Government of Canada | Gouvernement du Canada
Veterans Ombudsman | Ombudsman des vétérans

Report of the Veterans Ombudsman
October 2012

Honouring and Connecting with Canada's Veterans: a National Veterans Identification Card

Canada

OFFICE OF THE VETERANS OMBUDSMAN
360 Albert Street, Suite 1560
Ottawa, Ontario K1R 7X7
Calls within Canada (Toll-free): 1-877-330-4343
Calls from outside Canada (Collect): 1-902-626-2919
Email: info@ombudsman-veterans.gc.ca

This publication is also available in electronic format at
www.ombudsman-veterans.gc.ca

V104-3/2012E-PDF
978-1-100-21306-4

Government of Canada / Gouvernement du Canada
Veterans Ombudsman / Ombudsman des vétérans

October 5, 2012

The Honourable Steven Blaney, P.C., M.P.
Minister of Veterans Affairs
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Minister:

I am pleased to submit to you the report *Honouring and Connecting with Canada's Veterans: a National Veterans Identification Card*.

It has always been my belief that an identification card would be of great benefit to Veterans and to Veterans Affairs Canada. The report covers issues such as the purposes of the card, card features and capabilities, as well as some notional cost and timeline information.

In addition, I am of the view that the time has come for former members of the Royal Canadian Mounted Police to be formally recognized as Veterans. RCMP members, side by side with their military counterparts, have historically protected Canadians at home and abroad while often being put in harm's way. Yet, they have never been formally recognized by the Government of Canada as Veterans.

I look forward to discussing the recommendations at your earliest convenience.

Yours sincerely,

Guy Parent
Veterans Ombudsman

Canada

TABLE OF CONTENTS

THE MANDATE OF THE VETERANS OMBUDSMAN

The Office of the Veterans Ombudsman, created by Order in Council,[1] works to ensure that Veterans, serving members of the Canadian Forces and the RCMP, and other clients of Veterans Affairs Canada, are treated respectfully in accordance with the *Veterans Bill of Rights,* and receive the services and benefits that they require in a fair, timely and efficient manner.

The Office addresses complaints, emerging and systemic issues related to programs and services provided or administered by the Department of Veterans Affairs, as well as systemic issues related to the Veterans Review and Appeal Board.

The Veterans Ombudsman is an independent and impartial officer who is committed to ensuring that Veterans and other clients of Veterans Affairs Canada are treated fairly. The Ombudsman measures fairness in terms of **adequacy** (Are the right programs and services in place to meet the needs?), **sufficiency** (Are the right programs and services sufficiently resourced?), and **accessibility** (Are eligibility criteria creating unfair barriers, and can the benefits and services provided by Veterans Affairs Canada be accessed quickly and easily?).

VETERANS BILL OF RIGHTS

In accordance with the *Veterans Bill of Rights,* Veterans and all other clients of Veterans Affairs have the right to:

- Be treated with respect, dignity, fairness and courtesy.
- Take part in discussions that involve them and their family.
- Have someone with them for support when they deal with Veterans Affairs.
- Receive clear, easy-to-understand information about programs and services, in English or French, as set out in the *Official Languages Act.*
- Have their privacy protected as set out in the *Privacy Act.*
- Receive benefits and services as set out in published service standards and to know their appeal rights.

You have the right to make a complaint and have the matter looked into if they feel that any of their rights have not been upheld.

[1] Order in Council P.C. 207-530, April 3, 2007.

REPORT SUMMARY

Veterans Affairs Canada has overall responsibility for Canada's nearly 750,000 Veterans, including the provision of health treatment and financial benefits to ill and injured Veterans and assistance with their transition to civilian life. The Veterans Ombudsman has long-standing concerns about the Department's ability to reach out to, and maintain contact with the larger group of Veterans, other than those who are already its clients.

The Veterans Ombudsman proposes the issuance of a *National Veterans Identification Card* as a means of facilitating the Department's efforts to establish contact and proactively communicate with Veterans. The requirement to renew the card on a periodic basis would enable Veterans Affairs Canada to maintain contact with Veterans and inform them of changes to programs and services. It would also facilitate the assessment of new service needs and planning for future resource allocations.

Meeting the requirements of an official government-issued identification document and employing modern technology[2], the *National Veterans Identification Card* could also be personalized to specify the bearer's eligibilities to benefits provided by the Department and other organizations and programs, such as the Canadian Forces Appreciation Program.

Of equal importance to the Veterans Ombudsman is the benefit that the card would have in facilitating the transition from membership in the Canadian Forces or the Royal Canadian Mounted Police (RCMP) to membership in the community of Veterans. The issuance of the *National Veterans Identification Card* to serving members of the Canadian Forces and the RCMP at the time of their release would complete their transition to civilian life in a formal and meaningful way by providing them with a tangible symbol of valued membership and recognition as Veterans.

The Veterans Ombudsman feels strongly about the need for a *National Veterans Identification Card:*

> *There is no official card issued by the Government of Canada that clearly identifies eligible former members as Veterans, either for commemorative purposes or for the purpose of providing benefits and services. I believe that a National Veterans Identification Card would fill that void and provide our Veterans with a tangible and nationally recognized means of identifying themselves as Veterans. It would be an additional way for the Government of Canada to thank them for their service and to recognize them not only for who they were but for who they are:* ***Veterans****!*

[2] The services of a consultant, E-CARD ID Products Ltd., were retained to report on the mechanics of card technology, identity issuance systems, and the potential uses of an identification card for Canada's Veterans. Analysis of the means and cost of implementing such an identification card is discussed in detail in the consultant's report entitled *Identity Cards and Veterans Affairs Canada* (refer to Annex).

The Veterans Ombudsman also proposes that the current definition of a *veteran* for commemorative purposes[3] be amended to include former members of the RCMP. RCMP members, side-by-side with their military counterparts, have historically protected Canadians at home and abroad, while often being put in harm's way. Yet, they have never been formally recognized by the Government of Canada as Veterans.

VETERANS OMBUDSMAN'S RECOMMENDATIONS

RECOMMENDATION 1 – That the Minister of Veterans Affairs, in consultation with the Minister of National Defence and the Minister of Public Safety, amend the current definition of a *veteran* for commemoration purposes to include former members of the RCMP.

RECOMMENDATION 2 – That Veterans Affairs Canada broadly publicize and make prominent on its Web site and in appropriate publications the definition of a *veteran* for commemoration purposes.

RECOMMENDATION 3 – That the Minister of Veterans Affairs, in consultation with the Minister of National Defence and the Minister of Public Safety, pursue, as a priority, the development of a *National Veterans Identification Card* that meets the standards for a government-issued identity document.

RECOMMENDATION 4 – That Veterans Affairs Canada, in consultation with the Canadian Forces and the RCMP, pursue a strategy for the issuance of a *National Veterans Identification Card* to Veterans and releasing members of the Canadian Forces and the RCMP.

[3] The current definition of a *veteran* for commemorative purposes includes all former members of the Canadian Forces who have completed basic training and have been honourably released, including those who served in the Reserve Force, special duty areas and on domestic duty.

THE ISSUE

By virtue of its enabling legislation, Veterans Affairs Canada has overall responsibility for Canada's nearly 750,000 Veterans, including the provision of health treatment and financial benefits to ill and injured Veterans and assistance with their transition to civilian life. But none of Canada's Veterans currently have a tangible and nationally recognized means of identifying themselves as Veterans, and thereby acknowledging their service and attesting to their entitlement to be considered for such benefits as may accrue from that status. As a result, these individuals and their family members may, at times, be challenged in demonstrating eligibility for those benefits and services and even in being formally recognized as Veterans by the nation in whose interest they served.

As Senator Roméo A. Dallaire said:

> *…being released from the forces and handing in your ID card and your uniform doesn't mean that the forces are out of you…what you need is a bridge to the next entity…to continue that loyalty you've committed to, particularly if you're a veteran…*[4]

Even more succinctly, Bruce Ferguson, National President of the Canadian Merchant Navy Veterans Association, called for "…an improved identification system so that, when merchant seamen apply for aid they will not be turned away as non-veterans." He went on to be more specific, calling for "…an ID card — with our pictures on it that says we are veterans."[5]

By the same token, while Veterans Affairs Canada is generally well engaged with its current Veteran clients, it is challenged to identify, reach out to, and maintain contact with the larger group of Veterans and their families who are not its clients at the present time, but who constitute its potential client population. This affects the Department's ability to forecast trends and evolving demand for services; inform proactively these potential clients of changing benefit regimes, programs and eligibility; and apportion necessary resources to deliver the requisite services.

The Veterans Ombudsman has raised his concerns about these issues on numerous occasions, encouraging the Department to bring about improvements to its communications and outreach efforts as important elements of its transformation agenda, and arguing that a

[4] House of Commons Standing Committee on Veterans Affairs, Number 029, 3rd Session, 40th Parliament, November 18, 2010, page 5, http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-E.PDF.

[5] Senate Standing Committee on National Security and Defence, Proceedings of the Subcommittee on Veterans Affairs, Issues No. 4, 2nd Session, 39th Parliament, April 16, 2008, page 20 and 21, http://www.parl.gc.ca/Content/SEN/Committee/392/vete/pdf/04issue.pdf.

sustained and proactive outreach campaign would very likely increase demand for the Department's programs and result in a larger-than-projected client base.[6]

In its report *Improving Services to Improve Quality of Life for Veterans and their Families,* the House of Commons Standing Committee on Veterans Affairs also took specific note of this issue:

> *Once they have left the CF [Canadian Forces] or the RCMP, veterans cannot be identified or located unless they themselves voluntarily request services from VAC [Veterans Affairs]. This limits VAC's ability to reach veterans who might at some point need certain services; for example, mental health problems may not show up for months or even years after an individual leaves the CF or the RCMP.*[7]

Indeed, establishing and maintaining contact with *all* Canadian Veterans, vis-à-vis a successful outreach program by Veterans Affairs Canada, has been a recurrent focus of concern for parliamentarians.[8]

In response, the Veterans Ombudsman, in testimony before the House of Commons Standing Committee on Veterans Affairs, called for the issuance of an identification card for all Veterans, clearly recognizing them as Veterans and "…providing the basis of a tracking system, whereby all Veterans can be reached, including Reservists."[9]

To this end, the Office of the Veterans Ombudsman engaged a consultant, E-CARD ID Products Ltd., to report on the mechanics of card technology, identity issuance systems, and the potential uses of an identification card for Canada's Veterans (refer to Annex).

---

[6] Office of the Veterans Ombudsman, *2010–2011 Annual Report, One Veteran: A Matter of Fairness*.

[7] House of Commons Standing Committee on Veterans Affairs Report: *Improving Services to Improve Quality of Life for Veterans and Their Families*, 1st Session, 41st Parliament, May 2012, page 56, http://www.parl.gc.ca/content/hoc/Committee/411/ACVA/Reports/RP5506979/acvarp05/acvarp05-e.pdf.

[8] House of Commons Standing Committee on Veterans Affairs, Number 029, 3rd Session, 40th Parliament, November 18, 2010, http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-e.pdf.

[9] House of Commons Standing Committee on Veterans Affairs Report: *Improving Services to Improve Quality of Life for Veterans and Their Families*, 1st Session, 41st Parliament, May 2012, page 20, http://www.parl.gc.ca/content/hoc/Committee/411/ACVA/Reports/RP5506979/acvarp05/acvarp05-e.pdf.

