Specification

Payment Gateway Services

OCSD/ITS

**Contract Reference: PS/20/48**

**Date: 22/02/2021**

**Version: 0.14**

[1. Introduction 3](#_Toc64889549)

[2. Background to the Requirement 3](#_Toc64889550)

[3. Procurement Timetable 3](#_Toc64889551)

[4. Scope 4](#_Toc64889552)

[5. Implementation and Deliverables 4](#_Toc64889553)

[6. Specifying Goods and / or Services 5](#_Toc64889554)

[6.1 Functional 5](#_Toc64889555)

[6.2 Service Provision 11](#_Toc64889556)

[6.3 Testing and Integration 15](#_Toc64889557)

[6.4 Merchant Acquirer Integration 15](#_Toc64889558)

[6.5 Service Monitoring 17](#_Toc64889559)

[6.6 Reporting, Refunds and Queries 18](#_Toc64889560)

[6.7 Service Levels and Service Credits 20](#_Toc64889561)

[6.8 Future Services 22](#_Toc64889562)

[6.9 Social Value 22](#_Toc64889563)

[6.10 Prompt Payment Considerations 24](#_Toc64889564)

[6.11 Supply Chain Visibility 24](#_Toc64889565)

[6.12 Management Charges and Information 25](#_Toc64889566)

[7. Quality Assurance Requirements 25](#_Toc64889567)

[8. Other Requirements 26](#_Toc64889568)

[9. Management and Contract Administration 33](#_Toc64889569)

[10. Training / Skills / Knowledge Transfer 38](#_Toc64889570)

[11. Arrangement for End of Contract 38](#_Toc64889571)

[12. Evaluation Criteria 39](#_Toc64889572)

[13. Points of Contact 43](#_Toc64889573)

[14. Annexes: 44](#_Toc64889574)

[Annex 1 – Evaluation Criteria: 44](#_Toc64889575)

Annex 2 - [MTC Schedule 20: Schedule of Processing, Personal Data & Data Subjects Schedule [X]: Schedule of Processing, Personal Data & Data Subjects 50](#_Toc64889576)

Annex 3 – Pricing Schedule 52

## 1. Introduction

The Department for Transport (DfT) invites proposals for the following **SERVICES**. This contract will be subject to the Cabinet Office Mid-Tier Contract Terms and Conditions (MTC)

The Driver and Vehicle Licensing Agency (DVLA) is an Executive Agency of the Department for Transport, based in Swansea and employs around 5,000 staff. The Agency’s primary aims are to facilitate road safety and general law enforcement by maintaining accurate registers of drivers and vehicle keepers and to collect Vehicle Excise Duty.

## 2. Background to the Requirement

DVLA currently takes payments for a number of online and telephone services including Electronic Vehicle Licensing, Personalised Registrations, Driving Licence applications and Penalty Payments totalling around 28 million payment transactions per year.

DVLA requires a Payment Card Industry (PCI) compliant payment gateway that complies with banking standards, aligns with our customer needs and is able to integrate seamlessly into digital and telephony services.

The Payment Gateway must provide multi-channel support across online and telephony payments, with customisable hosted payment pages or iFrame, usable on a variety of devices, including mobile devices, in both English and Welsh.

The solution must provide a PCI compliant payment authorisation and settlement platform that is able to handle peak loads of 120 transactions per second with 24/7/365 availability. Incident support must also be available 24/7/365 for Priority 1 and 2 incidents as a minimum.

## 3. Procurement Timetable

|  |  |
| --- | --- |
| **Description**  | **Date** |
| ITT Pack Issued | 18th March 2021 |
| MS Teams Call to Discuss Pricing Schedule with Bidders\* | 23rd and 24th March 2021 |
| Clarification Questions End Date | 2nd April 2021 |
| Responses | 16th April 2021 |
| Analysis/Evaluation | 14th May 2021 |
| Award | 16th August 2021 |
| Transition Period  | 16th August 2021 – 30th April 2022 |
| Current Contract Expires | 30th April 2022 |

\*There is the option to have a Microsoft Teams meeting or telephone conference with DVLA to discuss completion of Annex 3 (Pricing Schedule).

There are several hourly slots available on 23rd and 24th March 2021 as follows:

• Slot 1 – 23rd March 2021 at 12:00hrs-13:00hrs

• Slot 2 – 24th March 2021 at 13:00hrs-14:00hrs

Please arrange with the Procurement Contact listed in Section 14 Points of Contact, to book your slot, if you would like to take up this opportunity by 15:00 hours on 22nd March 2021.

## 4. Scope

This service will be used for DVLA’s online and telephony channels for services including, but not limited to, Electronic Vehicle Licensing, Personalised Registrations, Driving Licence applications and Penalty Payments.

DVLA services total circa 28 million payment transactions per year currently. This is expected to increase in the future as new digital services are introduced and digital uptake increases.

DVLA have prepared a probability analysis of the volume of payment card traffic that is anticipated over the duration of the contractual term, which is embedded below for consideration:



DVLA are keen to ensure that new payment methods and technologies are explored and used where these are of benefit to customers throughout the life of the contract, including but not limited to:

* Support for digital wallet transactions including mobile transactions (e.g. Apple Pay, Android Pay etc).
* Support for open banking transactions

## 5. Implementation and Deliverables

The service will need to be in place and fully operational on 01 May 2022 when the current agreement expires.

The contract for this service will commence on 01 May 2022 and be for a duration of 3 years with two optional 12-month extension periods to be agreed annually.

The deliverables for this service are detailed in Section 6.

The Solution Provider shall work with the Authority and Authority’s existing Merchant Card Acquiring Services and Payment Gateway Services to agree their implementation plan or plans if appropriate to transition to the Payment Gateway Services as required by the Authority including, if required, providing support for migrating any existing recurring payments received by the Authority’s’ existing Payment Gateway Services and existing Merchant Card Acquiring Services but transition is not mandated.

The Contractor shall provide a detailed implementation plan. This shall include but not be limited to:

* Communications
* Training (encompassing both Contractor staff and any training necessary for the Authority if appropriate)
* Milestones; and
* Milestone Dates.
* Demonstrate how this implementation plan will provide an effective transition from the current service providers to the new contracted service.
* TUPE if applicable

## 6. Specifying Goods and / or Services

The overall mandatory requirements for this service are as follows

### 6.1 Functional

* The solution must provide a PCI DSS Level 1 Certified Payment Authorisation and Settlement Platform that meets the following requirements.
* The Supplier must provide evidence of the PCI DSS certification

The solution must:

* be able to handle, as a minimum, DVLA’s peak business volumes 120 Transactions Per Second (TPS) and average load of 30 TPS
* be available 24/7/365 in the live environment with a minimum of 99.7% availability per month for all users. The Authority seeks to procure a service that consistently exceeds this, and the Supplier must provide detail of their actual expected availability
* be supported 24/7/365 for, as a minimum Priority 1 and 2 incidents.
* provide confirmation of settlement no later than 6am on the calendar day following the transaction for payment reconciliation. This must be by transaction for each business service.

**6.1.1 User Facing**

**6.1.1.1 Mandatory Requirements**

The Supplier will provide a solution which:

* + Provides one or more seamless mechanisms for transition from the Authority’s website to the Payment Gateway Services so it appears to the Payer that they are still on the Authority’s website and these mechanisms shall be specified e.g. hosted payment page. The transition shall include ensuring that the Payer is aware that they are entering a secure environment.
	+ Provide a Customisable Hosted Payment Page and/or iFrame. The Payment Gateway pages for Payers can be customised, by the Supplier and/or the Authority. This includes, but not necessarily limited to, the customisation of:
		- Card type acceptance including ordering of card types
		- APMs
		- Copy
		- Branding
		- Logos
		- Colour schemes
		- Fonts
		- Phrases
		- Wording
		- Contact details
		- Currencies
* The Supplier shall provide details of all encrypted (TLS 1.2 and subsequent as amended from time to time, for example, TLS 1.3 as now defined in IETF RFC 8446, August 2018 or other approved secure industry standard). Integration mechanisms for use by the Authority.
	+ frame
	+ Hosted payment page
	+ Mobile SDKs
	+ Silent order POST
	+ Other.
* The Supplier shall provide the Authority with a well-documented real time HyperText Transfer Protocol Secure (HTTPS) Application Programme Interface (API) to capture payment details through their own payment pages or equivalent before the Transaction is processed.
	+ Be available in both English & Welsh and allow the customer to complete the full journey in their chosen language.
	+ Be both desktop and mobile friendly
	+ Be compatible with the majority of common browsers such as, but not limited to, Google Chrome, Mozilla Firefox, Opera, Microsoft Edge, Microsoft Internet Explorer 11, Safari and Samsung Internet. As a minimum, the service will have an equivalent level of browser support to GOV.UK.
	+ Payment Gateway pages rendered correctly for compatibility with devices with variable screen sizes, including, but not necessarily limited to:
		- Desktops
		- Laptops
		- Smart phones
		- Tablet devices
		- Other software only devices as standards allow now and, in the future,
		- Other.
	+ Align with the appropriate GDS style guide or any other style guide defined by DVLA.
	+ Ensure that all PSP related payment pages are accessible and adhere to a minimum of WCAG (Web Content Accessibility Guidelines) 2.0 level AA and UK Equality Act (2010) legislation as updated from time to time.
	+ Support for all major card schemes including for example Visa Credit and Debit, Mastercard Credit and Debit, American Express and be able to configure acceptable card issuers on a service by service basis.
	+ allow users to store cards and re-use and remove (and/or edit) stored cards where applicable to that transaction
* If required by the Authority, the Supplier shall provide the Authority with auto populated or manual entry payment page(s) in order to capture the data required to process payments and provide the Authority with the relevant reporting information, but not necessarily limited to, the following fields:
	+ PAN (15 to 19 digits)
	+ CSC (3 & 4 digits)
	+ Amount
	+ Expiry end date
	+ Individual Payer name
	+ Authority identifier (Company ID (CID))
	+ Authority Transaction description reference
	+ Start date (where required)
	+ Secure link to APM providers as required by those providers or any other regulatory standards
	+ Authority Payer identifier
	+ Items/services purchased
	+ Email address
	+ Individual Payer billing address including post code.
* The Supplier shall support a mechanism to enable the Authority to take Cardholder Not Present transactions in a call centre environment including IVR (which may be run by a 3rd party or the Authority), usually referred to as Mail Order/Telephone Order and Supplier shall state how they support this mechanism being PCI-DSS compliant.

