Home Office

AUTHORITY: The Secretary of State for the Home Department

SCHEDULE 2
STATEMENT OF REQUIREMENTS

Front End Services (FES) UK

OVERVIEW OF SERVICES TO BE DELIVERED

1.1 Introduction

The Secretary of State for the Home Department, acting through UK Visas and Immigration (UKVI), is the Authority procuring FES (UK). UKVI is a department within the Home Office and has customers in the UK who include but are not limited to:

- those seeking to extend permissions to work or study in the UK;
- those seeking to extend permissions to stay or settle with family;
- those seeking to evidence their rights as European Economic Area nationals and family members; and
- those progressing from earlier immigration permissions to British nationality.

UKVI is responsible for making millions of decisions every year about who has the right to visit or stay in the country, with a firm emphasis on national security and a culture of Customer satisfaction for people who come here legally. UKVI's vision is to be a world-leading immigration service working for a safe and prosperous UK. To that end, two of our key missions are to deliver world-class Customer service and to control migration. UKVI's challenge is to transform services in a way that enhances Customer experience and controls outcomes. A focus of our transformation programme is modernising the services through which our Customers interact with us. The vast majority of our Customers have common needs that can be delivered in a coherent model, which lends itself to commercial supply.

This Statement of Requirements (SOR) document has been written with these objectives in mind and describes the Authority's Business Requirements, which shall be fulfilled by the Supplier in providing a solution. In respect of the Business Requirements set out in this document, the Supplier shall ensure that its solution meets:

- all the Business Requirements set out in this SOR;
- the Service Agreement of the Agreement;
- the requirements of all Schedules in the Agreement; and
- the proposed Customer journey.

1.2 Overview of Business Requirements

Business Requirements apply across all of the Home Nations. They represent the core elements of the Authority's Application Process and consist of the below subsets of Service Packages. Each Service Package contains a set of requirements that must be fulfilled by the Supplier (these individual elements are depicted with an 'R' pre-fix):

Service Package 1 (SP1): General Requirements-

- Facilities
- Branding
- Service Availability
- Consistent and Professional Delivery
- Physical Customer Journey
- Online Customer Journey
- Continuous Improvement
- Reputational Damage
- Service Standards
- Service Management
- Management Information and Reporting
- Respecting Religious / Cultural Sensitivities
- Recruitment
- Personnel Identification
- Training
- Security and Confidentiality
- Supplier Contingency Plan
- Continuity of Service Levels
- Testing, Mobilisation and Transition
- Management Information/Audit
- Website
- Complaints Procedure

Service Package 2 (SP2): Identity Check

- Customer identity confirmation
- Non-compliance
- Unique Application Number
- Supporting Evidence not provided

Service Package 3 (SP3): Biometric Capture

- Provision and Installation
- Functionality
- Operation
- Environment
- Use of data
- Connections
- Access control
- Biometric Capture Process
- Contingency
- Transmission
- Digital Recording

Service Package 4 (SP4): Digitisation of Supporting Evidence

Service Package 5 (SP5): Digitisation

- Self Upload
- Lost Evidence
- Damaged Evidence
- Lost and Damaged Evidence compensation
- Digitisation General – Exceptions
- Digitisation General – Categorisation
- Checklist Confirmation
- Digitisation specifications and requirements

- Data Transfer
- Passport check and digitise
- Passport Submission
- Travel Document and Evidence Referral

Service Package 6 (SP6): Priority

Service Package 7 (SP7): Non-Digital Applications

Service Package 8 (SP8): Added Value and Bespoke Services

- Added Value Services
- Bespoke Services

Service Package 9 (SP9): System Integration

- Integrate with existing Authority systems.
- IT Service Management

1.3 Supporting Schedules

In the event that there is any conflict between this Schedule 2 (**Statement of Requirements**) and Schedule 3 (**Supplier's Solution**), then Schedule 2 will prevail, in accordance with the Services Agreement.

1.4 Potential Future Requirements

Potential Future Requirements are Business Requirements which need not be met by the Supplier at the Effective Date, but which may need to be fulfilled in the future, if the Authority requests them (at its sole discretion). The Authority will require flexibility from the Supplier to respond to the changing environment. These changes will be introduced via the Change Control Procedure as detailed in Schedule 10 (**Change Control Procedures**) and the content of the Service Agreement of this contract.

The Authority has deemed a number of potential service requirements as Potential Future Requirements. These are requirements for services the Authority is not in a position to define sufficiently to contract for at present, but nevertheless sees the possibility for later in the contract.

