RETOURNER LES SOUMISSIONS À :
RETURN RESPONSES TO :
SARAH.AHMED@CANADA.CA

Bidder's Legal Name and Address (ensure the Bidder's complete legal name is properly set out)
Raison sociale et adresse du soumissionnaire (s'assurer que le nom légal complet du soumissionnaire est correctement indiqué)

____

____

____

Procurement Business Number (PBN)
Numéro d'entreprise-approvisionnement (NEA)

____

Bidder MUST identify below the name and title of the individual authorized to sign on behalf of the Bidder – Le soumissionnaire DOIT indiquer ci-dessous le nom et le titre de la personne autorisée à signer au nom du soumissionnaire

____
Name /Nom

____
Title/Titre

____
Signature

____
Date
(____)____________________________________
Telephone No. – Nº de téléphone
(____)____________________________________
Fax No. – Nº de télécopieur

____
E-mail address – Adresse de courriel

REQUEST FOR INFORMATION /
DEMANDE D'INFORMATION

Title – Sujet Entepise Mobile Device Management Request for Information GESTION DES APPAREILS MOBILES D'ENTREPRISE Demande d'information (DDI)	
Solicitation No. – Nº de l'invitation R000034918	**Date** November 23, 2018
Client Reference No. – N° référence du client 34918	
Solicitation closes – L'invitation prend fin on – December 7, 2018 at 2:00 P.M. le - 7 décembre 2018 à 14 h	**Time zone – Fuseau horaire** EDT /HAE Eastern Daylight Time/ Heure avancée de l'Est
Contracting Authority – Autorité contractante Sarah.Ahmed@canada.ca Shared Services Canada | Services partagés Canada Procurement and Vendor Relationships | Achats et relations avec les fournisseurs 180 Kent, 13th Floor, Room 13-144 Ottawa, Ontario K1G 4A8	
Telephone No. – Nº de téléphone (613)240-3126	
Fax No. – Nº de télécopieur (613) 960-6007	
Destination NOT APPLICABLE SANS OBJET	

Service | Innovation | Value

ENTERPRISE MOBILE DEVICE MANAGEMENT

REQUEST FOR INFORMATION

INDUSTRY CONSULTATION PACKAGE

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

1 Overview

Shared Services Canada (SSC) was created in August 4, 2011 to fundamentally transform how the Government of Canada (GC) manages its information technology (IT) infrastructure to better support the delivery of programs and services to Canadians. Specifically, SSC was established to maintain and improve IT service delivery, generate savings and implement government-wide solutions that are modern, reliable and secure. The Department has the mandate to operate and transform email, data centre, telecommunications and cyber and IT security services for more than forty-three federal GC departments and agencies ("partners").

SSC's Network and End Users Branch (NEUB) is responsible for providing enterprise, end-user focused solutions, both nationally and internationally, to the GC. The Enterprise Mobile Device Management (EMDM) service supports mobile devices secure access to GC assets. The current service iteration was deployed under a critical need to support smartphones other than those using the BlackBerry operating system, and whose goal was simply feature parity with the multiple technical solutions previously in place.

With the success of the EMDM service launch, it is time to focus on the strategic evolution of the service. This will further support the GC's overarching goal of providing modernized services and tools to both citizens and its internal users. A significant portion of this process involves industry engagement, ensuring that the GC's unique setting can be understood from an integration perspective with common industry practices. In cases where gaps are identified, either the GC will need to change, the tools will require modification, or the requirement will be re-evaluated.

The objective of this Request for Information (RFI) is to obtain industry feedback in order to assist SSC in the creation of a strategic source methodology for services or solutions that will support the evolution of the EMDM service.

2 Introduction

This consultation is a key activity in the Industry Consultation phase relating to the management of mobile devices. As the GC moves increasingly to a mobile workforce, it is essential that the proper tools be in place to support the migration, as well as the necessary security controls to protect the GC's assets. Further, as the majority of devices to be deployed within the GC have comparable, if not identical, devices available for consumer use, the expectations of functionality are at odds with the GC's security-first approach. The goal of EMDM is to find the appropriate balance where users are empowered to do their assigned tasks without putting the GC at undue risk.

