SCOTTISH PROCUREMENT

CONTRACT FOR THE PROVISION OF THE SCOTTISH GOVERNMENT BETA PAYMENTS PROJECT

INFORMATION AND INSTRUCTIONS TO TENDERERS

SP- 20 - 007

GENERAL INFORMATION FOR TENDERERS

Overview of the Requirement

Invitation to Tender (ITT) – Reference SP-20-007 – Contract Agreement for the Scottish Government Beta Payments Project

Due for Return by: 24 August 2020 – 12 noon

Overview of the Requirement

1. Overview of the Requirement

1.1 The Scottish Ministers, on behalf of Scottish Government, wish to award a Contract Agreement for the Beta Payments Project.

1.2 The Contract term is a term of 24 months with the option of further 5 extensions of 12 months which may be exercised wholly at the discretion of the Scottish Ministers

1.3 The contract commencement date is expected to be September 2020.

2. Background Information

2.1 The main objectives of the contract are:-

- Successful sourcing of a commercial partner to deliver the Beta phase of the Scottish Government Payments Programme
- Ensuring there are no barriers to moving from the Beta phase to the Live service.
- The project delivers on the following strategies:
  - Digital Strategy for Scotland
  - National Performance Framework
  - SG Procurement Strategy
  - Public Sector Reform Strategy

3. Tender Information

3.1 Tenderers must bear all costs incurred in the preparation and submission of their tender documents.

3.2 In addition, it is the responsibility of the Tenderer to obtain at their own expense, any additional information necessary for the preparation of the tender.

3.3 All information supplied by the Scottish Ministers in connection with the Invitation to Tender shall be treated as confidential by Tenderers except that such information may be disclosed for the purpose of obtaining sureties and quotations necessary for the preparation and submission of the tender.

3.4 Tenderers may be required to provide a Parent Company Guarantee. Tenderers must make it clear in their tender submission if they are not able conform to this requirement.

3.5 EU Exit:-
We reserve the right to treat any bid which is caveated by reference to the UK exiting the EU with or without a deal as non-compliant and, as with most procurement exercises, a bidder in submitting its price for evaluation does so in acceptance of all business risks and circumstances arising from time to time.

4. Evaluation Criteria

4.1 Tenderers will be evaluated against a series of Selection and Award criteria which are included in the Technical and Commercial envelopes within PCS-T (accessible through the advert in Public Contracts Scotland).

5. Language and Currency

5.1 Tenders must be submitted in the English language and priced in pounds sterling (£) exclusive of VAT.

6. Period of Offer Validity

6.1 Tenders shall remain valid and open for acceptance for 6 months after the tender submission deadline.

6.2 In exceptional circumstances, the Authority’s point of contact may request that the Tenderer extend the validity period for a specified additional period. Except for manifest error or as may otherwise expressly be agreed by both the Authority and the Tenderer, the contents of submitted Tenders will be deemed to be binding upon the Tenderer and open for acceptance by the Authority for the duration of the validity period. The Tenderer is therefore cautioned to verify its proposal before submission to the Authority since it is the Tenderer’s responsibility to ensure that a full appreciation, understanding and comprehension of the Services required, stated or implicit has been achieved prior to Tender submission. No claims will be accepted for items that arise from the Tenderer’s failure to meet these requirements.

7. Instructions for the Completion & Submission of Tender Documentation

7.1 The Invitation to Tender (ITT) must be completed and returned electronically through the PCS-T web portal – and specifically for the Digital Technology Services – Dynamic Purchasing System (Lot 1). Full guidance on the submission process is provided at the System Guidance document within the attachments for this ITT. No hard copies will be accepted. Correspondence connected with this ITT that requires attention before the closing date must be submitted using the PCS-T portal messaging area for this ITT.

7.2 Tenderers must complete all the questions as detailed in the Technical and Commercial Envelopes in the PCS-T System. Tenderers must complete the Technical and Commercial Envelopes within the ITT which comprises of questions relevant to every service under the Contract.

7.3 The Tender with the highest scoring compliant tender will be awarded the contract. In the event of a tie for the winning Tenderer the Authority reserves the right to appoint the tied Tenderer who obtained the highest quality score. In the event of a tie on scores, the Contract will awarded to the tied Tenderer with the highest score for the technical responses based on the following questions 3.1, then 1.2 and then 1.4.

7.4 All questions in the "Technical Envelope" and "Commercial Envelope" must be answered before the Tenderer submits their response.

7.5 Question weightings and Section Weightings, are detailed in the Evaluation Guide which are explained in this document at the 'Tender Evaluation Methodology' section. (Section 10)

7.6 The document "*ITT – Schedule 2b -Technical Response – Beta Payments Project*" provides a template which contains questions relating to the Contract Agreement and supporting Schedules. All questions should be answered using the template provided, which should then be attached to the question titled 'Tender Document Upload' within Section 1, Technical Envelope, in PCS-Tender, question 1.1.3. Please ensure you have answered all of the questions in the template before uploading and submitting your response. The 'Technical Response' question has been set as mandatory so the system will not allow you to submit your tender without first attaching your response document.

7.7 Treat each question and response in isolation and answer each question in full. Tenderers should not assume evaluators will read more than one answer so do not cross-refer between answers. Supporting information should not be sent in isolation, but only in support of specific questions where requested. Do not use links unless expressly directed to do so.

7.8 Only information provided as a direct response to a question will be evaluated. Tenderers should respond to the questions on the basis that the Authority has no prior knowledge of your organisation. Information and detail which forms part of the general company literature or promotional brochures, etc., will not form part of the evaluation process. General or irrelevant marketing material should not be included.

7.9 Please note for all responses in the ITT (particularly for questions where longer responses are required) it is helpful if Tenderers use plain English and punctuate their answers where appropriate using headings, sections and/or bullet points. This will assist evaluators to find the information necessary to enable them to score accurately.

7.10 The document "*Beta Payments Project – Commercial Evaluation Template*" should be completed then uploaded into the Commercial - Price Section of the Commercial envelope – Question 2.1.1 in PCS-Tender.

7.11 Tenderers must demonstrate their level of cyber security within their organisation and be need to complete the relevant Supplier Assurance Questionnaire (SAQ) using the Scottish Cyber Assessment Service (SCAS).
The Cyber Risk Profile for this contract is Moderate (The second highest)
A link to SCAS can be found here: https://cyberassessment.gov.scot/ .
Tenderers should use the link provided and enter the following unique Cyber Risk Assessment Reference numbers – RAR - VHBD2YM9. It is a requirement upon all tenders to complete the questionnaire on the SCAS site and submit a downloadable SAQ report as part of the tenderers submission.
Tenderers are recommended to access the SAQ at the start of the tendering process, so ensure adequate time to complete all questions.
The Supplier Assurance Questionnaire must be completed and attached to Section 1 Technical Envelope in PCS Tender 1.1.4. Please note although this is mandatory to complete, it does not have pass / fail criteria and a Cyber Implementation Plan will be completed to address any mitigation actions that will be necessary.

7.12 The Authority will not enter into detailed discussions with Tenderers in relation to its requirements at this stage. All questions regarding the content of this ITT should be directed through the dedicated PCS-T messaging area by **17 August 2020 – 5 pm**. No other form of communication will be accepted.

7.13 If the Authority considers any questions or requests for clarification to be of material significance, both the query and the response will be communicated to all Tenderers that have expressed interest in this ITT. The Authority will take steps not to identify the source of the query. Tenderers should indicate if they do not want their question and response circulated. The Authority reserves the right to circulate if not doing so would breach the principle of equal treatment. The Authority will aim to have a response to all questions raised by bidders 5 days before the tender return date.