**6.1.1.1 Optional Requirements**

* The Supplier shall provide The Authority with the option to automatically confirm payment with the Payer via email and where required manage all communication with the Payer.
* Where required, the Supplier shall provide the Authority with the functionality to customise receipt emails. shall be able to customise the following as a minimum, but not necessarily limited to:
	+ Branding
	+ Text
	+ Contact details
	+ Website details
	+ Web links to enquiry forms.

**6.1.2 Non-User Facing**

**6.1.2.1 Mandatory Requirements**

The Supplier will provide a solution which:

* + Provides encryption and submission of card payment data captured through hosted payment pages, including the onward submission of transaction authorisation and settlement requests to specified third parties (e.g. acquirers, card providers).
	+ Provides all necessary validation, authorisation and settlement functions required to support the service including agreed cut off times
	+ Delivers settlement files directly to the DVLA’s acquirers via the relevant acquirer’s network, in the format agreed with the relevant acquirer.
	+ Is hosted on a resilient and fault tolerant platform.
* Provide details of secure, encrypted (as above) API integration connections from other PCI compliant Level 1 Service providers.
* The Supplier shall ensure a secure connection (TLS 1.2 standard and as amended and upgraded from time to time, for example, TLS 1.3 as now defined in IETF RFC 8446, August 2018 or other approved secure industry standard) is used between the Authority’s website, the Authority’s’ points of presence, and the Supplier’s Payment Gateway Services at all times. This connectivity shall be of sufficient capacity and shall cover, but shall not necessarily be limited to:
	+ Internet connection
	+ Any emerging connectivity of sufficient security and capacity
	+ Broadband
	+ MPLS
* Provide the facility to accept and securely process recurring and repeat payments through the Payment Gateway Services as required.
* The Supplier shall apply an administrative fee in line with DVLA requirements based on payment card type.
* Support card authorisation using industry standards for CVV2 verification and 3D secure authentication (3D Secure 1.0 and EMVCO 3-D Secure 2.2 as amended or replaced)
* Support non-3d Secure payments until such a time that these become obsolete.
* Provide Industry standard fraud prevention and detection tools.
* Conform to latest GDPR and Industry Payment Services regulations (e.g. PSD2).
* Provide tools and integrations to support full reconciliation of all systems.
* Multi-channel support – online (ecommerce) and telephone (MOTO) transactions (both via an agent and an automated IVR system).
* Supplier shall provide a mechanism so that cardholder data and sensitive authentication data does not necessarily need to pass through the Authority’s main computers
* Supplier shall provide a mechanism where Cardholder data shall be returned to the Authority as a one-to-one mapped token which can be stored by the Authority main computers and a masked PAN showing only the first 6 and last 4 digits, or optionally only the last 4
* Supplier is responsible for converting token on reuse to a PAN to enable subsequent payments without Payer needing to enter PAN details and so facilitating one-click payment
* Supplier cannot retain PCI-DSS defined sensitive authentication data except for a strictly limited period, example 15 minutes as allowed by PCI standards.
* Supplier shall provide a mechanism to tokenise cardholder data out with a payment
* Supplier shall provide a mechanism to bulk tokenise the Authority’s existing cardholder data, with PCI compliance, to assist in any necessary transition from an existing Supplier to the new Supplier
* Supplier shall provide for secure communication from Authority point of presence equipment and will generate a token and masked PAN as for payment pages. Identical PANs will generate the same token across payment pages and point of presence (all channels) to allow true omni channel operation and post purchase MI
* Supplier shall state whether they use a 3rd party external tokeniser or a 3rd party in-house tokeniser or a Supplier developed own tokeniser
* Supplier’s tokenisation services shall be selectable by service for the Authority.
* The Supplier shall, where requested by the Authority in the Call Off, allow for encrypted API connection, with full transaction data including sensitive payment card or APM details from another PCI compliant Level 1 Service provider,
* The Payment Gateway Services will provide a mechanism to alert the Authority by secure API or alternative secure mechanism if the status of a transaction changes after authorisation or settlement and the Authority will not be obliged to use any or all of these mechanisms.

**6.1.2.2 Optional Requirements**

* Supplier shall provide a mechanism that exposes card scheme Payment Account Reference (PAR) values where card have been stored in ApplePay or G Pay devices, as these stored PANs do not equal original cardholder data
* Supplier shall state whether they would consider providing token services to other gateways
* The Supplier shall state what mechanism and 3rd party systems they support to enable PCI-DSS compliance in the Authority’s call centre environment, for example, DTMF masking, IVR.

### 6.2 Service Provision

**6.2.1 Mandatory Requirements**

* The solution, and provider, must have the ability to update and adapt to changes in technology and legislation and work with the Authority to implement these.
* The solution, and provider, must have the ability to update and adapt to changes in requirement as a result of customer feedback, Authority requirements or changes in the payment industry.
* The Supplier shall ensure that Payment Gateway Services and systems provided to Authority to take payments are in line with current industry standards in order that the Payment Gateway Services will reliably process each transaction within defined service levels (see Section 6.7 ) excluding time outboard of the Payment Gateway Service to Supplier’s Merchant Card Acquiring Service providers, card scheme networks and APM providers.
* The Supplier shall ensure that there is a segregation of the Authority’s data and that of any other merchants to avoid exposing the Authority’s data to unauthorised third parties.
* The Supplier shall apply all SCA exemptions, where allowed and requested by the Authority, on transactions and shall specify to the Authority how they take advantage of the SCA exemptions allowed under PSD2.

The solution provider will:

* Provide a dedicated service management function.
* Provide a defined escalation process.
* Have a defined incident management handling process including communication plans, prioritisation levels, response and resolution targets and root cause analysis.
* Maximum amount and duration of scheduled maintenance must not exceed levels agreed with the Authority at the call off stage, normally this would not exceed three hours in any calendar month.
* Provide appropriate notice, timescales to be agreed with the Authority depending on complexity, where testing or changes are required by the Authority to their systems. The Supplier must demonstrate how they will provide a forward view to the Authority or all planned and anticipated changes.
	+ Where a change is purely on the Supplier side, a minimum of 5 working days’ notice must be given, unless otherwise agreed with the Authority by exception.
	+ Where change will also be required to be carried out by the Authority, a minimum of three months’ notice would be expected to be given to the Authority, unless otherwise agreed with the Authority by exception.
* Must adhere to ISO/ISEC 27001 standards or equivalent
* Provide a detailed change process demonstrating how they will deliver changes to the solution in response to both Authority and industry led developments.
* Audited system changes by supplier must be recorded and available throughout the life of the contract. These must be made available to the Authority within a reasonable timescale as agreed with the Authority at the time.
* Inform the Authority of new payment innovations and methods that become available and make such innovations and methods available in order that they can be implemented by the Authority if required
* Inform the Authority of new payment initiatives, mandates and/or regulations and impact assess these against these against the provision
* Provide the Authority with details and information of new APMs as and when they become available within their offering and shall ensure that if required by the Authority Payment Gateway Services can accept them
* Support a request to provide the Authority with details of new card IIN (BIN) ranges, and the IIN (BIN)s of Card Schemes in use, as and when they are provided by the Card Schemes and Supplier’s Merchant Card Acquiring Service providers, and shall ensure that there is no constraint imposed by the Supplier on the Authority acceptance of the new IIN (BIN)s and IIN (BIN) ranges from the date they are available in the market and Supplier shall state the mechanisms for provision including by file transfer and by API .
* Provide a list of commercial and corporate BINs to allow the surcharging of these card types

Provide a dedicated business and technical helpdesk relevant to the Services, accessible by either phone, SMS, email and/or online portal, to include but not necessarily limited to:

* Incidents
* Problems
* Alerts
* Queries
* Payer queries
* Software
* Hardware
* Complaints

A Help/Service desk or equivalent must be available 24x7 365 days a year for call logging for, as a minimum, P1 and P2 incidents

The Supplier must define how they prioritise calls and incidents in relation to this service. The Supplier must specify their response times for initial response, updates, and resolution.