2.1 Objective

The objective of this Request for Information (RFI) is to obtain industry feedback in order to assist SSC in the evolution of its mobile device management service offerings. It is planned that the end result is a competed process, where the proposed offerings would:

- Innovate the solution space so that the GC moves towards a modern workspace;
- Provide Proof of Concepts (POC) for both function and integration demonstrations;
- Maintain strategic alignment across the GC, in particular with Blueprint 2020 and the GC IT Strategic Plan;
- Develop a strategic partnership with industry, with facilitated integration into developing areas of technology.

Through this document, SSC is seeking formal feedback from industry on the following items:

1. The business challenges identified within the use cases;
2. Industry best practices for managing mobile devices;
3. Industry's perspective on the challenges and drivers within the GC, with respect to larger GC transformational initiatives, such as Blueprint 2020[1] and the GC IT Strategic Plan[2].

Though this consultation phase, SSC will incorporate the feedback into both a strategy for mobile device management, and a procurement approach to enable said strategy.

2.2 Scope

This is not a bid solicitation. This RFI process will not result in the award of any contract.

Potential suppliers of any goods or services described in this document should not reserve stock or facilities nor allocate resources because of any information contained in this document. Nor will this Industry Consultation activity result in the creation of any source list.

Therefore, if any potential supplier responds to this process, it will not preclude that supplier from participating in any future procurement. This process is simply intended to solicit feedback from industry with respect to the subject matter described in this document.

2.3 Instructions for Response

2.3.1 Response Costs

SSC will not reimburse any organization for expenses incurred in responding to this RFI.

2.3.2 Treatment of Responses

Use of Responses: Responses will not be formally evaluated. However; the responses received may be used by Canada to develop or modify the procurement approach, as well as any draft documentation contained in this document. Canada will review all responses received by the RFI closing date. Canada may, in its discretion, review responses received after the closing date.

Review Team: A review team composed of representatives of SSC and its Partners (where applicable) will review the responses. Canada reserves the right to hire any independent consultant, or use any GC resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

Confidentiality: Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the Access to Information Act.

2.3.3 Follow-Up

The Government of Canada may, at its discretion, contact any respondents to follow up with additional questions or for clarification of any aspect of a written response. Based on the level of detail in the responses, the Government of Canada may request a follow-up clarification meeting with certain respondents.

[1] https://www.canada.ca/en/privy-council/topics/blueprint-2020-public-service-renewal.html

[2] https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html

2.3.4 RFI Contents

This document remains a work in progress and Respondents should not assume that new clauses or requirements will not be added to any Response solicitation that is ultimately published by Canada. Nor should Respondents assume that none of the clauses or requirements will be deleted or revised. Comments regarding any aspect of the draft document are welcome.

2.3.5 Volumetric Data

The data contained within this document is being provided to Respondents purely for information purposes. Although it represents the best information currently available to SSC, Canada does not guarantee the data is complete, up to date, or free from error.

2.3.6 Response Format

Cover Page: If the response includes multiple volumes, Respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number and the full legal name of the Respondent.

Title Page: The first page of each volume of the response, after the cover page, should be the title page, which should contain:

(i) The title of the Respondent's response and the volume number;

(ii) The name and address of the Respondent;

(iii) The name, address and telephone number of the Respondent's contact;

(iv) The date, and

(v) The process number.

Maximum Number of Pages of Response: Fifteen pages, this is to ensure that SSC can review all responses in a timely manner.

2.3.7 Enquiries

Since this is not a Response solicitation, Canada will not necessarily respond to enquiries in writing or by circulating answers to all Respondents. However, Respondents with questions regarding this RFI may direct their enquiries to:

Contracting Authority: Sarah Ahmed

Shared Services Canada
180 Kent Street
Ottawa, Ontario
K1R 7Y2

Email Address:	Sarah.Ahmed@canada.ca
Telephone:	613-240-3126

2.3.8 Submission of Responses

(a) Responses must be submitted electronically by the date and time indicated to the address indicated on page 1.

(b) Suppliers must submit their Responses either as PDF documents attached to their email or as documents that can be opened with the Microsoft Office Suite of applications.

