should be noted that alternative card vendors that promoted high security- and privacy-conscious products were dismissed on the basis of product scalability.[53] Specifically, BC's adoption of vendor partners has been significantly shaped by the decisions and purchasing power of the Federal Government of Canada. In 2010, the federal government tendered a request for proposals for a credential brokerage service (CBS) to facilitate identity authentication associated with

---

[50] Subsequent to this report being written, documents were released from OCIO after a prolonged FOIA process.

[51] Correspondence between representatives in ICBC and Ministry of Health, February 7, 2011.

[52] IBM. (2007). "IBM Identity Management Point of View," *OCIO* (website). Published August 30, 2007. Last accessed November 25, 2012. Available at: http://www.cio.gov.bc.ca/local/cio/idim/documents/ibm_appendix.pdf

[53] Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.

delivering online services. The contract was to delegate identity authentication associated with providing government services to the winning bidder. SecureKey, the only respondent to the competition, was awarded a $41 million dollar contract over 3 years (with future options for extension).

With the Government of Canada, SecureKey is currently involved with over 15 departments, notably including Human Resources and Development Canada (HRDC) and Canada Revenue Agency (CRA). As part of SecureKey's stated intention of "wrapping up Canada," the company intends to fold in all remaining provinces into its services and extend the scope of credential service providers beyond the private banking sector. They expect to have "the bulk of Canadian departments online" with SecureKey's CBS by the end of 2012.[54]

SecureKey's status as a "trusted" credential brokerage service is integrated with Eurocard, Mastercard, and Visa (EMV) physical standards governing the physical attributes of the card. Compounded with the growth of standardized Near Field Communication (NFC) mobile devices - devices that can communicate over very short distances using contemporary Radio Frequency Identification (RFID) protocols - all of the aforementioned elements contribute to the technical fulfillment the Government of Canada's stated vision to provide "seamless, cross-jurisdictional, user-centric, multi-channel service delivery experience when interacting with government."[55] In addition to providing identity management and authentication services for the Government of Canada, this vendor has also been contracted to provide core identity management infrastructure for the British Columbia Services Card.

The BC government adopted the SecureKey solution (without tendering a full request for vendors) to authenticate the legitimacy of provincial residents' identity documents prior to delivering online or offline government services.[56] The decision to adopt

---

[54] Code Technology. (2012). ""SecureKey - The Interview," *CodeTechnology* (website). Published September 24, 2012. Last accessed November 26, 2012. Available at: http://codetechnology.wordpress.com/2012/09/24/securekey-the-interview/

[55] D. Nikolejsin (CIO, BC) and M. Rosciszewski (Directeur, Direction des politiques, QC). (2007). "A Pan-Canadian Strategy for Identity Management and Authentication," *OCIO BC* (website). Published July 31, 2007. Last accessed November 25, 2012. Available at: http://www.cio.gov.bc.ca/local/cio/idim/documents/idma_final_report.pdf

[56] Province of British Columbia. (2012). "Notice of Intent (Notice of Internet #SATP-290)," Published 2012. Last accessed November 26, 2012. Available at: http://bccla.org/wp-content/uploads/2012/10/20120101-BC-Services-Card-notice-of-intent.pdf. See also: V. Gogolek. (2012). "Is B.C.'s New CareCard Another Technological Quagmire For Province?" *Huffpost British Columbia.* Published October 31, 2012. Last accessed November 25, 2012. Available at: http://www.huffingtonpost.ca/vincent-gogolek/bc-new-carecard_b_2041307.html

SecureKey, arguably, demonstrates that the provincial government is attempting to 'futureproof' the BC Services Card, insofar as the decision to work with SecureKey will facilitate integration with the Federal government initiatives.[57] Ultimately, however, in terms of vendor requirements it is SecureKey's ability to massively provide government credential brokering services in short order, while integrating with other federal initiatives, that has driven the adoption of this vendor's platform. Privacy and security requirements have played secondary determinate roles.

Situating the BC Services Card

When we contrast the BC situation with common international drivers, we find that business drivers - efficiency, cost, and perceived security benefits that combat fraud - have motivated the BC adoption of integrated drivers license/Services Card identity documents. In addition, the opportunity to leverage ICBC's facial recognition technology at the point of enrolment in the Services Card initiative is recognized as important: this technology is believed to reduce fraud by avoiding the repeated issuance of 'legitimate' provincial documents to the same person using different breeder documents.[58] Futureproofing, or ensuring that the document process will operate for subsequent identity initiatives has also been a driver, though perhaps not a terribly significant one. We also find that these drivers have been situated above prospective privacy concerns; privacy officials have either been largely ignored or avoided.[59] Moreover, legislation that would have precluded massive provincial data sharing initiatives, such as that contemplated under the BC Services Card initiative, was changed before the Ministry of Health (seemingly) conducted detailed risk, security, or privacy assessments.

Government does not seem to believe that advocates will measurably limit or delay the program, based on their relative lack of success in preventing EDLs. Advocacy against the Services Card has been supported, in a sense, by ICBC's privacy-related inhibitors but based on available documents ICBC and advocates have not closely collaborated with one another. It is significant to note, however, that documents pertaining to the proposed Services Card have *only* been released from ICBC under provincial access to

[57] Interview with a representative of the Office of the Chief Information Officer on November 13, 2012. See also: Office of the Chief Information Officer. (2010). "IM/IT Enablers Strategy for Citizens @ The Centre: B.C. Government 2.0". Pp. 21. Documents released under FOIA in 2013 also suggest that pan-Canadian integration is an expected long-term goal from SecureKey's perspective.
[58] Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.
[59] We do note that, in recent weeks, the role of the OIPC has been highlighted by the Minister of Health Services and that Minister in the BC government were at least publicly receptive of the OIPC's evaluation of 'phase one' of the Service Card's deployment.

information laws. MoH and OCIO alike have largely stonewalled the public,[60] with one member of the OCIO telling us that the relative lack of public pushback concerning the government's identity card system can be linked to the lack of publicly available information about the system. It should be noted, however, that this same individual has been very helpful in providing personal interviews.[61]

In the absence of presenting information to the general public, public advocates seem to have had limited success in delaying the new Services Card, based on documentary evidence. To date, it has been delays experienced by government that have slowed the rate of deployment, not public campaigning by advocates. Still, the current government proposal has been on the table for a considerable period of time: it's possible that the most current initiative will collapse under its own weight and there is a remote possibility that it could be turned into an election issue in 2013.

Consequently, while drivers in BC have some commonalities with international identity efforts, the common elements that limit or restrict such projects - principled and practical opposition - have thus far failed to stem the drive towards the new cards. Having provided an account of the current drivers and inhibitors, we turn to provide an outline of the technical infrastructure being built around this project.

Section Three - BC Technical Infrastructure

Implementing BC's IM/IT infrastructure entails a dramatic transformation of the province's existing digital networks. The introduction of the new Services Card is accompanied by a digital overhaul in the government's capacity to deliver everyday services. In the following section, we detail the technological and architectural facets of the IM/IT infrastructure implicated in the BC Services Card program. In particular, we engage in a detailed review of the technical aspects and key standards of the BC Services Card itself, including its reliance on NFC technology. We also provide an in-depth analysis of data flow across government networks associated with using the BC Services Card in-person and online. In our analysis of data mobility we pay particular attention to the private vendor, SecureKey, which is a central actor in authenticating of identities throughout the Services Card initiative.

[60] We note that, since drafting this document, the OCIO's office has provided documents after a protracted FOIA process.
[61] Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.

The Smart Card's Attributes

IBM currently holds the contract for producing BC's Services Card. In terms of physical attributes, the card will be fabricated out of layered polycarbonate plastic, featuring embedded holography and laser engraved markings for photo and text images which are meant to provide a "high assurance" that the cards are not forged.[62] The new card includes the same personal information and magnetic stripe specific to existing BC driver's licenses.[63] However, to better secure data the Services Card will be equipped with an embedded microprocessor (chip) that provides cryptographic proofing functions. This chip will serve as a principle electronic component of authenticating individuals to e-government services.

The new Services Card will leverage ICBC's existing Facial Recognition Technology (FRT) systems. At enrollment, Services Card recipients will have their images taken as templates that are subsequently matched against the existing ICBC databases to ensure that a single person is not registered under more than one identity. This matching functionality will entail extending ICBC's existing Facial Recognition Application to "support the ability to recognize matches and unexpected mismatches between health card images and [drivers license] images."[64] Operationally, processes for evaluating mismatches will be established, and facial recognition software and algorithm licenses will need to increase by one million images.[65] The BC government will use 'ABIS' facial recognition algorithms to identify matches. With regards to FRT, ICBC has written,

> Facial Recognition will be done against all photos captured by ICBC's image capture process (approx 26-27% hit on 1,000,000 photos) to support Personal Health Number (PHN) fraud investigation.[66]

In the case of 'hits' either ICBC or MoH will be responsible for auditing for accuracy, depending on whether the image was taken for drivers license or Services Card

---

[62] C. Rose (Public Affairs Bureau, BC Ministry of Public Safety and Solicitor General) and A. Grossman (ICBC Communications). (2009). "High-Tech Driver's License To Help Stop ID Theft, Fraud," *Government of British Columbia*. Published February 9, 2009. Last accessed November 27, 2012. Available at: http://www2.news.gov.bc.ca/news_releases_2005-2009/2009PSSG0012-000157.htm

[63] Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.

[64] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 31, 2010 (Version 2.6). Pp. 27.