These future services include:

- Volume fluctuation.
- Working with other Her Majesty's Government Departments and other Government Departments.
- Interview Facilitation Services. If required, the Supplier would provide a digital solution to allow Customers to be remotely interviewed by the Authority. The Supplier would be expected to provide the premises, hardware and software, ensuring connectivity with Authority systems for interviewers, should this service be called upon.

BUSINESS REQUIREMENTS

2.1 General

Number	Requirement	Description	Authority Responsibilities
R1-01	**Facilities**	The Supplier shall provide the best balance of Customer experience and value for money through a flexible network of Service Point Locations with sufficient capacity to manage volumes; taking into consideration demand characteristics such as Customer type and seasonality, where relevant. The Supplier's Services shall be available as a minimum to all Home Nations: England, Northern Ireland, Scotland and Wales. (Scotland includes the Scottish Mainland plus Shetland Islands, Orkney Islands and the Outer Hebrides). The Supplier shall provide Service Point Locations that comply with The Equality Act 2010 (including full compliance with the disability discrimination provisions). The Supplier shall provide Service Point Locations that comply with Health and Safety Act 1974 Legislation. Facilities exceptions- The Supplier shall offer a Service solution for specific Customer groups who are unable to travel to a Service Point Location. Any solution shall conform to all other requirements for the Services, unless explicitly stated to the contrary.	The Authority will supply The Equality Act 2010 and Health and Safety Act 1974 Legislation.

Number	Requirement	Description	Authority Responsibilities
R1-02	**Branding**	The Supplier shall provide consistent branding throughout the Service Point Location following brand guidelines provided by the Authority. This includes, where relevant, both external and internal printed (signage, posters and leaflets) media, digital and audio visual communications. The Supplier shall seek Authority agreement for third parties communicating in Service Point Locations. Where Service Point Locations are shared, the Authority shall provide guidance on the appropriate share of communications and branding. The Supplier shall ensure that all Service Point Locations have a professional look and feel.	The Authority will provide brand guidelines in relation to branding including all shared Service Point Locations.
R1-03	**Service Availability**	In each of the Service Point Locations the Supplier shall ensure they have the availability for Customer attendance. All Customers will be able to attend their chosen Service Point Location within [Redacted due to commercial sensitivity] working days of completing their online application. The Supplier shall note any additional Services they can offer to meet Customer volume (see Added Value Services and Bespoke Services).	

Number	Requirement	Description	Authority Responsibilities
R1-04	**Consistent and Professional Delivery**	The Supplier shall observe the following relationship principles throughout the duration of the Contract: (a) the Supplier and Authority will operate under shared objectives, values and behaviours which will be agreed between the parties from time to time; (b) mutual trust based on openness and honesty about how the relationship is working and what issues in relation to it need to be resolved; (c) recognition that the successful delivery of the Services relies on the strength of the relationships between the parties and a commitment to work together to deliver the Services and any agreed or required service improvements; The Supplier shall be, and remain at all times, registered with the Office of the Immigration Services Commissioner for the provision of immigration services or immigration advice (if required to do so by virtue of section 84(1) of the Immigration and Asylum Act 1999) and comply with the relevant terms of such registration.	
R1-05	**Physical Customer Journey**	The Supplier shall provide an efficient, seamless and quality Customer experience at each Service Point Location in order to manage the volume of Customers as outlined in the data room and Schedule 7 (**Performance Levels (KPIs)**).	

Number	Requirement	Description	Authority Responsibilities
R1-06	**Online Customer Journey**	The Supplier shall be expected to understand and manage demand (the volume of Customers), most of whom will begin their journey online through an application portal on the Authority's digital service (the gov.uk platform). Once the Customer has completed the Application Detail through this Authority portal, the Supplier will receive part of that detail to inform the mechanism the Supplier may choose to manage demand and to enable the Customer to select and pay for any further Services they may choose directly from the Supplier. The Supplier may be required to direct the Customer back to the Authority's digital service to enable the Customer to complete the application process. All of this should be as seamless an experience as possible. Exact Customer Application Details transferred will be agreed between the Authority and the Supplier.	
R1-07	**Continuous Improvement**	The Supplier shall be able to demonstrate and utilise Customer Insight techniques to continually improve its current and future Services provision. The Supplier shall work with the Authority to develop and propose future solutions for all aspects of the Services.	The Authority will work with the Supplier on future Services solutions.
R1-08	**Reputational Damage**	The Supplier shall safeguard all data and personal information, in accordance with Schedule 4 **(Security)**. The Supplier will report all potential breaches to the Authority according to the processes set out at Schedule 4 **(Security)**. The Supplier shall adhere to the Authority's press/media policy.	The Authority will provide its press/media policy.