(c) Suppliers may submit their responses in multiple emails, but all emails must arrive before the solicitation closing date and time to be evaluated as part of the response. The maximum email size that can be received by SSC is 10 MB. Suppliers should ensure that they submit their response in multiple emails if their attachments will cause the email to exceed that size.

(d) The time at which the response is received by SSC will be determined by the "Sent Time" indicated in the email received by SSC at the Email Address for RFI Submission.

(e) During the two hours leading up to the closing date and time, an SSC representative will monitor the Email Address for RFI Submission and will be available by telephone at the Contracting Authority's telephone number). If the Supplier is experiencing difficulties transmitting the email, the Supplier should contact SSC immediately.

(f) Canada will not be responsible for any technical problems experienced by the Supplier in submitting its response, unless Canada's systems are responsible for a delay in delivering the email to the SSC Email Address for RFI Submission.

(g) In the case of emergency, SSC has the discretion to accept a hand delivered (in person by a representative of the Supplier or by courier) of a hard copy submission that includes the entire response. However, the hand delivered response must be received by the closing date and time. As indicated above, an SSC representative will be available at the Contracting Authority's telephone number during the two hours before the solicitation closing date and time to receive responses submitted in this way. The only circumstances in which SSC will accept a delayed hand delivered response is if the Supplier can show that the SSC representative was unavailable to receive the hand delivered response, and attempts were made during the two hours before the solicitation closing date and time to make delivery.

(i) A response delivered to the specified email identified as the "Email Address for RFI Submission" after the closing date and time but before the contract award date may be considered, provided the Supplier can prove the delay is due solely to a delay in delivery that can be attributed to:

1) Canada's systems causing a delay in delivering the emailed submission to the SSC Email Address for RFI Submission; and

2) The Supplier can show that attempts were made during the two hours before the solicitation closing date and time to hand deliver the submission, but the SSC representative was unavailable to receive the hand delivered submission.

(ii) Misrouting, traffic volume, weather disturbances, labour disputes or any other causes for the late delivery of arrangements are not acceptable reasons for the arrangement to be accepted by SSC."

3 Context

3.1 Background

EMDM was a tactical deployment of functionality to meet a critical and immediate need to replace its fleet of over 100,000 BlackBerry 10 devices with secure alternatives. The solution as deployed used an existing licensed product (BlackBerry's Unified End Point Management – UEM) and in-house infrastructure. While functional, many of the time sensitive decisions taken require further scrutiny to ensure that they align with both the GC's overall objectives, but also with SSC's operational mandate.

In a larger scope, end-point management (EPM) encompasses all network-enabled devices in use within the GC – in particular desktop/laptop devices. These devices are currently over 1,000,000 such devices in use across the GC, all primarily managed by Partner support services.

3.2 Vision

The current GC vision for mobile management can be summarized by the following:

Enable the Public Service by implementing mobile services that will allow a unified and secured experience across any device, from any location.

The EMDM evolution aims to review the previous assumptions, confirm requirements with all stakeholders, and better position the GC towards the future. A significant portion of this process involves industry engagement, ensuring that the GC's unique setting can be understood from an integration perspective with common industry practices. In cases where gaps are identified between the GC's vision and the industry direction, either the GC will need to change, the tools will require modification, or the requirement will be re-evaluated. For example, while industry is heavily investing in the model of Bring Your Own Device (BYOD), there are numerous challenges that prevent the GC from widely adopting such a model. The Use Cases described further in this document provide situations where the GC has identified challenges between the current state, its current vision, and industry direction.

