Mobility as a Service (MaaS)
# Contents

1. Introduction to Mobility as a Service ..............................................2
2. Service Definition ............................................................................3
   2.1 Functionality & Features – Blackberry Enterprise Server ..............3
   2.2 Functionality & Features – iOS MDM ........................................3
   2.3 Functionality & Features – Windows Phone .................................3
   2.4 Functionality & Features – Android Mini Compute Stick ..............4
   2.5 Access Methods .....................................................................4
3. Differentiators ...............................................................................5
4. Commercials ..................................................................................6
   4.1 Mobility as a Service Pricing ..................................................6
   4.2 Mobile Tariff Pricing .............................................................6
5. Information Assurance ...................................................................7
6. Service Levels ...............................................................................8
7. Additional Information ...................................................................10
   7.1 Service Constraints ..............................................................10
   7.2 Termination ..........................................................................11
   7.3 Ordering and Invoicing Process ..............................................11
   7.4 Financial Recompense model ................................................11
   7.5 Customer Responsibilities ....................................................12
   7.6 Training ..............................................................................12
   7.7 Trial Service .......................................................................12
1 Introduction to Mobility as a Service

MaaS offers several device types that can be used within a single organisation. By providing the correct level of functionality to each user, this will ensure your optimum cost of ownership.

Delivered as a fully managed solution with 24/7 support, you will never have to worry about the security, integrity or delivery of the mobile device management platform again. With a guaranteed service level and predictable monthly costs, you can experience significantly lower total cost of ownership for your mobile device management needs.

Highlights

The Sentinel Mobility as a Service Offering includes the following:

- Provisioned from fully accredited cloud infrastructure
- Private Government “Community Cloud” Offering
- Full Exchange functionality – fully synchronised email, calendar, and contacts on your device
- Lower costs – no need to deploy a Blackberry Enterprise Server or MDM for iOS devices / Android Mini Compute Stick/Windows Phone
- Mobile application deployment management
- Remote wipe functionality.
- Flexible working, eliminating dead time
- Fully GPG 13 Compliant (DETER) Service
2 Service Definition

2.1 Functionality & Features – Blackberry Enterprise Server
- Wireless over the air device configuration
- Two-way synchronisation of email, calendar, address book, and tasks
- Remote email settings; out of office replies, email filters and auto-signatures directly from Blackberry devices
- Locked down to CESG security guidance for data consumption
- Security Features:
  - Remote Device Wipe
  - Remote Password Reset
  - Restrictions on device features
  - Email account & configuration settings

2.2 Functionality & Features – iOS MDM
- Deploy iOS devices in-line with Cabinet Office guidance for OFFICIAL – Good Known State
- Provisioned to prevent jail-breaking & malicious code upload
- Apply CESG lock-down template across organisations or have granular policies per user group
- Access native iOS apps – via the AppSelect app portal
- Access other Sentinel tenancy services such as RDP, files or VDI
- Use an iOS device natively, no need for ‘bubble’ technology
- Security Features:
  - Remote Device Wipe
  - Remote Password Reset
  - Always on VPN
  - Restrictions on device features – e.g. camera, Face Time
  - Email account & configuration settings

2.3 Functionality & Features – Windows Phone
- Deploy devices in-line with Cabinet Office guidance for OFFICIAL
- Provisioned to prevent jail-breaking & malicious code upload
- Apply CESG lock-down template across organisations or have granular policies per user group
- Access native Windows apps
- Access other Sentinel tenancy services such as RDP, files or VDI
- Security Features:
  - Remote Device Wipe
  - Remote Password Reset
  - Always on VPN
  - Restrictions on device features
2.4 Functionality & Features – Android Mini Compute Stick

- Deploy Android devices in-line with Cabinet Office guidance for OFFICIAL
- Provisioned to prevent jail-breaking & malicious code upload
- Apply lock-down template across organisations or have granular policies per user group
- Android Mini Compute Stick apps – via centrally deployed MDM
- Access other Sentinel tenancy services such as RDP, files or VDI
- Security Features:
  - Remote Device Wipe
  - Remote Password Reset
  - IKEv2 VPN over the internet
  - Encrypted user environment
  - Connects directly to a TV or monitor

1 - Subject to departmental security approval
2 – Additional Service Fees

SCC’s Sentinel platform is housed within its Tier 3+ Datacentre and provides resiliency at all levels of the infrastructure, providing a stable, reliable infrastructure platform.

This service is deployed in a highly available, no single point of failure configuration. The service also makes use of SCC’s secondary Data Centre as a cold standby facility in the event of a disaster recovery scenario.