Number	Requirement	Description	Authority Responsibilities
R1-09	**Service Standards**	The Supplier shall maintain Service Standards across all Service Point Locations in line with Schedule 2 **(Statement of Requirements),** Schedule 27 **(Information Technology (IT))** and Schedule 7 (**Performance Levels (KPIs)**).	
R1-10	**Service Management**	The Supplier shall attend all meetings as outlined in Schedule 8 **(Governance and Contract Management).** The Supplier shall identify and maintain at least one point of contact who will be available during the Core Service Hours to be defined.	
R1-11	**Management Information and Reporting**	The Supplier shall provide all Management Information and data as outlined in Schedule 14 **(Management Information and Reporting).**	
R1-12	**Respecting Religious / Cultural Sensitivities**	The Supplier shall deliver the Services whilst treating Customers in a way that respects any religious or cultural sensitivity in adherence with The Equality Act 2010.	
R1-13	**Recruitment**	The Authority shall approve Supplier Personnel in accordance with the requirements of the staff vetting procedure and will ensure that all staff have the appropriate Security Clearance and training to meet the Services agreed with the Authority as per Schedule 11 **(Personnel and Key Representatives)**.	The Authority will make clear Security clearance and training required to meet Services agreed as per Schedule 11 **(Personnel and Key Representatives).**
R1-14	**Personnel Identification**	All Supplier Personnel shall possess and display clear identification whilst providing the Services to Customers at the Service Point.	

Number	Requirement	Description	Authority Responsibilities
R1-15	**Training**	The Supplier shall ensure that the Supplier Personnel are adequately trained and vetted, in accordance with Schedule 11 (**Personnel and Key Representatives**), to undertake their duties in line with this Schedule 2 (**Statement Of Requirements)** and all Contract Schedules. The Supplier shall keep accurate training records in accordance with Schedule 7 (**Performance Levels (KPIs)).**	

Number	Requirement	Description	Authority Responsibilities
R1-16	**Security and Confidentiality**	The Supplier shall ensure that the Services are provided and operated in a manner which supports Authority compliance with the Her Majesty's Government (HMG) Security Policy Framework (SPF) in current and future versions. The HMG Security Policy Framework can be accessed at http://www.gov.uk/government/publications/security-policy-framework and is updated periodically. It includes by reference HMG IA Standards, Good Practice Guides and other guidance produced by NCSC (National Cyber Security Centre). It is the responsibility of the Supplier to ensure that they understand these standards and guidance and employ resources (e.g. cyber security specialists) to interpret them. All digital solutions must comply with controls as specified by the Authority in Schedule 4 **(Security)** and the classification of all data will be OFFICIAL. The Supplier shall allow access to the Authority on request, to conduct on-site inspections for the purposes of fraud prevention, security policy and security requirements and compliance monitoring in line with Schedule 4 **(Security).**	The Authority will provide HMG Security Policy Framework (SPF) in current and future versions, which can be accessed at http://www.gov.uk/government/publications/security-policy-framework and includes by reference HMG IA Standards, Good Practice Guides and other guidance produced by NCSC (National Cyber Security Centre). The Authority is responsible for carrying out on-site inspections for the purposes of fraud prevention, security policy and security requirements.

Number	Requirement	Description	Authority Responsibilities
R1-17	**Supplier Contingency Plan**	The Supplier shall provide a contingency plan as part of the Supplier's solution detailing how the Services will continue to be provided during business disruptions, disasters and emergencies in line with Schedule 21 **(Business Continuity Disaster Recovery (BCDR) Plan)**. The Supplier shall outline how the Services will continue to be provided during these incidents and follow the processes outlined at Schedule 21 **(Business Continuity/Disaster Recovery (BCDR) Plan)**. The Supplier shall document their Business Continuity and Disaster Recovery plan (BCDR). The BCDR Plan will clearly set out the conditions and/or circumstances under which it will be invoked and will specify the Supplier's approach to recovering the Services in the event of disruptive incidents, including recovery timescales and strategies and crisis management processes.	
R1-18	**Continuity of Service Levels**	The Supplier shall provide day-to-day business continuity management for the Services in order to continue to meet the requirements in Schedule 7 **(Performance Levels (KPIs)).**	Authority to provide Schedule 7 **(Performance Levels (KPIs))**.
R1-19	**Testing, Mobilisation and Transition**	The Supplier shall support the testing of all digital solutions including Biometric Capture, and will provide appropriate IT support services during the installation/testing phase in accordance with Schedule 5 **(Implementation (Mobilisation and Transition)** and in line with the required timescales for go live.	The Authority will make available Schedule 5 **(Implementation (Mobilisation and Transition)** and will confirm timescales for go live.