7.14 Tenderers are asked to provide a single point of contact in their organisation for their response to the ITT in PCS-T. The Authority shall not be responsible for contacting Tenderers through any route other than the nominated PCS-T contact. Tenderers must therefore keep their contact details on the PCS-T system up to date or they will be unable to receive communications from the Authority. Tenderers must also undertake to notify any changes to their single point of contact promptly.

7.15 Completed Invitation to Tenders must be submitted via PCS-T portal by the deadline of **24 August 2020 – 12 noon.** All submissions from the Tenderers will remain sealed on the PCS-T system until the deadline. Please note that your response will not actually be submitted until you press the "submit response" button. You will then receive a confirmation email that your response has been received. You may amend your submitted response up until the closing deadline.

The Authority will not be able to see your response until the closing deadline date has passed.

7.16 We strongly advise that you submit your electronic response well in advance of the deadline to allow sufficient time for uploading.

7.17 Tenderers are reminded that they can check and amend their submissions after they have been submitted and up until the deadline. In the event that a Tenderer submits their tender more than once, PCS-T will only accept the final version of the tender submission.

7.18 Any attachments to be added into the PCS-Tender system must be virus checked using up-to-date virus software, with any viruses found removed, before uploading into the system.

7.19 The Scottish Ministers shall not be liable for the loss, damage or destruction of files submitted via the PCS-Tender system, however caused. Corruption or issues regarding readability of files submitted via the PCS-Tender system will not be discovered by the Scottish Ministers until after the tender submission deadline.

7.20 If you experience any technical difficulties, please seek advice through the PCS-T customer services helpline on 0800 069 8630 or via the contact us link on the webpage. The Authority cannot assist you with technical matters and PCS-T customer services cannot help you once the tender return deadline has passed.

7.21 Should you decline to tender the Authority would request that you provide a brief reason for doing so. This information will help us improve our tender processes in future. Any responses of this nature will be kept confidential.

8. Award Criteria

8.1 The Authority is not bound to accept the lowest cost or any tender. The Award Criteria will include consideration of Technical (Quality) aspects as well as Commercial (Price).

8.2 Each tender will be subjected to a Technical and Commercial evaluation. The aim of the evaluations is to select tenders which represents the Most Economically Advantageous Tender (MEAT). Upon completion of the Technical (Quality) evaluation and the Price (Commercial) evaluation, Tenders will be subject to a Price/Quality Ratio (PQR) calculation.

8.3 The PQR to be used will be 30% Price to 70% Quality and the PQR calculation will determine the Most Economically Advantageous Tenderer.

8.4 The Technical (Quality) evaluation will assess how well each tender has met the criteria set down in the Technical Envelope. The Commercial (Price) evaluation will assess how well each tender has met the criteria set down in the Commercial Envelope. The Tenderer must therefore take care to ensure that in their tender they address and make clear how they propose to fulfil each aspect of the Invitation to Tender.

8.5 To complete the MEAT evaluation, a tender rating system will be used and the criteria and weightings for this are explained in this document at Section 'Tender Evaluation Methodology'

8.6 Any Contract Agreement awarded as a result of this tendering exercise will be subject to the agreed Terms and Conditions as issued with this tender.

9. Indicative Procurement Timetable

9.1 The Authority has provided an indicative timetable of Procurement activity, below. Please note that the dates below are best estimates and may be subject to change.

Date By	Activity
13 July 2020	Issue ITT via Public Contracts Scotland - Tender website (DPS)
17 August 2020 5pm	Final date for clarification questions
24 August 2020 12 noon	Tender return date
18 September 2020	Complete evaluation of Tender responses
w/c 28 September 2020	Contract Agreement Award

10. Tender Evaluation Methodology

Tender Evaluation

10.1 The Authority will evaluate tenderers proposals on the basis of the Most Economically Advantageous Tender. This will be done using a combination of the technical and commercial scores awarded to each bidder. The Technical response will be evaluated independently of the Commercial response

10.2 The evaluation of tenders will be led by Digital Commercial Services in collaboration with representatives from across Scottish Government.

10.3 Prior to commencing the evaluation of tenderers technical and commercial responses, all tender submissions will be checked for completeness and accuracy by Digital Commercial Services.

10.4 Only information provided as a direct response to the Invitation to Tender will be evaluated. Tenderers should not embed URLs in response to any questions as these will not be evaluated. Information and detail which forms part of general company literature or marketing or promotional material etc. should not be submitted by tenderers and will not be evaluated.

Tender Evaluation – Submission of Proposals

10.5 In order to be considered for award, Tenderers must:

- Read all of the tender documents contained within the Buyer Attachments section on PCS-Tender.

- Complete upload any attachments, including the Form of Tender, within PCS-Tender.

- Complete and upload the document titled '*'ITT – Schedule 2b -Technical Response – Beta Payments Project*'' within the Technical Response of PCS-Tender.

- Complete and upload the document titled *'Beta Payments Project - Commercial Evaluation Template'* within the Commercial Response within PCS-Tender.

- Complete and submit the *'Scottish Cyber Assessment Service Supplier Assurance Questionnaire'* .

Tender Evaluation – Process

10.6 The evaluation will be conducted in as follows:

- Tenders will be assessed to ensure compliance with the Instructions to Tenderers. Any Tenderer failing to comply with these instructions may be eliminated from the procurement.

- An evaluation of each answer in the Technical (Quality) Response section. Failure to answer all questions contained in the Technical Response Template will reduce the maximum score available.

- An evaluation of the Commercial (Price) Response.

Tender Evaluation – Scoring

10.7 The evaluation panel will score Tenderers' responses to the Technical response against the published criteria.

10.8 Each section contains a number of questions with a combined total score of 100%. Sub-sections are individually weighted to reflect their importance. Each section is weighted to a combined total of 100%. Unless explicitly stated otherwise in the ITT, evaluators will award a score in accordance with the criteria below:

0% - Unacceptable	Nil or inadequate response. Fails to demonstrate an ability to meet the requirement.
25% - Poor	Response is partially relevant and poor. The response addresses some elements of the requirement but contains insufficient/limited detail or explanation to demonstrate how the requirement will be fulfilled.
50% - Acceptable	Response is relevant and acceptable. The response addresses a broad understanding of the requirement but may lack details on how the requirement will be fulfilled in certain areas.
75% - Good	Response is relevant and good. The response is sufficiently detailed to demonstrate a good understanding and provides details on how the requirements will be fulfilled.
100% - Excellent	Response is completely relevant and excellent overall. The response is comprehensive, unambiguous and demonstrates a thorough understanding of the requirement and provides details of how the requirement will be met in full.

11. Price–Quality (Commercial–Technical) Ratio

11.1 The overall award criteria will be based on 70% Quality (Technical) and 30% Price (Commercial).

Quality (Technical) Evaluation – 70 %

11.2 The Quality (Technical) response which will account for 70% the total Price-Quality ratio, will be scored out of 100% and each section and sub-section will be weighted as detailed in the table below. (Please note Section and Question numbers reflect the numbering contained in PCS-Tender)

11.3 The marks awarded will be based on the evidence submitted in the tender submissions, including any relevant attachments. Evaluators will consider each submission independently of other evaluators. Each evaluator will award a mark (0%, 25%, 50%, 75%, 100%) for each question in accordance with the methodology detailed in 10.8 above.

11.4 Once each Evaluator has independently evaluated each of the tender submissions, a Moderation Meeting will be held between the Evaluators. This meeting takes place to ensure that the questions and answers have been understood in the same way by the different Evaluators. The final score for each question will then be calculated using the mean average of the individual scores of all evaluators. (Mean average scores will be rounded to 2 decimal places) The arithmetical mean average of all evaluators’ scores will then be multiplied by the relevant question weighting to give the final weighted score for each question.

11.5 Each question weighted score, in a section, will then be added together to provide a total for each section and this will be multiplied by the relevant section weighting to give the total section weighted score. The section weighted scores will be added together to give the total of the technical section scores.

