National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

The Common Access Card

Major Anonymous

JCSP 49

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 49

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Exercise Solo Flight – Exercice Solo Flight

The Common Access Card

Major Anonymous

THE COMMON ACCESS CARD: A STEP IN THE RIGHT DIRECTION

It is important to note that this paper is UNCLASSIFIED. As a result, the research conducted in support of this topic is from open sources and does not contain any CLASSIFIED information.

The Common Access Card (CAC) is a United States of America (USA) Department of Defense (DoD) identification card that is issued to active-duty military personnel, reserve component personnel, civilian employees, and eligible contractors to access military facilities and information systems. The CAC is a smart card that essentially stores information such as an individual's name, rank, Social Security Number, Department of Defense Identification Number (DoD ID), and other identifying information[1].

History of the CAC

The concept of using a smart card as a replacement to traditional military ID dates back to the Persian Gulf War of the early 1990s. At that time, the USA military had an identification card system that was not secure enough to manage all of the services that the military offered. In response, the DoD began to explore the idea of using smart cards as a means to authenticate and verify the identities of its personnel.[2] Initially, the CAC combined identification and building access into once card. Then in 1998, the DoD issued the first CAC to support public-key infrastructure (PKI) authentication and encryption[3]. Over the next 25 years, the CAC has undergone several changes, and its use has grown largely and rapidly.

Use of the CAC in the USA DoD

Today, the CAC supports numerous functions of the USA DoD. Firstly, it remains an identification card. All DoD members (serving and civilian) have their personal information (including but limited to full name, rank, Social Security Number, Department of Defense Identification Number (DoD ID)) accessible with one swipe. By having this all available on one card, it makes identification verification simple when moving between bases and overseas theatre of operations[4].

The CAC is also used by DoD personnel to access secure facilities. As many DoD facilities require higher level of security clearances and authorizations in order to access, traditional identification cards are not sufficient. The CAC is used not only to verify the identity of members, but if the member has the required clearances and authorizations to be granted access to restricted areas[5]. In addition, the CAC itself can be used for physical access control. The CAC can be used as part of a physical access control system (PACS) lessening the

[1] US DoD 2021 (CAC)
[2] US DoD 2022 (CAC)
[3] US DoD 2021 (PKI)
[4] US DoD 2021 (CAC)
[5] US DoD 2022 (CAC)

requirement for multiple keys and passes depending on where the member is required[6]. The CAC holder's identity and authorizations are verified through the card's microchip before granting access to any restricted area.

The DoD utilizes the secure nature of the CAC by implementing digital certificates on each card that allow for access to secure online communication, encryption and digital signature capability. The certificate is authenticated with one password or pin. Thus limited the requirement for each system to have its own password. It also limits security incidents and increases traceability as the card and password/pin are required for access. The CAC is used to access DoD information systems that require PKI authentication and encryption[7]. The CAC provides secure access to sensitive information and protects against unauthorized access. Another use for the CAC is digital signatures. It provides PKI-based digital signatures that are legally binding and recognized by the DoD. Digital signatures can be used to sign and encrypt emails and documents, as well as to authenticate users to online services[8]. This minimizes passwords and logins for several different sites, thus creating efficiencies and allowing productivity to persist as members are not waiting for passwords to reset due to having to remember multiple accounts for multiple systems. The CAC also allows for secure access to email. It provides a secure channel for sending and receiving email on the DoD network. Users can gain access by inserting their CAC into a card reader and entering their PIN. As the CAC contains the required digital authorization certificates, it allows for greater ease to facilitate remote work/work from home. As the CAC is a whole of DoD initiative, the member is not required to be at one location to access. Should the need to change locations: due to postings, operations, or need to work from a third location, the member will be able to access the required DoD information systems securely[9].