Number	Requirement	Description	Authority Responsibilities
R1-20	**Management Information/ Audit**	For audit purposes the Supplier shall provide a digital means of maintaining information and managing contact with Customers that can be viewed and accessed by the Authority. All interactions will be audited, applying. Authority Security Standards in accordance with Schedule 4 **(Security)**, including, but not limited to: • Administration, reporting, changes to access privileges, interface and support operations performed and be able to retrieve/view audit information using search criteria based on; • user name, identity and machine identification, • date/time, • location, • type of operation and exceptions applied, • success or fail status and reason why; or • combinations of these.	

Number	Requirement	Description	Authority Responsibilities
R1-21	**Website**	The Supplier shall provide a website or other digital interface that interacts with the GOV.UK platform. As a minimum, the website will communicate availability and locations of the Services. Any website or other digital interface provided by the Supplier will be required to demonstrate it is designed and developed to continually meet the Government Digital Service Standards, which can be accessed at https://www.gov.uk/service-manual/digital-by-default. The Supplier shall operate any website 24*7*365 with the availability of 99.5% (excluding outage for planned maintenance). The response time for page loading and page refreshes from an Authority connection, excluding report generation, should not exceed 2 seconds for 95% of requests, with a 99% percentile response time of 5 seconds. The Authority shall approve the addition of any third party advertising including positioning.	Government Digital Service Standards can be accessed at https://www.gov.uk/service-manual/digital-by-default. GDS assess websites against the standards.
R1-22	**Complaints Procedure**	The Supplier shall develop, implement and maintain procedures and systems for complaint management. The Supplier shall develop, implement and maintain procedures and systems to refer Authority specific complaints in line with Schedule 26 **(Complaints Handling)** and meet Service Standards set out in Schedule 7 **(Performance Levels (KPIs)).**	The Authority shall provide; Schedule 26 **(Complaints Handling),** Schedule 7 **(Performance Levels (KPIs)),** and will confirm which are 'Authority specific complaints'.

2.2 Identity Check

Number	Requirement	Description	Authority Responsibilities
R1-23	**Customer identity confirmation**	With the exception of customers defined in R1-52, only those who have a Unique Application Number (UAN) obtained from the Authority should be allowed to submit their Supporting Evidence and/or proceed to biometric capture. The Supplier shall check every Customer's identity at each stage of the process. In delivering this requirement, as a minimum, the Supplier shall ensure that: • all Customers must use their passport or travel document as identification unless otherwise agreed by the Authority; • the identity evidence is checked to ensure the biographic details (name, date of birth, nationality, gender and travel document number as presented) match those recorded; and • Customer's photographic identity document is checked to ensure it bears suitable likeness to the Customer. The Supplier shall work with the Authority to accept alternative forms of identity in exceptional circumstances but only where approved by the Authority. The Supplier should seek to continually improve identity assurance in line with R1-07 from the Effective Date.	

Number	Requirement	Description	Authority Responsibilities
R1-24	**Non-compliance**	In the event a Customer refuses to undertake any of the required Service Components, the Supplier shall be responsible for advising the Customer that their Application may become invalid and, if applicable, the Supplier shall ensure the Customer signs a disclaimer stating they wish to proceed with their Application.	
R1-25	**Unique Application Number**	The Unique Application Number (UAN) provided by the Authority is the primary key for associating Customer/Application and volume management activities. The Supplier shall ensure all Supporting Evidence, images and Biometric Data collated includes the UAN associated to the Customer as part of the Metadata.	The Authority will provide a UAN to the Customer via online application.
R1-26	**Supporting Evidence not provided**	The Supplier shall give the Customer the opportunity to provide Supporting Evidence within the same working day of their initial visit to the Service Point before progressing with the Application. The Supplier is to ensure that if the Customer chooses not to provide the Supporting Evidence the Customer can proceed with the Application on the condition that the Customer sign and confirm that this omission was highlighted to them by the Supplier. In the event that a Customer does not provide the required Supporting Evidence on the same day as their initial visit to a Service Point, or chooses not to continue with their Application, the Supplier is to make provision for a Customer to attend a Service Point at a later date in accordance with the Authority's "Standard Operating Procedures" document.	The Authority will provide Standard Operating Procedures.

