### Attachment 10b - Framework Schedule 1 (Specification Appendix B) Lot 6 Additional Technical Requirements

### Overview

* 1. The service includes all Buyer and Payee User Interfaces and Transaction services.

### Buyer User Journey

* 1. The Buyer User Journey shall be developed between the Authority and the Supplier during agreed consultation phase of the Implementation Period.

### Implementation Period

* 1. The Implementation Period means the period after the Framework Award Date during which the Co-Design will be agreed and the date you will implement the Specification and Co-Designed services for User Acceptance Testing (Lot 6 Go-Live date).
  2. Within the first three weeks of the Implementation Period, You shall appoint an implementation team with a named implementation manager who shall have a minimum of two (2) years’ experience in a relevant Payment Acceptance and online portal environment to develop the Co-Design stage and start to develop the Buyer Journey.
  3. The timings of Co-Design shall be agreed between Us and You in the period of collaboration as set out in paragraph 3.2 above.
  4. Resources must be maintained during the implementation period irrespective of other Framework Supplier activities.
  5. The objective of Co-Design is for the Authority and the successful Tenderer (Supplier) to develop and agree an ambitious and viable proposition that would successfully provide the support that the Authority and Buyers require, which includes those areas highlighted in this Appendix B, set out in Framework Schedule 1 (Specification) and Appendix A – Technical Requirements, including, but not limited to, the following (the timings of Co-Design are to be clarified in due course):
     1. The extent of the Authority’s obligations under the Contract;
     2. The impact of the Services on Buyers;
     3. Services’ innovation;
     4. The use of technology to support Buyers;
     5. Changes in the Services;
     6. Branding of Services;
     7. Collaborative marketing approach;
     8. Buyer focus groups User Acceptance Testing and creating a Buyer journey to suit Buyers; and
     9. Any additional design of the Services

## Service Security

### Security Architectural Principles

* 1. 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>.

* 1. 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.
  2. The service provided must be ***designed*** *to achieve the following minimum****security goals***:
     1. make an initial compromise of the system difficult;
     2. limit the impact of any compromise;
     3. make disruption of the system difficult; and
     4. make detection of a compromise easy
  3. An attacker can attempt to subvert **technology, people and processes** to undermine security, a Supplier’s security architecture shall consider all the technology, people and processes relating to the service.
  4. In support of achieving the security goals, outlined above, the Supplier shall undertake the following security controls:
     1. Incorporate the security standards defined with the Crown Commercial Service Digital and Technology Strategy into the Service Specification. 
     2. Evidence compliance with the HMG Minimum Cyber Security Standard <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard>
     3. 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>
     4. 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>
     5. 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>
     6. Comply with the relevant Supplier Information Security Assurance Policy
  5. The Supplier shall nominate an individual who is responsible for ensuring achievement of the security goals described above and will work with the Authority to ensure these are acted upon.

### Data Management

* 1. 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.
  2. We believe there may be higher Customer take up if the Service is hosted in the United Kingdom, but this is not a mandatory requirement.
  3. The Supplier shall provide the data to the Authority as and when required, and in a format specified by the Authority.

### Transaction Security

* 1. 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>
  2. 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>.
  3. 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.
  4. 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.
  5. 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/>

* 1. 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.
  2. 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.
  3. CCS will work with you as required to ensure the proportionality of the contract and establish the:
     1. accreditation/assurance plan prior to Go Live Date and during the Term of the Agreement;
     2. Roles and Responsibility of the various Stakeholders within the Organisation.
  4. 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>

* 1. 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 Customers.
  2. 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.
  3. 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

* 1. 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

* 1. **Sandbox:** The Service should include a test or Sandbox environment for Customers. This will allow a Customer to setup and test service usage without incurring fees. Switching from Sandbox to Production should be minimal effort for the Customer.
  2. **Production:** The service must include a live or Production environment for Customers. This will be used for live transactions.

### Customer Onboarding

* 1. Customers 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.

### Customer Offboarding

* 1. At the end of the service contract period Customers 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 Customer will be considered offboarded 30 days after their last transaction has been completed and any dispute period finished.

### Service Availability

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

### Service Updates

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

### Service Disputes

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

### End of Service Provision

* 1. End of service provision will be enacted 30 days after the last contracted Customer of the service is offboarded (see above). As part of the service termination, all Customer 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

* 1. If for any reason the Service Provision is Terminated whilst Customers are still in Production, the service provider must complete all transactions, including the dispute period, and allow the bulk transition of Customers 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

* 1. 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 Customers should be able to setup multiple payments without creating multiple service accounts.

### Payee Offboarding

* 1. 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

* 1. The service must provide dispute management capabilities between the Customer and Payee.

### Payee Refunds

* 1. The service must provide refund capabilities between the Customer and Payee.

## Management Information

### Transaction Data

* 1. To support disputes, refunds and report each Customer/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 Customer 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 Customers and Payees.

### Management & Usage Reporting

* 1. 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, Customer ID, Transaction Date, Amount and any reference information but NOT account data.