BACKGROUND

CANADA'S VETERANS

Any consideration of providing identification cards to Canada's Veterans must certainly begin with a common understanding of the term *veteran* for commemoration purposes, given that there is no all-inclusive definition of the term.[10]

In 2001, the then Minister of Veterans Affairs announced that henceforth all former members of the Canadian Forces, including those who served in the Reserve Force, special duty areas and on domestic duty, would be recognized as Veterans provided they had met their occupational classification training requirements and had been honourably released. The definition was adopted in recognition of "…the potential risk that all Canadian Forces members are exposed to when they swear the Oath of Allegiance and don a Canadian uniform."[11] The definition was revised in 2008, replacing the requirement for completion of occupational training to that of simply basic training, and, to this day, stands as the official Government of Canada definition of a *veteran* for commemoration purposes.[12]

The historical context is somewhat lost with the current definition but it is broadly accepted that those who served in the two World Wars and the Korean War are Veterans, including members of the Merchant Navy who were officially recognized as Veterans by the Government of Canada in 1992.

[10] While beyond the scope of this report, it bears mentioning that over the course of many years following conflicts from the First World War until the present day, eligibilities for programs and benefits have often been described in the applicable Acts or Regulations in terms of who was a Veteran. The end result is that there are numerous definitions of the term *veteran*, tied to benefit eligibilities. The tying of benefit eligibilities to service circumstances is an issue of concern to the Veterans Ombudsman who, under the *One Veteran* theme, has been calling for benefit eligibilities for new programs and services to be defined in terms of needs rather than service circumstances.

[11] Speaking notes for *the Honourable* Ronald J. Duhamel, Minister of Veterans Affairs, Appearance before the Standing Committee on National Defence and Veterans Affairs, March 29, 2001, http://www.veterans.gc.ca/eng/department/press/viewspeech/149

[12] This change was made after realizing that, for two reasons, the completion of occupational classification training was not the best criteria for defining the amount of service necessary for the right to call oneself a Veteran. The first reason pertained to the inequity that the requirement caused between occupations given widely varying lengths of occupational training. The second reason pertained to the fact that members who have completed basic training and are awaiting occupational training may be put in harm's way when deployed domestically for special duty operations. For these reasons, completion of basic training was felt to be a more appropriate requirement.

Of concern to the Veterans Ombudsman is the fact that the official Government of Canada definition of a *veteran* for commemoration purposes does not include former members of the RCMP.

RCMP military activities date back to the Northwest Rebellion, the Boer War, and the two World Wars. It is a little known fact that the RCMP was also sent to Siberia as a military force in 1918–1919. The RCMP has officially been recognized with battle honours, which are traditionally only awarded to military units. Its members who served during the Second World War were eligible for the Canadian Volunteer Service Medal, and for benefits as Veterans of that service. In recent history, the RCMP continues to serve side-by-side with Canadian Forces personnel in almost every conflict where Canada has committed support, including peacekeeping operations and high-risk patrols in Afghanistan. RCMP members are also eligible for the Canadian Peacekeeping Service Medal.[13]

The Veterans Ombudsman is of the view that the time has come for former members of the RCMP to be formally recognized as Veterans.

RECOMMENDATION 1 – That the Minister of Veterans Affairs, in consultation with the Minister of National Defence and the Minister of Public Safety, amend the current definition of a *veteran* for commemoration purposes to include former members of the RCMP.

RECOMMENDATION 2 – That Veterans Affairs Canada broadly publicize and make prominent on its Web site and in appropriate publications the definition of a *veteran* for commemoration purposes.

[13] In 1904, following the Second Boer War, King Edward VII honoured the RCMP (then called the North West Mounted Police (NWMP)) for its achievements with the Royal designation, thus becoming the Royal North West Mounted Police (RNWMP). In 1920, the RNWMP was changed to the RCMP. In 1921, following the achievements of the RCMP in the First World War (the RNWMP at that time), King George V awarded the Force the official status of a Dragoon Regiment and, in 1935, with the entitlement of displaying Battle honours on a guidon (colours are given to infantry regiments whereas guidons are provided to Mounted or Dragoon regiments)(Unique to any Police Force).The Battle honours recognized are: North West Canada 1885 (Rebellion); South Africa 1900–1902; The Great War: France and Flanders 1918; Siberia 1918–1919; the Second World War: Europe, 1939–1945 (as the 1st Canadian Provost Corps). Also, the RCMP was honoured on two occasions to relieve the Queen's Life Guards (Horse Guard) as a regiment of Dragoons, the first time in 1937 leading to the coronation of King George the VI, and more recently in 2012 for the Queen's Diamond Jubilee.

SIZE OF THE VETERAN POPULATION

It is useful to assess the size of the population of Veterans who would be the recipients of an identification card, and the population of still-serving Canadian Forces and RCMP members who represent future card recipients.

There are nearly 750,000 Canadian Forces and RCMP Veterans; 100,000 Canadian Forces members (Regular and Reserve Forces) and 23,000 members of the RCMP. Some 140,000 Veterans and serving members of the Canadian Forces and the RCMP, plus more than 78,000 survivors of deceased Veterans receive benefits and services from Veterans Affairs Canada.

CARDS ISSUED TO VETERANS AND SERVING MEMBERS

Before discussing a *National Veterans Identification Card*, it is important to note that currently, there is no official (i.e.: government-issued) document, such as a card, that identifies former members of the Canadian Forces and the RCMP as Veterans. In fact, some Veterans have no document whatsoever indicating that they served (in the military, etc.), while others have documents (cards) of varying utility, but in no case containing a declaration that the bearer is a Veteran.

Veterans who served during the Second World War and the Korean War may have some document attesting to their honourable release or demobilization following their service, but as far as can be determined, none were issued a government identification card identifying them as Veterans.

The following is a list and description of the various cards now in circulation:

Certificate of Service

All Canadian Forces members at the time of release are issued a Certificate of Service, which is a large-sized document with an official seal attesting to their years of service.

Record of Service Card (NDI 75)[14]

The NDI 75 card is issued upon release to Regular Force and Reserve Force members who have at least 10 years of service. Initially, the card was issued only to Regular Force members with a minimum of 25 years of service.

The card, which is non-renewable, bears the former member's service number, last used identification photograph, years of service, and rank on release. It does not contain the date of birth or other identification information (height, weight, hair and eye colour, etc.). It bears a serial number and a specific statement in bold letters that it is *NOT* an identification card. Nowhere on the card is there any mention that the bearer is a Veteran.

[14] Note: 'NDI' stands for National Defence Identification

The NDI 75 card is simply what its title says it is: a record of service, showing the length of service, and is useful for proof of previous military employment.

RCMP Retired Member Card

Former members of the RCMP are issued a non-renewable card which contains a photograph, date of birth, and other identification information (height, weight, hair and eye colour). It also indicates the former member's rank and retirement date, and contains a statement authorizing the member to wear his or her uniform. It lacks a card number and does not indicate that the bearer is a Veteran.

Veterans Affairs Canada Health Identification Card

Veterans Affairs Canada issues a Health Identification card to clients receiving treatment benefits from the Department. The card bears the client's name and client number, plus a coded area to indicate the medical services and benefits to which the bearer is entitled. The card lacks a photograph and other identification information, and except for the mention of Veterans Affairs Canada on the card, nowhere does it indicate that the bearer is a Veteran.

Canadian Forces Appreciation Program Card

Current and former members of the Canadian Forces, current civilian employees of the Department of National Defence, immediate family members of these groups, and other eligible individuals can apply for the Canadian Forces Appreciation Program card.[15]

The card is non-renewable and has no identification information or photograph. It has a unique card number and describes the bearer's status as a Canadian Forces member, former member, civilian or family member. The reverse of the card has a prominent statement that it is *NOT* an identification card, and must be used with "valid photo identification." Nowhere does the card indicate that the bearer is a Veteran.

The card is used with valid photo identification to confirm eligibility for the benefits (discounts) of the Canadian Forces Appreciation Program. The Program is a non-public funds initiative of the Canadian Forces Personnel and Family Support Services, an organization under the Chief of Military Personnel. Information collected through the application process for the card and by the number assigned on the card is used by the Program to track membership and communicate details of new benefits and Program partners.

In summary, there is no official card issued by the Government of Canada that clearly identifies eligible former members as Veterans, either for commemorative purposes, or for the purpose of providing benefits and services.

[15] Note: In this case 'other individuals' includes employees and former employees of the Communications Security Establishment, employees of the Non-Public Funds, employees of Military Family Resource Centres, and foreign military personnel serving on exchange with the Canadian Forces.

DISCUSSION

In order to properly discharge its responsibilities, Veterans Affairs Canada clearly has a need to establish and maintain contact with Canada's Veterans. Once a member leaves the Canadian Forces or the RCMP, the obligation of those organizations to maintain contact or communicate with the former member ceases. Issues of health care needs accruing from service and assistance in the transition to civilian life for former members and their families become the purview of Veterans Affairs Canada, under one or more Acts of Parliament. This was also the case for those who served in the military during the two World Wars and the Korean War, including former members of the Merchant Navy. Once released, they ceased to be the responsibility of their former service, and their needs became the responsibility of Veterans Affairs Canada.

It is at the very core of the nature of military and police institutions that they are highly cohesive and paternalistic organizations where care and concern for serving members balances the loyalty, dedication and risk-taking that is routinely demanded of them. Clear identification of membership in these organizations during service, vis-à-vis a uniform and official identity card, is not only a requirement for security and command structure, it is an essential reassurance of having an *identity* as a valued member of a respected team, and of not being alone.

But when the uniform is taken off and the identification card is turned in upon retirement or release, the reassurance, and often even the individual's identity and sense of self-worth is likewise affected, to be replaced by the challenges of entering a civilian world without the bond of membership while perhaps suffering the effects of years of service. In these circumstances, what is needed, as Senator Roméo A. Dallaire so eloquently put it, is "…a bridge to the next entity…particularly if you're a veteran…"[16] This is the operating environment of Veterans Affairs Canada with its mandate for "…the care, treatment or re-establishment in civil society…" of former members: Veterans.

It is also the operating environment of the Canadian Forces Chief of Defence Staff with the mandate, conferred in the *National Defence Act*, to use non-public property (including funds) "…for the benefit of all or any officers and non-commissioned members or former officers and non-commissioned members, or their dependants."[17] The aforementioned Canadian Forces Appreciation Program seeks to establish and maintain contact with Canadian Forces members, former members (Veterans) and their families in order to make available a continually changing array of discount offers from partner businesses and organizations. Although the card issued

[16] House of Commons Standing Committee on Veterans Affairs, Number 029, 3rd Session, 40th Parliament, November 18, 2010, page 5, http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-E.PDF.

[17] *National Defence Act*, R.S.C., 1985, c. N-5 (Section 2) http://laws-lois.justice.gc.ca/eng/acts/N-5/page-1.html.

through the Program does not include a photograph, identifying information, or the word veteran, it has conferred a sense of re-engagement and renewed belonging upon some recipient Veterans who may have felt somewhat left behind over the years. This is not insignificant.

To a degree, this is the commemoration and recognition function that a *National Veterans Identification Card* would fulfil; being a tangible and substantive part of that 'bridge', as Senator Roméo A. Dallaire described it, from membership in various uniformed services to membership in the broader community of Veterans, recognized and valued ('*appreciated')* by the nation for what they have done on behalf of Canada and its citizens. It is also in part, the function that Veterans Affairs is challenged to accomplish, that of establishing and maintaining contact with Veterans who are not its clients for the purposes of informing them and forecasting needs.