[65] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 31, 2010 (Version 2.6). Pp. 28.

[66] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 31, 2010 (Version 2.6). Pp. 14.

issuance.[67] From documents provided it is unclear whether ICBC has a methodology for calculating false negatives/positives, nor whether a confidence rating on collected biometric data is performed on a per-record basis.[68] These methodologies determine how effective the FRT system is, insofar as it ascertains whether templates that are stored are suitably accurate for mass identity validation processes.

The physical design and functionality of the BC Services Card is premised on the payment card industry standard known as EMV and, as of Q2 2012, there are approximately 1.55 billion EMV compliant payment cards in use globally.[69] This scalability will presumably be helpful for future interoperability between consumer and public services.[70]

The communications protocol between the contactless chip and the reader relies on NFC, which involves a set of technological standards governing communications protocol (and data exchange) based on already existing RFID technology. Specifically, NFC relies ISO 19092, whereas Type A/B proximity cards rely on ISO 14443, and vicinity cards on ISO 15693. ISO 14443 cards have nominal read ranges of up to 10cm, whereas ISO 15693 cards operate at up to 1m range. The BC Services Card will use the ISO 14443 standard[71] and IBM will be instrumental in readying the actual cards for the government.[72] Our report, from here, proceeds on the assumption that proximity A/B technologies will be used.

---

[67] S. van der Merwe. (2010). "Government Care Card Initiative: ICBC Program Model," Drafted August 19, 2010 (Version 2.4). Pp. 12.

[68] For more on the significance of confidence ratings pursuant to large Canadian government databases, see the "Accuracy and Security section of C. A. Parsons, J. Savirimuthu, R. Wipond, and K. McArthur. (2012). "ANPR: Code and Rhetorics of Compliance," Published September 4, 2012. Last accessed November 26, 2012. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2141127. Requests for clarification concerning ICBC's confidence ratings received unhelpful responses.

[69] EMVCo (2012). "About EMV", Last accessed on November 26, 2012. Available at: http://www.emvco.com/about_emv.aspx

[70] Though outside the scope of this report, it is imperative to note that the EMV "Chip and PIN" security system has been significantly breached, with attacks on the system having been weaponized and now used in the wild. See: M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson. (2012). "Chip and Skim: cloning EMV cards with the pre-play attack," Computer Laboratory, University of Cambridge, UK. Published 2012. Last accessed November 26, 2012. Available at: http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf

[71] British Columbia Ministry of Citizen and Labour Services, Office of the Chief Information Officer (2012). "Information Management / Information Technology Standards Manual," p. 47, last updated July 3, 2012.

[72] Correspondence with representative of the Office of the Chief Information Officer, December 13, 2012.

NFC is increasingly used for identification and payment purposes, with Japanese student IDs sometimes being stored on NFC to facilitate class registration, food purchase, and other commercial uses, and more generally in Japan and South Korea for mobile payments.[73] The technology is also being trialed, in Canada, for mobile payments. Current standards primarily establish how transmissions between devices should occur, whereas the specific *content* that can be transferred continues to fluctuate.[74] In interviews we have conducted, we have alternately been told that NFC data communications will be encrypted[75] and that they will not be encrypted.[76] [77]

NFC protocols can be broken into a series of categories, with the 'lowest' layer of the communication at the bottom of the list and 'highest' layer at the top:

- Application Layer: NFC typically formats data according to the NFC Data Exchange Format (NDEF), which contains multiple identifiers to describe the types of data to expect (e.g. URI, MIME). Significantly, NDEF does not "make any assumptions about the types of payload that are carried within NDEF messages or about the message exchange patterns implied by such messages"[78]
- Tag Types: refers to Type 1, 2, 3, 4, and NFC Formatted Tags
- Protocol: is responsible for actually transmitting data to be sent or received. NFC supports a multitude of protocols, with dominant ones including Type 1 (Topaz), MIFARE Classic, Type 2 (MIFARE Ultralight), Type 3, Type 4 (DESFire), LLCP (P2P)
- Initialization Anticollision Protocol Application: defines how NFC-enabled devices become aware of one another and initialize communications. Given that

[73] A. Paus. (2007). "Near Field Communications in Cell Phones," Published 2007. Last accessed November 25, 2012. Available at: http://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/near_field_communication_in_cell_phones.pdf
[74] For examples in the variance between content that can be transferred, see: C. Miller. (2012). "Exploring the NFC Attack Surface," *BlackHat 12*. Published August 13, 2012. Last accessed November 25, 2012. Available at: http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf
[75] Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.
[76] Communication with Office of the Chief Information Officer representative on December 13, 2012.
[77] Documents received in 2013 suggest that the unique number embedded in the NFC chip will not be encrypted, though cryptographic proofing will be used to confirm the chip and, by extension, the number's authenticity.
[78] NFC Forum. (2006). "NFC Data Exchange Format (NDEF)," *NFC Forum* (Website). Published July 24, 2006. Last accessed November 26, 2012.

little data is exchanged at this point, it is seen as relatively uninteresting to attack[79]
- Physical and Radio Frequency: is defined in ISO 14443 A-2, and describes the protocols to transfer data

When considering the NFC specifications it is important to recognize that there are two principle elements: the NFC tag and the reader itself. In terms of the reader, there will be various ways of handling NFC code; most significantly, the NFC Service *will* vary across devices and across operating systems installed in devices, including payment readers and mobile technologies. Android, as an example, has a 3-layer NFC Services stack, whereas Nokia's MeeGo operating system features a 9-layer stack.[80] As will be discussed, this variance in stack handling creates a varied attack surface, that is, it creates a means to 'hack' the NFC communications channel. Further, since operating systems let NFC tags write data to more of the file system as the protocol is adapted, it is becoming more challenging to 'sandbox' NFC requests. Consequently, it is becoming harder to ensure that NFC commands are kept within intended smartphone processing containers. The result is that commands issued vis-à-vis NDEF are 'breaking free' of applications that they are meant to run in, with the effect that NFC can be used to compromise the security of mobile phones or computers that can read NFC chips.

BC Government Database Architecture

Having discussed the characteristics of the card itself we now turn to cover the database architecture associated with the IM/IT and Services Card system. Throughout we identify key standards that are used (where they have been disclosed to us) and SecureKey's prominent role in authenticating identities throughout the Services Card initiative.[81]

---

[79] C. Miller. (2012). "Exploring the NFC Attack Surface," *BlackHat 12*. Published August 13, 2012. Last accessed November 25, 2012. Available at: http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf

[80] C. Miller. (2012). "Exploring the NFC Attack Surface," *BlackHat 12*. Published August 13, 2012. Last accessed November 25, 2012. Available at: http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf

[81] The following description of how the Services Card interface with various elements of the MoH and other actors was communicated to us by a member of the OCIO's office in an interview November 27, 2012. At their request, our interviews were *not* recorded. To date, we do not have a definitive diagram that details data flows for the Services Card. As such, we have recounted the data flows to the best of our ability, but recognize that our presentation may contain some inaccuracies.

Many Point Of Service (POS) computers in MoH use either Cerner or Meditech as their primary electronic record keeping applications and use a Windows operating system.[82] At these particular POSes, a USB device with card reader will be attached that interoperates with SecureKey software. When a patient's Services Card is tapped on the reader, the POS application will invoke the SecureKey software to communicate with the NFC equipped card. The reader accesses the card number (i.e. PAN) and the cryptogram generated by the card.[83] The SecureKey application on the POS then communicates with an OCIO server after verifying the authenticity of the cryptogram. In this communication with the OCIO, SecureKey verifies that the PAN is still active. The following description summarizes what this document flow looks like:

Validating the NFC Chip

Stage 1: Card → USB reader; a cryptogram is created to confirm chip authenticity
Stage 2: USB reader → SecureKey; SecureKey interacts with the POS to receive the PAN and cryptogram generated in Stage 1. After validating the cryptogram and confirming a valid card is present, the PAN is sent to the OCIO.
Stage 3: SecureKey → OCIO; after confirming the authenticity of the cryptogram, SecureKey communicates with the OCIO to confirm that the PAN remains active

Upon confirming that the PAN is active the OCIO will release a Meaningless But Unique Number (MBUN) specific to the user and provide it to SecureKey. Given that the PAN is confirmed active, the POS and SecureKey software securely exchange session tokens using OAuth 2.0, an open standard for authentication. The SecureKey server then transforms the MBUN into a Persistent Anonymous Identifier (PAI) relevant to the service the BC resident is trying to access (i.e. a resident will have one PAI for MoH, another for Citizen Services, and so on). The PAI is then transmitted to the POS. This process is summarized as follows:

Validating the Cardholder

Stage 4: OCIO → SecureKey; OCIO transmits MBUN to SecureKey
Stage 5: POS ←→ SecureKey; since card was authenticated in Stage 3, an encrypted (TLS) OAuth 2.0 session is established
Stage 6: SecureKey + MBUN = PAI; SecureKey translates MBUN to PAI

---

[82] While not addressed in our scenarios, in some cases a EMV payment terminal may also be involved in the generation of secret key information. Critically, EMV has a series of different standards, including static data authentication, dynamic data authentication, and combined data authentication. All have demonstrable security vulnerabilities. For more, see R. Anderson. (2007). "10.6.1 EMV," *Security Engineering (Second Edition)*. Indianapolis: Wiley.
[83] It remains unclear to us how this proof is guaranteed or the cryptographic methods are used in arriving at card-present verification.