11.6 The total of the technical section scores will be multiplied by the Quality (Technical) Award Criteria weighting i.e. (%) to give the overall Technical (Quality) score.

11.7 For the avoidance of doubt, a tenderer can only achieve the maximum Quality (Technical) score i.e. 70% if the arithmetical mean average score achieved for each Quality (Technical) question is 100%. This will result in Overall Technical (Quality) Score of 70%.

See Annex A for an illustrative example of the Technical Score calculation

11.8 Tenderers must complete the Commercial Envelope contained in PCS-Tender, including the attachment of the Commercial Evaluation Template.

11.9 The technical response will account for 70% of the total score. The ratio, will be scored out of 100% and each section as follows:

Section	**Section Weighting**	**Sub Weighting**
Section 1 – Cultural Fit and Proposed Teams	35%	
Question 1.1 – Cultural Fit		10%
Question 1.2 – Proposed Teams		40%
Question 1.3 – On-boarding		10%
Question 1.4 –Scaling the Team		40%
Section 2 – User Centred Design	20%	
Question 2.1 – User Centre Design Approach		50%
Question 2.2 – User Centre Design Support		50%
Section 3 – Technical Solution	40%	
Question 3.1 – Outline Design		50%
Question 3.2 – Support		15%
Question 3.3 – Use of Knowledge		5%
Question 3.4 - Licencing		15%

Question 3.5 – Hosting		15%
Section 4 – Corporate Social Responsibility	5%	
Question 4.1 – Fair Work Matters		100%

Pricing Evaluation

NOTE: The following details the process in respect to the pricing that Tenderers will enter for the purposes of the pricing evaluation. All prices are to be entered in to the Commercial Evaluation Template. More detailed instructions are included in the template.

Under the section criteria

11.10 Tenderers are to provide a price for the roles listed in Commercial Evaluation Template. Tenderers should note that the resources which they detail in this document must directly relate to the information provided in the answer given for Question 1.2 in the Technical Questions (Schedule 2B)

11.11 The Price (Commercial) response, which will account for 30% of the total Price-Quality ratio, will be scored out of 100%.

The Tenderer with the lowest “Total Tender Price” will be awarded 100% of the available Price (Commercial) score i.e. 30%. All other Tenderers will be awarded a score proportionate to that of the highest score calculated as follows:

Price Score = [Lowest Tendered Price / Tenderer’s Price x 100] x 30%

A worked example is provided in Annex A below.

Total Score & Award

11.12 Tenderers Quality (Technical) score and Price (Commercial) score will be combined to give a total score for each compliant tender.

11.13 Scottish Ministers will award the contract to the winning supplier.

12. CONDITIONS OF TENDERING

Right to Reject and/or Disqualify

12.1 The Authority reserves the right to reject or exclude from the procurement process a Tender, where the Tenderer has failed to submit a response which is in compliance with the requirements of the ITT; the ITT response is submitted late;

is completed incorrectly or is incomplete; the Tenderer fails to respond in satisfactory terms to a request by the Authority for supplementary information or to provide clarity in relation to the Tenderer's response to the ITT; or the Tenderer or any of its sub-contractors or consortium members is/are guilty of serious misrepresentation in relation to its response to the ITT and/or the procurement process.

Tenderer Composition

12.2 In the event that a Tenderer alters its composition (which shall include, but not be limited to, a change in the identity of any entity named in the ITT response whose capacity has been relied upon in responding to the ITT), the Authority reserves the right to request that any proposed reconstituted Tenderer complete the selection part of the ITT i.e. Business Probity, Criminal Convictions and Financial Standing for re-evaluation in accordance with the criteria used in relation to the evaluation of the original ITT response.

Late Tenders

12.3 It is the responsibility of all Tenderers to ensure that their ITT response is submitted no later than the appointed date and time. Responses received after that time may not be considered. Completed Tenders may be submitted at any time before the closing date.

Relevant and Appropriate Responses

12.4 Tenderers must ensure that they read each question carefully, that all answers you provide are relevant, and that each question is completed in full. All information must be provided in English. Only information provided as a direct response to the questions contained in the ITT will be evaluated.

12.5 Supplementary documentation may be uploaded as part of your response where you have been directed to do so. Such material must be clearly marked and named in accordance with the instructions.

12.6 Once you have submitted your response to this ITT you will receive an automated system e-mail confirming receipt of your submitted response.

Requests for Clarification or Further Information

12.7 Subject to the terms of the Regulations, the Authority expressly reserves the right to require a Tenderer to provide additional written information supplementing or clarifying any of the information provided by that Tenderer in response to requests for information or questions contained in the ITT.

Misleading or Falsification of Documents

12.8 The Tenderer should be aware that should any of its responses be found to be deliberately misleading or falsified, the bidding organisation may be disqualified from the tender process. If the Tenderer provides false information regarding any criminal convictions or business probity the Tenderer may also be guilty of a criminal offence.

Freedom of Information

12.9 Nothing in this ITT shall preclude the Authority from making public, under the Freedom of Information (Scotland) Act 2002(“FOISA”) and/or the Environmental Information (Scotland) Regulations 2004 (“EIRS”) or otherwise, details of all matters relating to this ITT and responses thereto unless such details fall within an exemption under FOISA and/or EIRS as may be applicable at the discretion of the Authority and the Authority (at its sole discretion) consider that such exemption shall apply, and (in respect of commercially sensitive information only) a Tenderer has advised the Authority in writing that disclosure of specified information would or would be likely to substantially prejudice the commercial interests of any person (including but not limited to the Tenderer or the Authority).

12.10 Tenderers should also note that the receipt of any material or document marked “confidential” or equivalent by the Authority should not be taken to mean that the Authority accepts any duty of confidence by virtue of that marking.

Constitution of Contracts

12.11 No information contained in this ITT or in any communication made between the Authority and any Tenderers in connection with this ITT shall be relied upon as constituting a contract, agreement, warranty or representation as to the Authority’s ultimate decision in relation to the requirement which is the subject matter of this ITT or that any contract or framework agreement shall be awarded or entered into pursuant to this ITT.

Canvassing

12.12 Direct or indirect canvassing of any elected official, public sector employee or agent by any Tenderer concerning this requirement, or any attempt to procure information from any elected official, public sector employee or agent concerning this ITT may result in the disqualification of the Tenderer from consideration for this requirement.

Right to Cancel, Clarify or Vary the Process

12.13 Subject to the terms of the Regulations, the Authority expressly reserves the right to change, without notice, the basis of, or the procedures for, this procurement process or to terminate the process at any time.

Non-Conclusive

12.14 The ITT does not purport to be all-inclusive or to contain all of the information that a Tenderer, or any of its sub-contractors or any consortium member, may require. Tenderers must make their own independent assessment in relation to the subject matter of this ITT and all matters relevant thereto after making investigation and taking such professional advice as they deem necessary. In no circumstances shall the Authority or its advisors, consultants, employees or agent incur any liability or responsibility arising out of or in respect of the issue of this ITT.

No Representation or Warranty

12.15 The Authority, its advisers, officers, members, employees, other staff and agents: make no representation or warranty (express or implied) as to the accuracy, reasonableness or completeness of the information contained in this ITT; accept no responsibility for the information contained in this ITT or for its fairness, accuracy or completeness; shall not be liable for any loss or damage (other than in respect of fraudulent misrepresentation) as a result of reliance on the information contained in this ITT or any subsequent communication.

Collusion

12.16 The Tenderer certifies that this is a bona fide tender submission, intended to be competitive, and it has not fixed or adjusted the tender by, under or in accordance with any agreement or arrangement with any other person or Tenderer. The Tenderer also certifies that it has not done and it undertakes that it will not do at any time before the returnable date for this tender any of the following acts:-

- Communicating to any person the content of the tender herewith submitted;

- Entering into any agreement or arrangement with any person that he/she shall refrain from submitting a tender or as to the content of any tender to be submitted; and

- Offering or paying or giving or agreeing to pay or give any sum of money or consideration directly or indirectly to any Tenderer for doing or having done or causing or having caused to be done in relation to any other tender or proposed tender for the said work any act or thing of the sort described above.