The importance for Veterans Affairs Canada to establish and maintain contact with *all* Veterans, clients or otherwise, has been often referred to in testimony before both Senate and House of Commons Committees as well as in a report of the House of Commons Standing Committee on Veterans Affairs:

> *The need for the department [Veterans Affairs Canada] to reach out to all war service veterans requiring services, not just to those who are already clients of its programs was highlighted…during testimony heard by the Committee.*[18]

Indeed, Veterans Affairs Canada received a similar message directly from Veterans who participated in focus groups as part of a 2010 New Veterans Charter Evaluation equating, in part "recognizing Veterans" with "being entirely proactive…checking in on them before they come to you [Veterans Affairs Canada]…following-up with them to see how they are doing."[19] This "following-up", which has also been referred to as monitoring, is considered particularly important for Veterans with the potential for deferred onset of operational stress injuries.[20] In fact, among focus group participants, there was consensus that "…some Veterans may be depressed and stressed and therefore less likely to contact VAC [Veterans Affairs Canada] themselves…the department should take the initiative."[21]

---

[18] House of Commons Standing Committee on Veterans Affairs Report: *Resetting the Bar for Veterans Health Care: The Veterans Independence Program and The Veterans Health Care Review,* 2nd Session, 39th Parliament, May 2008, page 9, http://www.parl.gc.ca/content/hoc/Committee/392/ACVA/Reports/RP3517720/acvarp01/acvarp01-e.pdf.

[19] Veterans Affairs Canada, Report: *New Veterans Charter Evaluation – Phase II, Annex G,* August 2010, pages 31 and 56, http://www.veterans.gc.ca/pdf/deptReports/2010-08-nvce-p2.pdf.

[20] House of Commons Standing Committee on Veterans Affairs Report: *Improving Services to Improve Quality of Life for Veterans and Their Families*, 1st Session, 41st Parliament, May 2012, page 27 http://www.parl.gc.ca/content/hoc/Committee/411/ACVA/Reports/RP5506979/acvarp05/acvarp05-e.pdf.

[21] Veterans Affairs Canada, Report: *New Veterans Charter Evaluation – Phase II, Annex G,* August 2010, page 39, internet, http://www.veterans.gc.ca/pdf/deptReports/2010-08-nvce-p2.pdf.

A specific group highlighted as facing particular challenges in terms of support and access to care after release is the Reserve Force. Reservists often return home to locations far removed from the Base of the unit in which they served on deployment and therefore may have more limited access to the network of support available to their counterparts in the Regular Force.[22] Senator Roméo A. Dallaire discusses the challenges faced by Reservists in the following terms:

> *For the reservist who ends up in all kinds of villages across the country and decides to quit, there is very little follow-up on how they're being taken care of. That's why you're ending up with more soldiers in front of the courts. You'll see a lot of reservists there because they've been nearly abandoned.*[23]

He also predicts that the impact of the scaling-down of the Afghan mission will see an increase in operational stress injuries among Veterans and their families who had so far been able to sustain the stress of multiple tours.[24] This raises the issue of anticipating future needs and the number of Veterans who may require services and where, which is important information for Veterans Affairs Canada to have when making decisions about resource allocation. This is an issue that straddles the mandates and responsibilities of both Veterans Affairs Canada and the Canadian Forces/Department of National Defence during the transition from serving member to Veteran.[25]

In this regard, it has been recommended that Veterans Affairs Canada work with the Department of National Defence towards the goal of standardizing their records systems and using the military members' service numbers instead of assigning a separate Veterans Affairs Canada client number, which would facilitate the transfer of files upon release and foster a more seamless transition.[26] This could be extended to RCMP Veterans as well.

---

[22] House of Commons Standing Committee on Veterans Affairs Report: *Resetting the Bar for Veterans Health Care: The Veterans Independence Program and The Veterans Health Care Review,* 2nd Session, 39th Parliament, May 2008, page 17, http://www.parl.gc.ca/content/hoc/Committee/392/ACVA/Reports/RP3517720/acvarp01/acvarp01-e.pdf.

[23] House of Commons Standing Committee on Veterans Affairs, Number 029, 3rd Session, 40th Parliament, page 3 http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-E.PDF.

[24] House of Commons Standing Committee on Veterans Affairs, 3rd Session, 40th Parliament, page 2, http://www.parl.gc.ca/content/hoc/Committee/403/ACVA/Evidence/EV4795104/ACVAEV29-E.PDF.

[25] House of Commons Standing Committee on Veterans Affairs Report: *Resetting the Bar for Veterans Health Care: The Veterans Independence Program and The Veterans Health Care Review,* 2nd Session, 39th Parliament, May 2008, page 11, http://www.parl.gc.ca/content/hoc/Committee/392/ACVA/Reports/RP3517720/acvarp01/acvarp01-e.pdf

[26] House of Commons Standing Committee on Veterans Affairs Report: *Resetting the Bar for Veterans Health Care: The Veterans Independence Program and The Veterans Health Care Review,* 2nd Session, 39th Parliament, May 2008, page 16, http://www.parl.gc.ca/content/hoc/Committee/392/ACVA/Reports/RP3517720/acvarp01/acvarp01-e.pdf.

Issuing a *National Veterans Identification Card* to releasing members would complete the transition in a tangible and meaningful way, by formally acknowledging their Veteran status and providing contact information for assistance. The card would be a record of service and also comply with the requirements of a government-issued identification document.

By making use of available technologies, as described in the report *Identity Cards and Veterans Affairs Canada*, the card could also be personalized to specify individual entitlements and eligibilities for various benefits and services provided by Veterans Affairs Canada, as well as discounts and other offers from industry partners, such as through the Canadian Forces Appreciation Program. This multiple functionality would eliminate the need for Veterans to carry more than one card, something they have clearly expressed no desire to do.[27]

The requirement to renew the card and update the photograph on a periodic basis, possibly by distributed means from local sites, would enable Veterans Affairs Canada to maintain contact with Veterans and inform them of changes to programs and services. It would also permit the assessment of new service needs, and planning for future resource allocations.

Analysis of the means and cost of implementing such an identification card is discussed in detail in the consultant's report entitled *Identity Cards and Veterans Affairs Canada* (refer to the Annex). The consultant, E-CARD ID Products Ltd., projects the cost of issuing a (nominal) one million cards with chip technology[28] via a centralized issuance system as being $5.20 per card, or $5.2 million overall, plus the costs of distributed enrolment (i.e., applicants would attend one of a number of 'sites' across the country to be photographed and enrolled) at $1.5 million. These figures are very generous and assume a very aggressive enrolment strategy that would occur within a single calendar year and encompass *all* current Veterans (there are nearly 750,000 Veterans, which is well below the one million cards used as a costing assumption).

In fact, as the experience of the Canadian Forces Appreciation Program card issuance has shown, locating current Veterans, particularly former Canadian Forces Reservists and many former Regular Force members not in receipt of disability benefits, is no easy task and will take time, measured in *years*. To reach the existing Veteran population, contact will need to be made via several avenues, including mailings, announcement of the program in various media such as Veteran organizations' magazines and publications, and through the direct assistance of some Veteran organizations. Issuing the card to serving members at the time of their release would eliminate the need to locate them at a future time and would halt the annual increase in the number of Veterans without a card (about 6,000 releases and retirements per year).

Veteran organizations, distributed as they are across the country, may also afford an avenue of facilitated and economical enrolment using volunteers and local facilities. Well beyond the

[27] House of Commons Standing Committee on Veterans Affairs Report: *Improving Services to Improve Quality of Life for Veterans and Their Families,* 1st Session, 41st Parliament, May 2012, page 20, http://www.parl.gc.ca/content/hoc/Committee/411/ACVA/Reports/RP5506979/acvarp05/acvarp05-e.pdf.

[28] Note: Use of cards with chip technology (at a $0.70/card premium) extends the photograph's validity period versus cards with simply a photograph and magnetic stripe, which reduces renewal frequency and overall costs.

scope of this report, these possibilities need to be considered in the course of developing an implementation plan, but suffice to say that once as many existing Veterans as possible have been offered or issued cards, the steady state cost of issuance will likely be in the order of less than $300,000 annually.

Thus, a *National Veterans Identification Card* issued to Veterans could viably replace the four cards described previously: the Canadian Forces Record of Service card (NDI 75), the RCMP Retired Member's card, the Veterans Affairs Canada Health Identification card and the Canadian Forces Appreciation card. It would also provide a card to other Veterans, such as former Merchant Navy members.

The quality and utility of such a card would reinforce the sense of value that the Government ascribes to *service*. This would meet the commemorative needs of Veterans to be *identified* and *recognized*, forging a link among the various groups of former members to a common status, that of being Veterans. Indeed, as noted in the report *Identity Cards and Veterans Affairs Canada*, this is "…what an identification card really does – binds a diverse group of people to a common brand or entity."[29]

> **RECOMMENDATION 3** – That the Minister of Veterans Affairs, in consultation with the Minister of National Defence and the Minister of Public Safety, pursue, as a priority, the development of a *National Veterans Identification Card* that meets the standards for a government-issued identity document.

> **RECOMMENDATION 4** – That Veterans Affairs Canada, in consultation with the Canadian Forces and the RCMP, pursue a strategy for the issuance of a *National Veterans Identification Card* to Veterans and releasing members of the Canadian Forces and the RCMP.

[29] Annex: E-Card ID Products Ltd., *Identity Cards and Veterans Affairs Canada,* 2012, page 21.

REPORT HIGHLIGHTS: IDENTITY CARDS AND VETERANS AFFAIRS CANADA

The Office of the Veterans Ombudsman engaged a consultant, E-CARD ID Products Ltd., to report on the mechanics of card technology, identity issuance systems, and the potential uses of an identification card for Canada's Veterans. The following are highlights from the report.

- It is important to determine at the outset what the purpose(s) of the identification card is/are to be.
- From a security and privacy standpoint, adhere to federal and provincial regulations and policies, and only capture and store information that is actually going to be used.
- Identity documents should contain a variety of security features, both electronic and physical; no single method of authentication should be relied upon 100 percent of the time.
- Although advanced electronic, non-card means of identification are rapidly evolving, extensive and expensive infrastructure is necessary to support them, whereas the traditional identification card, even with chip technology, is relatively inexpensive.
- Magnetic stripe cards are less secure than chip technology cards which can incorporate authentication features to extend the valid period of the card photo.
- Cards can be issued centrally or from distributed locations; distributed issuance is faster and avoids problems with mail or courier delivery but costs significantly (37%) more than centralized issuance, which offers better security.
- Renewal of cards can be done centrally or via distributed issuance.
- The report provides some sense of costs and timelines for the issuance of (notionally) one million 'smart' cards (i.e., with chip technology) through a centralized issuance program and assuming all data on recipients is available.
- Cost/benefit analysis of identity card use is very difficult; it is often not possible to put a monetary value on what an identification card really does – bind a diverse group of people to a common brand or entity.

CONCLUSION AND RECOMMENDATIONS

Veterans Affairs Canada has overall responsibility for Canada's nearly 750,000 Veterans, including the provision of health treatment and financial benefits to ill and injured Veterans and assistance with their transition to civilian life.

While the Department is generally well engaged with its approximately 140,000 Veteran and still-serving clients, it is challenged to identify, establish and maintain contact with the larger group of Veterans and their families who are not its clients at the present time, but who constitute its potential client population. The ability to establish and maintain contact with Veterans has recurrently been identified by parliamentarians, the Veterans Ombudsman and Veterans alike as critical to effective intervention and care.

In addition, Canada's Veterans currently have no tangible and nationally recognized means of identifying themselves as Veterans.