Stage 7: SecureKey → POS; SecureKey sends the PAI to POS

After the MoH POS has acquired the PAI that is specific to the ministry (i.e. MoH has one PAI linked to an individual, whereas another ministry will have a separate PAI linked to the same individual) it has to be translated into Personal Health Number (PHN) because the government's Electronic Health Record applications (Meditech and Cerner) only 'understand' the PHN. To translate the PAI, MoH will lookup the PAI, correlate it with the PHN associated with the individual, and pass that to the POS.

Translating the PAI

Stage 8: POS → MoH client registry; POS sends the PAI to MoH to look up the linked PHN
Stage 9: MoH client registry → POS; MoH transmits the PHN to the POS

This concludes the electronic transactions and will have verified the cryptographic validity of the NFC chip, transmitted information between the MoH and OCIO to verify that the Services Card is still active for use, and ultimately enabled the POS operator to retrieve record(s) associated with the Services Card that has been presented. Ultimately, in this process the system only has to really cryptographically verify the card and access the PHN associated with the card's owner; since the owner is physically present other visual evaluation can be performed to check that the card in question belongs to the individual requesting service. This means that two-factor authentication (e.g. secret password, PIN, etc) is not *necessarily* required, though some POSes could adopt two-factor authentication. Our research indicates that the MoH has not adequately prepared for this process.[84]

Significantly, where online services operate as the POS, a slightly different process and set of standards applies. The following outlines an online situation.

When a user goes to MoH's website to look up their prescription history, protocols based on the Security Assertion Markup Language (SAML) are used to facilitate single-sign on. Here, the MoH website is engaged in a SAML-based authentication process and subsequently directs the user to the OCIO's website for authentication. The website initiates the SecureKey software residing on the client's computer and prompts the user to tap their card. SecureKey then performs a chip validation with the OCIO (see stages 1 - 3) and provides the MBUN (stage 4). The core difference arises during the OAuth process (stage 5); specifically, a two-factor authentication process is used. This means that a user is prompted to enter their passcode before the session is established. After

[84] Interview with a representative of the Office of the Chief Information Officer on November 27, 2012.

successfully entering the passcode data flows according to stages 6-9, with the difference being that instead of a MoH POS being served data, it is the Internet-enabled client that is served the information.

A key privacy consideration for the OCIO, as the primary program authority within the BC IM/IT framework, is how to handle log records. At the time of writing the OCIO was still forming its internal data management policy concerning the storage of log information associated with card usage.[85] It is also important to note, from a privacy standpoint, that SecureKey engages in its own event tracking and could provide event logs associated with a PAI that might be requested by a Relay Party (RP), such as MoH, though in its routine course of business SecureKey is not supposed to know who is the relaying party. Specifically, SecureKey logs the card number, the card cryptogram, and the MBUN in each authenticated transaction it processes. Further, SecureKey can also use the MBUN to go to the Credentialing Party (government, banks) and acquire details of an authentication event to be shared with the RP.

SSL/TLS/SSH

The BC IM/IT architecture assumes the ability to securely use the public Internet to transfer data across government Ministries and to SecureKey. Government documents reveal that Secure Sockets Layer/Transport Security Layer (SSL/TLS) will be used to provide transport-level security. SSL/TLS facilitate trust in online communications, insofar as web browsers (e.g. Internet Explorer 9/10, Google Chrome) and applications rely on the protocols to cryptographically protect communications against eavesdropping and tampering.

TLS employs a host of encryption algorithms and key exchange protocols, and is meant to be extensible. Contemporary systems use key exchange mechanisms and encryption ciphers to ensure that communications remain secured, even if encryption key material is compromised. More specifically, when a client makes a TLS connection it initiates a cryptographic negotiation so that the client and server can agree to the strongest form of mutually shared encryption. In the process of initiating the communication the browser and server exchange information that is used to create a single-use key to encrypt and decrypt information between the two parties. Under the contemporary TLS specification the server 'forgets' the single-use key after the communications is terminated. Thus, even if a communication was captured the third-party cannot decrypt what was transmitted.

[85] Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.

It is important to introduce another actor in the SSL/TLS process: certificate authorities (CA). When a client establishes a connection with a SSL/TLS capable server the client downloads a certificate from CA and evaluates it against a list of pre-stored trusted CA certificates. CAs fall into three categories: those trusted by the client ("root CAs"), those trusted by one of the root CAs ("intermediate CAs"), and CAs that are not trusted by browsers or in a chain of trust with a root or intermediate CA ("untrusted CAs"). The present CA system does not "prohibit a CA from issuing a certificate to a malicious third party. As a result the integrity of the CA-based public key infrastructure and the security users' communications depends upon hundreds of CAs around the world choosing to do the right thing."[86] In the SSL/TLS infrastructure, then, it is important to recognize the core actors as the clients/servers, SSL/TLS itself (insofar as there are different iterations of this means of securing the transport layer), and the CAs responsible for establishing trust in the first place.

Based on discussions with members of the OCIO's office we understand that TLS using temporary session keys will be supplemented by Secure Shell (SSH). SSH is used to establish a secure transport layer between client and server. It relies on public key cryptography to establish a shared secret and (consequently) a securely encoded communications tunnel. SSH-based communications can require either login/password challenges after the encrypted session is established to subsequently give the client access to the server. Alternately, the server can issue a challenge to the client and provide a public key to the client; if the client can decrypt the public key issued by the server using the client's own private key then the two parties can authenticate with one another.

Section Four - An Overview of Risks and Vulnerabilities

In this section we provide an overview of core risks and vulnerabilities that could be associated with the BC government's Services Card initiative. We identify concerns linked with specific technologies when we can but, given the relative scarcity of primary source documents that identify this information, many of the concerns we raise identify the *kinds* of questions that need to be answered and the *types* of vulnerabilities that such data systems possess. Importantly, when considering the security of these cards we were less concerned with how they *work* than how they *fail*.

[86] C. Soghoian and S. Stamm. (2010). "Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL," *SSRN*. Published April 16, 2010. Last accessed November 26, 2012. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1591033

This method of critique has been summarized by Bruce Schneier: "[w]hat matters is how the system might fail when used by someone intent on subverting that system: how it fails naturally, how it can be made to fail, and how failures might be exploited."[87]

We begin by considering risks associated with card issuance and forgery. These problems, while written in the context of the Services Card, arguably could (and do) apply to all publicly- and privately-issued physical identity tokens. We subsequently discuss data management and security processes. Here we are relatively general in our discussion; we have not been provided detailed technical information concerning the makeup of the BC government's networking infrastructure, and it is outside of the scope of this report to hypothesize broadly about this infrastructure. However, given that public data will be traversing over the public Internet we do account for SSL/TLS/SSH vulnerabilities and how such vulnerabilities might be leveraged. The NFC chips that will be used with the cards are also examined, as are the problems associated with reading NFC tags using mobile phones. We conclude by identifying the function creep issues associated with the Services Card, and how such creep could endanger BC residents' personal information.

Importantly, we would like to recognize that the aim of 'security' is not to establish impenetrable walls that perfectly - and permanently - secure systems from attackers. Instead, security systems should impose friction and resource costs that are in excess of the costs associated with defeating the systems. In other words, the aim of security processes is to make it more costly to 'beat the system' than the payoff or reward associated with compromising whatever you are securing. This said, any system should presume that existing defenses will be defeated and, as a result, be fluid enough to permit security improvements and rotations to keep the attacker 'behind' the defender. The challenge in the case of the Services Card, of course, is simultaneously establishing high degrees of friction, while maintaining maneuverability, across extensively used public (and, in the future, private) systems and institutions.

Enrollment

The security of identity documents begins - and often ends - with the strength of enrollment processes. In what follows, we identify mechanisms that could be leveraged to attack the point of service; the POS is critical because it is where breeder documents' authenticity is established for subsequent credential issuance. This means that POS

[87] B. Schneier. (2004). "A National ID Card Wouldn't Make Us Safer," *Bruce Schneier* (Originally Minneapolis Times). Published April 1, 2004. Last accessed November 27, 2012. Available at: https://www.schneier.com/essay-034.html

staff must be able to detect false breeder documents that are used to establish the trust needed to receive a Services Card.

Specifically, the Services Card relies on biometric functionalities to offer secondary means of authenticating the individual's identity at issuance. An image of the person applying for a card is taken at the POS and converted to a Facial Recognition Template (FRT) that is compared against the templates in a centralized image database. The template is used to ensure that the same person isn't applying for identity documents under multiple identities. ICBC FRT's systems are presently set to a sensitivity threshold that causes 25-7% of submitted images to move to secondary evaluation.[88] It remains unclear what percentage of these threshold images are verifiable positives or false positives. More significantly, the *false accept* rate - instances where fraudulent biometric images are successfully submitted to ICBC and do not result in a 'hit' requiring secondary evaluation - remains unclear. Consequently a confidence rating for the database, or potential means for reliably falsely enrolling individuals, remains unclear. Of course it is also important that there are no bad actors responsible for evaluating threshold images at registration given that such actors could undermine ICBC's existing secondary screening processes.

In effect, POS staff need to be 'good' actors and not attackers, or complicit in attacks to generate fraudulent identity documents. These kinds of problems are endemic to *any* credentialing system.[89] ICBC/MoH business processes alleviate some attack surfaces by introducing the need to visit ICBC locations to produce documents and have them verified prior to credential disclosure (undermining the temporal, distance, and rapidity advantages that online attackers have over physically-limited foes). Such surfaces may also be reduced by delaying the provision of the documents on the basis of identity evaluation and possibly investigating individual applicants based on uncertainty surrounding breeder document authenticity.