For example:

Priority 1 Emergency situation; critical impact

Priority 2 Severe failure and loss of resilience; no work-around possible. Testing environment outage

Priority 3 Function affected: otherwise operational

Priority 4 Minor fault; generally, fully operational

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Priority 1 | Priority 2 | Priority 3 | Priority 4 |
| Initial Response | 30 mins | 1 hour | 4 hours\* | 1 Working Day |
| Update interval | 1 hour | 2 hours | 12 hours\* | Weekly |
| Resolution | 2 hours | 4 hours | 1 week | 2 weeks |

\*Within business hours Mon-Fri 8am to 5pm excluding Bank Holidays.

The Supplier shall provide support to the Authority and where applicable the Authority’s other providers within an agreed timetable and including, but not necessarily limited to:

* Set-up of MIDs
* Set-up of TIDs
* Adding to existing MIDs and TIDS, as required
* Supply and interfacing to of hardwired PDQ Terminals (including Contactless)
* Supply and interfacing to of wireless PDQ Terminals (including Contactless)
* Supply and interfacing to of Bluetooth PDQ Terminals (including Contactless)
* Electronic PDQ card payment terminals (including Contactless)
* MPOS equipment
* Data transmission to the supplier
* Interfacing with varying front and back end technology
* Interfacing with contactless alternatives
* Alternative card charging mechanisms
* Fraud minimisation
* Risk management systems
* Incident management
* Reporting files and systems
* Changes in card interchange rates and scheme fees
* Chargebacks
* Information on changes in legislation affecting the Payment Gateway Services
* Technical support and incident management
* Interaction and support with third party suppliers
* Connectivity to Merchant Card Acquiring Services
* Help prevent identified individual Payers from making payments
* Help to find details of payments made by individual Payers
* A dedicated technical helpdesk for in and out-of-hours telephone or email queries/issues
* System availability
* Declines optimisation
* Marketplace regulatory support to manage flow of funds through relevant FCA licenses and contracts with sub-entities
* Items/services purchased.
* Helping a Payer make and complete a payment
* The Supplier shall allow the Authority to sign contracts with APMs directly or to allow Supplier’s Payment Gateway to take settlement of the APM funds on its behalf (known as the Collect Model) and manage associated settlement risk, refunds etc. as if they were Card Payments
* The Supplier shall state whether they support any mechanisms to share their data. including tokens and fraud data with other Payment Gateways
* The Supplier shall respond in writing to all queries, including complaints, from the Authority within 3 Working Days, There may be some limited circumstances where an urgent reply may be required more quickly, in this event the Supplier will be required to work with the Authority to meet the required timescale as specified.
* The Authority is obliged to respond to ad-hoc Ministerial and other official queries (“Official Correspondence”) within strict timescales, for which a contribution from the Supplier may be crucial. In such cases, the Supplier shall provide such contributions in writing within the timescale agreed with the Authority at the point of request.
* **6.2.2 Optional Requirements**
* Provide a public facing web page showing the status of their service and any incidents or issues affecting it at that time.

**6.3 Testing and Integration**

* **6.3.1 Mandatory Requirements**
* The solution provider must provide detailed integration documentation and support via face to face or telephone as appropriate.
* The provider will work with DVLA to test and integrate with any new products and services.
* The Supplier shall provide, a sandbox environment for the Authority and, and where integration is required with other suppliers, its other providers to allow for production-like testing of integration and new releases, including the use of any identifiers that are in use for the production environment and to allow for penetration testing to verify the end-to-end security of the integrated and test accounts
* Environment availability and account set up must be provided in line with the Service Levels specified in Section 6.7

###  Merchant Acquirer Integration

**6.4.1 Mandatory Requirements**

* Integrate with any Merchant Acquirer used by the Authority so that the Authority are not required to invest in a bespoke network or new infrastructure to facilitate the Merchant Card Acquiring Service.
* Payment Gateway Services connectivity to any required Merchant Card Acquiring Service shall be secure and high capacity and shall cover, but shall not necessarily be limited to:
	+ - Internet connection
		- Any connectivity of sufficient security and capacity
		- Broadband
		- MPLS
* The Supplier shall assign a unique Identifier to the Authority. The unique Identifier used shall be agreed by the Supplier and Authority and will map to the Merchant Card Acquiring Service CID where appropriate.
* The Supplier shall engage and work with the Authority and Authority Merchant Card Acquiring Service providers and APM providers as required in order to set-up and assign merchant IDs (MIDs), Terminal IDs (TIDs), and groups of MIDs and TIDs, and other identifiers for APM providers and shall ensure that the set-up reflects the structure required by the Authority.
* Where a new MID is required this must be set up and available to use within 5 working days of the Authority’s request
* The Supplier shall link the Authority’ APM identifiers to specific Authority bank accounts where Supplier is operating a Collect model, where more than one APM settlement is aggregated by the Supplier for the Authority, and facilitate separation by, but not necessarily limited to:
* Lines of business
* Different teams
* Work streams
* Currencies
* The Supplier shall verify the accuracy of Authority’ MIDs and TIDs, and the required separation to ensure that the implementation is completed correctly.
* The Supplier shall not delete/purge any inactive MIDs or TIDs without express permission of the Authority.
* The Supplier shall ensure that the Authority can accept and settle transactions in GBP and where required into multiple MIDs and TIDs.
* The Supplier shall ensure the Authority can assign each Transaction a unique, custom identifier that shall be agreed by the Supplier and the Authority and shall be included in all dataflows and reports.
* The Authority shall be able to select a floor limit, in consultation with the Supplier and the Authority Merchant Card Acquiring providers including the Supplier’s and those as allowed under 3.4 above, including a zero limit that requires all transactions to be authorised to confirm sufficient funds are in the Payer’s account prior to the transaction being processed and an offline floor limit for use when the Merchant Card Acquiring equipment fails to communicate with the Supplier.
* The Supplier shall agree a process and other mechanisms with the Authority that shall allow only designated Authority personnel or their authorised representatives acting as agents to issue Refunds by manual intervention.
* Where the Authority own or rent Merchant Card Acquiring equipment that is used to accept payments under separate contracts, on the Authority’s authorisation, the Supplier shall work with the Authority’s third party suppliers, as if they are the Authority, to connect the Merchant Card Acquiring equipment to the Payment Gateway Services at a reasonable and non-discriminatory charge to be agreed by the parties, to ensure all payments are processed and to any issues are resolved in accordance with the Authority’s KPI’s and the Authority’s Service Levels.
* The Supplier will assist as required Authority additional Merchant Card Acquiring and Supplier’s Merchant Card Acquiring Service and additional Merchant Card Acquiring Equipment Service providers under 4.3 below and Supplier’s Merchant Equipment Service provider with configuring equipment to initiate end of day procedures or single message transaction submission when this becomes an industry standard
* When each Transaction is processed, the Payment Gateway Services shall facilitate authorisation of Transactions to provide the Authority with a response, including all codes allowed by card scheme and APM rules, indicating the status of each Transaction submitted, including, but not necessarily limited to
	+ Approve
	+ Decline
	+ Other APM responses as defined by the APM provider
	+ Refer
	+ Decline and pick up
* The Supplier shall ensure that for each unique Transaction reference, payment is only taken once enabling the Authority to notify the Payer accordingly with a customisable message written by the Authority in agreement with the Supplier.
* The Supplier shall ensure that any callback URL comes from a specified range of Internet Protocol (IP) addresses, which shall be communicated to the Authority, to enable the callback URL to be permitted through the Authority’ firewalls and validated within applications as an extra security measure.
* The Supplier shall allow The Authority to register different Uniform Resource Locators (URL) relating to receiving notification of either authorisation approval or decline.

### Service Monitoring

* **6.5.1 Mandatory Requirements**
* The Supplier shall provide a secure web-based interface hosted by the Supplier and remotely accessible to the Authority. This must provide the Authority with management reporting functionality including but not limited to:
	+ The ability to run real time and historic queries by service
	+ All transaction details by service
* The Authority must be able to export reports from the interface as detailed in Section 6.6
* The Supplier must provide detail of their service monitoring provision
* Where the Supplier detects unusual patterns of activity that might indicate malicious activities, for example a denial of service attack or distributed denial of service attack the Supplier shall inform the Authority’s designated security contact immediately by alerting via email and SMS.
* **6.5.2 Optional Requirements**
* The Supplier should provide the Authority with the functionality to monitor Supplier’s availability, transaction completion rates and Transaction timings.