The Veterans Ombudsman has proposed the issuance of a *National Veterans Identification Card* to facilitate contact with Veterans by the Department and provide former members with formal recognition of their service and identification as Veterans.

A National Veterans Identification Card could replace several cards currently issued to former service members by the Canadian Forces, the RCMP and Veterans Affairs Canada, none of which identifies bearers as Veterans. Meeting the requirements of a government-issued identification document and employing modern technology, the *National Veterans Identification Card* could also be personalized to specify the bearer's eligibilities to services and benefits, such as those provided by Veterans Affairs Canada and the Canadian Forces Appreciation Program.

Issuing the *National Veterans Identification Card* to all Veterans will take time and effort as there is no simple way of reaching out to many of them. Issuing cards to serving members at the time of their release would eliminate the need to locate them at a future time for that purpose, and halt the annual increase in the number of Veterans without a card (there are about 6,000 releases and retirements per year). In addition, the issuance of the card to releasing members would complete their transition to civilian society in a formal and meaningful way by providing them with a tangible symbol of valued membership and recognition as Veterans.

Finally, the Veterans Ombudsman also proposes that the current definition of a *veteran* for commemoration purposes be amended to include former members of the RCMP. RCMP members, side-by-side with their military counterparts, have historically protected Canadians at

home and abroad, while often being put in harm's way. Yet, they have never been formally recognized by the Government of Canada as Veterans.

The Veterans Ombudsman makes the following four recommendations:

RECOMMENDATION 1 – That the Minister of Veterans Affairs, in consultation with the Minister of National Defence and the Minister of Public Safety, amend the current definition of a *veteran* for commemoration purposes to include former members of the RCMP.

RECOMMENDATION 2 – That Veterans Affairs Canada broadly publicize and make prominent on its Web site and in appropriate publications the definition of a *veteran* for commemorative purposes.

RECOMMENDATION 3 – That the Minister of Veterans Affairs, in consultation with the Minister of National Defence and the Minister of Public Safety, pursue, as a priority, the development of a *National Veterans Identification Card* that meets the standards for a government-issued identity document.

RECOMMENDATION 4 – That Veterans Affairs Canada, in consultation with the Canadian Forces and the RCMP, pursue a strategy for the issuance of a *National Veterans Identification Card* to Veterans and releasing members of the Canadian Forces and the RCMP.

ANNEX

IDENTITY CARDS AND VETERANS AFFAIRS CANADA

A report on card technology, identity issuance systems, and the potential uses of ID cards for Canada's Veterans.

KYLE FAIRFIELD, BA, BED, CPP
E-CARD ID PRODUCTS LTD.

VERSION 1.10

Table of Contents

What is an Identity (ID) Card?

A card can be considered an ID card if it is able to correctly establish a person's identity to the degree of certainty required within the framework that it is designed to operate. This overall framework is sometimes called the card "ecosystem".

There is no published national standard in Canada for an ID card. Each Federal, Provincial and Municipal Government ministry usually has its own standards (ie. Transport Canada has a variety of designs for Inspectors, Air Marshall, Civilian Staff, CATSA Restricted Area cards, etc.) which are designed to meet the requirements of its ecosystem. Some of the cards are visual only (ie. operates as a flash pass for a visual check only) while others have embedded electronics for automated authentication.

The most important question to ask, prior to choosing any specific type of card technology or printing methodology, is "how will the card be used?" From this statement of use or purpose, the appropriate type of technology can be chosen and applied.

If the card is going to be used for visual verification only, we recommend incorporating the following variable elements.

- Photograph
- First and Last Name
- Card Number
- Issuing Authority
- Issue Date
- Expiry Date

If the card is going to authenticated electronically, then there really is no limitation or requirement for printing anything on the card. In the case of certain law enforcement agencies, their security building passes often are completely blank except for a small 3cm square photograph of the card holder. If these passes are found by someone other than the cardholder, there is doubt as to which building or doors the card will operate.

Card Types and their Potential Applications

Card Composition

Standard Plastic Cards

Plastic Cards are usually made from 100% PVC, but can be combined with PET material in order to increase the longevity of the card. PVC (Poly Vinyl Chloride) becomes brittle over time and is prone to breaking after being exposed to the elements. In order to increase the card lifespan, other components such as PET (Polyester) need to be added to the card composition. Cards with a combination of materials are called Composite Cards.

Composite cards

Composite Cards may have 40% PET and 60% PVC and may yield a 3-5 year life in good environmental conditions. PVC and Composite cards are personalized with card printers using a dye-sublimation process. An additional layer of laminate can be applied to the card during this personalization process to prevent damage to the printed area, and increase the card life.

Polycarbonate (PC)

Polycarbonate Cards (PC) are widely used in Drivers License programs. PC cards can be laser engraved for a much longer lasting image, and the cards themselves are virtually indestructible due to the materials used. PC cards can have a lifespan of up to 10 years.

In addition to the type of materials used (see above), additional technology can be placed on or inside the card body. With MR (machine readable) elements, the possibility of human error in the data collection process is eliminated.

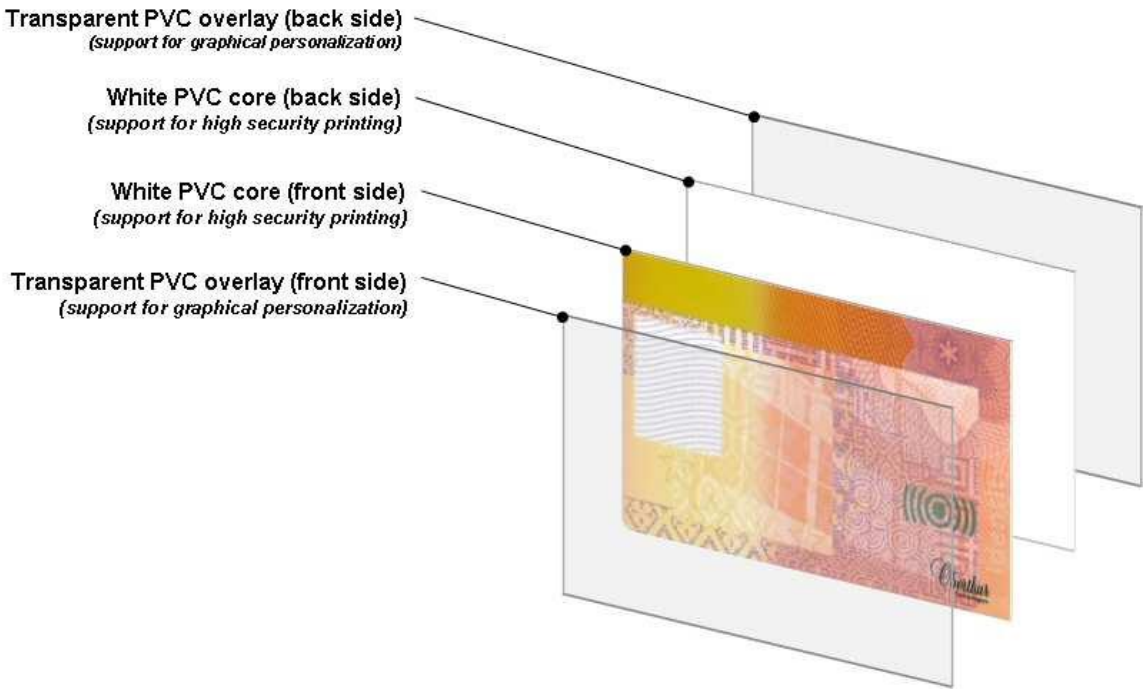

Fig 1. Multiple layers on a PVC card, before personalization

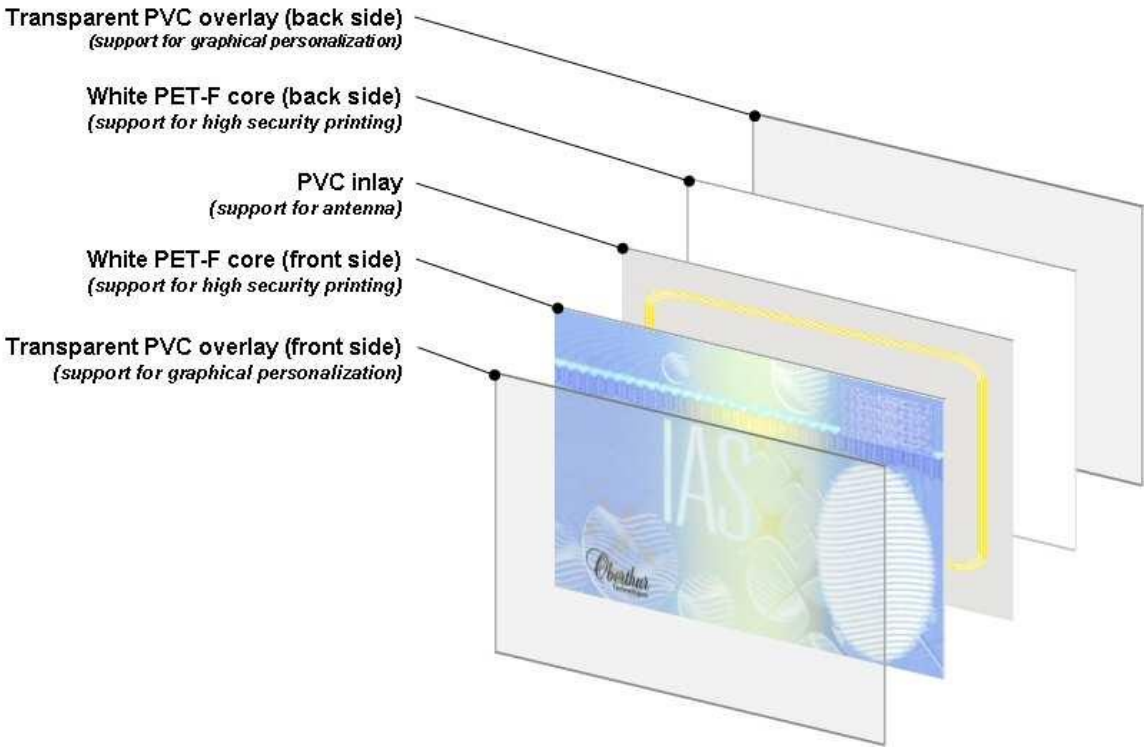

Fig 2. Multiple layered PET Card composition, before personalization

Card Technology

Barcode

A bar code (also barcode) is an optical machine-readable representation of data. Originally, bar codes represented data in the widths (lines) and the spacing of parallel lines and may be referred to as linear or 1D (1 dimensional) barcodes or symbologies. But they also come in patterns of squares, dots, hexagons and other geometric patterns within images termed 2D (2 dimensional) matrix codes or symbologies. In spite of there being no bars, 2D systems are generally referred to as barcodes as well.

Barcodes can only store limited amounts of information (for example, a 14 digit number) and cannot be modified once printed or they will not work. They are generally used as product identifiers in retail stores, and are commonly used on ID cards. The most common application is Time and Attendance, and Library check-out systems.

Barcodes offer little to no security, and can be copied without difficulty.

Embossing

Embossing refers to the raised letters or numbers on the card surface. On a financial card, there are two sizes of type, one for the card numbers and one for the name. On the back of the card, another number (usually 3 or 4 digits) is placed on the card by the embossing machine, however the letters are not raised. That process is called “indenting”.

Embossed cards are easily duplicated, offer no security, and are today are only used where carbon-copy forms are required.