Physical Card Protections

ICBC Drivers Licenses and the new Services Card adopt a series of defense-in-depth strategies; in addition to generally making substrate modification challenging the cards use specialized holographic images and province-specific imagery. However, the means of tampering with cards varies and well-resourced attackers historically defeat card

[88] Communication with ICBC staff, November 27, 2012.

[89] While not a popular position, any security system that will be overlaid on existing infrastructure must consider the possibility of the organization/system having *already* been compromised. Thus, new systems should try to develop processes that prevent existing bad actors from expanding their actions to the new service offering(s).

security mechanisms time after time; numbers are ground down and account numbers re-embossed, if profitable then cards are re-engineered and re-produced in increasingly sophisticated document creation labs, and supplies can be stolen from the trusted vendor to subsequently produce the cards.[90] Brands has written,

> Even though manufacturers work hard to improve smartcard tamper-resistance, mass production smartcards will likely never be able to withstand invasive physical attacks for more than a few years following their release. New sophisticated apparatus will appear, and existing apparatus is being improved all the time. Organized crime will hire expertise comparable to that in national laboratories, and sophisticated tools are increasingly being accessible to hackers and undergraduate students at technical universities.[91]

Importantly, defeating physical-layer protections is "about fooling people, not beating hardware" because all that is required - at the physical layer - is for the individual examining the document to believe that it is authentic. Consequently, tampering with the physical card has to be sufficient to fool government service representatives and seem sufficiently authentic for technological processes to verify the document's authenticity.

History teaches us that smartcard chips often succumb to being tampered with when sufficient resources are provided to a suitably motivated attacker. Problematically, audits of smartcard chips have historically been limited, though they are improving with major credit companies requiring penetration testing of their issued chips.[92] It remains unclear what kinds of penetration audits have been performed against proposed NFC chips for the Services Card; a brief examination of the history of microcontrollers reveals how techniques such as power differential analysis are commonly used to reveal a chips' secrets. There is no reason to expect that attackers will not continue to innovate as chip-based security measures become increasingly sophisticated.[93] It is in light of such attacks that smartcards, ideally, are designed under the assumption that secret key information will leak and still be capable of securely and

---

[90] Each of these attacks is described, in brief, in R. Anderson. (2007). "Physical Tamper Resistance," *Security Engineering (Second Edition)*. Indianapolis: Wiley.

[91] S. A. Brands. (2000). *Rethinking Public Key Infrastructures and Digital Certificates*. Cambridge, Mass.: The MIT Press. Pp. 229.

[92] For more on the poor incentives surrounding security evaluations, see R. Anderson. (2007). "17.7.4 Security-By-Obscurity," *Security Engineering (Second Edition)*. Indianapolis: Wiley. Pp. 517.

[93] For a brief overview of how smartcards and microcontrollers have been attacked, see R. Anderson. (2007). "16.6 Smartcards and Microcontrollers," *Security Engineering (Second Edition)*. Indianapolis: Wiley. Pp. 499-514.

reliably authenticating an individual for a government service offering. Mitigating steps can involve unique independent secret keys, smartcard design that can "detect, trace and contain fraud" by means of establishing core security features in software instead of hardware, and clear migration strategies from one generation of smartcard system to the next.[94]

Data Management and Security

While in the previous section we noted that SSL/TLS/SSH will be used to secure data as it crosses the public Internet,[95] at present we believe that TLS (with forward secrecy) has been chosen along with SSH.[96] Forward secrecy refers to a process whereby the secret key information that is stored in a cryptographic session is deleted after use. This deletion process ensures that captured encrypted communications cannot be decrypted, and so keeps things 'secret' after the communication has concluded. SSH refers to a network protocol used to cryptographically secure communications data. In what follows we outline some ways of attacking or weakening this encryption layer, as well as some of the broader issues that could affect the data transfer network providing BC services more generally.

Security experts recognize SSL/TLS as a fundamentally broken system,[97] with a series of problems being tightly associated with trust stasis. Specifically, when certificates issued by root or intermediate CAs are relied upon it is possible for a third-party attacker to have similar certificates issued from another root/intermediate CA and perform a Man-In-The-Middle (MITM) attack. Since most web clients 'trust' such certificates by default, and since they lack clear means of effectively evaluating general

---

[94] S. A. Brands. (2000). *Rethinking Public Key Infrastructures and Digital Certificates*. Cambridge, Mass.: The MIT Press. Pp. 229-330.

[95] We infer that the public Internet is used to transit data based on communications between K. McKinnon and K. Thomson, May 12, 2010. Specifically, the email reads "Regarding the transmissions of the information from the ICBC mainframe to the Shared Services mainframe, please be aware that portions of this network are *not considered private* and are *provided by Telus*." (emphasis in document provided through FOI request).

[96] Communication with ICBC staff, November 27, 2012.

[97] For more, see S. Gallagher. (2011). "New javascript hacking tool can intercept paypal and other secure sessions," Ars Technica, September 21, 2011. Last accessed on November 26, 2012. Available at: http://arstechnica.com/business/2011/09/new-javascript-hacking-tool-can-intercept-paypal-other-secure-sessions/; A. Arnbak and N. Van Eijk. (2012) "Certificate Authority Collapse," Draft of paper prepared for TPRC's 40th Research Conference on Communication, Information and Internet Policy. Last accessed on November 25, 2012. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409

trustworthiness over time, they demonstrate a kind of 'trust once, trust forever' state.[98] Research has shown that state actors can, and non-state actors have, issued such fraudulent certificates to engage in MITM attacks.[99] Further, at present, revocation and other techniques intended to remove trust in 'bad' certificates remain weak and often ineffective.[100] Moreover, in a survey of certificate deployment, only 16% of sites properly implemented Hypertext Transfer Protocol Secure (HTTPS) to carry out certificate-based authentication.[101] While there are many off-the-shelf APIs that facilitate the secure processing of credential information, such as those used by major payment vendors, it is *essential* that these APIs are subject to a rigorous code audit before being deployed. This position is based on recent findings that revealed grossly incorrect handling of certificate-based authentication.[102] In terms of SSH, the core issue

---

[98] In exceptional situations a CA's status can be revoked, but even in the case of major security breaches this action is not always taken because revoking a CA could 'break' SSL deployments across the Internet.

[99] C. Soghoian and S. Stamm. (2010). "Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL," *SSRN*. Published April 16, 2010. Last accessed November 26, 2012. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1591033; C. Parsons. (2011). "Security, Hierarchy, and Network Governance," *Technology, Thoughts, and Trinkets* (blog). Published March 28, 2011. Last accessed November 27, 2012. Available at: http://www.christopher-parsons.com/blog/technology/security-hierarchy-and-networked-governance/; C. Soghoian. (2011). "The forces that led to the DigiNotar hack," *slight paranoia* (blog). Published September 18, 2011. Last accessed November 27, 2012. Available at: http://paranoia.dubfire.net/2011/09/forces-that-led-to-diginotar-hack.html; K. McArthur. (2011). "Comodogate," *unrest.ca* (blog). Published April 1, 2011. Last accessed November 27, 2012. Available at: http://www.unrest.ca/comodogate; J. Appelbaum. (2011). "The DigiNotar Debacle, and what you should do about it," *TOR*. Published August 31, 2011. Last accessed November 27, 2012. Available at: https://blog.torproject.org/blog/diginotar-debacle-and-what-you-should-do-about-it; M. Hypponen. (2011). "Rogue SSL Certificates ("Case Comodogate")," *F-Secure*. Published March 23, 2011. Last accessed November 27, 2012. Available at: http://www.f-secure.com/weblog/archives/00002128.html; K. McArthur. (2011). "DigiNotar, GlobaSign, StartCom, and the #MostSophisticatedHackOfAllTime," *unrest.ca*. Published August 8, 2011. Last accessed November 27, 2012. Available at: http://www.unrest.ca/DigiNotar-GlobaSign-StartCom-and-the-MostSophisticatedHackOfAllTime

[100] A. Langley. (2012). "Revocation checking and Chrome's CRL," *ImperialViolet*. Published February 5, 2012. Last accessed November 27, 2012. Available at: http://www.imperialviolet.org/2012/02/05/crlsets.html; K. McArthur. (2011). "DigiNotar, GlobaSign, StartCom, and the #MostSophisticatedHackOfAllTime," *unrest.ca*. Published August 8, 2011. Last accessed November 27, 2012. Available at: http://www.unrest.ca/DigiNotar-GlobaSign-StartCom-and-the-MostSophisticatedHackOfAllTime

[101] N. Vratonjic, J. Freudiger, V. Bindschaedler, J-P. Hubaux. (2011). "The Inconvenient Truth about Web Certificates," The Workshop on Economics of Information Security (WEIS), Fairfax, Virginia, USA. Last accessed November 27, 2012. Available at: http://infoscience.epfl.ch/record/165676

[102] K. McArthur. (2012). "#PeerJacking - SSL Ecommerce Attacks Against Online Commerce," *unrest.ca*. Published August 3, 2012. Last accessed November 27, 2012. Available at: http://www.unrest.ca/peerjacking; K. McArthur. (2012). "#PeerJacking - SSL Ecosystem Attacks Against Online Commerce (update)," *unrest.ca*. Published August 22, 2012. Last accessed November 27, 2012.

is where an eavesdropper 'listens in' on the exchange of secret information used to establish a connection.[103] Ultimately, SSL/TLS vulnerabilities mean that next-generation techniques such as certificate pinning[104] or a more agile trust system[105] should be adopted to offer high levels of trust in this method of securing the transport layer. In terms of SSH, adopting a key-based authentication system can evade some of the SSH eavesdropping attacks, where it is possible to derive meaning from secret communications by observing significant volumes of encrypted communications.