2.3 Biometric Capture

Number	Requirement	Description	Authority Responsibilities
R1-27	**Provision and Installation**	The Supplier shall provide all biometric capture solutions to be used in their Service Point Locations in accordance with the "Biometric Standards – Requirements and Information for Partners and their Suppliers" document. The Supplier will meet volume demand and fluctuations. The Supplier shall install the biometric capture solutions at Service Point Locations to align with the Authority "Best Practice for Biometric Capture" document.	The Authority will provide Biometric Standards – Requirements and Information for Partners and their Suppliers documentation. The Authority will make available the Authority Best Practice for Biometric Capture documentation.
R1-28	**Functionality**	The Supplier shall use their biometric capture solutions exclusively for recording related data entry, fingerprints, signatures and image capture of the Customer wishing to make an application at a Service Point. The biometric capture solution will be able to record only one or some of the components as and when identified by the Authority. The Supplier's biometric capture solutions shall identify Priority and Standard application types. Priority Biometric Data Captures should be sent to the Authority in line with Schedule 7 **(Performance Levels (KPIs)).** The Supplier shall provide override functionality to align with the agreed list of permissible exceptions defined by the Authority.	The Authority will provide Schedule 7 **(Performance Levels (KPIs)).** The Authority will make available the Authority Best Practice for Biometric Capture documentation.
R1-29	**Operation**	The Supplier shall be responsible for the operation and maintenance of their biometric capture solutions including developing any security instructions and the Authority's "Standard Operating Procedures" document.	

Number	Requirement	Description	Authority Responsibilities
R1-30	**Environment**	The Supplier shall ensure that their biometric capture solutions are suitable for different Customer groups, including disabled Customers and children, in accordance with the Authority "Best Practice for Biometric Capture" document. The Supplier shall ensure that there is privacy for Customers whilst providing their Biometric Data. The Supplier shall ensure that the biometric capture environment enables the capture of facial photo images conforming to the "Biometric Standards – Requirements and Information for Partners and their Suppliers" document and the Authority "Best Practice for Biometric Capture" document.	The Authority will provide the Authority Best Practice for Biometric Capture documentation.
R1-31	**Use of data**	The Supplier shall not use Biometric Data in any way other than that which is authorised under the Agreement, or that which the Authority may stipulate.	
R1-32	**Connections**	The Supplier shall only connect Authority approved devices to their biometric capture solution. The Supplier shall provide the full connectivity to transmit the Biometric Data to the Authority. The Supplier shall ensure sufficient levels of bandwidth and availability to meet the Authority's requirements and any increased volume.	The Authority will Authorise devices to be used for biometric capture solutions. The Authority will provide consent before the Supplier is to attempt to interface with Authority systems.
R1-33	**Access control**	The Supplier shall implement appropriate access control for authorised users. The Supplier will have auditable processes in place to support this.	

Number	Requirement	Description	Authority Responsibilities
R1-34	**Biometric Capture Process**	The Supplier shall ensure that all Biometric Data (biographical data, 10 finger-scans, facial images and signature) is captured, collated and transmitted to the Authority in line with the Authority "Best Practice for Biometric Capture" document. The Supplier shall ensure their biometric capture solution has the functionality to capture and amend Biometric Data as required in line with the details of the Primary Identification document as specified by the Authority. The Supplier shall provide Management Information (MI) on the quality of the Biometric Data captured in accordance with the Authority Biometric Standards.	The Authority will provide the Authority Best Practice for Biometric Capture documentation and the Authority Biometric Standards. The Authority will specify the details of the Primary Identification document.
R1-35	**Contingency**	The Supplier shall develop and follow an agreed contingency process for failures in the network, hardware, software, or power, as agreed with the Authority.	The Authority will agree a contingency process.

Number	Requirement	Description	Authority Responsibilities
R1-36	**Transmission**	The Supplier shall ensure that Biometric Data is successfully transmitted to the Authority in accordance with the “Interface Control Document” (ICD). The Supplier shall put in place a process to notify the Authority if there is outstanding Customer Biometric Data awaiting transmission to the Authority, including Priority Biometric Data capture. The Supplier shall provide a mechanism for liaison with the Authority for all matters relating to the transmission including planned outages, emergency issues and other matters requiring the Supplier’s attention. The Supplier shall collaborate with the Authority in the resolution of issues taking such steps as may be required to restore normal service.	The Authority will provide the appropriate ICD.