###  Reporting, Refunds and Queries

* **6.6.1 Mandatory Requirements**

There must be a SaaS cloud solution with web service API (RESTful would be the preferred solution but not mandatory, Supplier must specify the type of API intended to be used) for authorisation, daily settlement, refunds, and enquiries.

* The Supplier shall provide a comprehensive range of standard reports which shall be clear and easy to understand, with the Authority able to specify the reporting hierarchy and a method of producing ad-hoc reports.
* The Supplier must provide details of how reports can be accessed via a portal and how reports will be sent to the Authority as required.

The Supplier shall provide Authority with a Refund report including any information required by Authority to execute a full or partial Reversal or Refund (credit to cardholder) of a Transaction easily, promptly and to the original payment method.

The Supplier shall provide a complete audit trail enabling Authority the ability to identify individual payments so all Refunds can be returned to the original payment mechanism.

* The Supplier must detail what secure methods will be used to send reports to the Authority (e.g. SFTP, secure email, etc)
* The Supplier shall provide a chargeback report.
* The Supplier shall ensure that an online system to manage Transaction data is provided to the Authority, the Supplier must specify any limitations in terms of data size or numbers of reports that apply.
* The Supplier shall provide the Authority with the facility to produce, download and export reports so that payment processes can be managed. Supplier must specify the format(s) in which these will be made available (e.g. Excel, CSV, space, or comma delimited, etc.)
* The Supplier shall provide The Authority with payment data and the facility to produce, download and export statements and reports by service so that The Authority can manage their payment processes.
* The Supplier shall provide The Authority with a report of processed Transactions by service to enable The Authority to update their accounting and cash management systems and to provide the capability to search for individual Transactions or groups of Transactions by, but not necessarily limited to, the following fields:
	+ Transaction data as above.
	+ Summary at various levels including but not limited to, – CID, MID, TID, Payment types (card/APM types), Gross payments/Gross refunds
* The Supplier shall provide The Authority with the reports above at various time intervals including but not limited to intraday (ad-hoc), end of day (by 07.00 on the next day), end of month, quarterly and annual.
* The Supplier shall provide The Authority with access to an online system to provide real-time access to view all card/Alternative Payment Method Transactions, including, but not necessarily limited to the transaction data above.
* The Supplier shall ensure that any online reporting system provided to The Authority does not limit the number and type of reports that can be generated and/or downloaded in any given period, or the number of times the Transaction status can be queried via a web interface or API.
* The Supplier shall ensure The Authority are able to obtain, at any time, an accurate real-time view of their Merchant Card Acquiring Services and APM payments.
* The Supplier shall provide The Authority with online access to a report, or provide a report in accordance with the Authority’ delivery methods and frequencies, with details including, but not necessarily limited to:
	+ Declined Transactions
	+ Lost Transactions
	+ Abandoned Transactions
	+ Drop offs
* Data must be kept real-time available before archive or secondary storage for a minimum of one year.
* Where data has been archived or placed in secondary storage, this must be able to be accessed and made available within one working day

Settlement status should be available in near real time (e.g. via API). Where this is not possible, a secure download of settlement data by individual transaction (whether gross or net settlement) to the Authority to include at least all debits and credits and any other information as agreed between the Supplier and the Authority before 07.00 UK time

### Service Levels and Service Credits

**Service Levels**

|  |  |
| --- | --- |
| Service Criteria | Performance Measure(Measured by Calendar Month except where noted) |
| Production (live) Service fully available for processing transactions over all channels **NB** Minimum acceptable availability is 99.7%, however the Authority seeks to procure a service that consistently exceeds this, and the Supplier should provide detail of their actual expected availability | 99.7% Scheduled maintenance within agreed limits is excluded from this calculation. |
| Response time per transaction does not exceed 1 second | 99% **measured daily** |
| 365/24/7 Helpdesk Availability for P1 and P2 calls  | 100%Scheduled maintenance may be excluded from this calculation |
| Business hours helpdesk availability for all other calls | 100%Scheduled maintenance may be excluded from this calculation |
| Helpdesk response times as agreed with the Authority | 100% |
| MID, TID and other business identifiers set up within 5 working days | 100% |
| Test accounts set up within 5 working days | 100% |
| Availability of reporting portal  | 99.8% |
| Change requests responded to within 10 working days. This will include a full impact assessment unless explicitly agreed with the Authority | 100% |
| Test environment availability for testing transactions over all channels  | 98% Scheduled maintenance within agreed limits is excluded from this calculation. |

**Service Credits**

|  |  |  |  |
| --- | --- | --- | --- |
| Service Criteria | Performance Measure(Measured by Calendar Month unless otherwise stated) | Service CreditPeak(as a percentage of monthly invoice)  | Service CreditOff Peak(as a percentage of monthly invoice) |
| Production (live) Service fully available for processing transactions over all channels  | 99.7% Scheduled maintenance within agreed limits is excluded from this calculation. | 20% Partial outages will attract a 10% credit  | 10%Partial outages will attract a 5% credit |
| Response time per transaction does not exceed 1 second | 99% **measured daily** | 10% | 5% |
| Test environment availability for testing transactions over all channels  | 98% measured by calendar monthScheduled maintenance within agreed limits is excluded from this calculation. | 5% | 5% |

Peak: 8am-10pm during first and last two days of any calendar month (Inc Bank Holidays)

Off Peak: All other times

### 6.8 Future Services

In addition, DVLA would also welcome your plans and solutions regarding how you would support and deliver future changes in the payment industry, including but not limited to:

* Support for digital wallet transactions including mobile transactions (e.g. Apple Pay, Android Pay etc).
* Support for open banking transactions

### 6.9 Social Value

The successful supplier will demonstrate how they deliver social benefits that support key social outcomes that are highlighted in the table below

Evaluation of the social value aspect of bids will ensure all potential suppliers, including SMEs, VCSEs and those new to government business, can successfully bid by describing what they will deliver and how they will deliver it (i.e. it is the quality of what is being offered that will count in the evaluation, not the quantity).

A weighting of 10% of the overall score has been allocated to social value and included in the Evaluation Criteria (Section 13).

|  |  |  |
| --- | --- | --- |
| **Theme** | **Policy Outcome**  | **Delivery Objective – What good looks like** |
| Fighting climate change  | Effective stewardship of the environment:1. Commitment to Net Zero Carbon Emissions
 | Activities that: Deliver additional environmental benefits in the performance of the contract including working towards net zero greenhouse gas emissions.  |
| Equal opportunity  | Tackle workforce inequality:1. Commitment to eliminate Gender Pay Gap
 | Activities that: Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce, particularly gender pay gap initiatives |
| Wellbeing | Improve community integration:1. Commitment to tackle digital and financial exclusion

Commitment to provide financial literacy training | Activities that: Demonstrate collaboration with users and communities in the co-design and delivery of the contract to support strong integrated communities, primarily around support schemes and assistance to reduce and/or prevent digital and financial exclusion Demonstrate collaboration with users and communities in the co-design and delivery of the contract to support strong integrated communities, primarily around support schemes and assistance to improve financial literacy  |

 **Social Value KPIs**

Progress on social value measures will be discussed and reported on as part of contract review meetings and the strategic supplier forum.

|  |  |
| --- | --- |
| Key Performance Indicator | Measurement |
| A net zero company will set and pursue an ambitious 1.5°C aligned science-based target for its full value-chain emissions. Any remaining hard-to-decarbonise emissions can be compensated using certified greenhouse gas removal. The boundary must be global scopes 1, 2 and 3 for the organisation. | Report on current position and annually report on rate of progress  |
| Publishing and monitoring pay gaps, and develop action plans to tackle the causes | Report on current position and annually report on progress towards reducing pay gaps by extending reporting to ethnicity and disability, and collecting annual statistics |
| A commitment to supporting financial capability schemes and initiatives within the UK | Number of people-hours spent supporting through volunteering or the amount of funding provided to underwrite the costs of schemes provided by MAS and other accredited bodies |
| A commitment to tackling financial and digital exclusion schemes and initiatives within the UK  | Number of people-hours spent supporting through volunteering or the amount of funding provided to underwrite the costs of schemes provided by Good Things Foundation, Joseph Rowntree Foundation, “leave nobody in the dark campaign and other similar schemes |

**6.10 Prompt Payment Considerations**

**Selection criterion:** If you intend to use a supply chain for this contract, you must demonstrate you have effective systems in place to ensure a reliable supply chain.

### 6.11 Supply Chain Visibility

Improving visibility of subcontract opportunities available to SMEs and VCSEs in the supply chain

 The Supplier shall:

6.11.1 (a) subject to clause 6.11.3, advertise on Contracts Finder all subcontract opportunities arising from or in connection with the provision of Services above a minimum threshold of £25,000 that arise during the Contract Period.

6.11.1 (b) within 90 days of awarding a subcontract to a subcontractor, update the notice on Contracts Finder with details of the successful subcontractor.

6.11.1 (c) monitor the number, type and value of the subcontract opportunities placed on

Contracts Finder advertised and awarded in its supply chain during the Contract

Period.