Like all aspects of the BC Government's e-government initiative, the card authentication process could be negatively impacted by targeted Distributed Denial of Service (DDOS) attacks. A DDOS attack generally involves using multiple systems to flood the bandwidth or resources of a targeted system or network. Should existing DDOS mitigation techniques be insufficient in the face of an attacker, elements of the network could be inaccessible to one another, and service delivery could be negatively affected. Given the increased use of DDOS for civil disobedience purposes, and the relative affordability of botnets to launch DDOS attack, the move to e-government and e-Health systems associated with the Services Card will have to consider the increase in attack opportunities arising from heightened dependence on network-based government service delivery.[106] It is significant to recognize that DDOS attacks have

---

Available at: http://www.unrest.ca/peerjacking-updateAug2012; K. McArthur. (2012). "Responsible Disclosure and the Academy," *unrest.ca*. Published October 23, 2012. Last accessed November 27, 2012. Available at: http://www.unrest.ca/responsible-disclosure-and-the-academy; Canadian Cyber Incident Response Centre. (2011). "Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certification Verification," *Public Safety Canada*. Published December 20, 2011. Last accessed November 27, 2012. Available at: http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx; M. Georgiev, S. Iyengar, S. Jana, R. Anubha, D. Boneh, V. Shmatikov. (2012). "The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software," CCS 12. Published 2012. Last accessed November 27, 2012. Available at: http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf

[103] G. Danezis and R. Clayton. (2008). "Introducing Traffic Analysis," in A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. De Capitani di Vimercati (eds). *Digital Privacy: Theory, Technologies, and Practices*. New York: Auerbach Publications. Pp. 102.

[104] A. Langley. (2011). "Public Key Pinning," *ImperialViolet*. Published May 4, 2011. Last accessed November 27, 2012. Available at: http://www.imperialviolet.org/2011/05/04/pinning.html

[105] M. Marlinspike. (2011). "SSL And The Future Of Authenticity," *Blackhat USA 2011*. Published August 18, 2011. Last accessed November 27, 2012. Available at: https://www.youtube.com/watch?v=Z7Wl2FW2TcA

[106] For more about the increase in DDOS attacks against infrastructure, see Arbor. (2011). "Worldwide Infrastructure Security Report," *Arbor Networks*.

been used in disrupting other governments' e-service capabilities, and that existing DDOS attacks can outstrip any of the defenses commonly in operation today.[107]

In discussions with the OCIO's office, we have learned that OAuth 2.0 will be used to authenticate the POS and SecureKey. The core benefit of attacking the OAuth channel would be to subsequently control the authentication process between the POS and SecureKey. OAuth 2.0 will be used and its framework actively depends on SSL/TLS to provide message confidentiality. Consequently, it suffers from trust issues common to SSL/TLS generally, as have been previously discussed.

In addition to OAuth 2.0, SAML will also be used as part of some single log on processes; while the intent of SAML is good - to let individuals access a series of webpages/services without having to respond to authentication challenges each time - the protocol does have noted issues. Specifically, attacks have shown that single sign-on can be broken for large commercial deployments of the protocol,[108] it can prospectively be subjected to DNS-based spoofing (where false resolving information is introduced to dynamic name system resolvers that direct web address locators to Internet Protocol addresses),[109] and poor implementations of the technology can leave it vulnerable to spoofing attacks.[110]

Of course, in addition to technical data management issues there are threats associated with bad actors within the organizations themselves. We know that such actors drive or enable a vast number of attacks by exploiting their existing privileges within the data

---

[107] C. Morales. (2012). "How likely is a DDoS Armageddon attack?" *Arbor Networks Security Blog*. Published November 28, 2012. Last accessed November 29, 2012. Available at: http://ddos.arbornetworks.com/2012/11/how-likely-is-a-ddos-armageddon-attack

[108] A. Armando, R. Carbone, L. Compagna, J. Cuellar, and L. Tobarra. (2008). "Formal Analysis of SAML 2.0 Web Browser Single Sign-On: Breaking the SAML-based Single Sign-On for Google Apps," FSME. Presented October 27, 2008. Last accessed November 28, 2012. Available at: http://ai-lab.it/alessandro/pub/fmse9-armando.pdf; see also J. Somorovsky, A. Mayer, J. Schwenk, M. Kampmann, and M. Jensen. (2012). "On Breaking SAML: Be Whoever You Want to Be," *21st Usenix Security Symposium*. August 8-10, 2012. Last updated August 23, 2012. Last accessed November 27, 2012. Available at: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final91-8-23-12.pdf

[109] H. Simon. (2004). "SAML: The Secret to Centralized Identity Management," Published December 4, 2004. Last accessed November 28, 2012. Available at: http://people.cs.vt.edu/~kafura/cs6204/Readings/Authentication/SAML_Quick_Overview.html

[110] K. Kiani. (2012). "Four Attacks on OAuth - How to Secure Your OAuth Implementation: A technical study of an emerging open-protocol technology and its security implications," *SANS Institute Reading Room*. Last accessed November 28, 2012. Available at: https://www.sans.org/reading_room/whitepapers/application/attacks-oauth-secure-oauth-implementation_33644

networks. While logging and auditing data access can help, this is only as effective as an administrator can certifiably demonstrate that a credential used to access data is positively linked to the individual using the credential itself. Moreover, in terms of data mobility, there is the risk that non-linked data capture tools are used to retain data on non-administrated devices after an appropriate access of a patient's data has concluded. For example, while an employee might appropriately call up information about patient A, they could inappropriately take a picture of the screen or write down what was recalled in the data query. Of course, these are not novel concerns, but instead constitute a regular threat that is routinely expressed in contemporary digitized and non-digitized data archive systems alike.

NFC Chips

Stefan Brands has stated that "[w]hile it is true that smartcards enhance the perception of privacy, perception and fact are two very different things."[111] In what follows we outline specific means of undermining the security related to the NFC chips that the BC Services Card plans to integrate.

To begin, eavesdropping is an issue for these cards. While NFC cards are *meant* to be read from no more than 10cm away, it is possible to read the cards from up to 50m away. This was demonstrated in research conducted by Gerhard Hancke. His research relies on a relay attack, where an attacker relays a message to the smart card, at a distance, and the card subsequently responds. To be successful, an attacker must capture information from the card remotely and transmit the information via a relay to either a storage unit (for subsequent efforts to decrypt information) or to a terminal that the attacker controls. Such attacks are "invisible to application layer security and therefore new protection measures should focus on the physical layer. An attacker wishing to forward data between a card and reader that are a distance apart will be unable to avoid causing a delay in the system."[112] Mediating such attacks would require distance bounding protocols to prevent relay attacks, though, as of 2007, "the practical implementation for a low-cost passive token with limited resources remains a problem to be solved."[113] In payment systems it has been theorized how this attack could be used

[111] S. A. Brands. (2000). *Rethinking Public Key Infrastructures and Digital Certificates*. Cambridge, Mass.: The MIT Press. Pp. 219.

[112] While it may be unlikely that a POS terminal installed by MoH or ICBC is compromised, the potential for a smartphone with NFC functionality being controlled by the attacker is a likely possibility. Reasons for this arise later in this section.

[113] G. Hancke. (2005). "A Practical Relay Attack on ISO 14443 Proximity Cards," Cambridge Laboratory Report. Published 2005. Last accessed November 26, 2012. Available at: http://www.rfidblog.org.uk/hancke-rfidrelay.pdf

for defrauding purposes - essentially by having the "victim" of the skimming and "attacker" who skimmed conspire with one another - though similar analyses of health systems do not seem to have been conducted as of yet.[114]

Another attack vector entails simply disrupting the communications with a jamming device;[115] RFID jammers are difficult to stymie, short of either increasing reader power in excess of that of the jammer or (preferably) identifying the source of the jamming and stopping it. While such an attack would not falsely insert information into a system it could undermine the perceived security benefits associated with using the Services Card identifier in a short-distance transmission system. In literature, this is defined as 'data destruction,' and Innopay notes that "[o]perating such equipment requires basic electronic engineering skills." While the Innopay's report goes on to state that "[t]here is no benefit for the distributer however besides that the transaction is made impossible"[116] this could be the very intent of the attack; where/if the electronic Services identifier is a prerequisite to service delivery a jamming system could hinder government service delivery. Employing a jamming device at a major social crisis, then, could impede efficient service.[117] Importantly, jamming systems for other electronic communications systems are readily available;[118] it is likely that similar jamming systems could be developed for 'lulz' or more directly aggressive purposes.[119]

---

[114] R. Anderson. (2007). "10.6.1.3 Combined Data Authentication," *Security Engineering (Second Edition)*. Indianapolis: Wiley.

[115] A. Paus. (2007). "Near Field Communications in Cell Phones," Published 2007. Last accessed November 25, 2012. Available at: http://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/near_field_communication_in_cell_phones.pdf

[116] Innopay. (2009). "Mobile Payments 2010: Market analysis and overview," *Innopay*. Published November 2009. Last accessed November 26, 2012. Available at: http://www.scribd.com/doc/50584038/27/NFC-Security-issues

[117] It has to be noted, however, that there is a health number identifier on the back of the card; thus, while jamming mobile communications could prevent *any* call to a health database, where a wireline connection exists the physical identifier could be used to compensate for loss of wireless communication systems.