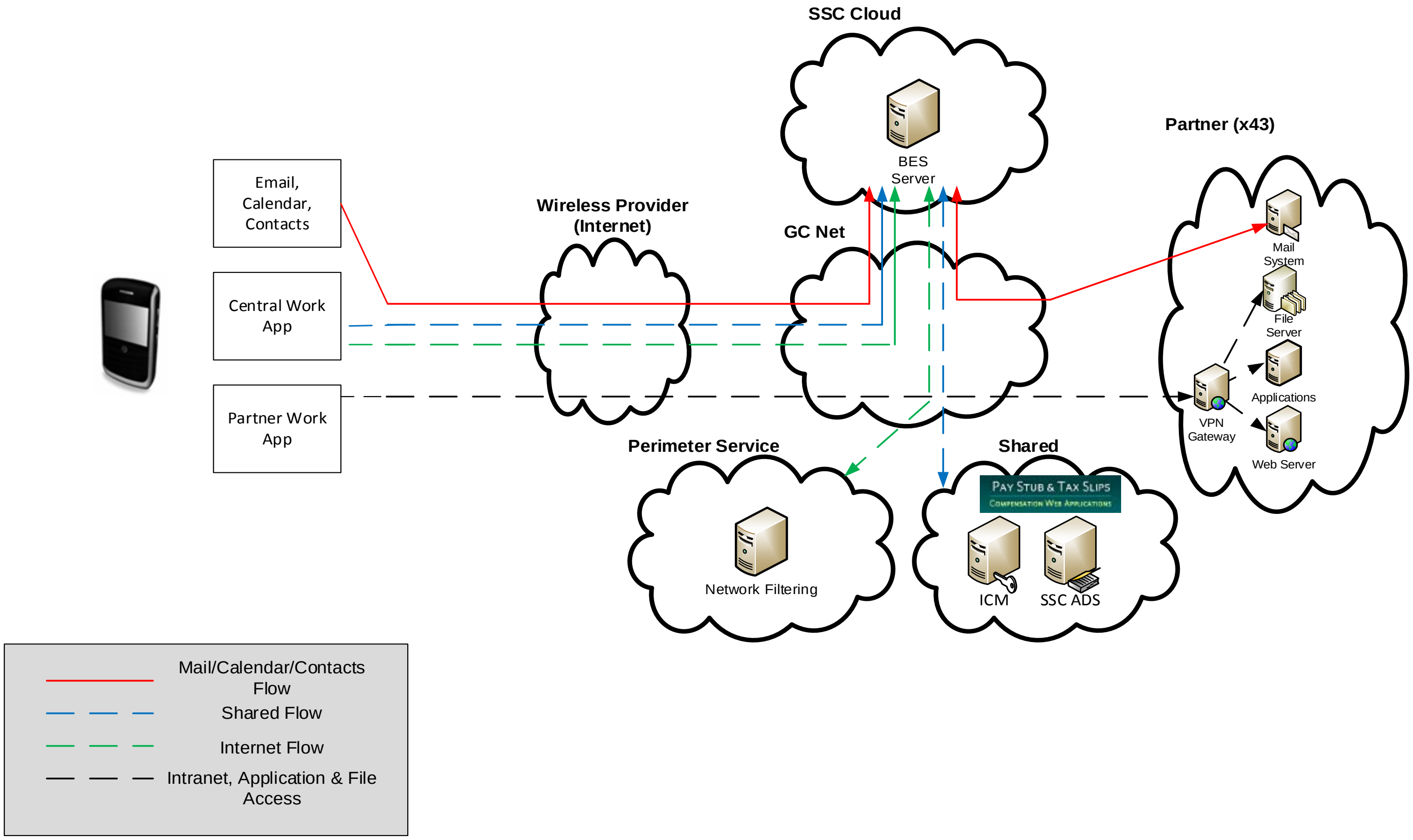
Since the inception of the EMDM service less than 1 year ago, the quantity of mobile devices managed has grown by 20%, and is expected to reach over 200,000 by March 2020.

The current EMDM strategy focused on a core set of principles:

1. An enhanced mobile user experience.
    - This will ensure that regardless of location, a user can access the necessary services, applications, and data to complete their work.
2. A modern take on security.
    - This will ensure that security controls are placed where appropriate, so that security is seen as an enabler.
3. A common user experience.
    - This will ensure that a user can easily transition between devices and maintain the same experience and functionality.
4. A device-agnostic support structure.
    - This will ensure that management services can securely support any device today, and ensure that devices from tomorrow can be easily integrated.
5. A centrally-managed service offering.
    - This will ensure improved service levels and response times due to a set of standardized support processes.

4 Foundational Elements

The image below presents a conceptual view of the current EMDM service.