Magnetic Stripe

A magnetic stripe card is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called a magstripe, is read by physical contact and swiping past a reading head. Magnetic stripe cards are commonly used in credit cards (in the USA), identity cards, and transportation tickets.

A number of International Organization for Standardization standards, ISO 7810, ISO 7811, ISO 7812, ISO 7813, and ISO 4909, define the physical properties of the card, including size, flexibility, location of the magstripe, and magnetic characteristics. They also provide the standards for financial cards, including the allocation of card number ranges to different card issuing institutions.

Magstripes come in two main varieties: high-coercivity (HiCo) at 4000 Oe and

low-coercivity (LoCo) at 300 Oe. HiCo mag stripes are also commonly available at 2750 Oe. High-coercivity magstripes are harder to erase, and therefore are appropriate for cards that are frequently used or that need to have a long life. Low-coercivity magstripes require a lower amount of magnetic energy to record, and hence the card writers are much cheaper than machines which are capable of recording high-coercivity magstripes. A card reader can read either type of magstripe, and a high-coercivity card writer may write both high and low-coercivity cards (most have two settings, but writing a LoCo card in HiCo may sometimes work), while a low-coercivity card writer may write only low-coercivity cards.

High coercivity stripes are resistant to damage from most magnets likely to be owned by consumers. Low coercivity stripes are easily damaged by even a brief contact with a magnetic purse strap or fastener.

A unique number is encoded on the mag stripe which allows for machine reading (as opposed to human reading, with the errors inherent in that process). Mag stripes offer little security from forgery as they can be read and replicated with simple equipment. However, within an ecosystem that requires PIN or additional information, the mag stripe can be a very cost effective technology to identify a cardholder and authorize their transactions.

Smart Card

This is a generic term that indicates that the card has smarts, or a "brain" onboard. It is also known as an IC, or Integrated Circuit, card. Smart Cards are very secure as they allow for encryption of the transaction process, and mutual authentication with its ecosystem (ie. both the card and the ecosystem prove to each other that they were made for each other.)

The two main types of IC cards are Memory and Processor.

- Memory cards simply store data, and offer little protection against forgery.
- Processor cards have secure microcontrollers onboard that authenticate the transaction and can conduct multiple read/write actions, as well as execute logic and calculations.

There are two types of smart card "interfaces": Contact and Contactless.

- Contact smart cards have a visible chip on the card which comes in contact with a reader.
- Contactless cards have the chip embedded under the surface and an antennae coil inside the layers of plastic. The chip and antennae are not visible on a Contactless card. Contactless smart cards are sometimes

referred to as RFID (Radio Frequency Identification) cards.

It is also possible to have cards with both technologies built into the card:

- Hybrid - two chips on the card, one supporting contact and one supporting contactless interface.

- Dual Interface - a single chip on the card with the contact and contactless interface connected.

Card specifications are numerous and very helpful information is available on the technical details on websites such as Wikipedia. The following ISO specifications are generally associated with the use of cards:

- ISO 7610 - card size and dimensions
- ISO 7611 - embossing and mag encoding
- ISO 7618 - embedded chip and contact surfaces
- ISO 14443 and 15693 - standards for contactless transmission
- ISO 18092 - NFC (Near Field Communication) standards

While Smart Cards can solve a lot of the authentication issues surrounding identity, their use depends on a system of distributed terminals that know how to process the data that the smart card presents. The purchase and personalization of the smart card becomes a fraction of the cost of the entire card ecosystem.

Card Security

Security features on a credential can be divided into two main areas: physical and electronic.

Physical Security Features

Each card should have multiple features built into the construction that prevent or deter forgery. There are four major levels of physical security features:

- Level 1 – Easily recognized features, viewable by the naked eye. An example of this would be the photograph, hologram, or guilloche design.
- Level 2 – Use of a verification tool is required, such as a UV lamp or loupe.
- Level 3 – Features are detected by forensics inspection, usually results in the destruction of the document.
- Level 4 – A security feature known only to the manufacturer and no one else.

Examples of Physical Card Security features are:

- Embedded Hologram – Difficult to copy, an embedded hologram, applied below the surface of a PVC card, allows for direct-to-card printing on the entire surface of the card - including the hologram.
- Holographic Overlaminates - These laminates are applied directly to the surface of printed cards. In addition to providing the anti-counterfeiting benefits of holograms, they also provide added protection to the printed surface of the PVC card. They protect against reader abrasion and normal wear and tear. Holographic designs can also be printed on the Re-transfer film.
- Iridescent Inks and Custom Foil Stamping - The diffractive properties of foil and iridescent inks afford the same anti-counterfeiting properties as holograms. They cannot accurately be reproduced. These are available in a variety of colors and patterns and can be used to custom print any image on PVC cards, Teslin, laminates and paper. They can be applied in the shape of your logo or any other image unique to your organization.
- Thermochromatic Inks - The pre-printed inks are temperature sensitive, and change colour when exposed to heat source, such as a fingerprint.

- Rainbow – Technique with two or four colours of inks printed simultaneously on the whole card surface to create a gentle controlled merging of the colours, similar to the effect seen in a rainbow.

- Micro-text Printing – Extra small print. Most copy devices are not able to duplicate the tight resolution of micro-text printing without obvious flaws. Often, a deliberate error is placed in the text for easy detection using a magnifying glass.

- Guilloche – Pattern of very fine interwoven lines which form a unique image that can only be re-created with the equipment software and parameters used in creating the original design.

- UV and Infrared Printing - A UV or infrared printed design can only be viewed with special equipment. By incorporating a custom design printed in this fashion, fraudulent badge reproduction can be eliminated.

- Ghost image – Secondary photo of the card holder formed by laser perforation, visible by transmitted light.

- Tactile engraving – text that is laser engraved on a card surface to create a tactile effect.

- Anti-scan pattern – Delimited area with a special background combing fine lines and merging colours which makes it impossible to photocopy.

- Color coding - using different badge colors to depict varying levels of access is an easy and efficient method to increase security. Colors are an obvious visual identifier that can be quickly confirmed from a distance.

- Sequential numbering - Including a sequential number on the badge that can be cross-referenced with information in a database. This offers an additional check that the person carrying the badge is indeed authorized to do so.

- Watermarking - An anti-counterfeiting process that embeds an image (similar to the way money is watermarked) into plastic cards. This can be viewed by holding the card up to any light source.

- Bar Code Security Mask - Security cover to mask bar code.

Fig 3. Examples of Card Security Features

With the advent of multiple means of electronic authentication using smart cards and networks, very often the use of visual forgery detection devices is overlooked. However, in the event that the electronic authentication of the credential document cannot be completed (ie. chip is damaged etc.), internationally accepted standards require additional features within the document that allow for authentication. ICAO (International Civil Aviation Authority), based in Montreal, QC, specifies that any issued Identity Credential is still valid, EVEN IF the chip does not work. The chip on the card is just ONE of the many security features. As criminal elements will always focus on the weakest link do conduct fraudulent activity, it is critical to include physical credential features that significantly reduce the possibility of counterfeiting.

Electronic Security Features

In most systems today, information is stored on a network in order to enable access from multiple points. Storing the data in one place, and ensuring secure access from multiple points, allows for data integrity and non-duplication of resources or information.

In the identity environment, the card is usually used an enabler to access, not a storage facility.

Both a magnetic stripe card and a smart card have a unique identifier (UI) stored on the card. During any transaction, the UI is communicated to the system for authentication, and upon approval the information is shared with the reader/device that is requesting the information.

The main difference between a magnetic stripe and the chip is SECURITY.

For less than $200, a magnetic stripe card can be read and duplicated. There is no authentication of the card itself with the system. The system only knows that a valid number has been presented, but no verification of the card itself is done - the system cannot tell the difference between an original or a duplicated card.

With Smart Cards, card authentication is at the core of all transactions - the system can have a high degree of assurance that no duplication or alteration of the card has been attempted. The level of assurance binds the card to the transaction to the degree of certainty required, and the system can share the information with the reader/device knowing that the card itself is authorized to share/receive that information.

This process is called Mutual Authentication (MA).

Card Applications

Identity Credentials can be used in a variety of applications.

Identity
Establishing the identity of the card holder is the key function of the card. An accurate reliable document establishes trust between the card holder and the agency using the card.

Financial
All the major banks and processing merchants in Canada have migrated to EMV, based on contact and contactless smartcards. The ability of the Smart Card to resist tampering and duplication is a major factor in the decrease in fraud.

Physical Security
Many companies have already transitioned to contactless smart cards as a means of increasing the security of buildings. Smart Cards authenticate with the access control door reader prior to exchanging the secret key information to unlock the card numbers for verification.

Information Protection, or Logical Security
Today, smart cards can be used to secure Logical Access to control PC and network use. The card can also be used to encrypt emails, transmissions, transactions and login requests. Smart Cards can be used to support a PKI (Public Key Infrastructure) environment where a very high degree of certainty is required.

Health/Medical
Cards can support the identity claim of the card holder, and allow access to services reserved for those who are authorized. In addition, on a smart card, portable health records can be saved on the memory for use and authentication. In the USA, ex-military veterans use their Identity Card to access health services at a network of Veterans' Hospitals across the country.

Membership/Loyalty
Cards can be used as a "flash pass" or declining balance. Flash pass means the card holder presents the card for a discount, while declining balance indicates that the card access a database of information where the value of the card is stored. The transaction can deduct a certain amount off the card holder's account, or record their purchase for future discounts.

Document Encryption and Exchange

Using secure certificates stored on the smart card, emails and other electronic documents can be signed to ensure:

- authenticity of the sender
- non-alteration of the document in transit
- non-repudiation (sender cannot deny sending it)

Convergence

This is a term used to describe the ongoing combination of applications onto a single credential (ie. one single smart card can open the door, login to your computer, authenticate your network access requests, and pay for your lunch at the cafeteria checkout.) Multiple applications can use multiple technologies stored on the card.

Standards-Based Approach - an overview of PIV

** Based on information from Smart Card Alliance publication IC-08002*

PIV, or Personal Identity Verification, is a US Federal Government standard developed post 9/11 to establish a robust identity management framework . Government and Industry in the US have worked for over 10 years to develop a standardized identification process for proving an individual's identity and providing them with a secure identity credential.

History

On August 27, 2004, the White House issued a Homeland Security Presidential Directive 12 (HSPD-12) mandating the need to "enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification." HSPD-12 called for the use of a common identification credential.

As a result of this directive, in early 2005 the National Institute of Standards and Technology (NIST) published a Federal Information Processing Standards (FIPS) publication numbered 201, titled "Personal Identity Verification (PIV) of Federal Employees and Contractors". FIPS 201 provides an identity management framework that enterprises should regard as a best practice in the design and implementation of their own identity management programs.

FIPS 201 defines the identity vetting, enrollment and issuance requirements for a common identity credential and the technical specifications for a government and contractor ID card, or the "PIV" card.

PIV cards can only be issued by Federal agencies. There are two other varieties of PIV:

- PIV-I standards for "Interoperable" and is a card built to the same technology specifications but is issued by other agencies that do Federal work and require access to Federal resources. PIV-I is used by other non-Federal government agencies and large Federal government contractors such as Lockheed Martin or Boeing.
- CIV (formerly PIV-C) standards for Commercial Identity Verification, and is a standard for Commercial use. CIV cards can be issued by any commercial entity following their own policies and procedures, but the smart card chip conforms to the same technical standard.

The impact of FIPS 201

Identity cards and badges have evolved from printed tokens to secure documents that incorporate machine-readable technology. Legacy credentials asserted a privilege and, to bind the credential to the holder, identity information may have been printed or even written on the card or badge surface.