Number	Requirement	Description	Authority Responsibilities
R1-37	**Digital Recording**	The Supplier shall capture all Biometric Data in a way that is indexable and accessible by the Authority. The Supplier shall ensure that the Digital Recording clearly identifies the Customer (and any other persons who may be present) having their Biometrics Captured and can be used as clear evidence of identifying unlawful acts that might take place during the entire Biometric Capture process. The Supplier shall ensure that the Digital Recording File can be supported by the Authority's current system (as at July 2017 – Operating System Windows 2007 is in use by the Authority). The Supplier shall ensure that the Digital Recording Files are accessible to the Authority in accordance with the time period set out in Schedule 7 **(Performance Levels (KPIs))**, or on request of the Authority if required sooner. The Supplier shall retain the Digital Recording Files for a period as agreed with the Authority. The Supplier shall ensure that the Digital Recording Files are secured against accidental or intentional modification or destruction at the location where the recording is made.	The Authority shall make available Schedule 7 **(Performance Levels (KPIs)).** The Authority will communicate with the Supplier on agreeing the timeframe digital recordings are retained.

2.4 Digitisation of Supporting Evidence

Number	Requirement	Description	Authority Responsibilities
R1-38	**Digitisation of Supporting Evidence**	The Supplier shall be responsible for digitising Supporting Evidence received from the Customer, or from source on behalf of the Customer, as per the Authority's "Standard Operating Procedure" document and transmitting the Supporting Evidence to the Authority in accordance with Schedule 7 (**Performance Levels** (KPIs))**.** The Supplier shall: A) Receive in digitised format as outlined in the ICD and/or digitise all Supporting Evidence to the appropriate quality as specified by the Authority in the correct format and in a legible manner in accordance with the digital "Interface Control Document" (ICD). The Supplier must ensure quality control is undertaken consistently throughout the process to ensure that digitised evidence meets the Authority's quality standards. B) Handle any other items presented by the Customer including media items such as; DVDs, video cassettes, USB-type memory sticks in accordance with "Standard Operating Procedures" document. C) Not allow any alteration of the Supporting Evidence once digitised from the original copies provided by the Customer. The Supplier shall be responsible for the security of the Customer's Supporting Evidence immediately upon receipt from the Customer. Upon receipt, the Supplier shall ensure all Supporting Evidence provided by the	All Supporting Evidence shall be handled, managed or digitised in accordance with the Standard Operating Procedures as provided by the Authority. The Authority shall provide the digital Interface Control Document (ICD). The Authority shall provide Schedule 7 (Performance Levels (KPIs))**.**

Number	Requirement	Description	Authority Responsibilities
		Customer is managed in accordance with "Standard Operating Procedures" document. The Supplier shall retain all Customers' digitised Supporting Evidence for thirty (30) calendar days following their attendance at a Service Point. The Supplier shall be required to notify the Customer that their original Supporting Evidence may be required by the Authority at a later date.	

2.5 Digitisation

Number	Requirement	Description	Authority Responsibilities
R1-39	**Self Upload**	The Supplier shall provide a Self Upload solution, as specified by the Authority, to self upload digitised Supporting Evidence and transmit securely to the Authority in accordance with the ICD. The Supplier's Self Upload solution must include the ability to upload digitised Supporting Evidence at different stages of the process either prior, during or after attendance at a Service Point as directed by the Authority. The Self Upload solution must be configurable to enable the Authority to direct which Customer groups can utilise this solution. Self upload may include: A) Scan or take photograph of paper evidence B) Upload existing electronic evidence (e.g. PDF) C) Upload digital file using web site, device or mobile phone The Supplier shall provide a solution to ensure all self upload evidence provided meet quality standards and link to the UAN as specified by the Authority. The Supplier shall be responsible for the maintenance and repair of the Self Upload solution ensuring continuity of the Service.	Authority to provide the ICD.