4.1 Networks

The GC operates as a large entity with hundreds of distinct networks in use for its user base. Few of these networks allow for bi-directional traffic, and instead operate under the concept of a hub/spoke model. For example, the network for DND is not accessible by FINANCE users, and vice versa. The majority of department resources (email, files, and applications) are within this specific network zone, and authentication is done within that network layer.

The GC does operate a shared network infrastructure – GCCloud – which is accessible by departmental networks. Departments that wish to share their resources with this network must either expose them through a DMZ, or implement a reverse-proxy function to allow access. The current EMDM service is located within the GCCloud.

4.2 Directories

Each department runs one or more directory services for their resource access requirements. There are no GC standards applied to this model, though there are a few common themes.

SSC operates a shared meta-directory service based on Microsoft Active Directory (AD). This directory service will pull data from the departmental directories. This then allows for shared services to access the meta-directory in order to grant access to GC users, rather than having to connect to multiple directories. The limitations here are that the data sets are only partially standardized, and duplicate data sets are present.

4.3 Email

SSC operates numerous email environments for its clients in one of 4 possible variants.

- The @canada.ca (YES) service provides a private-cloud based service on MS Exchange 2013 for approximately 125,000 users across 20+ departments.
- MS Exchange 2007-2016 environments in departmental networks. A project is in place to ensure everyone is at a minimum 2010 version by end March 2019.
- GroupWise environments in department networks that are targeted to be replaced by MS Exchange within 2 years.
- Lotus Notes environments in department networks that allow applications to send/receive mail. All user email accounts are to be transferred to the YES service by end of December 2018.

4.4 Credentials

Each departmental directory has a set of credentials that is used for their specific resource set. A generic set of credentials is synchronized to the SSC shared meta-directory, which allows basic desktop access in the respective networks. Application-specific credentials (e.g. to a GIS application) are not shared outside of a department, and require local authentication to that application.

Additional assurance level credentials are available to all GC users. The majority of users leveraged the SSC Internal Credential Management (ICM) service, provided soft-tokens leveraging the Entrust PKI infrastructure. Some departments, such as CRA, manage their own credential management service for their users, and ensure that a trust model exists between ICM and their respective services. DND, RCMP, and CBSA also leverage Entrust, but utilize hard tokens instead, which necessitated derived credentials for alternative use.

4.5 Services

Resources, applications, and services can be located in any network location, using any directory service, any set of credentials, and any authentication mechanism. This adds a significant amount of complexity for ongoing support.

EMDM has taken the position of standardization in this regard, specifically that authentication to services is done either at the service level, or using the same credentials used by EMDM. For example, if a user is trying to access GCpedia, EMDM will ensure that network access is established and the user is responsible for authenticating directly to the GCpedia service.

While there are multiple efforts to standardize at the GC level, none are past the proof of concept phase and are therefore too far before practical realization to be considered as core for mobility.

4.6 Mobile Devices

The mobile devices in use operate under one of two models – Corporate Owned, Business Only (COBO) or Corporate Owned, Personally Enabled (COPE). The former model mandates that all activities on the device are filtered through the GC and monitored for additional security control. The latter model provides a split operation where consumer functions can be accessed by users with only minimal security controls applied to the device, while work-related functions are more restricted. In order to apply these restrictions, mobile devices offer the concept of "containerization" where work and personal data cannot be shared. The particular mechanisms for ensuring this division vary to a large degree between operating systems.

4.7 Problem Summary

The core issue is that the GC is in the midst of a significant transformation at all IT layers, and the transition from non-homogeneous environments to a standardized services poses both significant known and unknown risks. SSC has made large strides to consolidate items where feasible (identity, device types, security policies) but there remains a large gap in relation to network access, Partner-specific resources, and authentication mechanisms to those resources.

As these foundational challenges will not be addressed in time for the evolution of the EMDM service, a significant problem remains as to how a standardized service can be provided, with access to a multitude of service protected through layers of IT security, while also providing an innovative and useful tool for the mobile workforce.

5 Use Case Baseline

A set of definitions and baseline is required in order to both simplify the complexity, and clearly communicate the overall intent of the EMDM Evolution. A full set of definitions of terms can be found in Annex A.

Given the GC's size and mobility requirements, there are essential requirements that must be met when considering the operational state of the service.

