## RM6118 Service Description

### Service Overview

The service includes all Client and Payee User Interfaces and Transaction services.

**Client User Journey**

The Client

**Payee User Journey**

The Payee

## Service Security

**Security Architectural Principles**

The Service Provider should adhere to the CCS Service Security Architectural Principles and as a Government service it will need to be delivered and operated under the HMG Security Policy Framework <https://www.gov.uk/government/publications/security-policy-framework>. In order to be able to consume a solution with the confidence, each HMG Department and CCS Suppliers has developed bespoke security profile which they expect the service to be assured against. However, in order that Crown Commercial is able to deliver common goods and services across Government, there is a need to define a common set of security controls.

The service provided must be ***designed*** *to achieve the following****security goals***:

* make an initial compromise of the system difficult
* limit the impact of any compromise
* make disruption of the system difficult
* make detection of a compromise easy

An attacker can attempt to subvert **technology,  people and processes** to undermine security, so security architecture must consider all the technology, people and processes relating to the service.

In support of achieving the security goals, outlined above, the service provider shall undertake the following security controls:

* Incorporate the security standards defined with the Crown Commercial Service Digital and Technology Strategy into the Service Specification. <https://intranet.crowncommercial.gov.uk/task/digital-and-technology-strategy-2018-21/>
* Evidence compliance with the HMG Minimum Cyber Security Standard <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard>
* Demonstrate delivery of the NCSC Cloud Security Principles outcomes <https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles>
* Evidence the Software Delivery Life cycle is undertaken securely through the application of the NCSC Secure Development and Deployment guidance.<https://www.ncsc.gov.uk/collection/developers-collection?curPage=/collection/developers-collection/principles>
* An CHECK/CREST IT Security Health Check (ITSHC) of the Service has been performed within 12 months of go-live and annually thereafter. The testing has been undertaken in accordance with HMG best practice. <https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance>
* Comply with the CCS Supplier Information Security Assurance Policy ref ##

The Supplier shall nominate an individual who is responsible for ensuring achievement of the security goals described above and will work will CCS to ensure these are acted upon.

**Data Management**

It is the responsibility of the Service Provider to ensure that all data obtained through this Agreement is kept up to date, accurate and is held and maintained within a secure system in the EEA or in a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. We believe there may be higher Client take up if the Service is hosted in the United Kingdom, but this only not a must have requirement. The data shall be provided to the Authority as and when required, and in a format specified by CCS

### Transaction Security

It is the responsibility of the Service Provider to ensure all data collected through this Contract is classified as OFFICIAL SENSITIVE under the Government Security Classifications Scheme. Further information can be found on the following link: <https://www.gov.uk/government/publications/government-security-classifications>

All employees who will be handling data collected as part of this Contract will be required to undergo basic recruitment checks, applying the requirements of the HMG Baseline Personnel Security Standard (BPSS) for all individuals with access to OFFICIAL SENSITIVE information. Further details can be found on the following link: <https://www.gov.uk/government/publications/hmg-personnel-security-controls>.

CCS reserves the right to request, and you should upon that request, undertake a further Security Check (SC) clearance for those individuals who have access to the entire data set or frequent and uncontrolled access to SECRET assets and/or occasional, supervised access to TOP SECRET assets.

The Service Provider should be able to demonstrate to CCS, at any time, that the business solutions meet the required levels of personal, procedural, policy, data and technical security as set out in this Specification and the Concession Contract.

The Service Provider must meet a minimum security standard of Cyber Essentials accreditation by Go Live Date. Further information can be found on the following link:

<https://www.cyberaware.gov.uk/cyberessentials/>

Software that interconnects with HMG systems or manage HMG data will be required to undergo assessment to identify technical risks. Proportionate assurance processes shall be demonstrated to provide confidence that these identified risks are properly managed.

The Service Provider will be required to demonstrate evidence of Cyber Security procedures at the relevant milestones as scheduled in schedule 9 of the Contract.

CCS will work with you as required to ensure the proportionality of the contract and establish the:

* accreditation/assurance plan prior to Go Live Date and during the Term of the Agreement;
* Roles and Responsibility of the various Stakeholders within the Organisation.

Before the Service Live Date and annually thereafter, the Service Provider will be required to undertake CHECK Assurance with an approved National Cyber Security Centre provider in accordance with Schedule 9. More information can be found on the following links:

<https://www.ncsc.gov.uk/scheme/penetration-testing>

<https://www.ncsc.gov.uk/articles/using-check-provider>

The Service Provider should comply with all current and future legislation appropriate to the secure operation and use of IT systems in providing services and systems to Clients.

Where the Service Provider proposes to use sub-contractors to provision part of the services and systems and these sub-contractors will be involved in handling commercially sensitive and/ or personal information with regard to the services and systems, such sub-contractors shall also be compliant with the above data security requirements.

The Service Provider must comply with the forthcoming EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018 when they come into force on 28 May 2018.