Number	Requirement	Description	Authority Responsibilities
R1-40	**Lost Evidence**	The Supplier shall have a method to identify Lost Evidence and appropriate procedures to locate the Lost Evidence. The Supplier is liable for any costs incurred due to Lost Evidence during the digitisation process.	
R1-41	**Damaged Evidence**	The Supplier shall notify the Authority when Supporting Evidence has been damaged whilst in the responsibility of the Supplier. The Authority shall be notified as soon as possible and within the same day as the event occurring in accordance with Schedule 7 (Performance Levels (KPIs))**.** The Supplier is responsible for Customer communications and management relating to Damaged Evidence.	
R1-42	**Lost and Damaged Evidence compensation**	In the event of Lost Evidence, or of Damaged Evidence, whilst in the responsibility of the Supplier, Service Credits shall be applied in accordance with Schedule 7 (Performance Levels (KPIs)). The Supplier is responsible for liaison with the Customer on compensation claims and is responsible for seeing such claims through to conclusion.	

Number	Requirement	Description	Authority Responsibilities
R1-43	**Digitisation General - Exceptions**	Where Customers provide non-format evidence which cannot be digitised, they should be asked to photocopy this evidence to a suitable standard that the Supplier can digitise. The Supplier shall be responsible for assessing the suitability of the Customer's Supporting Evidence regarding delicate/fragile, oversized or any considered inappropriate for the Supplier digital solution. Where Supporting Evidence is not suitable for digitisation then the Supplier shall provide an alternative solution to enable these items to be digitised. Where this is not possible, a referral to the Authority under the Exceptions Process will be required in accordance with the Authority's "Standard Operating Procedures" document.	The Authority shall provide the Standard Operating Procedures of Exceptions Process.
R1-44	**Digitisation General - Categorisation**	The Supplier shall ensure the Customer's Supporting Evidence is categorised in accordance with the Authority's "Standard Operating Procedures" document. The Supplier shall ensure the Customer's Supporting Evidence is digitised in accordance with the Authority's ICD.	The Authority shall supply Standard Operating Procedures in relation to categorisation of Supporting Evidence. The Authority shall provide the Authority's ICD.
R1-45	**Checklist Confirmation**	The Customer and Supplier shall confirm what Supporting Evidence has been provided by the Customer as directed by the Application Document Checklist. The Application Document Checklist and signed confirmation must be digitised and transmitted by the Supplier to the Authority as part of the Digitised Supporting Evidence in accordance to Schedule 7 (Performance Levels (KPIs))**.**	

Number	Requirement	Description	Authority Responsibilities
R1-46	**Digitisation specifications and requirements**	The Supplier's digitisation solution must have the flexibility to alter the configuration on the following areas as a minimum: • File type (for example PDF, JPEG etc. • Colour (Black and White, Colour and Grayscale) • Digital resolution (DPI • Compression value • Message size • Legibility The Authority shall specify the minimum standards for data transmitting within the ICD.	The Authority shall supply the ICD, and within specify the minimum standards for data transmitting.
R1-47	**Data Transfer**	Digitised Supporting Evidence shall be transmitted securely into Storage in accordance with ICD and the Authority Schedule 4 **(Security)** - paragraph 12, Data Security. Any digitised items which do not meet the specific requirements will be rejected, and the Supplier will be responsible for resolving and re-transmitting the Evidence Pack.	

Number	Requirement	Description	Authority Responsibilities
R1-48	**Passport check and digitise**	The Supplier should digitise the travel documents/passports where specified by the Authority through the Application Document Checklist using as a minimum a passport tri scan (normal, Infra-red and ultra-violet). The passport tri scan must meet minimum industry standard requirements. Prior to digitising the valid passport/travel document the Supplier shall: • Compare the Customer's passport photo against the Customer. • Conduct a check as prescribed by the Authority of the passport's optically variable safeguards and watermarks in accordance with the Authority's training. • Carry out a manual count of the passport pages to ensure all pages are present and sequential (i.e. pages run from 1-40 in the correct order and no pages are missing). To note, this instruction applies only to the valid passport/travel document. Any additional passports/travel documents the Customer wishes to supply should be treated as Supporting Evidence and copies provided for digitisation with all other Supporting Evidence.	The Authority shall provide Appropriate Fraud Training.
R1-49	**Passport Submission**	Unused	Unused

Number	Requirement	Description	Authority Responsibilities
R1-50	**Travel Document and Evidence Referral**	If the Supplier's staff has any concerns with the passport/Supporting Evidence after conducting the checks as per R1-48, it should be referred to the Authority as identified in the "Standard Operating Procedures" document.	The Authority is to provide Standard Operating Procedures regarding the referral process of concerns towards passport/Supporting Evidence.