[118] For more, see Sean Gallagher. (2012). "GPS jammers and spoofers threaten infrastructure, say researchers," *Ars Technica*. Published February 23, 2012. Last accessed November 26, 2012. Available at: http://arstechnica.com/business/2012/02/uk-research-measures-growing-gps-jamming-threat/; Ross Anderson. (2007). "19.4 Surveillance and Target Acquisition," in *Security Engineering (Second Edition)*. Indianapolis: Wiley Publishing, Inc.

[119] Indeed, using major search engines we discovered several efforts to jam 'Google Wallet', which relies on NFC, and instructions already exist for how to disrupt NFC using off-the-shelf equipment (e.g. JammerStore. (2012). "How to jam Google Wallet," *Jammer Wiki.* Published October 23, 2012. Last accessed November 26, 2012. Available at: http://wiki.jammer-store.com/questions/708/how-to-jam-google-wallet).

Until this point, we have largely focused on NFC from the perspective of a reader and a card; in what follows we consider the implications of integrating mobile devices' NFC functionality to read cards. We identify these concerns based on an interview with a member of the BC OCIO, who informed us that mobile technologies are being considered to read Services Card NFC chips and on the basis that the OCIO is currently testing this functionality with a Google Android device.[120] Moreover, SecureKey, the credential brokerage service, notes in their public literature how their service integrates with consumer-grade NFC-enabled mobile devices.[121] It should be noted that, at the moment, movements to mobile-based NFC authentication are conceptual: as such the government's decision to utilize these devices is not guaranteed.[122]

In terms of reading data using mobile devices, BC government documents make note that the Secure Element (SE) inside mobile phones will be leveraged to maximize data protection. In essence, users have limited access to the SE because it is controlled by a Trusted Service Manager (TSM), and cryptographic primitives can be used to transmit data[123] between the Services Card and mobile device. However, not all SE deployments are equal; they can have limited cryptographic libraries, old and/or insecure primes defined, lack trusted internal clocks, or be highly time-consuming. Consequently, a non-detailed and unilateral reliance on SE arguably misses the significant variances between SEs in different mobile phones and consequently their variable ability to mitigate attacks.[124]

Moreover, adopting mobile devices to read Services Card opens the phones themselves to attack. There are several elements that can be targeted; system bugs in the phones could be exploited using malicious tags, as could bugs in applications running on the device. Given that many contemporary smartphones and mobile phones alike will launch a Uniform Resource Identifier upon reading a NFC card, fraudulent cards could be used to automatically open malicious websites with 0-days computer exploits or other attack code. Such tags could be embedded in fraudulent documents or be 'written

[120] Interview with a representative of the Office of the Chief Information Officer on November 13, 2012.
[121] SecureKey. (Date Unknown). "Strong Authentication," *SecureKey* (website). Last accessed November 26, 2012. Available at: http://securekey.com/our-solutions/strong-authentication/
[122] Interview with a representative of the Office of the Chief Information Officer on November 27, 2012.
[123] G. Van Damme and K. Wouters. (2009). "Practical Experiences with NFC Security and mobile Phones," *Workshop on RFID Security, 2009*. Last accessed November 25, 2012. Available at: http://www.cosic.esat.kuleuven.be/rfidsec09/Papers/rfidsec2.pdf
[124] G. Van Damme and K. Wouters. (2009). "Practical Experiences with NFC Security and mobile Phones," *Workshop on RFID Security, 2009*. Last accessed November 25, 2012. Available at: http://www.cosic.esat.kuleuven.be/rfidsec09/Papers/rfidsec2.pdf

in' legitimate service provider tags.[125] It remains unclear - absent a full audit of how/whether SecureKey can effectively 'sandbox' NFC calls - whether SecureKey's mobile systems can mitigate these attacks on mobile devices.

While government discussions around the Services Card and security often revolve around protecting the efficient distribution of services to reduce fraud, what has (seemingly) been left out of the discussion is using a fraudulent - and malicious - Services Card NFC chip to attack government infrastructure. Specifically, the danger is that the smartphone itself could be compromised using well-known vulnerabilities and, as a result, let third-parties introduce hostile code onto a (semi-) trusted computing environment. In research released in late 2012, Charlie Miller discussed methods for attacking the network stacks of popular Android operating systems (2.3 and 4.0.1) as well as Nokia smartphones.[126] His results show that there are some, though limited, capabilities to inject hostile code at this layer but, when it comes to actually acting on NFC Data Exchange Format (NDEF) data, the attack surface expands. In the case of Android 4.0.1, or any Ice Cream Sandwich (ICS) Android device, "if an attacker can get the device to process an NFC tag, they can get it to visit a web site of their choosing in the Browser with no user interaction. Obviously, the Browser represents an extremely large attack surface, and in ICS, that attack surface is now available through NFC."[127] Android 4.1.1 has the same vulnerabilities. In the case of Nokia N9 MeeGo devices, an attacker can potentially force an automatic Bluetooth pairing. Given that various libraries will demonstrate vulnerabilities, updating the devices is essential - failure to rapidly update as new vulnerabilities are disclosed will open well-known attack vectors.

In essence, the usage of mobile devices for Services Card -related business opens a broad attack surface. Mobile devices would have to be rapidly updated to avoid open vulnerabilities, and networks need to be partitioned and firewalled from the devices. Moreover, given that new versions of operating systems might introduce novel vulnerabilities, a forensic code audit ought to be performed post-haste upon release, given that fixed vulnerabilities may subsequently be weaponized against non-updated devices. While it should not need to be said, though Android devices are popular

[125] C. Mulliner. (2008). "Attacking NFC Mobile Phones," *EUSecWest*. Published May 2008. Last accessed November 25, 2012. Available at: http://www.mulliner.org/nfc/feed/collin_mulliner_eusecwest08_attacking_nfc_phones.pdf

[126] C. Miller. (2012). "Exploring the NFC Attack Surface," *BlackHat 12*. Published August 13, 2012. Last accessed November 25, 2012. Available at: http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf

[127] C. Miller. (2012). "Exploring the NFC Attack Surface," *BlackHat 12*. Published August 13, 2012. Last accessed November 25, 2012. Available at: http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf

consumer devices they should not be adopted for authenticating government documents on the basis of poor vendor and telecom operator support for device updates; patches to Android devices are often available to end-users months or years after being released by Google.[128] As a result, vulnerabilities in mobile OSes can go unfixed by Canadian mobile phone providers for extensive periods of time. Finally, while the preceding critiques have been focused on *mobile* readers, readers built into laptops or attached to desktops should be treated with similar wariness and precautions.

In light of the fact that mobile and fixed computers that read NFC-enabled Services Card will require some kind of access to the government's network, there is the concern that an attacker could take control of the computer as a beachhead to breach other aspects of the government's network infrastructure. Consequently, the introduction of NFC-enabled devices for processing sensitive government data requires considerable planning and risk mitigation strategies. To date we have not seen documents from any BC Government Ministry, or from SecureKey (the vendor chosen as the CBS, and which is a strong advocate of NFC), or from federal or independent auditors that address *any* of these prospective attack points.

Function Creep

It's important to recognize that the proposed Services Card initiative is itself an example of function creep; the ICBC facial recognition system was initially implemented to conform with the Western Hemisphere Travel Initiative (WHTI), which forced the introduction of EDLs and enhanced identity cards to cross the border into the United States.[129] Since then, ICBC's biometric database has been offered for police uses[130] and now other government services want to use stored biometric templates for purposes in excess of why these templates were collected in the first place. ICBC has written that there are function creep-related issues around the dissemination of photographic and tombstone information with other agencies.[131] Moreover, there are issues around the expansion of the Services Card itself, insofar as BC Health Minister

[128] C. Johnston. (2012). "The checkered, slow history of Android handset updates," *Ars Technica*. Published December 21, 2012. Last accessed April 11, 2013. Available at: http://arstechnica.com/gadgets/2012/12/the-checkered-slow-history-of-android-handset-updates/

[129] Canada Border Services Agency. (2012). "Documents for entry into the United States: Enhanced Drivers License/Enhanced Identification Card,' *CBSA*. Last modified September 10, 2012. Last accessed November 28, 2012. Available at: http://www.cbsa-asfc.gc.ca/whti-ivho/edl-pcp-eng.html

[130] S. Hui. (2011). "ICBC offers facial-recognition technology to Vancouver police's riot investigation," *The Straight*. Published June 17, 2011. Last accessed November 28, 2012. Available at: http://www.straight.com/article-399779/vancouver/icbc-offers-facialrecognition-technology-vancouver-police%E2%80%99s-riot-investigation

[131] Correspondence between representatives from ICBC and the Ministry of Health, on February 7, 2011.

Mike de Jong stated that consolidating additional services around the card is an "obvious next step."[132] As the card is used to gain entry to more and more government services, it will be more and more likely to find new uses that aren't directly related to card authentication or specific service delivery.