6.11.1 (d) provide reports on the information at clause 6.11.1(c) to a Contracting Authority in the format and frequency as reasonably specified by the Contracting Authority; and

6.11.1 (e) promote Contracts Finder to its suppliers and encourage those organisations to register on Contracts Finder.

6.11.2 Each advert referred to at clause 6.11.1 (a) above shall provide a full and detailed

description of the subcontract opportunity with each of the mandatory fields being

completed on Contracts Finder by the Supplier.

6.11.3 The obligation at Clause 6.11.1 (a) shall only apply in respect of subcontract opportunities arising after the contract award date.

6.11.4 Notwithstanding clause 6.11.1, the Contracting Authority may by giving its prior written approval, agree that a subcontract opportunity is not required to be advertised on Contracts Finder.

**6.12 Management Charges and Information**

In addition to any other management information requirements set out in this

Contract, the Supplier agrees and acknowledges that it shall, at no charge, provide

timely, full, accurate and complete SME Management Information (MI) Reports to the Authority.

## 7. Quality Assurance Requirements

The solution provider will demonstrate how that they have an effective quality assurance system in place and demonstrate that they meet ISO9001 or equivalent standards.

The Supplier must demonstrate that they meet ISO 20022 or equivalent standards.

The Supplier must be authorised and regulated by the Financial Conduct Authority

## 8. Other Requirements

**8.1 Information Assurance**

|  |
| --- |
| **Removable Media**Tenderers should note that removable media is not permitted in the delivery of this Contract. Where there is a requirement for Contractor’s Staff to take data off site in electronic format, the DVLA will consider if it is appropriate to supply an encrypted hard drive.**Security Clearance****Level 2** Tenderers are required to confirm in their response that any Contractor’s Staff that will be accessing the DVLA Site to provide routine maintenance or have access to the DVLA site and DVLA systems have Baseline Personnel Security Standard clearance (BPSS). The BPSS comprises verification of the following four main elements:1. Identity;2. Employment History (past 3 years);3. Nationality and Immigration Status;4. Criminal Record Check (unspent convictions only).The aim of the Baseline Standard verification process is to provide an appropriate level of assurance as to the trustworthiness, integrity, and proper reliability of prospective staff.Tenderers are required to provide evidence of relevant Contractor’s Staff clearance in their response.**Information Supply Chain**Tenderers are required to confirm how DVLA Data will be securely managed at each stage of the Information Supply Chain. This applies to both Contractors and Sub-Contractors. Retention schedules will need to be defined and agreed prior to award of contract.**Processing of Government Data** This contract will require the successful tenderer to process Government data on DVLA’s behalf. The successful tenderer will be required to complete a Statement of Assurance Questionnaire during the Standstill Period, to satisfy DVLA that its data will be appropriately protected.The purpose of the Questionnaire is to assess the maturity of policies, systems and controls associated with the handling of our data. The Questionnaire was developed for use throughout the Government supply chain and is based on ISO27001 criteria and aligned to the HMG Security Policy Framework.Tenders are required to confirm their understanding and acceptance of the requirement to complete and return the Questionnaire during the Standstill Period.The completed Questionnaire will be assessed by our Information Assurance Group and DVLA will work with the successful tenderer to address any information aspects requiring improvement.The HMG Security Policy Framework requires Departments to conduct an annual compliance review of third-party suppliers. The Questionnaire will therefore need to be completed annually throughout the term of the contract to assess ongoing compliance. DVLA may also audit suppliers to validate the responses and evidence provided in the Questionnaire.**Processing Personal Data**Please note that the successful tenderer as part of the contract agrees to comply with all applicable requirements of the Data Protection legislation (including the General Data Protection Regulation ((EU) 2016/679), the Law Enforcement Directive (Directive (EU) 2016/680), and all applicable Law about the processing of personal data and privacy).**Data Protection Impact Assessment (DPIA)** Please note that the successful tenderer, as part of the contract, agrees to comply with the processes of a Data Protection Impact Assessment **(**DPIA) if required. Following identification of the preferred bidder, the DPIA must be completed satisfactorily and approved by DVLA’s Data Protection Officer prior to formal contract award and before any processing of data commences in relation to this contract.**Schedule of Processing, Personal Data and Data** The processing of personal data has been identified as part of this requirement. The ‘Schedule of Processing, Personal Data and Data Subjects’ (Annex 2) provides the written instructions to be followed when processing data relating to this contract.**Offshoring of Government Data** Government policy is that data it holds should be protected appropriately regardless of location. Offshoring is defined as “Any arrangement where the performance of any part of the services or a solution under a contract may occur outside the UK for domestic (UK) consumption.” When offshoring is described, the focus is typically on the physical location where data is hosted (such as where are the data centres located). Whilst physical location of data is a critical part of the offshoring question, it is important to understand how and where data might be logically accessed. Administrators or technical support staff may be located anywhere in the world, with logical access to data.Tenderers must indicate in their response whether any DVLA data supplied as part of the contract, would be offshored. If so, tenderers must confirm the location(s) including the location of any business continuity, disaster recovery and technical support staff.All Central Government Departments and Agencies are required to seek approval for any proposed offshoring activity, which ensures that information held offshore is appropriately managed and that pan-government risks are identified, tracked, and managed, where appropriate. In the event that the successful tenderer proposes to offshore any DVLA Data as part of the contract, they would be required to provide details about the processing to be carried out offshore, the privacy risks and the security controls in place to protect the data. If the intention is to store the information in a cloud environment outside the UK, the successful tenderer will also need to confirm the extent to which the environment complies with the cloud security principles. This information would be used to submit the offshoring proposal for approval. Any request to offshore must receive clearance prior to the commencement of any data processing activity.**Redundant Equipment** Any redundant equipment that will have captured any DVLA sourced data must be disposed of securely on the DVLA Site. |

**8.2 Cyber Security**

|  |
| --- |
| The Government has developed Cyber Essentials, in consultation with industry, to mitigate the risk from common internet-based threats.It will be mandatory for new Central Government contracts, which feature characteristics involving the handling of personal data and ICT systems designed to store or process data at the OFFICIAL level of the Government Security Classifications scheme (link below), to comply with Cyber Essentials.<https://www.gov.uk/government/publications/government-security-classifications>All potential tenderers for Central Government contracts, featuring the above characteristics, should make themselves aware of Cyber Essentials and the requirements for the appropriate level of certification. The link below to the Gov.uk website provides further information: <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>As this requirement features the above characteristics, you are required to demonstrate in your response that:* Your organisation has Cyber Essentials or Cyber Essentials Plus certification; **or**
* Your organisation will be able to secure Cyber Essentials or Cyber Essentials Plus certification prior to contract award; **or**
* Your organisation has other evidence to support that you have appropriate technical and organisational measures to mitigate the risk from common internet based threats in respect to the following five technical areas:
* Boundary firewalls and internet gateways
* Secure configuration
* Access control
* Malware protection
* Patch management

The successful tenderer will be required to provide evidence of Cyber Essentials or Cyber Essentials Plus certification ‘or equivalent’ (i.e. demonstrate they meet the five technical areas the Cyber Essentials Scheme covers) prior to contract award. This will be through the completion of the Statement of Assurance Questionnaire.The successful tenderer will be required to secure and provide evidence of Cyber Essentials or Cyber Essentials Plus re-certification ‘or equivalent’ (i.e. demonstrate they meet the five technical areas) on an annual basis.**Further information regarding the certification process can be found here:** <https://www.ncsc.gov.uk/cyberessentials/overview> |

**8.3 Data Sharing**

|  |
| --- |
| DVLA’s Contract Owner will work with the successful tenderer to implement any information sharing or data sharing procedures and associated DVLA requirements that may be needed at any point during the lifecycle of the contract.  Information or data sharing procedures will need to be formally assessed and approved by DVLA through the Agency’s Data Sharing Clearance Process, managed by DVLA’s Data Sharing Strategy & Compliance team (DSSC).  The Contractor will submit any requirements for information / data sharing via the Contract Owner to the DVLA who will consider the changes through this Data Sharing Clearance process.  Any proposals shall be considered and if approved an implementation plan will be formally offered to and accepted by both the DVLA and the Contractor before commencement. This approvals process is designed to assess and identify additional measures and safeguards that may be required to protect data to those already stated in this Statement of Requirement document. |

**8.4 Sustainability**

The DVLA is committed to reducing any negative impacts produced by our activities, products, and services. This aligns to the Government’s Greening Commitment which states we must: “Continue to buy more sustainable and efficient products and services with the aim of achieving the best long-term, overall value for money for society.”

DVLA is certified to ISO 14001:2015 and more information is available in our Environmental Policy at:

<https://www.gov.uk/government/publications/dvlas-environmental-policy>

Together with the social value deliverables outlined in section 6.9, the supplier shall:

* Where required, be able to provide data on carbon emissions related to the products / services being supplied to aid with DVLA scope 3 emission calculations.
* Provide the specified services without the use of single use plastic in line with government commitments.
* The Supplier shall provide their sustainability or environmental policy.