<table>
<thead>
<tr>
<th>Infrastructures Option</th>
<th>Availability SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual Site</td>
<td>99.95%</td>
</tr>
</tbody>
</table>

2.5 Access Methods

Connection to the Sentinel Mobility as a Service varies depending on the service taken:

- Blackberry – over any mobile network that supports mobile data and Blackberry Enterprise devices
- iOS MDM/Windows Phone - over any mobile network that supports mobile data or a WiFi network to facilitate the always on VPN
- Android Mini Compute Stick – over a WiFi network to the internet to facilitate connection of the VPN
3 Differentiators

SCC was the first pan-Government accredited provider of a G-Cloud platform. We have experience and capability across all cloud types (private, hybrid, community and public), combined with Information Assurance services that will help support PSN compliance. Potential customers can be assured that our maturity in providing Cloud based services differentiates SCC from a number of other SaaS cloud providers within the Digital Marketplace. Some differentiators include:

- **Accredited** – the entire platform inclusive of hardware, software and network is pan-government accredited for a multi-tenanted environment and we are an accredited PSN service provider (PSNSP) This means that the environment:
  - Offers a re-usable accreditation ensuring that a customer’s own internal security approvals process is significantly reduced
  - Greatly reduces risk
  - Ensures full compliance and assurance of the service according to the code of connections mandated by the PSN Authority for PSNSP’s.

- **Security Practice** – SCC utilises its own Information Assurance Practice to support the delivery of IT solutions into the government marketplace. We have found this internal function to be hugely beneficial to customers in the end to end IA design through to accreditation sign off; the IA practice, although internal to SCC, is independent to the operation of the platform, as such, supports the separation of duties principle without being 3rd parties for this additional critical service

- **Quality** – Quality and continuous improvement are integral to our business strategy and we continually improve our processes, systems, procedures and people. Our services are underpinned by certification for process and procedures (ISO 9001), environment (14001), security (27001), ITIL (20000), and health and safety (OHSAS 18001)

- **Managed** – the tenancy can be fully managed, reducing the burden on your organisations own internal IT staff meaning that the uptime availability provision is leveraged to ensure any failures are handled appropriately and in accordance with agreed procedures. This leaves a customer’s own IT teams to concentrate on their core services and not worry about the underpinning infrastructure

- **UK Sovereignty** – UK Data Centres and therefore not subject to Off Shoring or Near Shoring restrictions

- **Network Operation Centre (NOC)** – Allows us to provide, configure, manage and maintain a new environment or provide cost effective enhancements for an existing solution

- **Security Operation Centre (SOC)** – Where we monitor, assess and protect customers enterprise information systems

- **Owned Infrastructure** – SCC owned utilising internal security cleared resources, meaning that as Prime Contractor we are accountable for the contract and not reliant on 3rd parties

- **Network Connectivity** – Ability to connect to the Sentinel platform via the Internet, the GCF and the PSN Government Networks

- **24x7 Support** – SCC employed UK based, SC cleared, Cloud engineers available 24x7

- **ITIL Aligned Service** – SCC’s Service Management tools and service are fully aligned to ITIL and are certified to ISO 20000 – including Incident, Change, and Problem Management
4 Commercials

4.1 Mobility as a Service Pricing

The following table provides the pricing for the MaaS service offerings (per month):

<table>
<thead>
<tr>
<th>Service</th>
<th>Price per user per month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blackberry</td>
<td>£32</td>
</tr>
<tr>
<td>iOS MDM</td>
<td>£18.50</td>
</tr>
<tr>
<td>Windows Phone</td>
<td>£18.50</td>
</tr>
<tr>
<td>Android Mini Compute Stick</td>
<td>£18 (inc. device)</td>
</tr>
</tbody>
</table>

4.2 Mobile Tariff Pricing

<table>
<thead>
<tr>
<th>Service</th>
<th>Price per user per month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice and Data Connectivity Option</td>
<td></td>
</tr>
<tr>
<td>2Gb Unlimited</td>
<td>£21</td>
</tr>
<tr>
<td>6Gb Unlimited</td>
<td>£29</td>
</tr>
</tbody>
</table>

- Minimum 2 Year commitment
- Unlimited tariffs include free calls on network, to other mobile networks, voicemail and 01, 02 & 03 numbers.
- Fair usage policy applies (up to 10,000 minutes & texts)
- Out of Bundle Cost @ 33p per minute
- Non Geographic (084/7) @ 45p per minute