Conflict of Interest

12.17 Tenderers must disclose in their ITT response (by answering the conflict of interest questions found within the ITT’s qualification envelope) any circumstances, including, without limitation, personal financial and business activities that would, or may be likely to, give rise to a conflict of interest between the Authority and/or any sub-contractors or members of the Tenderer’s consortium and the Tenderer. Where a Tenderer identifies any actual or potential conflicts of interest in their response to this ITT, it must state how it intends to avoid such conflicts. The Authority reserves the right to reject any response to this ITT which, in the Authority’s opinion, gives rise, or may be likely to give rise to, a conflict of interest.

Consortium Bids

12.18 You will be required to indicate if you are intending to form a Consortium, to deliver main elements of required services you are bidding for under this Contract Agreement.

12.19 The Lead Tenderer must answer all the qualification, technical and commercial ITT questions on behalf of the Consortium as a whole.

No Inducement or Incentive

12.20 The Invitation to Tender is issued on the basis that nothing contained in it shall constitute an inducement or incentive nor shall have in any other way persuaded a Tenderer to submit a tender or enter into any contractual agreement.

Privacy Notice

12.21 Please note the attached link to the Privacy Notice for ITTs.

https://www.gov.scot/publications/scottish-procurement-and-property-directorate-privacy-notice-for-invitation-to-tender-itt/

Annex A

A worked **example**** of the methodology applied to calculating the Quality (Technical) and Price (Commercial) scores using a Price-Quality Ratio of 30%-70% is shown below:

*****(Please note these tables are examples only and do not reflect actual % or values in the Payments Beta Phase Template)***

Quality (Technical) Score 70%

Question	Question Weighting	Section Weighting	Maximum Weighted Score per Question
1.1	40%	12.5%	5.00%
1.2	30%		3.75%
1.3	30%		3.75%

Evaluator scores below are for illustrative purposes only.

Question	Evaluator 1	Evaluator 2	Evaluator 3	Mean Average	Question Weighting	Section Weighting
1.1	75	50	75	(75+50+75)/3 = **66.67**	66.67*40%=**26.67**	26.67*12.5% **= 3.33**
1.2	100	75	75	(100+75+75)/3 = **83.33**	83.33*30% **= 25.00**	25.00*12.5% = **3.13**
1.3	100	100	100	(100+100+100)/3 = **100**	100*30% **= 30**	30.00*12.5% = **3.75**
					Total weighted section score	**10.3**

Total Price (Commercial) Score (30%)

Total Price (Commercial) Evaluation Score = [[Lowest Tendered Price / Tendered Price] x 100] x 30%

The score calculation to establish the Total Price Score are shown in the next 2 tables. Scores and prices below are for illustrative purposes only:

Tenderer	Total Weighted Price	Proportionate Score Relative to Lowest Price	Price Score (Maximum 30)
1	£351	(343/351)*100 = **97.7**	97.7*30% = **29.31**
2	£343	(343/343)*100 = **100**	100*30% = **30**
3	£397	(343/397)*100 = **86.4**	86.4*30%= **25.92**

Total Evaluation Score

- The Weighted Score of the Quality and Price evaluation is added together to give the Total Evaluation Score as shown below.
- Please note the scores below are for illustrative purposes only.

Tenderer	Technical Score (Example)	Technical Weighted Score (Example)		Price Weighted Score (from table above)		Total Evaluation Score	Rank
1	78	78*70% = **54.6**	+	**29.31**	**=**	**83.91**	**1**
2	68	68*70% = **47.6**	+	**30**	**=**	**77.6**	**2**
3	62	62*70% = **43.4**	+	**25.92**	**=**	**69.32**	**3**

Scottish Government
Riaghaltas na h-Alba
gov.scot

CONTRACT FOR THE PROVISION OF THE SCOTTISH GOVERNMENT BETA PAYMENTS PROJECT

SCHEDULE 2B

TECHNICAL RESPONSE TEMPLATE

SP-20-007

Instructions

Tenderers Guidance

Tenderers should complete the questions within this Technical Response Template in the spaces provided below each question. These will expand to accommodate your full response. However, Tenderers should aim to keep their answers as concise as possible. Tenderers are instructed to provide an answer for each question failure to do so may lead to the bid being deemed non-compliant.

Once complete Tenderers are requested to upload this document to the Technical Envelope within PCS-Tender Question 1.1.3.

Please ensure you have answered all of the questions in the document before uploading your response. Please note that there is a 100 MB file limit on attachment questions within PCS-Tender, contractors are advised to use a zip file or the general attachment area should Technical Responses exceed this limit. Contractors should aim to keep their answers as concise as possible.

The Technical Response contains questions relating to the Contract and supporting specification schedule. A reference has been provided against each question in parenthesis e.g. (Schedule 2a - Section 1).

The Information and Instruction to Tenderers document provides further information about the scoring and weighting of each section and the questions contained within.

Responses should provide a complete answer to each question without cross-referencing to other areas in the response template.

Only the information provided in the tender submission will be evaluated.

Tenderers must also provide details of any services which will be carried out by Sub-Contractors or Consortia members in delivering the core requirements and clearly articulate how this will be delivered in practice.

Tenderers should be aware that information provided in response to the questions contained within this document will be classified as Service Provider Sensitive Information (see clause 17 of the Contract Agreement) and will only be used by the evaluation panel to score the response.

The information will be treated as confidential, and all evaluators will be required to complete and sign a confidentially/non-disclosure and conflict of interest declaration prior to being given access to the tenderers responses.

Section 1. CULTURAL FIT AND PROPOSED TEAM – Section Weighting - 35%

Question 1.1 – CULTURAL FIT (Schedule 2A – Appendix G) – Question Weighting – 10%

It is important that Tenderers can demonstrate experience in working as part of a team within a complex organisation, providing detailed examples of:

- Projects or programmes involving multiple stakeholder organisations
- Challenging the status quo to improve ways of working
- Adapting to change, for instance as a result of a change in requirement
- Challenge and modifying project plans iteratively to ensure the best outcomes are delivered
- Surfacing problems early-on to anticipate risks and avoid failure

Tenderers should describe how they intend working with Scottish Government (SG) as part of a multi-disciplinary team which may include other suppliers, using Agile methodology.

They should also demonstrate the ability to work alongside third-party suppliers who may be involved in the quality assurance of their work and may hold a responsibility with respect to the approval by SG of certain service features.

Tenderers Response:

Question 1.2 – PROPOSED TEAM – (Schedule 2A – Appendix G) – Question Weighting – 40%

Tenderers should provide details of the proposed team they will provide to deliver the services over the two year Beta phase, and should include:

- An organisation chart outlining the team structure, accountability, communication and reporting structure, with a description of roles and responsibilities of staff members and how the work will be divided
- The response should specify all members of staff, including service delivery and service support
- An estimation of the number of days each role is required throughout the duration of the contract
- Details of who will project manage this contract, highlighting their experience and specific skill set in relation to this commission

Tenderers should provide explanations to support the choice of roles and their duration and responses should correspond to the roles proposed in the commercial template (Pricing), as well as the proposed number of man-days per role.

In addition, Tenderers should include summaries of curriculum vitae (CV) **for leadership and design roles only**, highlighting the skills and experience of their team members in relation to their proposed roles and demonstrating:

- Solutions and technologies previously worked with, which should include experience in the technologies included in the tenderer's proposal
- Experience in using Agile to deliver services
- Experience of designing and delivering services within a public sector landscape, or any similar relevant experience which may be transferable

CVs should be limited to two pages and must be provided as a separate attachment to the response.