To validate credentials rapidly, issuers must provide an infrastructure that can verify the current standing of the credential holder. Machine-readable credentials became the norm to facilitate rapid verification. As a result, credentials that are read visually fill a different role than credentials that are read electronically. A printed badge can assert both identity and a privilege. A credential that is read by an electronic system asserts identity only. The system determines the privileges authorized for the credential holder.

An increasing number of government organizations and corporate enterprises are now using smart cards as their employee identity credentials. A smart card-based identity credential stores the employee's identity information securely, so that the information can be accessed for fast, automated identity verification and used to determine the employee's authorization to access corporate resources.

Using smart cards enables the issuer to assert that the receiving party can place a high degree of trust in the information on the card. This information can include personal information (for example, a biometric or signed digital photo) or privileges (such as an electronic purse or digital certificates that allow computer logon). Additionally, because a smart card has computing power, it can require the user to provide authentication in the form of a PIN or, in some cases, a biometric before the card communicates with the interrogating system. And finally, a smart card can use cryptographic methods to establish a secure communication channel between the reader and the card (for example, using a challenge and response to require the interrogating system to authenticate itself to the smart card prior to any communication taking place).

In any secure identity credentialing system, the issuance process is as important as the credential’s security. The issuance process needs to bind the person to background identity checks and testing that take place before the credential is issued. After the credential is issued, the credential life cycle management process needs to incorporate authentication, revocation, and re-issuance processes. Relying parties will only trust a credential if they believe that the issuance and life cycle management processes are secure.

Significance of PIV

For the first time, organizations are able to take a standards-based approach to identity cards, and apply best practices to their card programs. FIPS 201 and the personal identity verification process identify a number of important steps:

Sponsorship. A sponsor's duty is to vouch for an applicant's need for an enterprise credential and authorize applicant enrollment. The sponsor may also authorize the cost incurred by the credentialing process.

Enrollment. The enrollment process is designed to verify the identity of an applicant and collect information from the applicant. Applicants must bring two forms of identification and are fingerprinted and photographed at enrollment. The information collected is used to perform suitability checks and create the credential.

Adjudication. Trusted adjudicators determine whether an applicant should receive a credential based on the results of the suitability check. Identity vetting procedures (e.g., criminal record checks, education, employment, credit history, and verification of claimed skills) are part of the adjudication process, with disqualifiers defined as part of vetting procedures. Successfully passing adjudication triggers credential production. The level of adjudication varies from organization to organization, depending on the level of security/access required. Adjudication can be structured so that individuals who need access to something like a network operations center or security operations center are subjected to more extensive adjudication.

Credential Production. Credentials can be personalized in a centralized facility or at local issuing stations. Relevant information is printed according to the standards, security features are added, and the electronic smart card chip is encoded with personal data.

Issuance and Activation. When an applicant arrives to pick up the personalized credential, the issuer verifies the applicant's identity by reverifying the identity documents presented at enrollment and matching the applicant's fingerprint to the one used to enroll. The credential is then "unlocked," digital certificates and a PIN are loaded onto the chip, and the credential is released to the applicant for use.

Credential Use. Activated credentials can be used to validate identity electronically and access secure physical locations and computer networks.

All of these process steps must be supported not only by technology but also by policies and procedures. It is only by the consistent execution and enforcement of policies and procedures that the overall integrity of the system can be ensured. FIPS 201 provides a best-practice framework for the entire identity proofing and

issuance process that can be used by enterprises implementing robust employee identity management systems.

The FIPS 201 PIV card offers the following advantages over other smart card-based approaches:

- It is supported by a wide range of manufacturers and integrators.
- It does not compel an organization to use a single vendor for key components.
- It provides flexible authentication, signature, and encryption functionality.
- It is well positioned to take advantage of emerging technologies, such as biometrics.
- As a standard that will be used by Federal agencies to issue credentials to millions of U.S. Federal employees and contractors, it has the advantage of scale.
- It provides the framework to support interoperable identity credentials across organizations.

Because of these factors, implementing a FIPS 201 PIV-card-based approach to identity credentials can be extremely beneficial to organizations outside of the U.S. Federal government. An organization using the FIPS 201 model and standard can take advantage of a high level of functionality at economical volume prices. The identity technology has been thoroughly scrutinized and is trusted at the highest levels. And the credentialing process is flexible and has been thoroughly vetted to represent best practice.

Choosing the Right Technology for your Organization

Conducting a standard Risk Assessment may assist the choice of Card Technology.

1. Understand your organization, its processes and the people and assets at risk.
2. Specify loss/risk events and vulnerabilities
3. Determine the impact and potential cost of a loss event
4. Perform a cost/benefit analysis

1. Understanding your organization:

A proper understanding of the purpose of the Veteran's Card needs to be developed. Specifically, what are the privileges associated with the card, and what benefits are offered in association with presenting the card and asserting correct identity? The following items should be considered:

- number of cards in operation
- time frame for initial distrubution
- distribution of the cards (national or global)
- distribution of the services provided, or locations where the card is to be presented
- types of services provided by the cards
- type of personal information being exchanged
- value of the services requested by the use of the card

2. Specifying loss/risk events:

Can the card be duplicated or altered?
Is the card bound to the card holder by use of a photo, PIN or biometric?
Can the card be used by someone other than the card holder?
Can the identity of the cardholder be stolen, changed or compromised?

3. Impact of a loss event

In the event a card is lost or stolen, what benefits may be accessed using the card?
What type of information may be compromised?
What is the cost of a loss event?
What is the estimated frequency of a loss event?

4. Cost/Benefit Analysis

Defining the benefits of the use of identity cards is usually a very difficult thing to do. Often, it is not possible to quantify the monetary value of what an identity card really does – binding a diverse group of people to a common brand or entity. There is an increased sense of "well-being" associated with this branding, and defining that in dollar terms is problematic.

It is important to compare what you are paying now for issuing your ID cards, to the cost of a new system and the benefits it will deliver. Without clearly defining the benefits to be delivered using the new card, a completed ROI will not be possible.

Basic ROI formula:

Cost of Existing Program – Cost of New Program = Actual Program Cost

$$\frac{\text{Actual Program Cost}}{\text{Benefits Delivered}} = \text{Return on Investment}$$

Smart Card Capabilities, Security and Storage

Smart Cards have the ability to store and retrieve data using their internal memory. Data is stored in containers. Each container is labeled and indexed so the Card knows what data is stored in what spot. Smart Cards can hold 1K, 4K, 64K, and 128K or more of information. In many scenarios where the card holder needs to be established as the authentic user of the card, biometrics (fingerprint or iris image) are stored on the card for comparison.

The major benefit of using a Smart Card is the card and cardholder authentication can be incorporated into your overall identity program. Smart Cards reduce the risk of information alteration, addition or deletion. With Smart Cards, a high level of assurance in the integrity of your identity program can be assumed, and higher levels of information or benefits can be exchanged.

Smart Card Security - Cryptogoraphy, PKI and CAs

There is a wealth of information widely available on the internet regarding cryptography and PKI.

At the heart of the smart card is the information stored on the chip in a secure environment. Each smartcard has a secure algorithm that is used to encrypt and decrypt information. This cryptography is protected against physical and virtual attacks using a variety of counter-measures.

PKI, or Public Key Infrastructure, is a set of hardware, software, people, policies and procedures need to create, manage, distribute, use, store and revoke digital certificates. A digital certificate is an electronic document that binds a key with an identity. There is a Public and a Private key used in PKI.

Private and Public keys can be generated by the card itself. The private key is stored on the card (it never leaves the card, ever) and the public key is shared with the Certificate Authority (CA). The CA then approves the validity of the public/private keys, and issues a Certificate. These certificates can be stored on the card, and compared with the CA whenever a transaction needs to be completed. By controlling the Certificate Revocation List (CRL) on the CA, the transaction can be validated as authentic and authorized. If the Certificate Authority withdraws the certificate, the transaction request by the card will be denied. This entire environment using keys, cryptography and certificate authorities is called PKI. It is, at present, the most secure method of authentication available.

The Future of Card Technology, and Best Practices

As the demand for security continues to grow, the industry is moving quickly to the use of Smart Cards where transactions and devices can be authenticated and secured. Smart Cards, with their onboard logic, calculations, and authentication processes, can be used to properly enforce the policies of privacy and security that most ID programs demand. They can operate in a widely distributed environment but be controlled centrally.

Best Practices

The list of best practices that apply to this project also apply to any identity management project.

1. Prioritize the business drivers at the start of the project and focus on the most urgent deliverables.
2. Engage stake-holders early and clearly articulate project deliverables and timelines. Involve them from the projects inception rather than deferring conversations with some of them until later. Any identity project involves complex issues of privacy, and these must be taken into account as part of the planning.
3. Engage executive level sponsorship. This helps resolve conflicts between stake-holders, and speeds the decision making processes.
4. Involve IT. This cannot be stressed enough. Once the project is delivered and installed, the first line of support will fall on this department. Their buy-in is critical to the success of your program.
5. Engage a technical resource (similar to # 3) who will be come the permanent system administrator of the identity project infrastructure, and involve them in product selection.
6. Measure success. Establish metrics to support each business driver and measure the results both before and after deployment.
7. Start with small, simple deliverables, and work up to more complex integrations and capabilities. Roll out functionality over time and constantly improve the product.
8. Plan for user acceptance, testing, and most importantly, user awareness programs. Education on the product is the single most important vehicle that will prompt users to begin preferring your program over other options.

Specifically, in the world of ID cards and identity verification, one key point is relevant. As in most cases, the newest technology available gets the most attention. In the world of identity documents, there has been a rush towards electronic authentication. Lost in the massive push towards smart cards and PKI is the interesting fact that the use of physical security features on cards has also increased dramatically.

It is vitally important that identity documents contain a variety of security features, both electronic and physical, to allow authentication on multiple levels. No one single method of authentication should be trusted 100% of the time.

The Future of Card Technology

The lifespan of the use of identity cards is a hotly debated topic, and has been for the past 10 years or so. Increasingly, we are seeing a demand for electronic authentication devices such as smart cards and tokens, and a recent surge in NFC (near field communication) technology.

With NFC, the chip that has traditionally resided on your credit card has moved to the mobile phone where a Secure Element (SE) on the chip contains a several items such as a Secure Identity Object (SIO) and certificates. These items are stored securely on the chip just like on a smart card and can be used in the PKI environment for financial and identity transactions. Some experts suggest that the card can be eliminated with this alternative technology.

However, it is important to consider the environment where the identity transaction is taking place, and whether or not there is an associated infrastructure available to support it.

Without an extensive (and expensive) infrastructure to support the use of electronic credentials, the traditional ID card is still the ideal form factor to assert identity. Incorporating physical security features that reduce the chance of forgery, the ID card is a relatively inexpensive mechanism, and is the ultimate fall-back position for identity verification when the power goes out.

If we look into our wallets today, there are a large number of credit card and identity documents we carry with us, each designed to assert identity to a different system. The companies that issue these cards have significant financial interests in maintaining their “top of wallet” status by offering a variety of benefits and services. The real estate on the card is an important marketing piece for these companies, and at present it is not clear how the “turf war” for consumers’ dollars will pan out. For example, if the NFC chip in the mobile phone holds the credit card information of a consumer, the branding of that credit provider has all but disappeared. Because of this, companies with a financial interest in a consumer’s identity continue to use the Card as the form factor of choice.

It is our opinion that the ID card as an identity document will remain a very important component of any identity program for the next 10 years.