<table>
<thead>
<tr>
<th>Service</th>
<th>Price per user per month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Only Connectivity Option</td>
<td></td>
</tr>
<tr>
<td>1Gb</td>
<td>£7.50</td>
</tr>
<tr>
<td>3Gb</td>
<td>£11</td>
</tr>
<tr>
<td>5Gb</td>
<td>£14.50</td>
</tr>
<tr>
<td>8Gb</td>
<td>£17.50</td>
</tr>
</tbody>
</table>

- Minimum 2 Year commitment
- Out of bundle usage @ 2.5p per MB in the UK
5 Information Assurance

Sentinel has achieved both Pan Government Accreditation (PGA) and PSN Accreditation for systems at OFFICIAL. The service has also been implemented with the following security features:

- Suitable for OFFICIAL assets under the GSC (Government Security Classifications Policy)
- PGA accredited Inter-Domain Gateway – designed to facilitate assured connectivity between higher security domains and lower security domains or for organisations that wish to move more sensitive data assets at OFFICIAL
- SCC also holds ISO9000, ISO14001, ISO20000 and ISO27001 certifications which underpin our business operations and Cloud Platform
- All datacentres are highly resilient Tier3+, and UK based
- SCC is a registered sponsor with the Defence Business Services National Security Vetting (DBS NSV) which enables us to sponsor and administer the applications of Security Check (SC) and also Developed Vetting (DV) with the appropriate sponsorship from a customer
- As a minimum, all staff are cleared to Baseline Personnel Security Standard (BPSS)
- In excess of 800 staff are Security Cleared and based in the UK
- Protective Monitoring (aligned with GPG13 - DETER) across all Sentinel platforms at the hypervisor layer and below
6 Service Levels

The Services shall be provided by SCC in accordance with the following Service Levels:

<table>
<thead>
<tr>
<th>Mobility as a Service</th>
<th>Service Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Availability (Dual Site)</td>
<td>99.95%</td>
</tr>
<tr>
<td>Hours of Support</td>
<td>24 Hours</td>
</tr>
<tr>
<td>Incident and Problem Management Levels</td>
<td>1 - 4</td>
</tr>
</tbody>
</table>

The following table provides a maximum time before a response to an incident is provided by Incident management:

<table>
<thead>
<tr>
<th>Priority-(Severity)</th>
<th>Availability SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - (Critical)</td>
<td>30 mins</td>
</tr>
<tr>
<td>2 - (High)</td>
<td>60 mins</td>
</tr>
<tr>
<td>3 – (Medium)</td>
<td>4 Hours</td>
</tr>
<tr>
<td>4 - (Low)</td>
<td>72 Hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Priority (Severity)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - (Critical)</td>
<td>An incident which involves service not available or a serious malfunction of the service with impact on Sentinel’s direct delivery to single or multiple customers</td>
</tr>
<tr>
<td></td>
<td>• Total loss of service to all users and no work-around available</td>
</tr>
<tr>
<td></td>
<td>• Loss of functionality resulting in Sentinel Customer users/workgroups being unable to continue with normal business processing</td>
</tr>
<tr>
<td></td>
<td>• Unavailability of one or more supported services</td>
</tr>
<tr>
<td></td>
<td>• Sentinel down</td>
</tr>
<tr>
<td>2 - (High)</td>
<td>An incident which involves service not available with impact on Sentinel’s single or multiple customers or a serious mal-function of the service with potential impact on Sentinel’s direct delivery to customers</td>
</tr>
<tr>
<td></td>
<td>Partial loss of service and work-around available</td>
</tr>
<tr>
<td></td>
<td>• Loss of functionality which severely impedes all or some Sentinel services</td>
</tr>
<tr>
<td></td>
<td>• Customers’ users/workgroups being able to continue with normal business processing</td>
</tr>
<tr>
<td></td>
<td>• Partial loss of availability of one or more supported service</td>
</tr>
</tbody>
</table>
| 3 – (Medium) | An incident that involves degradation or risk to quality of service with impact on one or more Sentinel customers  
- Issue not impeding Sentinel customers’ users/workgroups from being able to continue with normal business processing  
- Potential to cause more serious issue if not investigated and addressed |
| 4 - (Low) | An incident for which the final resolution is outside the control of Sentinel and Sentinel has used all reasonable endeavours to mitigate the impact of the incident to the Customer. Sentinel shall advise the Customer of the likely resolution date and shall notify progress against this date.  
General Service related questions and requests for information. |
7 Additional Information

7.1 Service Constraints

Service availability explicitly excludes mobile network availability, and any device connectivity issues (unless VPN specific for iOS & Android Mini Compute Stick service).

BlackBerry Enterprise devices can only be configured to access a single Sentinel Hosted Exchange Mailbox.

Due to CESG lockdown, Blackberry devices cannot access any mobile internet services.