In the event team members need to be replaced, Tenderers should describe how they will provide assurance that any alternative team members proposed are similarly or better qualified to undertake the role than those they are replacing. This can include, for instance, details on the size of the workforce and the capacity for Tenderers to provide alternative members of staff.

Tenderers must also provide details of any services which will be carried out by Sub-Contractors or Consortia members, and provide a sample of CVs in the same proportion for each organisation.

Tenderer Response:

<u>Question 1.3 – On-boarding – (Schedule 2A – Section 2.6 / Appendix G) – Question Weighting – 10%</u>

Tenderers are asked to provide details of how they will mobilise key members of their team by the Contract Commencement date, paying particular attention to circumstances around remote working, as outlined in Section 2.6, and also noting that security of data and personnel is important to SG.

Tenderers should include the following details, as a minimum, within their response:

a) How they propose structuring project initiation to agree on plans for delivering the project alongside SG
b) How throughout the project they will maintain on-going flexibility in resources to ensure changes in demands through sprint planning process can be met, and on-board new staff when required
c) Any processes outstanding for their proposed team members in order to obtain basic Disclosure Scotland certificates prior to the contract start date

Tenderer Response:

<u>Question 1.4 – SCALING THE TEAM – (Schedule 2A – Appendix I) – Question Weighting – 40%</u>

The next iteration of the payment project will require multiple and parallel workstreams to ensure that SG can deliver on the expectations of the Beta phase.

Tenderers should describe their approach to working at scale and managing the complexity of multiple work packages across delivery teams. They should describe how they expect to coordinate teams, for instance if there is a particular approach to:

- Combining the work of building a platform and on-boarding organisations onto the service
- Splitting software components between several teams
- Dividing testing across teams

Tenderers should describe the shape of the teams, but also surface what involvement is required from SG in each team. They should also indicate how they propose to minimise dependencies between the teams and what risks will need to be managed and how.

Tenderers must also provide details of any services which will be carried out by Sub-Contractors or Consortia members.
Tenderer Response:

2. USER CENTRED DESIGN – Section Weighting – 20%

Question 2.1 - USER CENTRED DESIGN APPROACH (Schedule 2A – Section 3) – Question Weighting – 50%

Tenderers should describe their approach and methodology to working collaboratively with operational staff, key stakeholders from public sector organisations and the project team. Responses should display how tenderers anticipate working according to Scottish Approach to Service Design. (https://www.gov.scot/publications/the-scottish-approach-to-service-design/)

Tenderers should include, as a minimum, details of the following:

a) Their approach to user research, including examples of how they would identify who they should be engaging with (e.g. reasons for engagement, level of involvement)
b) Their approach to co-design e.g. workshops, sense-making sessions etc.
c) How the tenderer expects to manage a co-design process, including participant recruitment and ethics
d) How the tenderer expects to make use of co-design tools and techniques, examples ideally spanning remote and in person user engagement
e) Their approach to sharing information and knowledge transfer within the project team
f) How the tenderer will handover the project e.g. mentor the SG team to take ownership of and support the service moving forward

Additionally, and following the impact of the COVID-19 pandemic (which means stakeholder and user engagement will be more complex), tenderers should indicate how they expect to approach user research and how some of the standard techniques have changed. This may for instance take into consideration constraints which come along with remote working, for instance in terms of adjusted timetables for those stakeholders who have to work flexibly at home.

Tenderers should also describe how they have used secure tools to ensure the confidentiality of conversations.

Tenderers must also provide details of any services which will be carried out by Sub-Contractors or Consortia members.

Tenderers Response:

Question 2.2 – DESIGN STANDARDS – (Schedule 2A – Section 3 / Appendix F) – Question Weighting – 50%

Tenders should describe how the Beta build will be designed, including:

- Information on how accessibility will be addressed

- What approach to usability testing will be used
- How the design will meet the criteria from the Digital First Service Standard
- Details of how User Experience (UX) will be factored into the design and development
- How the tenderer will include existing design patterns and libraries into the build

For reference, information on the Digital First Service Standard can be found by following this link: https://resources.mygov.scot/standards/digital-first/.

Tenderers must also provide details of any services which will be carried out by Sub-Contractors or Consortia members.

Tenderer Response:

3. TECHNICAL SOLUTION – Section Weighting – 40%

Question 3.1 - OUTLINE DESIGN - (Schedule 2A – Appendix A) – Question Weighting – 50%

The outline design provided in Appendix A of Schedule 2A – Specifications and Service Levels – describes SG's technical environments at the end of Alpha. The design was the result of iterations between SG and its partners, conducted over the course of Discovery and Alpha.

Code produced during these phases is available and is considered valuable for suppliers who wish to re-use it, however SG is aware that different technology choices are possible. In its current state the proposed design is subject to change, and this will depend on responses from tenderers and / or knowledge acquired by SG before and during delivery.

Tenderers are required to analyse the strengths and weaknesses of the design, and outline their approach to the design of Beta.

Within your response you should as a minimum:

a) Provide statements which support your critique (for both strengths and weaknesses)
b) Describe your reasoning for any design recommendations made
c) Identify any departures from the proposed architecture
d) Identify the benefits that you believe your recommendations bring to the solution
e) Highlight the risks of the proposed approach, and if relevant how some changes could help mitigate these risks
f) Identify any aspects of the proposed architecture that you believe cannot be achieved within the Beta development timeframe and support your statements with evidence

Tenderers must also provide details of any services which will be carried out by Sub-Contractors or Consortia members.

Tenderers Response:

Question 3.2 – SUPPORT - (Schedule 2A – Appendix E) – Question Weighting – 15%

Tenderers should describe how they propose to implement support arrangements once the service is operational and processing payments on behalf of public sector organisations partnering with the service in Beta.

Tenderers should also describe arrangements in place to ensure that the support team iterates with the project delivery team to ensure that the service is improved based on feedback.

Tenderers must also provide details of any services which will be carried out by Sub-Contractors or Consortia members.

Tenderer Response:

Question 3.3 – USE OF KNOWLEDGE - (Schedule 2A – Section 2.3 / Appendix D) – Question Weighting – 5%

Tenderers should describe how existing knowledge will be used within the project, and in particular they should describe:

- How they will bring any previous experience of other relevant implementations and demonstrate how these learnings will be applied to this service requirement.
- How they will consume and apply existing knowledge already collected by the SG Payments team, which will be shared with the supplier upon engagement, including for instance user research, technical knowledge or business process analysis.

In addition, tenderers should describe their approach to transferring knowledge to SG teams over the course of Beta and prior to the end of the contract.

Tenderer Response:

Question 3.4 – LICENSING – (Schedule 2A – Appendix C – NFR016/NFR033) – Question Weighting – 15%

Tenderers should describe their approach to licensing during and beyond Beta regarding technical components used by the payments project and not developed as part of the code.

In particular, tenderers should include in their response:

a) How they will prioritise the use of open-source components
b) The conditions under which they will use components which are not open source
c) Details of how they will ensure that the payment platform is not 'locked-in' to a technology product/s that will constrain future development of the payment platform and enables said technologies to be swapped for alternative technology product/s

Tenderers must also detail how this applies to any services which will be carried out by Sub-Contractors or Consortia members.

Tenderer Response:

Question 3.5 – CLOUD HOSTING – (Schedule 2A – Section 2 / Section 3 and Appendix C – NFR033) – Question Weighting – 15%

Tenderers should describe how they will manage the Cloud infrastructure in a way which will ensure that it is resilient and costs are optimised.