DoD benefits of using the CAC

A summary of the benefits of the CAC are as follows:

- Increase in security: The CAC provides a robust authentication system that can be used to authorize access to sensitive information and systems;
- Increases efficiency: The use of digital signatures eliminates the need for paper-based signatures and speeds up processes that require multiple signatures[10] (this has the potential to speed up in the in/out clearance process as an example);
- Cost effective: Although the initial set up costs may be significant, once the system is operational, the costs are minimal. The CAC provides multiple services, including identification, authentication, and physical and logical access control, in one card, which is certainly more cost effective than using several separate systems;

[6] US DoD 2022 (CAC)
[7] US DoD 2021 (PKI)
[8] US DoD 2021 (PKI)
[9] US DoD 2019 (CAC)
[10] Defense Manpower Data System 2013

- Enables mobility: The CAC enables personnel to access DoD systems and facilities from remote locations, which increases productivity and efficiency, all the while allowing members to work from home or from remote areas[11]; and
- Interoperability: The CAC is used across all branches of the military and provides a standard platform for interoperability. This is essential as members from all branches and elements could be required to work outside of their respective branches and elements within the DoD and throughout the world at American defence establishments[12].

DoD limitations of the CAC

Despite the many benefits, the CAC is not without its limitations:

Complexity: The CAC system is complex and personnel require specialized training to operate and maintain the system hardware and software[13];

Accessibility: The use of CAC can be difficult for individuals with disabilities or who do not have regular access to a CAC reader;

Loss or theft: Losing or having a CAC stolen can cause significant problems, as the CAC is the primary identification document for military personnel[14];

Compatibility issues: Sometimes compatibility issues can arise when using the CAC with third-party systems or products[15]; and

High start up cost: Issuing the CAC system is expensive. A complete overhaul of a system as large as a national military would be significant. Political buy-in would certainly be required for this sort of expenditure.

DoD CAC overall

The CAC is a crucial identity and access management tool used by the United States DoD across all branches of the military. The CAC provides a single card and one stop solution for identification, authentication, and access control to DoD facilities and information systems[16]. The use of the CAC increases security, improves efficiency, and enables personnel to access DoD systems and facilities from remote locations. This system does have its issues as well, such as the complexity, accessibility issues, compatibility concerns with third-party systems, and high start up costs. Despite theses limitations, the CAC remains a critical tool that plays an essential role in the security and operations of the United States DoD.

What similar countries use

The CAF has a tendency to compare itself to the US DoD despite the significant differences between the two organizations. Most notably: size/composition, resources, and political and public support. It is also important to consider the different levels of threat to

[11] Cox 2019
[12] Moroney 2011
[13] US Federal News Service 2011
[14] US Federal News Service 2011
[15] Moroney 2011
[16] Plyer 2002

national security there are in both countries. The USA has a far greater impact globally and has a greater number of threats they face with regards to national security. As a result, it is worth considering what more similarly structured and organized militaries use as their smart card equivalent to the CAC as the DoD system may be too far out of reach.

The first country to consider will be the Australian Defence Force (ADF). The ADF has its own unique identification card a security access system, which is different from the DoD CAC. The ADF uses the Defence Common Access Card (DCAC) as its standardized identification card for members of the ADF, including civilian employees[17]. The DCAC incorporates a number of security features such as a hologram, a microchip containing personal information, and a unique serial number that identifies the cardholder. The DCAC is used to provide secure access to defence establishments, vehicles, and equipment. It enables personnel to access classified information and assets, as well as to perform a range of other functions such as payroll, medical and dental services, transport, and accommodation[18].

In addition to the DCAC, the ADF also uses a variety of other security access systems to protect its people, information and assets. These include:

- Biometric systems: the ADF uses biometric technology such as fingerprint scanners, retinal scanners, and facial recognition systems to provide secure access control. The technologies identify a person based on their unique physical characteristics, increasing security and reducing the risk of unauthorized access[19];
- Smart card technology: the ADF uses smart cards for a range or purposes, such as secure access to information and physical assets. Smart cards contain embedded microprocessors that store and process data, allowing for secure authentication and encryption[20];
- Key management systems: the ADF uses key management systems to control access to secure areas and assets. These systems typically involve the use of specialized keys and locks that are virtually impossible to duplicate or pick[21]; and
- Passwords and PIN: the ADF also uses passwords and PIN to provide secure access to its systems and assets. These are typically used in combination with other security measures such as smart cards or biometric systems to provide multi-factor authentication.

The ADF has developed a comprehensive range of security access systems that ensure the safety and security of its personnel, information, and assets. These systems are constantly being reviewed and updated to keep pace with the latest advances in technology and to respond to emerging threats[22].