**8.5 Health and Safety**

DVLA has an Occupational Health and Safety Management System that is certificated to ISO45001. Further information on our Health & Safety Policy, is available on request from the Commercial Advisor. (See Section 14 for Points of Contact):

|  |
| --- |
| All contractors working in the Authority on any of our premises must fully comply with relevant health and safety legislation, together with health, safety and welfare policy and management arrangements applied by the Authority. If appropriate, these issues must be addressed at or before the award of the contract and may form part of the procurement process. Where requested, Contractors will be required to provide copies of their health and safety policy statement, risk assessments and method statements, clearly identifying any safety implications that their activities may have and how these will be managed. Contract management staff are responsible for checking health and safety information provided by contractors, and passing relevant information to local line management and staff. Contractors’ safety performance will be monitored and checked as part of normal contract management.Any contractors that are required to attend DVLA premises must adhere to the following. The contractor/company must have a current Covid-19 risk assessment. This will need to be shared with DVLA (H&S team HSAT@dvla.gov.uk )prior to their visit. The Authority has in a place a current Covid-19 risk assessment and this must be shared with the contractor/company, so they understand the arrangements and control measures in place to keep them safe. The contractor must confirm that that they have not travelled from abroad recently – or confirm if they have, they have isolated for the required period, before visiting site. The contractor must confirm that they are well and are not symptomatic at time of visit. The Authority’s host for the contactor must confirm who is their contact point within the Authority, and that they have discussed arrangements for Covid 19 while they are working on site. The host will need to keep a tracker of the locations visited by the contractor. Service Providers should: Have an appointed competent person responsible for H&S, details to be made available to the Authority on request* Have emergency arrangements and plans for their goods/product/service, and observe the Authority’s arrangements whilst on site, or through the course of the business or contract
* Have adequate provision for your own first aid when on site
* Have an accident reporting and recording process for all near miss, accidents/incidents, or violent and aggressive behaviours. Any incident on the Authority’s site should be reported immediately to the Authority’s Health and Safety Team
* Communicate with the Authority’s on any health and safety matter or issue in relation to the contract/product/supply of goods or service, notifying the Authority of any Health and Safety hazard, which may arise in connection with its supply of goods, products, or services
* Indemnify the Authority in the instance where failure of the company’s product/service, acts or omissions, with regards to health and safety, results in an economic penalty, time delay, issue, accident/incident or claim against the Agency
* Have suitable and sufficient insurance cover for all business/products/services supplied/that are provided to the Authority
* Have documented, suitable and sufficient, risk assessments and method statements, covering all significant activities and deliveries of products, goods and services. Copies to be made available to the Authority on request
* Provide suitable and sufficient health and safety training, information and instruction for all its employees/contractors/subcontractor. Records to be made available on request
* Engage with the Authority’s Security/Estates Management Group to arrange access to all the Authority’s premises/buildings
* Comply with all vehicle and driver legal requirements and the Authority’s policies whilst driving on premises or conducting business for the Authority
 |

* 1. **Business Continuity**
* The Supplier must have a robust and effective formal disaster recovery and business continuity management programme.
* The Supplier must test their disaster recovery, business and service continuity arrangements no less than once per annum and report outcomes to DVLA
* The Supplier must inform DVLA in writing within 24 hours of activation of any business continuity plan in relation to services provided to DVLA.
* The Supplier shall ensure that in the event of failure, the Supplier shall maintain failover capacity and data storage processes and Help desk support to affect a failover or disaster recovery operation.
* The Supplier shall ensure a robust business continuity and disaster recovery plan is in place for all Services and shall be able to demonstrate disaster recovery to ensure continuity of the Services APMs without loss, as and when required by the Authority. These must include the Recovery Time Objective and Recovery Point Objective for the service.
* Where multiple centres are used for business continuity these must, where other services providers have multiple centres, have secured active communications access with each of these centres.
* The Supplier shall provide the business continuity and disaster recovery plan to the Authority as part of the initial assessment process and this will be reviewed between the Supplier and the Authority. on a yearly basis or the business continuity and disaster recovery plan shall be certified by Supplier’s External Auditors as part of the initial assessment process and on a yearly basis as fit for purpose to enable Supplier to meet its obligations to the Authority
* The Supplier shall ensure that in the event of disaster recovery, connectivity between the Authority and the Services is maintained.
* The Supplier will demonstrate that they comply with the requirements of ISO22301 and hold up to date accreditation or equivalent.

**8.7 Use of DVLA Brands, Logos and Trademarks**

The Authority does not grant the successful supplier licence to use any of the Authority’s brands, logos or trademarks except for use in communications or official contract documentation, which is exchanged between the Authority and the successful supplier as part of their fulfilment of the Contract.

Approval for any further specific use of the Authority’s brands, logos or trademarks must be requested and obtained in writing from the Authority.

## 9. Management and Contract Administration

* 1. The Supplier and the Authority shall hold monthly Performance Review meetings throughout the contract Term, which shall be conducted face to face at mutually convenient premises at least once per quarter where restrictions in place at the time permit and by conference or video call on all other occasions. There will be no cost to the Authority for the Supplier’s attendance at any Performance Review meeting.
	2. Performance Review meetings shall include as a minimum a review of, for the previous Quarter:
1. the Supplier’s performance against the agreed Service Levels (see Section 6) Performance Failures, progress against proposed corrective actions, and Lessons Learned;
2. risks and issues relating to the Service;
3. Continuous Improvement activities; and
4. The ongoing Complaints Log.
	1. The Parties shall appoint the following key personnel as a minimum and shall provide each other with up to date contact details for each throughout the Contract Term:

|  |  |  |
| --- | --- | --- |
| **Role** | **Personnel of**  | **Point of contact for** |
| Contract Owner | Authority | * Day-to-day Service delivery and performance;
* Escalation of operational issues.
 |
| Acco**u**nt Manager | Supplier |
| Commercial Advisor | Authority | * Contractual queries or changes;
* Escalation of contractual issues.
 |
| Commercial Manager | Supplier | * Contractual queries or changes;
* Escalation of contractual issues.
 |
| Data Protection Officer | Supplier | * Discussion of security controls protecting DVLA information in this service
* Contact point for Data Incidents
 |

* 1. A Supplier representative shall be available to provide support to the Authority on operational and financial queries Monday – Friday during the Authority’s working hours of 08:00 – 17.00 (excluding Bank Holidays).
	2. The Supplier shall appoint a Contract Account Manager and tasks shall include, but not be limited to:
* Acting as an escalation point for queries, advice and issues;
* Identification of opportunities for improvements;
* Informing the Authority of new risks;
* Trend analysis;
* Preparation for Contract review meetings;
* Fulfilling requests for information from the Authority;
* Information security.
	1. The Suppliers Contract Account Manager shall also be responsible for liaison with the Authority’s key Operational Management team, the Contract Owner and the Commercial Advisor. In addition, they shall attend implementation meetings, as requested by the Authority.
	2. After Contract commencement the Supplier shall attend performance meetings at the Authority’s premises or participate remotely via teleconferences to review the progress of the contract, to discuss the management information and to review any problems that may have arisen in the preceding period. The frequency of these meetings is to be confirmed but will be at least every three months. These Contract performance review meetings will be conducted to an agreed agenda; the following elements are likely to be included:
* Performance analysis – Review of SLAs and KPIs
* Contractual/Operational Issues
* Compliance and satisfaction levels
* Business Continuity issues and updates
* Proposals for improvements on any area of the contract
* Financial stability
* Review of risk assessment
* Provide updates on any new security threats identified, including threats to personal data
* Any future relevant legislation changes
* Progress on Social Value criteria
	1. The Supplier shall ensure all minutes of meetings are recorded, agreed, and distributed electronically to the appropriate persons within five Working Days after the meeting.
	2. Any issues or queries raised by the Authority during the term of the contract will be logged and resolved within two Working Days. Anything that cannot be resolved within this timeframe will be escalated for discussion at service review meetings
	3. The Supplier shall prepare and maintain a contract and operational risk register in accordance with Authority’s instructions. The Supplier shall identify risks, allocate risk mitigation action and ownership, and report to the Authority on progress on mitigation at applicable risk review meetings to be agreed between the Supplier and the Authority.
	4. The Supplier shall advise the Authority immediately of any material issues which it would reasonably expect may generate complaints or receive regulatory or press attention.
	5. The Supplier shall ensure fully robust staffing and disciplinary procedures are in place and are applied for all Supplier personnel.

**Sub-contracting to Small and Medium Enterprises (SMEs):**

9.14 Small Medium Enterprises

DfT is committed to removing barriers to SME participation in its contracts, and would like to also actively encourage its larger suppliers to make their sub-contacts accessible to smaller companies and implement SME-friendly policies in their supply-chains (see our [website](http://www.dft.gov.uk/about/doing-business-with-us) for further information).

To help us measure the volume of business we do with SMEs, our Form of Tender document asks about the size of your own organisation and those in your supply chain.