This should describe:

- Which environments will be required for development, quality assurance and live operation (including disaster recovery arrangements)
- How tenderers will manage integration and deployment to ensure the most efficient processes for development are in place
- How they can ensure that SG does not incur costs for Cloud infrastructure which is not used
- How they will manage the Cloud infrastructure so that it is optimised in the best and most efficient way
- How the Cloud infrastructure will be held securely within the Cloud Hosting environment
- Where the Cloud infrastructure will be hosted and confirm, if not hosted within the UK, how this can be transferred to a UK with no or minimal disruption to the service

Tenderers must also provide details of any services which will be carried out by Sub-Contractors or Consortia members.

Tenderer Response:

4. Corporate Social Responsibility - Section Weighting – 5 %

Question 4.1 - Fair Work Matters - Question Weighting 100%

The Public Sector in Scotland is committed to the delivery of high quality public services, and recognises that this is critically dependent on a workforce that is well-rewarded, well-motivated, well-led, has access to appropriate opportunities for training and skills development, are diverse and is engaged in decision making. These factors are also important for workforce recruitment and retention, and thus continuity of service.

For example, the Scottish Government is committed to being a fair work employer, which includes:

- Implementation of a fair and equal pay policy that includes a commitment to supporting the real Living Wage, including, for example being a Scottish Living Wage Accredited employer;
- clear managerial responsibility to nurture talent and help individuals fulfil their potential through support for learning and development, including for example Investors in People, a strong commitment to Modern Apprenticeships and the development of Scotland's young workforce, including Investors in Young People;
- promoting equality of opportunity and developing a workforce which reflects the population of Scotland in terms of protected characteristics such as age, gender, religion or belief, race, sexual orientation and disability;
- providing stability of employment and hours of work, and avoiding exploitative employment practices, including for example no inappropriate use of zero-hours contracts; that is, contracts which compel staff to make themselves available for work offered.
- Supporting flexible working and support for family friendly working and wider work life balance, including through the Healthy Working Lives Award Programme;
- supporting genuine and progressive workforce engagement, including recognition of trade unions and engagement with staff

In order to ensure the highest standards of service quality in this contract we expect contractors to take a similarly positive approach to fair work practices as part of a fair and equitable employment and reward package.

Question

Please describe how you will commit to Fair Work practices for workers (including any agency or sub-contractor workers) and Community Benefits, engaged in the delivery of this contract.

Answers need not be constrained to, or be reflective of, any examples given alongside this question. Good answers will reassure evaluators that your company is adopting relevant fair work practices in the delivery of the contract in line with the Fair Work Framework, see also 1 pager What is Fair Work – Information Sheet**.** For information on community benefits please also see Community Benefits in Public Procurement**.**

In your response you should **describe how you are adopting the 'Fair Work First' practices, a minimum ask of suppliers:**

- investment in skills and training
- no inappropriate use of zero hours contracts (for example using zero hours contracts when people are working regular hours; exclusive contracts that stop flexible workers working for other people)
- action to tackle the gender pay gap
- genuine workforce engagement such as trade union or employee association recognition, and
- fair pay for workers (for example, the real Living Wage, see 1 pager What is the real Living Wage - Information Sheet)

And adopting wider fair work practices, which in respect of this contract can include, for example a positive approach to rewarding staff at a level that helps tackle inequality (for example paying the real Living Wage); improves the wider diversity of your staff, such as improving the gender balance in supervisory and management roles; provide skills and training, for example to ensure a high quality of customer service and skills regarding health / safety matters; opportunities to use skills which help staff fulfil their potential (for example offering genuine career progression opportunities or accommodating lateral career movement); provides flexible working arrangements to accommodate a work / life balance; avoids exploitative employment practices, such as through the use of umbrella companies and promotes security of employment and that your company will demonstrate organisational integrity with regards to the delivery of those policies.

This reassurance can include a variety of practices which demonstrate your approach to fair work and should be tangible and measurable examples that can be monitored and reported during contract management procedures.

Tenderers Response:

Scottish Government
Riaghaltas na h-Alba
gov.scot

CONTRACT FOR THE PROVISION OF THE SCOTTISH GOVERNMENT BETA PAYMENTS PROJECT

SCHEDULE 2A – SPECIFICATION AND SERVICE LEVELS

SP-20-007

1. Introduction

The Scottish Government (SG) is looking to transform the way it facilitates payments across government and the wider public sector, with a long-term vision to design a continually improving and reliable shared service.

New devolved powers are transforming the functions of government, and its associated agencies, for the people of Scotland – this includes ability to deliver taxes, benefits and develop our policies around citizen's rights.

Citizens are increasingly demanding better quality services from government, mirroring their experiences in everyday life. Consumer services are leading the way and rapidly evolving to take advantage of improving technologies and new ways of doing things. Government is often left lagging behind.

In this context we have established a particular set of opportunities regarding payments. All across the public sector, there is a need to plan, execute and measure financial transactions. This includes paying money out to, and receiving money from, businesses, charities and citizens, and across other parts of central government, government agencies and local government.

Although there is a common thread and set of processes that underpins benefits, pensions, grants, licenses, or taxes, there is as yet no means by which to administer payments in a consistent way that harnesses the potential of flexible modern technology.

The subject of this procurement is the Beta phase of Scottish Government's common payments service. This is planned as a two-year phase, with potential extension solely at the discretion of Scottish Government. During this time the successful bidder will work with SG's payments team to deliver an operational payment platform, undertaking the necessary user engagement, development and support arrangements to deliver live outbound payments for a select group of organisations. Plans will also be made to scale the service to other organisations.

Throughout this document a number of terms and acronyms are used. A full list and definition of these can be found in Appendix K: Definition of terms.

2. Work to date

2.1. The current payments landscape in Scotland

Scottish Government's Payments Project commenced in 2018 with the aim of investigating the options around delivery of a common payments service and undertook the initial development of a payments platform.

Development and implementation of a series of common operating platforms is a core element of Scottish Government's Digital Strategy. Published in 2017, this strategy recognises that common platforms and services can both provide the foundation for new digital public services as well as improving legacy systems, to deliver results more effectively and at lower cost through single points of investment. It further suggests that platforms that operate horizontally, or across the typical, vertical organisational structures of government offer a potential approach to public service reform.

For Scotland, a common payments service stands out as a logical platform to develop because:

- Scottish Government needs to be equipped to rapidly respond to a significant increase in its public service responsibilities and currently cannot scale payment services quickly or cost-effectively
- The public sector needs to be better equipped to introduce or significantly modify services to address rapidly changing socio political circumstances
- The demand for payment services as part of SG's portfolio of public service delivery is growing rapidly, particularly in Social Security. Due to the need to ensure safe and secure transition, the new Social Security system has a heavy reliance on the UK Government and this is both expensive to operate and difficult to change
- Legacy financial management systems, particularly Scottish Government's Enterprise Accounting System (SEAS), require substantial work to sustain business as usual
- For the user, payments processing with the public sector in Scotland is deeply inconsistent and often frustrating or broken
- There is a significant amount of inefficient and in some cases insecure manual processing of payments across the SG

A number of projects undertaken by, and involving, Scottish Government's Digital Directorate have already established that there are currently many ways of making and receiving payments across government and the public sector. This includes in-depth discovery and prototyping work on Grants, Licensing and Social Security.

Through SEAS, SG already has experience in using a centrally-managed service for payments across multiple organisations in the public sector. The common payments service initiative will build on this principle, provide the capacity to manage larger volumes of payments and greatly increase the number of organisations able to make use of a more automated and self-managed service. Critically for the Scottish Government, the introduction of a common payments service will allow us to design a future proof, scalable service while simultaneously supporting our current SEAS-based ledger.