Further, the change in legal standards for sharing information across the province, especially when combined with Ministerial delays or potentially 'uniquely' understanding how data sharing will function, could increase the number of locations that BC residents' data is retained. As more and more services are consolidated with Services Card -based data access, who gets access to what may vary: law enforcement could gain a deeper understanding of citizens upon arrest, or other government services develop deeper insight about their clients at times of service allocation and provision. While such expansions of the card are understandable they could reduce residents' desire to access government services with the card: where residents are uncertain of how accessing one type of government services could influence how other service providers subsequently interacted with them (e.g. using a card to authorize government benefits dispensation, and having a police officer subsequently gain access to that information at a later time) the 'solution' to preemptively stop such information leaks could be to avoid using specific government services. Similar concerns could arise as other, non-public, parties try and access information linked to the Services Card identifier, such as insurance companies. To be clear: the card assists in facilitating this sharing, but much of this sharing between government Ministries can happen absent of the Card, in virtue of recent changes to BC privacy law. Given that the province has already reshaped provincial law to facilitate government sharing of the information, members of the population might worry that similar legislative amendments could lead to increased sharing between public and private bodies.

Such concerns, of course, are not new nor are they unique to the Services Card situation: they are, however, prevalent, persistent, and in need of being directly addressed by the BC government.

So, What Does It All Mean?

While we have identified a series of prospective security issues with the proposed BC Services Card, what does this actually mean for service provision, what are likely attack points, and what do these vulnerabilities potentially mean for BC residents' privacy? In

[132] R. Shaw. (2012). "New CareCards to combat fraud," *Times Colonist*. Published May 20, 2011. Last accessed November 25, 2012. Available at: http://www2.canada.com/victoriatimescolonist/news/story.html?id=ab121170-2a70-4acc-9fe0-9cc801fac75a

what follows we briefly break down the implications of the system as currently proposed, and conclude with a series of warnings concerning the program and how the SecureKey project could (theoretically) be managed to increase BC residents' privacy.

The core issues around enrolment relate to bad actors: we know that the 'insider threat' is the core way that employers lose control of their data, either by employee negligence or malfeasance. A negligent employee and malfeasant employee could, in a Services Card situation, engage in detrimental actions that parallel those an existing ICBC staff could with regard to the BC Drivers License. Specifically, staff could be complicit in facilitating fraud - at the POS and, potentially, at the point of facial verification - or in exfiltrating data either for personal or criminal reasons. This might mean taking a picture/analogue recording of data for one's personal amusement or to subsequently make biographical information available to unauthorized third parties. These risks, both from a security and privacy perspective, already exist under ICBC's current business model. The Corporation presumably has measures in place to remedy such issues.[133] What changes with ICBC delivering a combined drivers license/Services Card is that more residents' data is prospectively available to bad actors in ICBC; whereas now such actors only have access to drivers' personal information or the residents that use the BC ID card, in the future residents who want access to BC-funded health care will have to visit an ICBC enrolment office.

With regard to the new cards' physical security properties, the fraud-based risks associated with the combined cards are in many respects equivalent to the existing drivers license insofar as new security properties - beyond the NFC chip - are not being proposed. As noted in the previous section it must be assumed that the authentication benefits ascribed to the NFC chip will be undermined over time in the face of sufficiently motivated attackers, and that physical card protections (e.g. holography) will eventually deteriorate as more sophisticated fraudsters produce the identity documents. With regards to biometric privacy, without confidence ratings for the biometric data mining it is challenging to ascertain - positively or negatively - whether the collection of this information is proportional or effective. Should there be high degrees of non-confidence in the data then BC residents may be providing information to the government in excess of its usefulness and, as such, this collection would be inappropriate.

[133] Note that we have no information concerning ICBC's fraud detection methods, or the rates of drivers license fraud in BC. As such, we are neither suggesting there are presently high nor low fraud rates, nor that there are many or few bad actors. Instead, we are simply describing a theoretical 'attacker' scenario.

While we raised a series of data management issues that were largely related to transport layer cryptography, the overall usefulness of attacking the BC system from this angle is unclear. TLS/SSH/OAuth 2.0 are all vulnerable to an attacker capable of penetrating the transport network in a series of locations; this might include centralized government routers (e.g. those in major hospitals/cities/OCIO) or private routers (e.g. SecureKey, TELUS). While the security of core routing appliances cannot be guaranteed this avenue of attack offers a non-ideal method of compromising BC residents' information on the basis that information transmitted between MoH terminals, SecureKey, and the OCIO use persistent but not immediately identifying numbers. As such, without additional server compromises (e.g. in the PAI lookup database, OCIO MBUN database) the information collected is arguably of minimal direct value. Where a DDOS is launched government services could be negatively impacted; what is important to understand in *how* those services might fail in the absence of data connectivity: does it provide a novel means of entering government systems? Such a worry is common for *any* Internet-connected government system and thus not novel in the BC Services Card environment, though with a transition to increasingly interconnected Ministry systems it is important to conduct audits of how the systems fail.

Perhaps most significantly, from a data management perspective, is that government *cannot* base security decisions on the trustworthiness of third parties: good security is not about trusting people. This means that the parties involved in the BC Services Card project should be seen as potentially compromised; most significantly, this means that SecureKey - the private partner responsible for facilitating the government's federated identity credentialing system - needs to have its products subject to technical audits, as well as assurances that employees are trusted actors.

The movement to increased online access to government services and documentation, significantly facilitated by the BC Services Card, will also broaden the value of attacking BC residents' computers. Value could be increased because yet more sensitive information will be made available through these known-insecure computing environments; even if the cryptographic functions between an NFC-reader, SecureKey, the OCIO, and particular Ministry database being queried can be secured, the display medium (i.e. the web browser) will remain a leaky and vulnerable piece of software. Attacks against SAML may also turn the benefits of single-sign on against BC residents and consequently facilitate third parties' capture (and subsequent use/dissemination) of highly personal information. Moreover, malware with screen capture and subsequent data exfiltration capabilities are common problems in today's PC world. There is no

reasonable expectation that such security problems will go away in the near future. To be blunt, NFC is *not* the solution to the woes of the computer client security world.

Since NFC is increasingly being used for banking and identity authentication purposes there will be more and more motivated attacks against its instantiations. Reader devices - and associated computing environments - may be compromised to grant unauthorized third-parties access to information from Ministry databases. Further, malicious tags could compromise the security of personally identifiable information stored on NFC-linked mobile or fixed computing systems. While this broader concern with NFC - that it could let third-parties compromise computing systems - remains in the absence of the BC Services Card, the government's formal adoption and advocacy of the technology could open yet another avenue to compromise government and residents' computer systems.

Ultimately, our concerns are dominantly focused on the bad actor problem and the (seeming) trust that the government has ascribed to the partners of the BC Services Card deployment. It remains unclear if the bad actor problem is an issue, at the moment, for ICBC. We have not researched what processes the Corporation has in place to identify and address such actors. Similarly, we have not seen documents from the OCIO concerning how they plan to identify and respond to bad actor scenarios, or any analysis that recognizes the potential harms linked with bad actors at SecureKey. Importantly, good security does not rely on trusting people, but in guarantees that technical and business processes maximize security. Trust in people should be recognized as helpful, though not necessary, for the safe and secure provision of Ministry services associated with the BC Services Card.

Section 5 - Further Securing the Services Card

Given the host of prospective vulnerabilities associated with the proposed BC Services Card initiative, in what follows we suggest some ways of better securing the Services Card. Though we have raised a suite of prospective technical concerns in the previous section of this report, we believe that the use of NFC technology may provide the most persistent point of vulnerability in the BC scheme. The second most persistent point of attack is at the level of the client that is accessing online web-based government services.

Our concerns surrounding NFC stem largely from known failures of manufacturers to adequately secure the NFC stack. Moreover, the capability of presenting malicious tags to NFC readers has the potential of subsequently infecting clients attached to readers

with malicious software. We suggest that, prior to deploying NFC-based technologies, that readers and reader software is subjected to extensive penetration testing, which includes efforts to fuzz the devices (i.e. encourage the readers/tag clients to crash in ways that reveal repeatable methods of injecting malicious code over NDEF) as well as forensic driver and protocol analyses. Results should be public, as should the protocol stacks, reader firmware, and client software, to encourage third parties to conduct their own testing.[134] The BC government should establish, clearly, that 'bug bounties' or other rewards are available for reporting code-based vulnerabilities. Such bounties must be equivalent to, or in excess of, the value of the vulnerabilities on the grey/black markets for such exploits. Only by establishing this kind of financial incentive for reporting the bugs is the government likely to receive warning of exploitable code. These efforts should be tied to public consultations with security experts concerning the privacy protectiveness and security elements associated with the Services Cards. The results of these consultations – along with information about resolved security deficiencies with the Cards – should be made public.

Of course, the Services Card system is largely tied to a private vendor, SecureKey. In interviews with members of the OCIO's office we have been told that Veracode provided a third-party review of SecureKey's CBS, which was sanctioned by the federal Treasury Board Secretariat. At present, we do not have a copy of this audit, nor had the BC government's OCIO evaluated it when we prepared this report in November 2012.[135] To date, the BC OCIO is reliant on the audit having been done properly and that no major errors were found; independent or provincial government audits *have not* been conducted. Given the significant integration of SecureKey technologies with BC government business processes for core service delivery, it seems appropriate that the BC government conduct ongoing audits of the SecureKey systems - client software, server software, and their implementation of NFC technologies - in order to assure BC residents that the company's technologies are suitably secure and reliable.

While such audits are demonstrative of due diligence by government authorities in the areas of security and privacy, audits themselves do little to prevent the likelihood of an attack. Enhancing security in the context of the BC Services Card, as mentioned previously, should impose friction and resource costs that are in excess of the costs linked with defeating the systems. There is no indication that flexible measures have been taken by the BC government that would advance such a scenario; critically, there

[134] It is important that, as part of this, exceptions around copyright provisions are set out to enable third-parties to legally attack the system.