If you tell us you are likely to sub-contract to SMEs, and are awarded this contract, we will send you a short questionnaire asking for further information. This data will help us contribute towards Government targets on the use of SMEs. We may also publish success stories and examples of good practice on our website.

9.2 Invoicing

 The Supplier shall ensure that all invoices and account payment queries received from the Authority are resolved in accordance with the agreed Service Levels

 The Supplier shall comply with the DVLA standard Invoicing Procedures detailed below:

|  |
| --- |
| **DVLA Invoicing Procedures**1. All invoices and/or credit notes must be an original document.
2. **Any correspondence/enquiries which are sent to the designated email address for invoices/credit notes and are not an original invoice and/or credit note will be deleted, with no action being taken.**
3. All invoices and/or credit notes will either need to be sent electronically as an attachment to an email or as a hard copy document through the post to the designated email or postal address listed below:

**\*Email**: ssainvoice@sharedservicesarvato.co.uk**Postal Address:** Shared Services arvato5 Sandringham ParkSwansea ValeSA7 0EA1. If an original invoice and/or credit note is sent electronically, then the same document **must not** be sent as a hard copy through the post and vice versa.
2. All electronics invoice and/or credit notes **must** be sent in a PDF format. Any documents which are received and are not in a PDF format will be deleted with no action being taken.
3. All invoices or credit notes must quote a valid Purchase Order number i.e. one that is in the format 8000XXXXXX. This will be found on the Purchase Order you receive.
4. A 10Mb maximum file size per email is applicable.
5. If the e-invoice is encrypted, this could result in the invoice being blocked by arvato email security filters.
6. The e-invoices **must not** include profanities, as these will also be blocked by arvato email security filters and may delay/stop the invoice being received.
7. You should not provide goods or services without receipt of a valid Purchase Order.
8. Do not undertake new work or supply goods or services in excess of the original Purchase Order Value.
9. If an incorrect Purchase Order number or no Purchase Order number is quoted the invoice will be returned to you. You will be able to handwrite the correct Purchase Order numbers on the invoices that are returned, however it is preferable that you change it on your system and reissue to ensure any future invoices are referenced correctly.
10. Credit notes should quote the Purchase Order number and your original invoice reference along with details of what the credit note applies to, particularly if it is not for the full value of the invoice.
11. Identify the business unit the invoice or credit note relates to e.g. DVLA.
12. Shared Services arvato cannot be responsible for any e-invoice until it has been received. Responsibility for ensuring the e-invoice is received by arvato in a timely manner lies with the supplier.

**All supplier invoices and payment enquiries must be directed to Shared Services arvato. If you contact the relevant business unit directly, they will direct you to Shared Services arvato.****How to Notify DVLA of a Change**If you change important information, such as your organisation’s contact or bank details, we will need written official correspondence. Please notify Shared Services arvato as soon as possible:**Tel:** 0844 892 0343**Email:** support@sharedservicesarvato.co.uk (Please do not email original invoices/credit notes to this email address)**Postal Address:** Shared Services arvato (SSa)5 Sandringham ParkSwansea ValeSA7 0EA**Enquiring about progress of payments** 1. For all payment and invoice queries you will need to contact the Shared Services arvato Service and Support Desk directly on 0844 892 0343. When calling you should quote the Purchase Order number, your vendor account number (if known) and the business unit you are invoicing e.g. DVLA.
2. You should ask for your communication to be logged on a “service ticket” along with your contact details. This will allow all issues relating to your query to be logged under a unique reference number.
3. You should quote the service ticket number in any follow up conversations.
4. If Shared Services arvato has the invoice but cannot release it for payment, you are required to take appropriate action to ensure it can be paid.
5. If the invoice has not been received by Shared Services arvato, the responsibility is on you to get the invoice to Shared Services arvato. If you are sending invoices to anyone other than Shared Services arvato, please change your customer invoicing address to Shared Services arvato.
6. If a response from Shared Services arvato is required, one will be provided to you within 10 working days.
7. If you have any remittance queries, these should be discussed with Shared Services arvato:

**Tel:** 0844 892 0343**Email**: support@sharedservicesarvato.co.uk (Please do not email original invoices/credit notes to this email address)1. You must also ensure that a statement is sent to Shared Services arvato monthly to aid prompt payment of invoices (email and postal address as above).
 |

## 10. Training / Skills / Knowledge Transfer

The Supplier will be expected to train the Authority staff on all relevant systems including use of reporting portals.

The Supplier will be expected to provide advice and guidance on any bespoke terminology used by their service or organisation.

## 11. Arrangement for End of Contract

The Contractor shall fully cooperate with the Authority to ensure a fair and transparent re-tendering process for this contract. This may require the Contractor to demonstrate separation between teams occupied on the existing Contract and those involved in tendering for the replacement contract to prevent actual (or perceived) conflicts of interest arising.

The Supplier must provide a high-level exit plan as part of their tender and will provide a detailed plan no later than 6 months prior to the contract expiry date.

## 12. Evaluation Criteria

|  |
| --- |
| **Tender Evaluation**The paragraphs below set out and explain the procedure, stages and process by which tenders will be assessed. The evaluation procedure is divided into two key stages;1. **Selection Stage**

For requirements with an estimated value above the FTS advertising threshold, DVLA will issue and assess responses to the Standard Selection Questionnaire (SSQ) in accordance with the “Selection Stage” below.1. **Award Stage**

DVLA will assess responses to the requirement in accordance with the “Award Stage” below.Tenders that do not meet the criteria at the Selection Stage may be disqualified from further consideration in this procurement and will not be evaluated at the Award Stage.**Selection Stage – Grounds for Exclusion**Where DVLA has issued an SSQ in the Invitation to Tender pack (ITT), the tenderer should complete the questionnaire in order for DVLA to assess whether there are any grounds for exclusion.**Mandatory Grounds for Exclusion**If a tenderer answers “Yes” to any statement in the Grounds for **Mandatory** Exclusion, it is very likely the tender will be rejected and disqualified from further participation in this procurement.**Discretionary Grounds for Exclusion**DVLA is entitled to exclude a tenderer from further participation in this procurement if any of the statements in response to the Grounds for **Discretionary** Exclusion apply. If a tenderer answers “Yes” to any statement, it is possible that the tender will be rejected and disqualified from further participation in this procurement. If any of the statements do apply, the tenderer should set out the full facts detailing any remedial actions taken. The information provided will be taken into account by DVLA in considering whether or not the tender will be permitted to proceed any further in this procurement.Following the Selection Stage, any tenders that have been excluded will not proceed to the Award Stage, and the tenderer/s will be notified in writing.**Award Stage**The Award Stage will comprise of the following elements:1. an evaluation of mandatory requirements, if applicable **(Mandatory Requirements)**. These will be assessed on a pass/fail basis. Tenders that fail any of the mandatory requirements may be disqualified from further consideration
2. an evaluation of the tender based on the quality criteria and social value criteria (if applicable) (**Quality Criteria**)
3. an evaluation of the prices tendered (**Financial / Price Criteria**).
 |

Selection will be based on the Evaluation Criteria, encompassing the most economically advantageous tender, which demonstrates a high degree of overall value for money, competence, credibility and ability to deliver.

Your tender will be evaluated using the following weightings **and** the criteria weightings set out at Annex 1, to obtain the optimal balance of quality and cost.

**Mandatory Requirements (if applicable)**

Annex 1 provides details of any elements/criteria considered as critical to the requirement. These are criteria, which will be evaluated on a pass/fail basis. A fail may result in the tender being excluded from further evaluation.

**Quality Criteria:**

Annex 1 provides details of the quality criteria on which tenders will be evaluated. This will list the primary criteria along with the allocated percentage weighting and a description of the specific requirement. The overall percentage allocated for the Quality Criteria is outlined in the Table “Overall Weighting Allocation” and the method used to allocate scores is outlined below.

|  |  |
| --- | --- |
| **Points awarded** | **Description** |
| **5** | The Tenderer demonstrates fully that they can meet the requirement as detailed in the Specification |
| **4** | Meets all requirements but with minor issues |
| **3** | Meets most requirements but with a few minor gaps or issues |
| **2** | Meets some requirements; major concerns |
| **1** | Meets few requirements; serious concerns |
| **0** | The method of fulfilling the stated requirement is inadequate / not addressed |

Based on the allocated score, a percentage will be calculated against each element using on the following calculation:

(Allocated Score

                                           X  Weighting

Maximum Score)

For example, “Quality Element 1” can be allocated a score between 0 and 5 but carries a weighting of 7%.

Supplier A is given a score of 4 for this element so receives a score of (4/5 x 7) = 5.6

Supplier B is given a score of 5 for this element so receives a score of (5/5 x 7) = 7

The scores for each element will then be added together to calculate the overall Quality Criteria score.

**Financial / Price Criteria**

Evaluation of the prices submitted will be performed separately by a Commercial Finance Accountant and details will not be made available to the Quality Evaluation Panel. This is to ensure fairness and avoid any subconscious influence of a lower price on the quality scoring. The overall percentage weighting allocated for the Financial/Price Criteria is outlined in the Table “Overall Weighting Allocation”.