## Service Provision

**Service Documentation**

Documentation for the service should cover the setup, management and configuration of the service. Documentation must be aligned with the current version of the service. Documentation must be available online and via PDF’s, and ideally be supported by a demonstration site.

**Service Environments**

**Sandbox:** The Service should include a test or Sandbox environment for Clients. This will allow a Client to setup and test service usage without incurring fees. Switching from Sandbox to Production should be minimal effort for the Client.

**Production:** The service must include a live or Production environment for Clients. This will be used for live transactions.

**Client Onboarding**

Clients should be able to plug-in the service using REST API’s. The Onboarding process should be as simple as possible and be configurable without changing code in the service.

**Client Offboarding**

At the end of the service contract period Clients should be able to manage (test, schedule and end) the transition from the current service to any new service provider without incurring additional costs, unless this is part of the contract agreement. The Client will be considered offboarded 30 days after their last transaction has been completed and any dispute period finished.

**Service Availability**

The service should be available 99.8% of the time; outside published and scheduled service maintenance times, and security patches/updates times. Clients should be notified of all scheduled/unscheduled service outages and availability figures published on a regular basis.

**Service Updates**

The Service Provider must ensure that any updates to the service are fully tested and secure before being applied. Unless Clients are notified and given the opportunity to test and schedule service updates, any service update must not impact on a Clients production environment. The service should be extensible by design and free to contracted Clients of the Service.

**Service Disputes**

The Service provider must have a dispute management process to support Clients. This must cover disputes between Client and Payee and Client and Service Provider. The Dispute process should be documented and regularly reviewed.

**End of Service Provision**

End of service provision will be enacted 30 days after the last contracted Client of the service is offboarded (see above). As part of the service termination, all Client data must be securely removed (see GDPR) and transactions logs cleared. Any end-of-service costs should be covered by the Service Provider within the Commercial Agreement, if not these costs must be covered in the Commercial Agreement.

**Service Termination**

If for any reason the Service Provision is Terminated whilst Clients are still in Production, the service provider must complete all transactions, including the dispute period, and allow the bulk transition of Clients onto a new service provider or via a managed termination of service process. Any Service Termination costs should be covered by the Service Provider within the Commercial Agreement, if not these costs must be covered in the Commercial Agreement.

## Service Usage

### Payee Onboarding

The service must allow a Payee to be on-boarded onto the service for free. The service must adhere to the FCA regulations that apply to the service provision. Payees that share Clients should be able to setup multiple payments without creating multiple service accounts.

### Payee Offboarding

The service must allow a Payee to close their account without incurring costs. All transactional data and history must be removed in accordance to GDPR and FCA regulations.

### Payee Disputes

The service must provide dispute management capabilities between the Client and Payee.

### Payee Refunds

The service must provide refund capabilities between the Client and Payee.

## Management Information

**Transaction Data**

To support disputes, refunds and report each Client/Payee transaction should be traceable and uniquely identified. Once a transaction is deemed to be completed; outside the dispute period and reported, the transaction data should be sort for Client and CCS reporting, however no account data should be available as per GDPR and/or FCA regulations. Storage of historical account data should be available without cost to Clients and Payees.

**Management & Usage Reporting**

The service provider should on an agreed and scheduled basis provide CCS with usage reports covering transactional and historical data. This should include the transaction ID, Payee ID, Client ID, Transaction Date, Amount and any reference information but NOT account data.

## Service Support

**Customer Service**

The Service Provider should provide a free of charge dedicated helpdesk service that complies with the following service description:

1. Operate from 09:00 - 17:30, Monday to Friday (excluding Public Holidays);
2. Provide out of hours capability for leaving voice messages to request assistance.
3. All calls shall be answered in accordance with defined Required Service Levels and Key Performance Indicators;
4. Maximum charge for calls shall be at standard network rate (excluding premium rate telephone numbers)
5. It is your responsibility to ensure all persons working on the Customer Service Desk are suitably trained and have the security clearance required. Security clearance requirements are detailed on the following link: <https://www.gov.uk/government/publications/security-policy-framework>

**Complaints Procedure**

It is the responsibility of the Service Provider to ensure a robust and auditable complaints procedure is implemented. This shall include, logging, investigating, managing, escalating and resolving complaints.

The complaints handling systems should be documented and a summary report on complaints received should be available on request, or as part of a service review meeting.

All complaints shall be logged and acknowledged within twenty four (24) hours of receipt. All complaints shall be resolved within five (5) working days of the complaint being raised. Any complaints that cannot be resolved in this timescale shall be communicated to the Buyer and escalated to the Supplier’s Account Manager and the Agreement Manager within Crown Commercial Service. A full audit trail of the complaints progress shall be maintained including actions and resolution timescales.

There should be an escalation procedure established for any complaints that have not been resolved within the specified timescale. Escalation procedures and timescales should be reviewed monthly.

**Continuous Improvement**

The Service should be continually improve throughout the Contract duration to deliver efficiencies, improvement and innovation opportunities.

The Service Provider should present new ways of working and innovation to CCS during Review meetings, in accordance with the requirements set out in the Contract.