[17] ADF 2018
[18] ADF 2018
[19] Abraham 2012
[20] Abraham 2012
[21] ADF 2018
[22] ADF 2018 Abraham 2012
[22] ADF 2018
[22] ADF 2018

The next country that will be discussed is France. In the French military, instead of using a Common Access Card system, they use a smart card system known as the "Carte Militaire". The Carte Militaire is a smart card that is used to authenticate the identity of military personnel and grant them access to various facilities and services on military installations. This card contains a microchip that stores information about the holder's rank, unit, and other relevant details. This information is used to verify the identity of the cardholder and to grant the access to secure locations and assets[23].

One of the primary advantages of the Carte Militaire system is its flexibility. The smart card can be used for a wide range of purposes including physical access control, time and attendance tracking, and even supply chain management. This flexibility makes it an attractive option for military organizations that need to manage complex logistics and security operations. This system is also highly secure. The smart card uses advanced encryption technology to protect the data stored on it, making it extremely difficult for unauthorized individuals to access or tamper with the information. This level of security is essential in military environments where sensitive information and equipment must be protected from theft or sabotage[24].

The Carte Militaire system used by the French military provides a highly effective and secure means of managing access control and other security-related tasks. While it may differ from the CAC system used by the US DoD, it still highlights the importance of effective identity and access management in military environments[25].

The final military that will be used for comparison is the Italian military. In Italy, the military identification system is called "Tesserino Militaire" (Military ID card). This card serves as the primary means of identification for the members of the Italian Armed Forces and is used in a variety of purposes. These include access control, physical and logical security, and personnel management[26]. Unlike the Common Access Card used by the US DoD, which uses a smart chip to store biometric and other sensitive data, the Tesserino Militare primarily relies on printed information and barcodes for authentication.

The card includes standard identification information such as the member's name, rank, photograph, and military branch. It also displays information related to the individual's job title, unit assignment, and eligibility for various benefits and services. A key feature of the Tesserino Militare is its use of a unique barcode on the back of the card. This barcode is used to verify the cardholder's identity when accessing secure areas or systems, and is often scanned using handheld devices or fixed scanners at entry points[27].

In addition to the physical card, the Italian military also uses a digital identification system known as "Sistema Informativo Difesa" (Defence Information System)[28]. This system provides a secure platform for military personnel to access information and services online, while also enabling secure communication between different units and branches of the military.

[23] Delmas 2011
[24] Delmas 2011
[25] The French Ministry of Defence 2015
[26] Italian Ministry of Defence 2020
[27] Italian Ministry of Defence 2020
[28] Italian Ministry of Defence 2018

The Defence Information System uses a variety of authentication methods to ensure that only authorized users can access the platform. These methods include username and password authentication, as well as one-time password tokens and digital certificates for enhanced security[29].

While the Tessernio Militare may not be as technologically advanced as some other military identification systems, it is still an important tool for ensuring the security and integrity of the Italian Armed Forces. By using a combination of printed information and unique barcodes, as well as digital authentication methods, the military is able to verify the identity of individuals and control access to sensitive areas and information[30].

What does the Canadian Armed Forces use?

In Canada, the CAF uses a number of different identification and access control systems, both for physical access to defence establishments, facilities, and for logistical access to computer networks and systems. While the CAF does use some forms of smart cards and other advanced technologies, these systems are not necessarily equivalent to the CAC used by the US DoD. One of the most commonly used identification systems in the CAF is the Defence Identity System (DIS)[31]. The DIS is a digital identity and access management system used to manage personnel records and enable secure access to sensitive systems and information. It is used by both military and civilian employees of the CAF.

The DIS uses a variety of authentication methods to verify the identity of users, including username and password authentication, two-factor authentication, and Public Key Infrastructure (PKI) smart cards. It also includes mechanisms for managing user privileges and accesses rights to different levels of information and resources. Another important component of the DIS is the Digital Service Record (DSR), which is used to manage personnel records for military personnel. The DSR contains information such as the member's name, rank, service number, training and education records, and deployment history[32].

In addition to the DIS, the CAF also uses a number of physical access control systems to manage entry to military facilities and areas. These systems include both traditional lock-and-key mechanisms as well as newer technology such as card readers and biometric scanners. This will vary depending on the military establishment in question. An example of a physical access control system used by the CAF is the Automated Access Control System (AACS)[33]. The AACS is a networked system of access control devices and software used to manage entry into sensitive military installations and facilities. It uses a combination of smart cards and PIN numbers to verify the identity of users and grant or deny access to different areas.