**Financial / Price Criteria Scoring Methodology:**

A Percentage Scoring Methodology will be used to evaluate all proposals for this requirement. This methodology is based on the following principles:

The lowest tendered price will be awarded the maximum score available. Each subsequent bid will be baselined to this score and will be awarded a percentage of the maximum score available. The calculation used is as follows:

 (Lowest Tendered Price

 X Maximum Score Available (i.e. Weighting)

Tender Price Submitted per Supplier)

For example, if the Financial/Price weighting allocation is 40%, the maximum score available is 40. Supplier A submits the lowest price of £100,000 and Supplier B submits a price of £180,000. Based on the above calculation Supplier A and B will receive the scores shown below:

Supplier A = 100k/100k x 40 = 40%

Supplier B = 100k/180k x 40 = 22.22%

**Overall Weighting Allocation**

|  |  |
| --- | --- |
| **Evaluation Criteria** | **Weighting** |
| **Quality Criteria and Social Value Criteria (if applicable)** | 80% |
| **Financial / Price Criteria** | 20% |
| **Total** | 100% |

**Calculation of Overall Score:**

The allocated score for the Quality and Social Value Criteria (where applicable) will be added to the Financial/Price Factor score to calculate the overall score for each tender (out of a max available 100%). The tender with the highest overall score will be deemed as successful.

## 13. Points of Contact

|  |  |  |
| --- | --- | --- |
| **Commercial Advisor** | Name | Patience Arinaitwe |
|  | e-mail | patience.arinaitwe@dvla.gov.uk |
| Address | Commercial Services DVLALongview RoadSwansea SA6 7JL |
| **Project Lead/Business Area Contact** |  | Alun Vaughan |
| e-mail | alun.vaughan@dvla.gov.uk |

**All queries/questions should be sent to the Commercial Advisor**

## 14. Annexes:

### Annex 1 – Evaluation Criteria:

**Mandatory Criteria**

| **Mandatory Criteria** | **Mandatory Criteria Description** | **Pass/Fail** |
| --- | --- | --- |
| **Functional** | Supplier is able to meet all requirements outlined in 6.1 |  |
| Supplier is able to meet all user facing requirements outlined in 6.1.1.1 |  |
| Supplier is able to meet all non-user facing requirements outlined in 6.1.2.1 |  |
| **Service Provision** | Supplier is able to meet all requirements outlined in 6.2.1 |  |
| **Testing and Integration** | Supplier is able to meet all requirements outlined in 6.3.1 |  |
| **Merchant Acquirer Integration** | Supplier is able to meet all requirements outlined in 6.4.1 |  |
| **Service Monitoring** | Supplier is able to meet all requirements outlined in 6.5.1 |  |
| **Refunds, Reporting and Queries** | Supplier is able to meet all requirements outlined in 6.6.1 |  |
| **Accreditations** | Supplier must provide proof of their current FCA accreditation |  |
| Supplier must provide proof of their current PCI DSS accreditation |  |

**Scored Quality Criteria**

| **Primary Scored Criteria** | **Primary Scored Criteria Weighting (%)** | **Scored Sub-criteria Description** | **Individual Scored Sub -Criteria Weighting (%)** |
| --- | --- | --- | --- |
| **Service Functionality****Service Management** | **33** | Please provide details of the availability of their service if this exceeds the mandatory 99.7% | 5% |
| Please refer to Section 6.1.1.2Please provide details of how you will provide confirmation of payment to customers. Where this involves sending an email, please provide details of how this will be carried out, examples of what will be contained in these, and how data security will be ensured.  | 1% |
| Please refer to Section 6.1.2.2Please provide detail of how you will provide a mechanism that exposes card scheme Payment Account Reference (PAR) values where card have been stored in ApplePay or G Pay devices, as these stored PANs do not equal original cardholder data  | 1%% |
| Please refer to Section 6.1.2.2Please state if, and if so how, you would provide your token services to other gateways | 1% |
| Please refer to Section 6.1.2.2Please state what mechanism and 3rd party systems you support to enable PCI-DSS compliance in the Authority’s call centre environment, for example, DTMF masking, IVR. | 1% |
| Please refer to Section 6.2.2Please confirm if you will be providing a public facing web page showing the status of the service and any incidents or issues affecting it at that time. If so, please provide details of what information will be provided. | 2% |
| Please provide details of the helpdesk facilities that will be made available as part of this service including but not limited to:* Available channels (E.g. phone, portal, email, etc)
* Opening hours
* Incident prioritisation and resolution times
* Resourcing
 | 5% |
| Please provide details of your change management processes | 5% |
| Provide details of your incident management process | 5% |
| Please demonstrate how you will manage and identify risk | 4% |
| Please demonstrate how reports will be made available to the Authority, and provide examples of the reports that should be provided | 3% |
| **Service Monitoring** | **5** | Please refer to Section 6.5.2Please describe how you will provide the Authority with the functionality to monitor Supplier’s availability, transaction completion rates and Transaction timings. | 5% |
| **Business Continuity** | **7** | Please provide business continuity and disaster recovery plans for this service detailing, but not limited to:* Physical and digital disruption
* Resourcing
* Disaster recovery
* Testing of plans including frequency

Please provide evidence of how you comply with the requirements of ISO22301 and provide up to date accreditation or equivalent. | 7% |
| **Quality Assurance** | **6** |  Please demonstrate that you have an effective quality assurance system in place and demonstrate that meets ISO9001 or equivalent standards and provide evidence of up to date accreditation if held. | 3% |
| Please demonstrate how you meet ISO20022 or equivalent standards and standards and provide evidence of up to date accreditation if held | 3% |
| **Sustainability** | **5** | Please detail how you will meet the requirements laid out in Section 8.4, including providing your environmental policy. | 5% |
| **Cyber Security** | **7** | Please provide evidence of how you meet the requirements in Section 8.2 and provide evidence of Cyber Essentials or Cyber Essential Plus accreditation if held. | 7% |
| **Information Security** | **7** | Please demonstrate how you adhere to the ISO27001 standards and provide evidence of up to date accreditation if held. | 7% |
| **Social Value Outcomes** | **10%** | Please provide details of how you will ensure you meet the Equal Opportunity requirements outlined in Section 6.9 | 3% |
| Please provide details of how you will ensure you meet the Climate Change requirements outlined in Section 6.9 | 3% |
| Please provide details of how you will ensure you meet the Digital and Financial Exclusion requirements outlined in Section 6.9 | 2% |
| Please provide details of how you will ensure you meet the Financial Literacy requirements outlined in Section 6.9 | 2% |
|  | **Total = 80%** |  |  |

**Financial/Pricing Criteria**

| **Primary Financial/Pricing Criteria** | **Financial/Pricing Weighting (%)** | **Description** |
| --- | --- | --- |
| **Pricing Requirements** | **20%** | **Refer to the Pricing Schedule for full details and further instruction** |
|  | **Total = 100%** |  |

**Annex 2 – MTC Schedule 20: Schedule of Processing, Personal Data & Data Subjects**

This Annex will be completed by the successful Supplier once selected, Suppliers can fill out Schedule 20 of Data Processing and submit it with their Tender to indicate their Joint Controller/Independent Controller status (this will not impact the outcome of the Evaluation).

This Schedule shall be completed by the Controller. The Controller may take account of the view of the Processor(s); however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller’s Data Protection Officer are: [**DPM@dvla.gov.uk].**
2. The contact details of the Processor’s Data Protection Officer are: [insert contact details].
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of the Controller and Processor | The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor in accordance with Clause [E1.1]. [**Guidance:** You may need to vary this section where (in the rare case) the Authority and Contractor have a different relationship. For example where the Parties are Joint Controllers of some Personal Data]: *“Notwithstanding Clause [E1.1] the Parties acknowledge that they are also Joint Controllers for the purposes of the Data Protection Legislation in respect of:****[Insert*** *the scope of Personal Data which the purposes and means of the processing is determined by the both Parties]**In respect of Personal Data under Joint Control, Clause [E1.1-E1.14] will not apply and the Parties agree to put in place a Joint Controller Agreement as outlined in Schedule [Y] instead.”* |
| Subject matter of the processing | *[This should be a high level, short description of what the processing is about i.e. its subject matter of the contract.* *Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public.]* |
| Duration of the processing | *[Clearly set out the duration of the processing including dates]* |
| Nature and purposes of the processing | *[Please be as specific as possible, but make sure that you cover all intended purposes.* *The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.**The purpose might include: employment processing, statutory obligation, recruitment assessment, etc.]* |
| Type of Personal Data being Processed | *[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data, etc.]* |
| Categories of Data Subject | *[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website, etc.]* |
| Plan for return and destruction of the data once the processing is completeUNLESS requirement under union or member state law to preserve that type of data | *[Describe how long the data will be retained for, how it be returned or destroyed]* |

### Annex 3: Pricing Schedule