[135] Since the initial drafting of this report we have been informed that the OCIO has reviewed these documents in January 2013, as has the OIPC.

is no documentary evidence that indicates the province is prepared for either class-break or 'act of God' scenarios, with the former referring to instances where either the cards themselves or software/cryptographic functions are broken, and the latter where major services - such as electricity, cellular coverage, or other necessities for digital service delivery - are disrupted for a prolonged period of time.[136] Further, we have not seen documents that recognize that the interest in attacking the cards and associated systems will increase as the card is more widely integrated with government services. As more and more uses are found for the cards they will be more useful identity credentials and, as a result, be targeted by better and better resourced adversaries.

While expanding the horizon of NFC readers into mobile electronics remains at a 'conceptual' stage in the BC IM/IT framework, such a move could present serious ramifications for privacy and security. Specifically, Android codebases are demonstrably insecure and, as NFC integration spreads throughout mobile operating systems, there is a danger of NFC-called operations 'breaking free' of any sandboxes that operating system manufacturers develop. Moreover, with each operating system update codebases can potentially change, potentially mandating a further audit of protocol codes to ensure that new faults have not been inadvertently introduced. This is significant not just for the provision of government services, but also because mobile devices have the potential to turn into a 'gateway' into government services more generally. With increased data collaboration across government ministries, this could mean that an attacker could burrow across one Ministry's databases or, perhaps more likely, make calls to other databases to access the personally identifiable information of BC residents using the mobile device's credentials.

A core innovation of the proposed Services Card is the use of ICBC's facial recognition databank to ascertain whether individuals have already enrolled for BC's driving or health services. As noted previously, the overall accuracy of such biometric evaluations remains uncertain. While ICBC has stated that slightly over a quarter of all applicants are processed to secondary screening - because an image has met a 'potential duplicate image' threshold - the rate of false/fraudulent enrollments remains unclear. Consequently, the actual confidence that can be established for the facial recognition system cannot be confirmed; should there be a high false positive *and* false negative rate it would call into question the capability of ICBC's system to mediate the believed (though not proven) rates of medical insurance fraud in BC. As a result, an audit of the ICBC database should be performed in a live-scenario to ascertain the appropriateness of the biometric enrollment; this means that long-term manual evaluations of the

[136] We note that 'Act of God' scenarios are particularly important to plan for in BC, given that large portions of the province's population resides along, or near, the Cascadia subduction zone.

effectiveness of accurate biometric template creation should be undertaken. Should it be found that confidence in matching is poor – if individuals can reliably create multiple 'unique' templates and thus not be detected as a multiple applicant – then ICBC's biometric systems should be reevaluated on the basis of potentially being an infringement on individuals' privacy without significantly advancing government anti-fraud objectives.

Data management policy surrounding log transactions present a further area of consideration, insofar as logging activity can be used to correlate pseudonymous identifiers across divergent institutions (e.g. OCIO, SecureKey, partner government institution) and thus undermine the government's proposed privacy model. In the absence of a clearly articulated data management policy regarding storage and retention of logs, both OCIO and SecureKey should be subject to external review of their database architecture. The potential for such linkages also raises the prospect that future government legislation could reduce the policy-driven privacy guarantees that are presently associated with the Services Card infrastructure.

In terms of SSL/TLS, root and intermediary-based certificates are prone to critical vulnerabilities. Of course, the capacity for bad actors to use SSL/TLS as a meaningful attack vector remain unclear; it would demand operating as a man in the middle of the data flow and subsequently either sniffing or modifying data traffic. There are likely alternate methods that would be more efficient to exfiltrate data from the Services Card networking environment. However, self-signed certificates that are commonly installed across client/server architectures might mitigate the use of fraudulently issued CA certificates, and a forward-looking system should be established to take advantage of certificate pinning. Implementing forward secrecy ensures that secret cryptographic material is deleted after use, and certificate pinning would cause Internet systems to refuse to transmit data if client devices (e.g. mobile phones or PCs) were not served pre-defined (and approved) certificates. Alternately, an agile trust framework that validates the 'trustworthiness' of a CA or certificate based on trusted assertions of the CA's or certificates' validity might be implemented.[137] Further, a reliance on SSH authentication wherever possible may mediate threats associated with fraudulent certificates, though could leave open SSH eavesdropping attacks. Similarly, reliance on SAML - while appropriate for many single sign on situations - should be evaluated in light of attacks on the protocol, to ensure that the government's implementations avoid the core threats facing the protocol.

[137] M. Marlinspike. (2011). "SSL And The Future Of Authenticity," *Blackhat USA 2011*. Published August 18, 2011. Last accessed November 27, 2012. Available at: https://www.youtube.com/watch?v=Z7Wl2FW2TcA

Conclusion

In 2006 the federal Liberal Party Immigration Minister, Denis Coderre, said that "... we cannot bury our heads in the sand anymore . . . Something is going on worldwide and we have to have that debate"[138] about national identity cards. That debate did not, and still has not, genuinely transpired at the federal level. Similarly, the BC government is not engaging in this discussion, despite its pushing forward with a provincial ID card intended, prospectively, to operate as a base for a subsequent national integration effort. The province has not engaged in a genuine discussion with its citizenry to ascertain whether the government's proposals are supported by the electorate and, by implementing the e-Health and identity management system without significant public involvement, the government is establishing necessary 'fail conditions' that could preclude the initiative from being perceived as a democratically legitimate program.

Apart from the limits presented by a lack of public engagement, this report calls for a careful appreciation of the technical constraints associated with the proposed BC Services Card initiative. A failure to carefully consider the risks and vulnerabilities associated with the provincial - and potentially national - identity system could lead to increased costs and risks if the design suffers catastrophic collapse or if core facets of the design can be successfully - and reliably - made vulnerable to attackers. Core drivers for this system revolve around efficiency of service delivery and the reduction of government costs: it is imperative that, if an e-credential initiative is to be generally implemented, that the province ensures it can actually meet its stated objectives and project drivers.

Security systems are meant to impose costs that are high enough to preclude, or delay, attackers. The BC Services Card system - as the thin edge of a national identity system - may bloom into a broad identity schema and, as such, the incentive to establish fraudulent identities or otherwise disrupt the system will grow as the system expands. Moreover, BC cannot ignore that their proposed system may turn into the core of a national identity scheme: in light of this, BC officials must consider the range of actors who are interested in disrupting a Canadian identity system and establish friction that is sufficient to limit such attacks. To date, we have not seen provincial or federal officials publicly comment or address the effectiveness of the BC system in defraying highly interested attacks on a proto-national system: it is time, if we are not going to

[138] D. Coderre. (2006). "Day Proposes National ID Card," *Canadian Press*. Published February 17, 2006. Archive version available at: http://www.tcscanada.net/canada-immigration-news/news-out.php?ueid=23

debate imposing an identity system itself, to publicly discuss the desperate need to adequately, and functionally, secure BC's proto-pan-Canadian identity institution.

Appendix A - Acronyms

AAMVA	American Association of Motor Vehicle Administrators
BC	British Columbia
BCID	British Columbia Identity Card
CA	Certificate Authority
CBS	Credential Brokerage Service
CCMTA	Canadian Council of Motor Transport Authorities
CP	Credential Provider
CRA	Canada Revenue Agency
DDOS	Distributed Denial of Service
DMV	Department of Motor Vehicles
DNS	Domain Name System
ICBC	Insurance Corporation of British Columbia
EDL	Enhanced Drivers License
EHIC	European Health Insurance Card
e-EHIC	Electronic European Health Insurance Card
EMR	Electronic Medical Record
EHR	Electronic Health Record
EMV	Europay, Mastercard, and Visa
EU	European Union
FRT	Facial Recognition Technology
FIPPA	Freedom of Information and Protection of Privacy Act
HRDC	Human Resources and Development Canada
HTTPS	Hypertext Transfer Protocol Secure
ICAO	International Civil Aviation Organization
IDIM	Identity Information Management
IM/IT	Information Management/Information Technology
IPS	Identity Protection Services
ISO	International Organization for Standards
LSE	London School of EconomicsM
MBUN	Meaningless But Unique Number
MFFD	Ministry of Children and Family Development
MIME	Multipurpose Internet Mail Extensions
MITM	Man in the Middle
MoH	Ministry of Health
MSP	Medical Services Plan
NDEF	NFC Data Exchange Format
NFC	Near Field Communications
OCIO	Office of the Chief Information Officer

PAI	Persistent Anonymous Identifiers
PHN	Personal Health Number
POS	Point of Service
RFID	Radio Frequency Identification
RP	Relying Party
SAML	Security Assertion Markup Language
SE	Secure Element
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Level Security
TSM	Trusted Service Manager
URI	Uniform Resource Locator
UK	United Kingdom
US	United States
USB	Universal Serial Bus
WHTI	Western Hemisphere Travel Initiative

Legal Information

Electronic version first published at www.blockg.ca in Canada in 2013 by BlockG Privacy and Security Consulting.

This research is funded through the Office of the Privacy Commissioner of Canada's Contributions Program.

BlockG Privacy and Security Consulting logo designed by Karen Yen of Can Poeti Branding and Design.

Document version 1.6.

Information presented in this document is for research and educational purposes only. These materials do not constitute solicitation or provision of legal advice. BlockG Privacy and Security Consulting makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Nothing herein should be used as a substitute for the legal advice of competent counsel.