- Highly available, secure and responsive mobile device service in order to support the GC's business needs
- Managed to Protected B security standards, as per ITSG 33 guidelines
- Support for international travel and foreign workers
- Support for Android and iOS devices, and optionally Windows and other emerging mobile devices with market share
- Policy enforcement: The ability to define, monitor and enforce mobile policies.
- Security and compliance: The ability to provide security controls such as authentication, encryption, device wipe and firewall support.
- Inventory management: The ability to inspect applications and devices and keep track of them for audit and refresh purposes.
- Software distribution: The ability to control installation, removal and operation of mobile applications.
- Administration and reporting: The ability for IT administrators to manage mobile deployments and users.
- IT service management: The ability to monitor mobile service usage, support the help desk.
- Network service model: The ability to monitor and optimize mobility costs and contracts.
- Delivery model: The ability to deliver MDM capabilities on-premises, as a hosted service or in the cloud.
- Integration: Ability to integrate with existing infrastructure components such as PKI, IdM and directory services.
- Support multi-tenancy, Customer administrator access control and user self-serve
- Support secure messaging across all supported mobile device platforms (s/MIME)
- Client self-sufficiency and service automation
- End Point Devices: Exploring extending support into end point devices, where appropriate

6 Use Case List

6.1 Use case 1 – New User

Statement: A GC user is to be issued a new standard mobile devices, with a default set of IT controls and mobile applications.

Question 1: How does an EMM manage the onboarding process so that the impact to the users is as small as possible, while ensuring that only authorized users/devices/applications are made accessible?

Question 2: How does it integrate with industry functions (e.g. Apple's Device Enrolment Program or Samsung's Knox Mobile Enrolment)?

Question 3: How does an EMM support the migration of users to the next generation service, as seamless and non-disruptive as possible to users?

6.2 Use case 2 – Travelling User

Statement: A GC user with an existing mobile device is scheduled to travel overseas to a high risk location for a defined period of time, and requires a new set of security controls and applications to be applied to the device.

Question 1: How does an EMM manage the transition to a different operating model with minimal impact to the user?

Question 2: What features can be applied to reduce the risk of data compromise and what controls can be put in place to safeguard Government assets, as well as the user's personal information?

6.3 Use case 3 – New Mobile Application

Statement: A department has purchased licenses for an application available on a commercial "application store" or an Independent Software Vendor (ISV) application or has a GC custom developed application and has requested that it be deployed to a subset of their users.

Question 1: How does an EMM manage the secure select deployment, so that the application only have access to the work resources with the department's network?

Question 2: How does it ensure that future updates to the application are applied in a timely and un-obtrusive manner?

Question 3: How can it support the license management of such an application, within or across multiple departments?

Question 4: How would this process differ for a custom developed application or ISV application that is not in a commercial application store?

6.4 Use case 4 – Secure Messaging

Statement: The GC uses secure email messaging (S/MIME) for all users, through a cross-certified credential service. Personally-assigned soft or hard tokens allow for distinct encryption to a targeted recipient. These credentials are not located within the user directory, shared directory, or email services – but rather a distinct credential-only Entrust PKI service.

Question 1: How does an EMM ensure integration of S/MIME messaging on mobile devices, so that the appropriate user credential is on the device to perform decryption, and that valid certificate lookup functions take place to the respective credential directories?

Question 2: How does an EMM support secure messaging without the use of PKI credentials?

6.5 Use Case 5 – Account Management

Statement: The GC has a complicated directory environment, supporting hundreds of thousands of accounts, that often generates duplication of effort and data.

Question: How does an EMM ensure that account management efforts are applied in an efficient manner, leveraging automation where at all possible?

6.6 Use case 6 – Multi-Tenancy

Statement: SSC supports over 50 distinct organizations, and must apply standard practices to all environments. It must also delegate high volume tasks (e.g. account modification) to organizations so that their respective support teams can offer services to their user base.

Question 1: How does an EMM ensure that there is a standard foundation of the service, yet allow for flexibility on a per-department basis?

Question 2: How does an EMM manage access controls so that roles can be applied at the service level, on a department level, and on a task-based level (e.g. only reset passwords for department X)?