Another physical access control system used by the CAF is the Building Access Control System (BACS), which is used to manage entry into military buildings and offices. The BACS include features such as electronic door locks, access control panels, and card readers to manage

[29] Italian Ministry of Defence 2020
[30] Italian Ministry of Defence 2018
[31] Canadian Government Office of Public Safety 2022
[32] Canadian Government Office of Public Safety 2022
[33] Canadian Government Office of Public Safety 2022

access to different areas of a building. In addition to these more specialized systems, the CAF also uses more general-purpose identity cards for military personnel. These cards contain basic information such as the member's name, rank, and service number, and are used for a wide range of purposes such as accessing medical services or receiving discounts from certain retailers.

While the CAF uses an assortment of different identification and access control systems, these systems may not be directly comparable to the CAC used by the US DoD, as these are many systems, and the DoD CAC is all on one card. However, as with the CAF, the use of smart cards, biometric scanners, and other advanced technologies is becoming increasingly critical to ensuring the security and integrity of military operations and resources.

Why the CAF should change

As previously mentioned, the CAC is a smart card that uses microchip technology to store and process data securely. It acts as a digital identity card for military personnel and civilian employees as well. The primary benefit to this system is the enhanced security. The microchip technology used in the card provides a high level of encryption and authentication, making it difficult for unauthorized individuals to access sensitive systems or areas. This particularly important to the CAF, as it routinely deals with classified information and often operates in high-risk environments. A CAC system would significantly reduce the risk of theft or misuse of sensitive data, as well as the possibility of physical security breaches[34].

Another advantage of the CAC system is increased efficiency. The card can be used to access multiple systems and areas, reducing the need for multiple login credentials, passwords, and physical keys. This streamlines the access process, saving time and increasing productivity. It also reduces the risk of errors or delays caused by forgotten or lost credentials[35]. The CAC system is also more cost effective in the long run. While there is a significant initial investment required to implement the system, the cost of maintaining and replacing physical keys and login credentials can be substantially higher over time[36]. Additionally, the CAC system requires less administrative support and paperwork, freeing up personnel for other tasks. The CAC system also has the potential to improve interoperability with allied forces. As the US DoD already uses this system, it would be easier for CAF personnel to work with their American counterparts and colleagues during joint operations and exercises. This would also facilitate more seamless sharing of information between the two countries, improving the overall security picture for both[37].

From an administrative perspective, the CAC system could create efficiencies in other areas. For a typical CAF member being posted to a new Base or Wing, it takes several days to complete an In-Clearance routine. This is due largely in part to the new member having to navigate throughout the Base or Wing (in some instances throughout a city) having to locate offices or CAF personnel for physical signatures. In Ottawa, newly posted members have to attend the National Defence Headquarters (NDHQ) to sign in and receive their new building passes (located in the west end of the city). They may work in a different part of the city,

[34] Wolfe 2019
[35] US DoD 2018 (CAC)
[36] Berthiaume 2021
[37] Moroney 2011

Canadian Joint Operations Center (CJOC) for example, which is located on the east end of the city (roughly a half hour commute away). They are also required to attend the Montfort hospital to sign into the Health Services (located in the Center city area), as well as their respective Mess (located downtown). This process could take a week to complete depending on resource and personnel availability. The CAC system would allow members to significantly decrease their in-clearance time requirements as their information is all loaded on the card. There would no longer be the requirement for members to have accounts at their previous bases closed and then wait in a que at the new location because being able to access systems, a process that can take weeks or even months. All information would be on the CAC, allowing for maximized handover times and continuity of work.

Although there would be challenges associated with the implementation of the CAC system, the benefits are significant enough to warrant consideration. Enhanced security, increased efficiency, and cost savings in the long run are all important factors that align with current CAF priorities. Additionally, the potential improvements in interoperability and information sharing make the CAC system an attractive option for any forward-thinking military organization. The US DoD has already demonstrated the effectiveness of the CAC system, and other countries such as Australia and the United Kingdom (currently in the process) are considering adopting similar systems. By following this trend, the CAF can position itself as a leader in military technology and further strengthen its position as a key player in global security operations[38]. There are also potential future applications for the CAC system that could further enhance the legitimacy of the system. The CAC could be used for biometric authentication, such as fingerprint or facial recognition, to further increase security. It could also be used for secure mobile transactions, allowing personnel to securely access mission-critical information from their mobile devices.