2.6 Priority Services

Number	Requirement	Description	Authority Responsibilities
R1-51	**Priority Services**	The Supplier shall process and submit all types of Priority Applications within the agreed service standards set by the Authority in Schedule 7 (**Performance Levels (KPIs**)). The Supplier shall use agreed naming conventions to identify Priority Applications in accordance with the Authority's "Standard Operating Procedures" document. The Authority shall approve any proposed bundling and marketing of Priority Services.	The Authority will supply Standard Operating Procedures in relation to agreed naming conventions.

2.7 Non-Digital Applications

Number	Requirement	Description	Authority Responsibilities
R1-52	**Exception – offline process – Continuation of application at Service Point Location**	For those Customers where no online form is available the supplier shall provide a solution to ensure the customers application process can be continued at the Service Point once the Authority has completed data entry and payment. The solution must allow attendance at Service Point Location, Biometric data capture and/or Supporting Evidence digitisation as outlined in R1-27 to R1-50. The Authority shall provide data on applicable routes that fall under this route.	

2.8 Added Value Services and Bespoke Services

Number	Requirement	Description	Authority Responsibilities
R1-53	**Added Value Services**	The Supplier shall offer and continually evolve a range of Added Value Services (AVS), through their knowledge of the market. The AVS could offer additional convenience, comfort and assistance to Customers and could include variations on delivery of the core Services as well as footfall products or services that may otherwise suit the Customer groups. Safeguards must be implemented to ensure that Customers are aware that the purchase of such AVS is not a mandatory requirement of the application process. The Supplier shall ensure AVS do not comprise of any age restricted or otherwise illegal or inappropriate services, or any services that could be seen as or are detrimental to protect the Brand, Reputation, Security and Confidentiality of the Authority. The Supplier shall adhere to relevant contract schedules when designing and delivering AVS.	

Number	Requirement	Description	Authority Responsibilities
R1-54	**Bespoke Services**	The Supplier shall offer bespoke Services for enrolment including provision of an on demand Service. The Supplier will need to standardise charges for the biometric enrolment element of the Service as regulated by the Authority's fee legislation, provided in the Data Room. The Supplier may offer these Services as part of an Added Value Service (AVS) package as highlighted in R1-53 providing they can demonstrate how charges relate back to the level set out in the Authority's fee regulations. The Supplier should ensure that the level of income, as generated by current Super Premium Mobile service (defined in the Data Room) is maintained. The Supplier will provide bespoke biometric Services outside a wider AVS package if requested by Customers.	

2.9 System Integration

R1-55	**Integrate with existing Authority systems**	The Supplier shall document and make available a System Design Document detailing the major system component, specification of items used in the solution covering servers, database, communication links and encryption methods for Production and Pre-Production environment. The Supplier shall transmit the Biometric Data and digitised Supporting Evidence from a central communication gateway that will be allowed to connect to the Authority. The network connectivity between the Supplier and the Authority will be established using secure VPN over the internet and through Internet Boundary Controls setup by the Authority. There will be no connection from individual Service Point Locations, static or mobile. The Supplier shall engage with the Authority to develop a Code of Connection. The Supplier shall use the Authority's Front End Services Application Programme Interface (FES API) to submit the digitised Supporting Evidence and Biometric Data. The FES API will provide endpoints – one for Supporting Evidence and another for Biometric Data. The Supplier shall not attempt to interface with any system belonging to the Authority without prior consent of the Authority. The Supplier shall be expected to package and send all the Biometric Data and metadata relating to one Customer in a single message to the FES API and similarly, package all digitised Supporting Evidence and metadata relating to one Customer in another message. The Authority will send an acknowledgement back on successful receipt of the data. In case of a failure/error response or absence of an acknowledgement, the Supplier will be expected to keep retrying until a successful acknowledgement is received from the Authority. The version of the Authority's FES API will change periodically and the Authority will notify the Supplier of those changes. The Supplier shall, if required make changes to their own systems to align with FES API changes	The Authority will work with the Supplier to agree a code of connection.

R1-56	**IT Service Management**	The Supplier shall, in collaboration with the Authority, produce a Service Delivery Model (SDM) to the satisfaction of the Authority in accordance with The Generic Service Obligations (GSOs) described in Schedule 27 **(Information Technology (IT))** Appendix 1 and to be aligned with the ITILv3 (2011) framework.	The Authority shall provide; GSOs Schedule 27 **(Information Technology (IT))** ITILv3 (2011) framework.