Card Issuance

There are two major methods of issuing identity cards: Centralized versus Distributed.

Distributed Card Issuance

A Distributed Card issuance project is used whenever there are significant delivery problems getting the identity documents into the hands of the card holder. A recent Drivers License program in Indonesia completed a few years ago using Digital Identification Solutions used a distributed approach to DL issuance. In that case, communication between the hundreds of small islands was difficult, and arranging for secure mail/delivery of the ID card was problematic. The problem was solved by implementing a methodology where the resident was able to apply and receive their ID card at the local office. Drivers Licenses were printed using desktop card printers.

Barcode, Mag Stripe and Smart Card chip encoding can be done at the same time as card personalization. It is now possible to do laser engraving using Desktop machines.

On average, Distributed Card Printing process are 37% more expensive than Central Issuance processes. Explicit costs involved in the Distributed model include, but are not limited to: Card protection, personnel costs, floor space, data capture stations, printer, server, server hosting and networking, maintenance and setup costs.

The Advantages of Distributed Issuance

Speed	Very fast Service to the client, usually minutes for the client to receive their identity card document.
Distribution	Problems with mail/courier losses are reduced or eliminated

The Disadvantages of Distributed Issuance

Card Stock Security	Managing a large inventory spread across the country is difficult. Missing stock is often not immediately reported. Lost or stolen stock jeopardizes the integrity of the entire identity program.
Printer Theft	Stolen ID Printers result in catastrophic downtime at the operations centre. The stolen printer may be used to create unauthorized documents that look identical to real ones.
Maintenance	Desktop card printers require maintenance and care
Staff costs	Trained staff are required to operate a card printer. Staff turnover results in unqualified staff operating the machines. Re-training costs are significant. Dedicated hardware support specialists required.
Overall Project Costs	Average about 37% higher than Central Issuance costs. (Source: Oberthur Technologies)

Central Card Issuance

Central Issuance (CI) processes are used when there are large numbers of cards to print, and a secure mail distribution system exists. A CI solution can handle the millions of cards needed initially, plus the ongoing replacements and new production.

In the CI process, data can be entered online or captured at remote offices. The data is stored on a central server for processing at a single site. The card stock and printing equipment is stored in a secure facility and trained and bonded personnel operate the equipment.

This CI process can be streamlined to include paper/letterhead printing, tabbing cards to paper, folding, envelope insertion and postage. In the final setup, it is standard for data to be sent electronically to the processing centre and boxes of sorted mail delivered to Canada Post at the end of the day. Usually, a central issuance processing facility can produce several thousand completed identity documents per day, depending on the complexity of the document.

CI processing centres can be set up by a client at their own location, or the entire identity document processing program can be outsourced to a trusted 3rd party.

The Disadvantages of Central Issuance

Speed	Clients have to wait approx.1 to 2 weeks to receive their identity documents.

The Advantages of Central Issuance

Volumes	Large numbers of cards per year (thousands to millions)
Equipment Security	Printing machines are kept in secure physical plants where only authorized entry is allowed.
Card Holders	Widely distributed over a geographical area
Business Continuity	Disaster recover, with fully automated backup and procedures in place
Identity Document Security	Card stock and printing processes are protected
Identity Document Protection	Unique forgery-resistant methods can be used, not available on desktop card printers
Identity Document Lifespan	Cards have a longer lifespan due to card construction and personalization processes
Flexibility	Can handle very large volumes initially (millions of cards) plus annual ongoing requirements
Future expansion	Incorporating smart card chips and advanced authentication functionality is available without re-tooling every printer/capture station in the country
Cost	On average, Central Issuance programs are 37% cheaper than Distributed Issuance over the lifespan of the card program.

Card Issuance Requirements

The requirements for issuing cards are different depending on the choice of either Distributed or Centralized printing.

Equipment & Software

In a Distributed Issuance model, the following equipment is needed at each location:

- PC
- Camera
- Secure network access devices (VPN, Firewalls, etc.)
- Card Printer and Laminator
- ** Optional: Smart Card Encoders
- Issuance Software License

In a Centralized Issuance model, the following equipment may be needed at each office location:

- all of the above, EXCEPT Card Printer and Laminator

The Card Printer and Laminator is the single most expensive item at a Distributed workstation, and may cost more than $12,000 depending on the capabilities required. Smart Card encoders can be built into the printers so they encode and print in a single step. These encoders would be required ONLY if smart card technology was used.

For both Distributed and Centralized printing, secure network access to a central server is required. The data is always stored centrally no matter which printing method is chosen.

In a Centralized Issuance model, a central location housing the printing equipment and card stock in a secure facility is required. Generally, these facilities are far more secure than each brand office, and offer a much higher degree of security. CCTV surveillance and Access Control, plus operators who are cleared and bonded, ensure a secure operating environment.

Staff

For distributed photo capture and printing stations, an operator can produce cards at a ratio of one operator to one station. In a centralized printing environment, a single operator can run multiple card printing stations, or two operators can operate a large piece of equipment designed to turn hundreds or thousands of cards per hour.
The following is a project equipment list for illustrative purposes only, in order to show what is really required for a large scale implementation using the Central

Issuance model. In this case, we are assuming 3 PCs per location (33 locations in all) in order to issue 1,000,000 cards in the first year of operation.

BILL OF MATERIAL

Function	Type of equipments	Technical Description	Qty	Spare / Total	Dev & Maint	Total Qty
Identity Document	Plastic cards	PETF cards with advanced security pre-printing	1000000	10000		1010000
Cards	SUB TOTAL					
Enrolment	Computer	Dell Optiplex 380 con windows XP Pro o equivalente	99			99
Enrolment	Antivirus	Fsecure	99			99
Enrolment	Flatbed scanner	Canon CanoScan Lide 100 or equivalent	66			66
Enrolment	Barcode reader	1DBR Motorola USB con PDF 417 o equivalente	99			99
Enrolment	APN	TBD	66			66
Enrolment	Cable	Cable RJ45 Cat. 6 (3m/PC)	99			99
Enrolment	SW	Provider SW	99			99
Enrolment	SUB TOTAL					
Personalization	Computer	Dell Optiplex 380 con windows XP Pro o equivalente	1	1		2
Personalization	Antivirus	Fsecure	1	1		2
Personalization	Cards printer	Datacard MX1000 or equivalent	1	1		2
Personalization	Cables	Cable RJ45 Cat. 6 (3m/PC)	1	1		2
Personalization	Laminator	Fasver 6041P	1	1		2
Personalization	SUB TOTAL					
Packing	Computer	Dell Optiplex 380 con windows XP Pro o equivalente	3	1		4
Packing	Antivirus	Fsecure	3	1		4
Packing	UPS	Dell UPS, Tower, 500W, 230V with two C13 to C14, 2M Input Cords - Kit	3	1		4
Packing	Network cable	Cable RJ45 Cat. 6 (3m/PC)	3	1		4
Packing	1D barcode reader	1DBR Motorola USB con PDF 417 o equivalente	3	1		4
Packing	Packing machine	Flexiwrap o equivalente	3	1		4
Packing	Packing list printer	HP LASER PRINTERS : HP 1505 o equivalente	3	1		4
Packing	SUB TOTAL					
Stock mgt / System admin	Computer	Dell Optiplex 380 con windows XP Pro o equivalente	1	1		2
Stock mgt / System admin	Antivirus	Fsecure	1	1		2
Stock mgt / System admin	Network cable	Cable RJ45 Cat. 6 (3m/PC)	1	1		2
Stock mgt / System admin	1D barcode reader	1DBR Motorola USB con PDF 417 o equivalente	1	1		2
Stock mgt / System admin	List printer	HP LASER PRINTERS : HP 1505 o equivalente	1	1		2
Stock mgt / System admin	SUB TOTAL					
Delivery	Computer	Dell Optiplex 380 con windows XP Pro o equivalente	33	1		34
Delivery	Antivirus	Fsecure	33	1		34
Delivery	Barcode reader	1DBR Motorola USB con PDF 417 o equivalente	33	1		34
Delivery	SUB TOTAL					
Personalization server	Server DBA	Processors	1			1
Personalization server	Rack	PE 4220 42U Rack with Doors and Side Panels, Standard Packaging	1			1
Personalization server	FTP server & Servers Push/pull input	PE R200 Quad Core Xeon X3330 (2.66GHz, 2x3MB, 1333MHz FSB, 95W TDP) or equivalent	1			1
Personalization server	Domain server	Processors Active Directory - Monitoring - Antivirus Server	1			1
Personalization server	LTO storing system	Dell Powervault 124 T LTO4	1			1
Personalization server	LTO tapes	LTO4 tapes	24			24
Personalization server	Backup	Symantec backup Exec + controller card for managing the tape saving system	1			1
Personalization server	Rackable UPS	Dell 4U Rack UPS + NMC, 5600W, 230V, Hardware/Electrician Required ~93-134 min Runtime	1			1
Personalization server	Server keyboard	Dell Querty Clavier Rack	1			1
Personalization server	Rackable screen	Dell LCD 17in avec rail	1			1
Personalization server	Power distribution unit	Dell power unit	1			1
Personalization server	Network cable	APC power cable	28			28
Personalization server	Network cable	Belkin Cordon Réseau RJ-45 Cat 5	28			28
Personalization server	Network cable	Belkin Cordon Réseau RJ-45 Cat 6	28			28
Personalization server	CPS License	Configuration, documentation included	1			1
Personalization server	SUB TOTAL					
Central server	Server DBA - Production	Processors	1			1
Central server	Rack	PE 4220 42U Rack with Doors and Side Panels, Standard Packaging	1			1
Central server	FTP server & Servers Push/pull input	PE R200 Quad Core Xeon X3330 (2.66GHz, 2x3MB, 1333MHz FSB, 95W TDP) or equivalent	1			1
Central server	Domain server	Processors Active Directory - Monitoring - Antivirus Server	1			1
Central server	LTO storing system	Dell Powervault 124 T LTO4	1			1
Central server	LTO tapes	LTO4 tapes	24			24
Central server	Backup	Symantec backup Exec + controller card for managing the tape saving system	1			1
Central server	Rackable UPS	Dell 4U Rack UPS + NMC, 5600W, 230V, Hardware/Electrician Required ~93-134 min Runtime	1			1
Central server	Server keyboard	Dell Querty Clavier Rack	1			1
Central server	Rackable screen	Dell LCD 17in avec rail	1			1
Central server	Power distribution unit	Dell power unit	1			1
Central server	Network cable	APC power cable	28			28
Central server	Network cable	Belkin Cordon Réseau RJ-45 Cat 5	28			28
Central server	Network cable	Belkin Cordon Réseau RJ-45 Cat 6	28			28
Central server	SUB TOTAL					
Enrolment & delivery server	Complejo Central / Hardware	Servidor DELL R610, Intel XEON, 12 GB Memoria, WIN SERVER 2008 R2, Raid Controllers, HD 250	1	1		2
Enrolment & delivery server	Complejo Central / Hardware	Dell Power Vault MD1220, 9TB storage	1	1		2
Enrolment & delivery server	Complejo Central / Hardware	Dell Tape Backup Unit. Powervault 124T LTO 4HH	1	1		2
Enrolment & delivery server	Complejo Central / Hardware	Router Firewall	1	1		2
Enrolment & delivery server	Complejo Central / Hardware	Server Rack	1			1
Enrolment & delivery server						
GRAND TOTAL						

Options for renewing the card

Standard printed ID cards, with an expiry date, cannot be renewed unless the entire card is re-printed. It is standard practice to keep the data on file for future use, so at the time of expiry, a new card can be printed and mailed to the recipient. It depends on your policy for photo age, but usually a photo over 5 years old is not deemed acceptable for use in a photo ID environment. With chip technology there are additional ways to authenticate the card in the ecosystem (other than using the photo alone) so a longer life span can be sustained.