What would it cost?

As mentioned at the outset of this paper, all information research conducted with regards to this topic has been obtained from open source and UNCLASSIFIED sources. As a result, the figures below are as accurate as possible with the constraints of the research. In terms of cost, there are several factors that need to be considered when estimating the price of implementing a CAC system for the CAF:

Infrastructure costs

A CAC system would require significant changes and upgrades to the CAF's information and technology (IT) infrastructure in order fully implement this change. Initially, there would be a requirement to update all servers, storage devices, data storage capabilities, network switches and routers. These updates would be required at each CAF base, wing and other facilities, including deployed operations[39]. These CAF-wide updates would need to be conduct simultaneously in order to ensure interoperability upon launching the CAC. Beyond an overhaul of IT infrastructure is the requirement to update and replace equipment will have to happen. This will include but is not limited to adding and replacing all technology required to produce and

[38] Wolfe 2019
[39] Army Financial Management and Comptroller 2016

update cards, card readers, printers, door keypads. In terms of software, licenses to support this new system and technology would also need to be acquired[40]. The financial impact of the implementation of a CAF CAC would be in the range of at least $20-$30 million dollars conservatively.

Card issuance and management

Implementing a CAC system would require the CAF to issue and manage a large number of smart cards to personnel across all branches and units of the military. In order for all of this new technology and equipment to be successfully used, a significant amount of training for the CAF will be required. This training will be required for the installation and maintenance of the new IT infrastructure and equipment. All CAF members will need to be informed of how the CAC card would work and the impacts it will have on their day-to-day operations. In order for a seamless implementation of a CAC, a significant number of personnel will be required to conduct this training. Once in place a new logistical framework will be to be developed in order to ensure support the distribution and management of the cards, hardware and software. This would also include managing the card issuance process, maintaining user profiles and enforcing access control polices[41]. The cost of these systems would vary depending on the scope of the project, but could very reasonably be assessed around $10-$20 million for a large-scale implementation.

Training

If the CAF were to adopt the CAC system, all CAF members (military and civilian) would be required to receive training on how to properly use the new cards and associated software systems. This would entail a significant investment in training programs, material, and personnel. To ensure that all CAF personnel are trained on proper use of the new CAC system, the CAF would need to invest in training programs, materials, and personnel[42]. This would include online courses, classroom instruction, and training materials such as manuals and videos. The cost of this training could range from $5-$10 million, depending on the extent of the training required.

Integration costs

The CAF would need to integrate the new CAC system with existing systems and processes, as well as with DoD systems to ensure interoperability and secure access to shared data resources. The cost of integrating the CAC system with existing systems and processes would depend on the extent of the integration required. To ensure interoperability (specifically with US DoD systems), the CAF would also be required to invest in systems integration and data conversion services to enable the secure transfer of data between systems[43]. These costs could range from $5-$15 million depending on the scope and complexity of the project.

[40] Berthiaume 2021
[41] Defense Manpower Data Center 2013
[42] CBC 2016
[43] Wolfe 2019

The estimated (conservatively) cost of implementing a CAC system for the CAF could land somewhere around $100, depending on the specific requirements of the project. While this appears to be a significant investment (especially considering the political climate surrounding the CAF currently), it is paramount to consider the potential benefits of a CAC system. Given the criticality regarding secure access to military systems and facilities, not to mention the importance of security in general, the investment in a CAC system may be easy to justify in the long run.

Why the CAF should remain status quo

One of the biggest hurdles that implementing a CAC system would have to over come is the initial start-up costs[44]. For clarity, over time the initial investment would make plenty of sense. The issue now is the current political climate and defence spending plans, asking for millions of dollars for a capital project that is not even technically required would likely be difficult to sell. Politicians and military leaders could argue that this type of investment would be better used to improve other areas of the military such as recruitment, retention, training, and equipment upgrades. Another concern is compatibility issues. The implementation of a CAC system could cause compatibility issues with other systems and technologies[45]. This could prevent interoperability with military allies (outside of those who have the same system) or other agencies, potential hindering cooperation or joint operations. Anytime something new is introduced to any organization there will be initial obstacles to overcome. In this case, the implementation of a new system would require personnel to learn how to use the CAC system, which could be a significant challenge. This could also take time away from other training or operational requirements. Mistakes during the learning process could result in unintended consequences, such as security and data breaches[46].