2.2. Discovery phase

Running from October 2018 – June 2019, there were two significant interlinking strands to the Discovery work:

- Creation of a business case to fully assess the current payments landscape and consider options and make recommendations for a future service. This included significant user research and business analysis across the Scottish public sector, and building an understanding of how other governments have approached similar challenges
- Development of a technical 'proof of concept' to test a number of key areas, including:
    - The ability to work with different organisations and data sources
    - Commercially assess if we could drive better value options for payment types
    - Use the data within the system to provide useful management information (MI) reporting
    - Scalability and volume processing
    - Minimising manual interventions and automating as much as we can

At a high level, the proof of concept covered ingestion of real legacy payment files; processing of inbound and outbound payments in a test environment; transaction reporting; reliability and bulk transaction testing and finally the transaction of real payments through the government banking partner.

Importantly, it also informed the business case by validating and challenging the project team's thinking and in doing so provided confidence based on practical hands-on experience and real data, rather than a hypothesis.

2.3. Alpha phase

The Alpha phase ran from September 2019 to March 2020 with the aim to develop the technology core of the platform and key capabilities of the service, and continue building knowledge by iterating with users. This involved taking forward some of the exploratory design and technology work undertaken in the previous proof of concept and developing it to an 'enterprise-grade', with an increased focus on scale and security. An overarching user story for Alpha was established: "As a public sector organisation, I want to be able pay a recipient, so that I can deliver the pay-out component of my service."

Based on the learnings from the Discovery phase and proof of concept, the Alpha phase prioritised bulk outbound payments. This is where the evidence base shows the greatest payment volumes, and therefore biggest demand, across the sector is. The largest volume of payments are to citizens for both pensions and benefits, which was a key factor in the decision to partner with three organisations who are key to the design and development of the service:

- As well as testing the end-to-end payment of a full benefit, alternative payment options such as voucher payments were tested. This is a critical part of the Social Security Agency (SSA) service and a necessary feature to ensure financial inclusion of, for example, the unbanked population in Scotland
- There is a need to provide the government with a trustable, auditable transaction history ensuring we have an immutable record of all payments – this was the focus of activity with Independent Living Fund (ILF) Scotland
- With Scottish Public Pensions Agency (SPPA) the focus was on international payments. SPPA currently pay 2,000 pensioners abroad every month, and there are potentially more efficient and cost effective ways of doing this

To co-design the service with each of the partners, Alpha started with a review of knowledge gained during Discovery and additional user research of current processes in each organisation to identify potential areas for improvement.

Through additional rounds of user testing with partner organisations, designs evolved into a distinct user Interface, which was subsequently implemented by the development team.

2.4. Alpha technology approach

In developing the technology, an approach (known as a "vertical slice" approach) was taken based on the following principles:

- There is a regular experience that a "big bang" approach is risky, can fail and/or overrun in time and on budgets
- To avoid this we identify areas where there is most value, and deliver these first
- This means we can provide usable capabilities earlier and reduce the risk of delivery
- Lower priorities are not de-scoped from the service

The overall structure of the Alpha work has built on, and learned from, the design used in the proof of concept stage. Whilst the overall target design conceived at proof of concept stage was for a build up a set of microservices, the emphasis was much more on understanding the integration of external service than on trying to assemble a production ready system. To that end the proof of concept codebase was monolithic even though the components of it were clearly separated in the code.

Whilst it was clear that significant elements of a payment platform already exist as separate components, there was no single off-the-shelf solution that would address the end-to-end functionality required.

At Alpha stage, there was still some balance between the need to learn and iterate rather than locking down the design, however there was a concerted effort to build components that could be taken forward to production with the minimum of additional work. All of the components were containerised into microservices orchestrated using Kubernetes and automatically scripted so that the environment can be created and torn down automatically in the Cloud or on a local development environment.

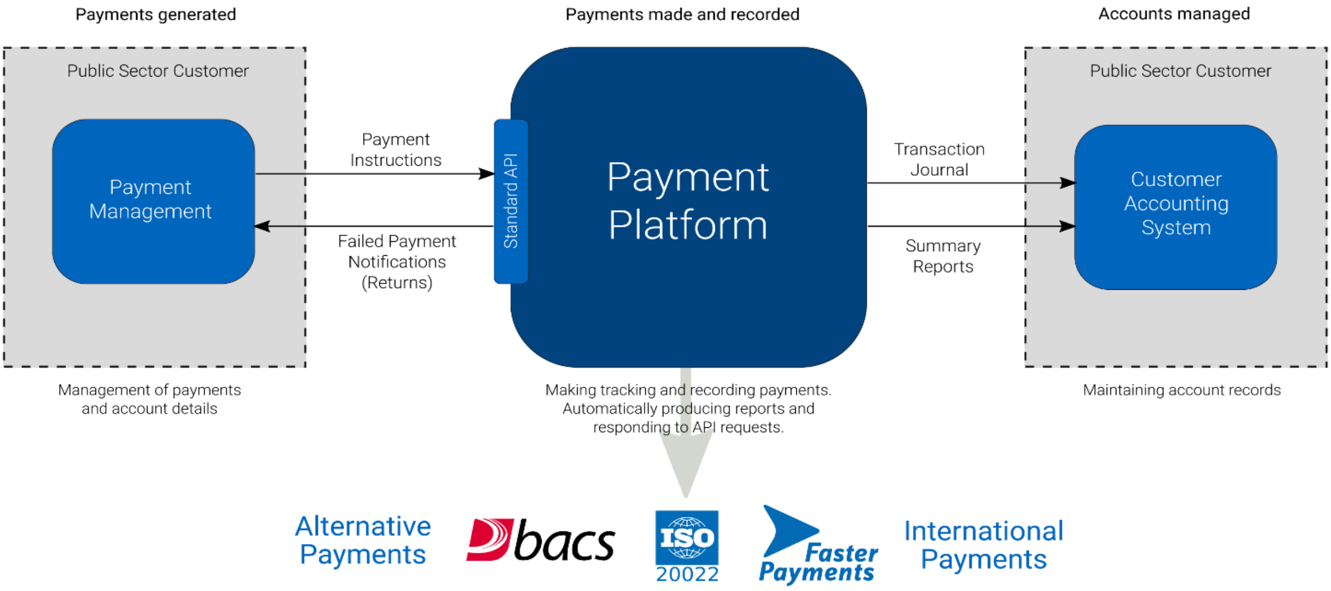
There was extensive use of off the shelf software as a service (SaaS) components from Amazon Web Services (AWS), but these were chosen and integrated in as generic a way as possible so that there are no fundamental and deep dependencies on particular AWS specific services.

2.5. Our long-term vision

The Business Case sets the course for designing a single, continually improving and reliable shared service. This service will allow Scottish Government to evolve payments services to meet changing user needs and minimise the need for individual client organisations to procure new technology, continue with inconsistent processes or rely on outdated systems.

The desire is to develop a standardised way of processing that is/has:

- Organisationally agnostic
- Secure and scalable
- Able to preserve transactional history
- Component-based, flexible and doesn’t break established workflows
- The ability to deliver management information and reporting at product core
- A clear set of rules of engagement for partner organisations to on-board and utilise the service
- The capability to connect multiple public sector organisations without them undertaking substantial technical work themselves
- Based around the needs of organisations and end users and has the ability to continually improve around changing needs


Payments generated
Payments made and recorded
Accounts managed
Public Sector Customer
Payment Management
Payment Instructions
Failed Payment Notifications (Returns)
Standard API
Payment Platform
Transaction Journal
Summary Reports
Public Sector Customer
Customer Accounting System
Management of payments and account details
Making tracking and recording payments. Automatically producing reports and responding to API requests.
Maintaining account records
Alternative Payments
bacs
ISO 20022
Faster Payments
International Payments

Payments process flow

We envisage that the payments platform will provide significant improvements to existing payments functionality and security, allowing its users to make their organisations more efficient and to provide a better service to their customers and partners. Specific features will include:

- Providing redundancy / fail-over for the payment system provider (PSP) by using multiple PSPs
- Combining BACS, Faster Payments, International Payments and alternative payments into one solution
- Providing mechanisms to automatically recover from issues like making late payments by using Faster Payments (even if the payment was originally submitted through BACS)
- Combining making payments with checking payment network return messages so users can track the success or failure of every payment in one place
- Interfacing with accounting systems so that it can act as the route not just for paying but for recording those payments in organisations accounts
- Implementing a non-repudiation framework, allowing organisations to simply prove the success or otherwise of transactions
- Providing consistent and easily accessible management information, including through a cloud service. Research consistently shows this is a recurring requirement.
- Requiring every organisation to digitally sign every payment request to enable automation and to significantly enhance the security over existing solutions

- Using immutable data stores so that all attempts to inject payments will be recorded and cannot be removed by any functionality of the system
- Providing a mechanism for tracking every payment from the organisations' originating systems through to completed transaction reports so that rogue payments can be identified even in the event of a major security breach
- Ensuring that all payments are encrypted in transit and storage and that development and operations team members have no command line access to systems running in production
- Providing a secure solution that meets both government standards and the security requirements of partner organisations

At a time when the UK Payments industry is undergoing massive change in ways that the public sector must conform to, and when cybercrime is ever increasing, it is unrealistic to expect every public sector organisation to have the necessary resource to individually address these changes and needs.