The card renewal process will depend on your program policies:

- Do you need to capture a new photo every 5 years?
- Do you require information from other sources or databases to verify the card life extension?
- Do you intend to issue one card for life, and then issue replacements if that card is lost/broken?
- What other systems or services are dependent on that card and how will renewal impact those systems?

In the Distributed Issuance model, card holders would visit the nearest office and submit a new photo and receive a new card on the spot.

In the Central Issuance model, card holders could upload a photo to a central website for processing, and new cards can be sent out via mail when the application process is completed.

Security and Privacy Considerations

Privacy considerations are driven by the present and future policies of your organization, and may be dependent on the province where the card holder resides. There is a Federal privacy policy, but the provincial policies supersede the federal one if a province actually has their own.

Usually, as long as you declare to the card holder the way in which you intend to use the information, you can capture almost any kind of info. The card holder must be informed and be a willing participant in this information exchange. It is recommended that Veterans Affairs seeks legal counsel in this regard.

As a general rule, only capture and store information that you actually are going to use. If you have no use for the fingerprint, then we recommend not capturing it. If you are not going to use the photograph, then don't capture it. (That substantially reduces the cost of your program too as you would eliminate the need for distributed capture photo stations at your offices.)

The effect of a Card Breach

Based on the two main types of cards discussed so far (Standard ID card versus Smart Card electronics), there are several considerations:

Standard ID Card
While the ID card contains personal information on the surface, the card itself is in the possession of the card holder. Securing the card from loss is the sole responsibility of the card holder. The loss of a single card only affects that single cardholder. It is important to incorporate forgery-resistant technology into the printed card so that duplication detection is enabled.

Smart Card
The Smart Card contains electronic data, often including the information printed on the surface. However, the data is stored in such a way that it cannot be removed with destruction. The data cannot be moved, copied, replicated or altered. In the highly unlikely event that this occurs, only the data from that one single card has been compromised while the integrity of the entire ID program is unaffected.

The effect of a System Breach

A system breach is far more serious. The entire database of card holders may be compromised. It is important that standard IT-based information access protocols and policies be followed.

Costing

Project Assumptions

General Details	
Project Duration	3 years
Number of working days / year	250 days
Number of working days / month	20 days
Number of working hours / day	8 hours
Enrolment	
Population to be enrolled	1,000,000 persons
Duration of enrolment phase	12 months
Duration of enrolment phase	240 days
Data Collection	
Number of Data Collection Sites	33
Number of teams at Data Collection Sites	1 team
Collection Site – Annual Qty processed (average)	30,303 cards
Collection Site – Daily Qty processed (average)	121
Personalization	
Number of Personalization Sites (Ottawa)	1
Number of teams at Personalization Site	2
Personalization Site, Qty of cards produced per year	1,000,000
Personalization Site, Qty of cards produced per day	4,000

Project Costs

Summary	
Number of Cardholders: 1,000,000	
Cards, PET-F (Polyester) with advanced security features	
Personalization (Verification, QC, Stock Management)	
Central System (Server and Administration HW)	
Consumables (Ribbons, Packing etc.)	
Implementation Fee (Project Management & SW)	
Maintenance (Annual Fee)	
Transportation & Delivery Costs	
Cards & Personalization System Price Per Card	**Est. $ 4.50 CAD**
Cards with CHIP, Personalization System Price Per Card	**Est. $ 5.20 CAD**

Note: Cards with CHIP are Polycarbonate cards with an embedded contact chip for strong authentication functionality. It does not include the distributed infrastructure (readers, network, servers, PKI and policies) needed for authentication processing. It only includes the cost to produce such a card.

Enrolment Stations Costing, 33 locations	
Enrolment HW, SW, Data Delivery to Central Site	
Implementation, Project Management & Development	
Maintenance & Transport/Delivery	
Enrolment Stations Subtotal	**$ 1,488,000**

Project Implementation Timelines

In order to issue 1,000,000 cards through a Centralized Issuance program, we estimate approx. 237 business days from start to finish. Production through a Distribute Issuance model would be slightly longer as the card printers used at each office location would take longer to implement and train, and would also take longer to produce this initial large volume of cards.

If, for illustrative purposes we assume a start date of August 6, 2012 to implement a Central Issuance solution, the last of the 1 million cards would be delivered by early July 2013.

On the following page, please see an approximate breakdown of a sample project plan, with dates and timelines, for your requirements.

CAN - Veterans ID project	DAYS	START DATE	END DATE		ACTORS
INITIALIZATION	**29 days**	**6-Aug-12**	**13-Sep-12**		
Purchasing order	1 day	6-Aug-12	6-Aug-12		CAN Government (CAN)
Internal Initialization Meeting	1 day	7-Aug-12	7-Aug-12	4	OTC YML ; OT LTS/GTS/PD/PROC/PM
Contract signature + downpayment	20 days	7-Aug-12	3-Sep-12	4	CAN ; OT Sales
SWs orders	1 day	13-Sep-12	13-Sep-12	12	OT PD
Project Plan Preparation	10 days	8-Aug-12	21-Aug-12	5	CAN; Enrolment supplier (Enrol); DTC,OT
Workshop to collect exhaustive requirements	5 days	22-Aug-12	28-Aug-12	8	CAN ; Enrol ; OT GTS/LTS/PM
Project Plan finalization	6.67 days	29-Aug-12	6-Sep-12	9	CAN ; Enrol,OT,DTC
Initialization meeting	3.33 days	6-Sep-12	11-Sep-12	10	CAN ; Enrol,OT,DTC
Firma del plan de Proyecto	1 day	12-Sep-12	12-Sep-12	11	CAN ; Enrol,OT
PLANNING	**46 days**	**13-Sep-12**	**15-Nov-12**		
TECHNICAL & FUNCTIONAL SPECIFICATIONS	46 days	13-Sep-12	15-Nov-12		
Raw materials delivery for Ok proof	25 days	13-Sep-12	17-Oct-12	12	OT PD
Ok Proof/BAT manufacturing	20 days	18-Oct-12	14-Nov-12	17	OT R&D
Ok Proof/BAT Approval	1 day	15-Nov-12	15-Nov-12	18	CAN,OT LTS/PM
Writing of Technical & Functional specifications	30 days	13-Sep-12	24-Oct-12	12	Enrol ; OT GTS/LTS,DTC
Approval	5 days	25-Oct-12	31-Oct-12	20	CAN ; OT LTS/PM
Dev & Qualification environment	2 days	1-Nov-12	2-Nov-12	21	OT GTS/R&D,Enrol,DTC
EXECUTION	**162 days**	**1-Nov-12**	**14-Jun-13**		
DEVELOPMENT OF SW & HW PROCUREMENT	**68 days**	**1-Nov-12**	**4-Feb-13**		
HW orders	3 days	1-Nov-12	5-Nov-12	21	Enrol,OT PD
HW manufacturing	65 days	6-Nov-12	4-Feb-13	27	Enrol,OT PD,DTC
Development of the SW solution	66 days	5-Nov-12	4-Feb-13	22	OT GTS/R&D,Enrol
CARDS MANUFACTURING	**130 days**	**16-Nov-12**	**16-May-13**		
Raw materials orders & delivery	45 days	16-Nov-12	17-Jan-13	19	OT PROC & PD
Manufacturing & delivery of the samples for Dev & Qualificaiton pur	15 days	18-Jan-13	7-Feb-13	32	OT Prod
Manufacturing of 500 000 cards	35 days	8-Feb-13	28-Mar-13	33	Enrol,OT PD,DTC
Manufacturing of 500 000 cards	35 days	29-Mar-13	16-May-13	34	OT GTS/R&D,Enrol
ACCEPTANCE TESTS	**15 days**	**5-Feb-13**	**25-Feb-13**		
FAT platform implementation in USA/FR	2 days	5-Feb-13	6-Feb-13	29	Enrol ; DTC ; OT GTS/LTS
Internal FAT	1 day	8-Feb-13	8-Feb-13	38,3	Enrol ; OT LTS/GTS
Modifications	10 days	11-Feb-13	22-Feb-13	39	Enrol,OT GTS
FAT with final customer	1 day	25-Feb-13	25-Feb-13	40	CAN ; Enrol ; OT LTS/PM
SHIPMENTS	**79 days**	**26-Feb-13**	**14-Jun-13**		
Confirmation HW storing site is ready	1 day	26-Feb-13	26-Feb-13	41	CAN
HW shipments	15 days	27-Feb-13	19-Mar-13	44	Enrol,OT PD/Logistics
Custom clearance	5 days	20-Mar-13	26-Mar-13	45	CAN
Transport from Custom to final customer safe vault	1 day	27-Mar-13	27-Mar-13	46	CAN
Confirmation HW reception	0 days	27-Mar-13	27-Mar-13	47	CAN
Cards Shipments	15 days	29-Mar-13	18-Apr-13	34	OT Logistics/CS
Custom clearance	5 days	19-Apr-13	25-Apr-13	49	CAN
Transport from Custom to final customer safe vault	1 day	26-Apr-13	26-Apr-13	50	CAN
Confirmation of reception	0 days	26-Apr-13	26-Apr-13	51	CAN
Cards Shipments	15 days	17-May-13	6-Jun-13	35	OT Logistics/CS
Custom clearance	5 days	7-Jun-13	13-Jun-13	53	CAN
Transport from Custom to final customer safe vault	1 day	14-Jun-13	14-Jun-13	54	CAN
Confirmation of reception	0 days	14-Jun-13	14-Jun-13	55	CAN
ON SITE IMPLEMENTATION	**49 days**	**28-Mar-13**	**4-Jun-13**		
CENTRAL SITE	**16 days**	**28-Mar-13**	**18-Apr-13**		
On site implementation - servers	5 days	28-Mar-13	3-Apr-13	48	Enrol ; OT GTS/LTS
On site implementation - Perso Line	5 days	4-Apr-13	10-Apr-13	61	OT GTS/LTS
On site implementation - Enrol Central servers	5 days	28-Mar-13	3-Apr-13	48	Enrol ; OT GTS
Users training	3 days	11-Apr-13	15-Apr-13	62	Enrol ; OT LTS
Administrators training	2 days	16-Apr-13	17-Apr-13	64	Enrol ; OT GTS
SAT	1 day	18-Apr-13	18-Apr-13	65	CAN ; Enrol ; OT LTS/PM
DECENTRALIZED SITES	**33 days**	**19-Apr-13**	**4-Jun-13**		
On site implementation 99 Enrolment workstations	33 days	19-Apr-13	4-Jun-13	66	Enrol ; OT GTS/LTS
Users training	33 days	19-Apr-13	4-Jun-13	66	Enrol ; OT LTS
SATs Capture sites	33 days	19-Apr-13	4-Jun-13	66	Enrol ; OT LTS/PM
Start up assistance	33 days	19-Apr-13	4-Jun-13	66	Enrol ; OT LTS
PROJECT CLOSING	**20 days**	**5-Jun-13**	**2-Jul-13**		
Collection of analysis & final reports from main team members	10 days	5-Jun-13	18-Jun-13	72	OT,OT PM,Enrol,DTC
Project final reports	5 days	19-Jun-13	25-Jun-13	75	OT PM
Archiving & lessons learn DBA	5 days	26-Jun-13	2-Jul-13	76	OT PM