It is also important to consider cybersecurity risks. Implementing a system such as the CAC requires upgrades and extensive networks of computers and servers. This is when the CAF would be most vulnerable to hacking attacks or cyber threats[47]. The risk of data breaches or other cyber-attacks could compromise the security of the military's sensitive information. From a reliability perspective, the CAC system is reliant on technology to work effectively. In the event of a technical issue, the system could be rendered useless, preventing access to critical resources or information. A reliance on technology could also be problematic in the event of power outages or other incidents that have the potential to disrupt the system's functionality[48].

The final, and perhaps the most relevant argument against the CAF switching to a CAC system, is the belief that there is a need to change at all. It could be argued that there is not a big enough threat to the security to the CAF that warrants changing the current system. Considering the previously mentioned factors, it would likely be very difficult to convince political and CAF leadership that changes are required (especially considering the initial cost). It is also important to note that neither the Canadian Security Intelligence Service (CSIS)[49] or the Communications

[44] Moroney 2011
[45] Business Wire 2006
[46] Moroney 2011
[47] Wolfe 2019
[48] Canadian Government Office of Public Safety 2022
[49] CSIS Member 2023

Security Establishment (CSE)[50] use a CAC (or similar) system. CSIS and CSE both use a system similar to CAF practices currently. Both of these agencies are regarded as having the highest standards for security in the country and are in line with what the CAF is doing.

Conclusion

The CAC is an US DoD identification card that is issued to active-duty military personnel, reserve component personnel, civilian employees, and eligible contractors to access military facilities and information systems. The CAC is a smart card that essentially stores information such as an individual's name, rank, Social Security Number, Department of Defense Identification Number (DoD ID), and other identifying information. The use of this card in the CAF could certainly create efficiencies in both security practices and administration. Its use in authentication systems, encryption purposes, digital signatures, and interoperability with our largest (and most important ally) the US DoD would make this a practical and sensible consideration for the CAF.

Despite the high initial start-up costs, compatibility issues, the time it would take to implement and the security concerns associated with that, training, political and CAF leadership buy in, and the perception t that the CAF is resistant to change, switching to a CAC system is still a step in the right direction for the CAF. It will be argued that the threat picture in Canada does not constitute a requirement for such a system, and that would not be wrong. However, that could all change by the time this paper has been submitted. When talking about security the old adage "it is better to have it and not need it than need it and not have it" fits very well here. With the daily advancements in technology and countries vying for technological advantages, it is critical that the CAF be prepared to move with the times. The current system that is being used is different depending on where you are in the country. This makes it difficult for interoperability in the CAF (let alone with our allies). The system is also tedious and makes it difficult for the In and Out Clearance processes, which wastes time and takes away from productivity. It is important for the CAF to be recognized a leader is security throughout the military community. Switching to a CAC system would help solidify this position and demonstrate to its' members that security is paramount to the force itself and to the country in general.

[50] CSE Member 2023

Bibliography

Abraham, Tamas. 2012. *Australian Defence Force Identity and Access Management (IdAM).* S&T Report, Department of Defence.

ADF. 2018. "Australian Department of Defence." *Defence Common Access Card (DCAC)-Department of Defence.* Accessed 02 2023. defence.gov.au/Security/DCAC.

Army Financial Management and Comptroller. 2016. "Army Financial Management and Comptroller." *Department of Defense Common Access Card. Army Financial Management and Comptroller.* Accessed 02 2023. asafm.army.mil.

Auditor General. 2012. *Security and Intelligence in the Department of Defence-Australian National Audit Office.* National Audit, Auditor General.

Australian Government. 2015. "Australian Government." *What is the Australian Force (ADF)-Australian Government.* Accessed 02 2023. australia.gov.au/about-government/defence.