Due to CESG lockdown Blackberry devices cannot open URLs from within emails or download attachments from emails.

The service shall be allocated a maintenance window between the hours of 23:00 and 06:00 and the window shall be allocated during service initiation.

The service shall be Change Managed in accordance with SCC change schedules, change boards will sit weekly and changes shall be carried out during the subsequent change window.

Configuration changes that cause a reboot/downtime but are deemed urgent shall not impact Availability metrics and SLAs and the associated charging mechanism.

SCC will not provide any application or middleware level support as part of the service offerings described within this agreement.

Exclusions

SCC will provide service and support for all aspects of the service as defined within scope of the service. The Service Levels Agreements (SLA’s) will measure SCC’s success in the delivery of those services.

Where external factors influence SCC’s ability to deliver against the contractual defined Service then SCC will not be liable for failure to meet the associated SLA’s. These include but are not limited to the following circumstances:

- 3rd Parties, not engaged by SCC, fail to deliver services in accordance with their contractual commitments
- 3rd Parties use the Sentinel environment outside recommended best practice
- Where customer requested configuration changes cause application downtime
- Application Configuration causes service instability

Any materials and labour provided in these circumstances will be subject to agreement of the parties in writing and;

- Provided on a reasonable endeavours basis (i.e. outside of the Service Levels) unless agreed otherwise by SCC in writing, and
- Charged as additional Ad-hoc Charges.
7.2 Termination

7.2.1 By Consumers (i.e. consumption)

A G-Cloud service shall commence on the Effective Date and shall, unless specified otherwise in the Order Form, continue for the Initial Term and shall remain in force thereafter unless and until terminated by either Party giving to the other not less than 30 days written notice, but shall be subject to earlier termination as referenced within the Termination/Consequence of Termination section of the standard SCC G-Cloud terms and conditions.

7.2.2 By the Supplier (removal of the G-Cloud Service)

A G-Cloud service shall commence on the Effective Date and shall, unless specified otherwise in the Order Form, continue for the Initial Term and shall remain in force thereafter unless and until terminated by either Party giving to the other not less than 30 days written notice, but shall be subject to earlier termination as referenced within the Termination/Consequence of Termination section of the standard SCC G-Cloud terms and conditions.

7.3 Ordering and Invoicing Process

SCC will provide ordering of G-Cloud services via an Account or Customer Service Manager.

A list of G-Cloud services can be compiled with quotations for those specific services. Once The Customer is satisfied that the requirement is met, it can then be converted into an order.

Once the services are enabled and confirmation of the ordered G-Cloud services is delivered to The Customer a monthly invoice in arrears will be generated against the order.

Should The Customers usage of the Service increase beyond the contracted volumes during any period then this will be retrospectively invoiced, at the next month end, as additional services.

7.4 Financial Recompense model

Service Credits

1. Subject to Clause 1.3 below, in the event that SCC fails to meet the SLA Target for the applicable Service Level*, then the Service Credit mechanism in Clause 1.2 shall apply;

2. SCC shall provide a rebate of 1% of the Monthly Charge for this Service, which is applicable over the Report Period for every 1% below the SLA Target to a maximum of 10 % rebate. The applicable Service Credit shall be deducted off the next invoice due to The Customer.

3. Payment by SCC of Service Credits to The Customer shall be in full and final settlement of SCCs liability to The Customer for failure to meet the Service Levels during the Report Period.

4. Service Levels will only be calculated against Storage Availability and not against Application availability. Service penalties against the loss of storage availability will not include other machines or applications impacted by that loss.

5. Service Credits will not be applied where it is determined that SCC are not responsible for the cause of the breach in Availability performance.
7.5 Customer Responsibilities

The customer responsibilities will be as follows:

- To request all system restores via the service change process or via the service desk
- To provide a Data Governance policy for the backup, restore and data retention of the Customer data incorporating policies for possible media handling, where required
- Procurement, maintenance and management of any Customer data communications lines not identified in the Technical Specification. This shall need to be properly defined and provided according to the appropriate code of connection
- Provision, maintenance and management, as the case may be, of any Customers software, operating systems, applications and data
- Administration, management and control of Users access to the data stored on the Mobility as a Service, Sentinel Infrastructure
- Should SCC determine that the Customers usage of Mobility as a Service is not compliant with best practice guidelines, the Customer must comply with SCC’s reasonable requests for change

7.6 Training

There is no training required within this Mobility as a Service.

7.7 Trial Service

SCC is happy to invite trial periods for this service. A minimum term of 1 month and a minimum of 10 users are required to establish the trial.
For more information contact

Kelvin Ayre

gcloud@scc.com

0121 766 7000