6.7 Use case 7 – Security Controls

Statement: The GC operates in a secure model, where access controls and services must meet Protected B security control requirements. These controls apply to not only the back end service, but also the mobile devices themselves.

Question 1: What security control options can be accessed through an EMM that ensure the stability and secure management of the entire service?

Question 2: What controls exist on the mobile device, so that if a breach is detected, it is addressed in such a fashion as to minimize the impact to the larger mass?

Question 3: How does it ensure that only approved devices are granted access?

Question 4: How does an EMM provide compliance messages to users?

Question 5: How does an EMM provide a user or administrator the ability to remotely apply compliance remediation to mobile devices?

6.8 Use case 8 – Self-Service

Statement: Calls for basic functions are expensive and timely. The need for more automation, integration, and use self-sufficiency is a core driver for all IT change within the GC.

Question 1: What features can an EMM provide to improve overall integration of a service, so that the interface is as seamless and responsive as possible to users?

Question 2: What high volume administrative tasks should be left to the user, and which should be restricted?

6.9 Use case 9 – Service Roadmap

Statement: Consumer technology changes at a much faster pace than typical GC operations, and has multiple dependencies on other platforms.

Question 1: How does an EMM ensure that they keep up to date with both industry developments, while ensuring that the core user requirements remain met?

Question 2: What is deemed an acceptable timeframe for a new mobile feature to be exposed within an EMM?

Question 3: How should the GC address the convergence of the mobile device and end point management markets?

6.10 Use case 10 – Privacy and Access

Statement: The GC assigns a very high priority to individual privacy, and ensuring access controls are restricted to those who require access. Only upon specific circumstances should an administrator ever have access to a user's personal information. In addition, collection of personal information should be transparent and restricted to a program requirement with the user's knowledge and consent and it should not be shared with a third party.

Question 1: How does an EMM ensure the privacy of a user, restricting access to only themselves, yet allowing for security investigations and audits to take place?

Question 2: What measures does an EMM take to protect the user from the collection of secondary personal information that the user is not aware of, such as location and voice information?

6.11 Use Case 11 – Integration with Cloud and On-Premise Email Systems

Statement: The GC intends to adopt email services in the cloud in the near future, but some departments will remain with on premise email services for the foreseeable future.

Question 1: How does an EMM integrate with cloud based services, such as Office 365?

Question 2: How does a cloud-based EMM service integrate with an on premise email environment, and are there particular remediation that the GC should undertake given its foundational elements?

6.12 Use Case 12 – Accessibility

Statement: Through the proposed Accessible Canada Act (Bill C-81) tabled to Parliament in June 2018, the GC has signalled an intention to identify and remove accessibility barriers, and prevent new barriers in several areas including information and communications technologies and the procurement of goods and services. In support of this, SSC is seeking to procure Information and Communications Technologies (ICT) that meets internationally recognized accessibility standards so that it is accessible for the user and administrator community.

Question 1: To what degree does the EMM meet the requirements of the Harmonised European Standard EN 301 549 V2.1.2 'Accessibility requirements for ICT products and services'[3] which include WCAG 2.1? If it does not meet or fully meet the requirements, does the product roadmap include accessibility enhancements and if so, will the evolution result in full compliance and by what target date?

Question 2: How does an EMM solution provide the ability for administrators to configure IT policies for users with disabilities to enable built-in and 3rd party features and tools on mobile devices to meet their accessibility requirements on both the personal side and work containers?

Question 3: Please describe any aspects of the EMM that surpass the Harmonised European Standard EN 301 549 V2.1.2 and/or WCAG 2.1 AA or could offer other Accessibility benefits to the GC

https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf

Annex A Document References

Name	Owner

Annex B Lexicon

Item	Full Name
Mobile Device	A device that offers full functionality without the requirement for physical connections. These include Smartphones, Tablets, and Laptops.
Smartphone	A mobile device that provides voice services through a telecommunications provider. Can include Android, iOS, Windows, and other mobile operating system platforms
Tablet	A mobile device that resembles a large form-factor Smartphone but does not offer voice services.
Laptop	A mobile devices that provides a full-feature experience with optional physical connections. Majority of devices use the Microsoft Windows operating system, with some using the Apple operating system.