Bergevin, Lise. 2019. *France Reveals Major Shake-Up of ARmed Forces.* News piece, BBC News.

Berthiaume, Lee. 2021. *Canadian Military IT Upgrade Costs Ballooning.* News piece, Ottawa: Global News Canada.

Business Wire. 2006. *U.S. Department of Defense Taps Fargo Electronics for Additional FIPS 201-Compliant Printer/Encoders to Support the Common Access Card Program.* New York: Business Wire.

Canadian Government Office of Public Safety. 2022. *Government Announces New Cyber Security Strategy.* Directive, Ottawa: Canadian Government Office of Public Safety.

CBC. 2016. "CBC News." *CBC News: $800 Million to Revamp Military's Information Management.* 09. Accessed 02 2023. cbc.ca/news/politics/ottawa-military.

Cox, Matthew. 2019. "Military.com." *Soldiers to get Wearable Token in Place of CAC for Battlefield Computer Access.* 08. Accessed 02 2023. military.com.

Defense Manpower Data Center (DMDC). 2008. *Applications of the Common Access CArd.* Washinton DC: DMDC.

Defense Manpower Data Center. 2013. "Defense Manpower Data Center." *DMDC: Guide to DoD Common Access Card Eligibility and Enrollment.* Accessed 02 2023. dwp.dmdc.osd.mil.

Defense News. 2020. "Defense News." *Canadian Military Awarded Contracts for New Logistics and Software Systems.* 06. Accessed 02 2023. defensenews.com/global/the-americas/2020/06/11canadian-military.

Delmas, Benoit. 2011. "Understanding the Catre Militaire." *The Local France.*

FEDweek. 2016. "FEDweek." *More Details on New Beginnings Released: How to Get a Common Access Card.* 07. Accessed 02 2023. fedweek.com.

Italian Ministry of Defence. 2018. *Defence: New Electronic Card Used by Military Personnel.* 07 20.

Italian Ministry of Defence. 2020. *Tesserino Militaire.* Italian Ministry of Defence, 02 16.

member, Anonymous CSE, interview by Major Kelly. 2023. (02).

Member, Anonymous CSIS, interview by Maj Kelly. 2023. (02).

Moroney, Jennifer. 2011. "Lessons from US ALLIES in Security Cooperation: the Case of Australia, France, and the UK." *RAND* 1-36.

Plyer, Kim. 2002. *CNO Trades Green ID Card for Common Access Card.* Newsletter, Washington, D.C.: United States Navy Supply Corps.

The French Ministry of Defence. 2015. *Le Carte Militaire.* Paris: The French Ministry of Defence.

Tomkins, Richard. 2013. *Why Most French Military Officers Have Carte Blanche.* News piece, Defence News.

US DoD. 2022. "Common Access Card (CAC): Information on Department of Defense (DoD)." *Defense.gov.* Accessed 02 2023. defense.gov/Experience/Common-Access-Card.

—. 2019. "Computer Security Resource Center: National Institute of Standards and Technology." *Common Access Card Readers and Cryptographic Modules.* 11. Accessed 02 2023. csrs.nist.gov.

—. 2018. "Computer Security Resource Center: National Institute of Standards and Technology." *FIPS 201-2 "Personal Identity Verification of Federal Employees and Contractors.* 05. Accessed 02 2023. https://csrc.nist.gov/.

—. 2021. "defense.gov." *DoD Instruction 8510.01 "Risk Management Framework for DoD IT".* 08. Accessed 02 2023. esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf.

—. 2018. "militarybenefits.com." *How to Access DoD Websites with a CAC.* Accessed 02 2023. militarybenefits.info.

—. 2021. "US Department of Defense." *CAC: DoD PKI.* 02. Accessed 02 2023. cac.mil.

US Federal News Service. 2011. *To Commonj Access Card or Not to Common Access Card-It's no Longer a Question.* Washington, D.C.: Us Federal News Service.

Ward, Alex. 2021. "France's Military is Shrinking, but is Still a Force to be Reckoned With." *VOX.*

West, David. 2014. "Academy to Improve Facility Access with New Common Access Card Proximity Readers." *Targeted News Service.*

Wolfe, Dennis. 2019. *Canadian Military Looking to Industry to Help Build a Better Cyber Defense.* News piece, Washington DC: Defense News.