At the same time, without a payment platform to take a central responsibility for these critical security capabilities and infrastructure changes, there is no other option for the public sector than to separately and repeatedly procure skills and services from the private sector or elsewhere.

The development of a transformational common payments service will not only act to shift the way in which Scottish Government has traditionally approached technology development and service delivery, but also save money and improve resilience in the longer term.

2.6. The scope of this procurement – Beta phase

The focus of this procurement is to build on the knowledge and understanding gained in the previous project phases (Discovery and Alpha) and undertake work to support the development of a Beta phase for a common payments service.

The Beta phase will consider how the payment platform will integrate with, and replace, the means by which organisations currently make payments to citizens and businesses, and prepare for the transition to a live service.

We are looking to engage a partner (or consortium) to assist the delivery of the following:

- To move the existing outbound payment function for partner organisations to the new common payments service and making live payments. We are proposing that we work with the same public sector partners as the Alpha phase – ILF Scotland, SPPA and Social Security, as well as other key users of existing central government functionality

- Detailed roll-out plans and a defined pipeline of organisations to on-board to the service beyond Beta, based on current organisational engagement and the next phase of service design
- Necessary integration work with SEAS to ensure the processing of transactions is recorded within the corporate ledger
- BACS, international and alternative payments, reflecting the vast majority of outbound payment journeys across the public sector
- A customer support function once organisations are making live payments, so organisations can reliably use the service
- A comprehensive plan for the next phase of development and transition to a live service, to include other payment channels, inbound payments and development of additional functionality

It is required that the successful bidder will embed staff members with the SG project team. In light of the current COVID-19 restrictions on social distancing and the fact that some Scottish Government offices are closed, it is anticipated that the supplier will work with the project team on a remote (virtual) basis using agile practices to deliver the desired project outcomes. This will remain in place until such time that the offices in Edinburgh are re-opened to staff and it is safe for third parties to be on-site. The joint SG and supplier team will work together on refining detailed planning tasks on a sprint by sprint basis, with the supplier providing the necessarily skilled/experienced resources. The supplier is expected to work alongside other suppliers engaged in the delivery of the Payments Project.

The supplier is responsible for ensuring all their staff proposed will hold Disclosure Scotland certificates and be Baseline Personnel Security Standard (BPSS) cleared, following SG processes, prior to the contract start date in order to work with SG systems and equipment as well as on-site in SG offices.

Important note: for the purposes of Scottish Government's BPSS you will require a Basic Disclosure certificate from Disclosure Scotland (https://www.mygov.scot/basic-disclosure), for which you should apply upon submission of your tender responses. Criminal Record Checks from the Disclosure and Barring Service will not suffice for the purposes of BPSS as these are valid in England and Wales only for public sector engagements.

The Supplier will be required to have a full capacity of resources to commence work in September 2020, with on-going flexibility in resources to ensure changes in demands throughout the project.

3. Overall requirements

The role of the supplier is to deliver, set up or develop the following project requirements:-

- Infrastructure:
  - A secure development environment
  - Environments for building, developing and testing in the cloud
  - A production cloud environment with disaster recovery options across multiple availability zones
- A Core payment platform with:
  - Authentication and permissions
  - A standard API
  - BACS processing
  - Payment return reconciliation
  - Faster payments processing
  - International payments processing
  - Alternative payments processing
  - Disaster emergency payments - enabling payments to be re-issued based on previous historical batches in the event of significant client system failure
  - Account validation
- A Platform UI which enables users to:
  - View, approve, cancel and recall payments
  - Administer products
  - On-board new customers
- Customer Integrations with common components for:
  - Independent Living Fund Scotland
  - Scottish Public Pensions Agency
  - Scottish Government’s Financial Services Division (FSD), specifically with SEAS
  - Social Security Scotland
  - Up to four additional organisations
- Management Information through:
  - MI system integration and standard configuration
- Monitoring including:
  - Health, system and component monitoring
  - Log management
  - Event tracing
  - User analytics

In carrying out this work the supplier will be required to:

- Manage and coordinate the delivery of these requirements in close partnership with the SG team
- Design and develop the architecture, software, and user interfaces, making extensive use of automated build, deployment and testing throughout the process
- Design and develop the software and user interfaces in accordance with Digital First Service Standard and Scottish Approach to Service Design (SAtSD), including carrying out any associated user research and service design alongside SG staff. As with previous phases we will continue to co-design with users and build iteratively to respond to their feedback and changing demands
- Conduct usability testing as required, at appropriate points agreed with SG
- Support the overall team through the Digital First Service Standard assessment by providing suitable evidence for the work that has been carried out
- Manage and control secure configuration and release into production
- Supplying and managing the required cloud infrastructure, in accordance with SG's security policies and in line with the NCSC cloud security guidance
- Monitor and manage the live service ensuring that it delivers the required service levels
- Undertaking the necessary handover arrangements and knowledge transfer to SG staff
- Deliver appropriate training and guidance to users of the service
- Set up the initial support operation to meet partner organisation needs during Beta
- Work with third parties such as Government Banking Service, RBS/NatWest and National Cyber Security Centre (NCSC) to ensure conformance to standards and protocols

A more detailed explanation of the high level architecture and a more detailed list of the functional and non-functional requirements can be found in:

- Appendix A: High level architecture
- Appendix B: Functional requirements
- Appendix C: Non-functional requirements
- Appendix D: Transitional requirements
- Appendix E: Service delivery
- Appendix F: Testing and static analysis
- Appendix G: Working together
- Appendix H: The technology foundation
- Appendix I: Milestone plan
- Appendix J: Links to further information
- Appendix K: Definition of terms

4. Contract Management

4.1. Contract Management

The contract will be managed based on the project's sprint cycle through formal fortnightly face-to-face meetings between Scottish Government and the supplier, and will require provision of assets such as highlight reports, burndown charts, and review of the project risk register.

The frequency and standing agenda of these meetings will be reviewed and adjusted if mutually agreed.

4.2. Timescales

The contract shall commence on September 2020 and will run for a 2 year period with the option to extend the contract at the sole discretion of the Scottish Government.

Each and any extension periods can be up to one year in length. The extension of the contract will be limited to a maximum of five years.

5. Budget

The budget for this project is £4 million – £5.5 million excluding VAT and suppliers should cost their proposal within this range.

The budget includes all costs associated with the delivery of this service including any cloud hosting and licencing/technology (as detailed within this Schedule 2A) costs which will be planned in advance by the supplier, and agreed by SG, throughout the duration of the contract, and then passed through to SG at cost whether a direct cost or from a 3rd party.

Therefore it should be noted that the budget above is not restricted only to the resources that the tenderer is proposing for the contract.

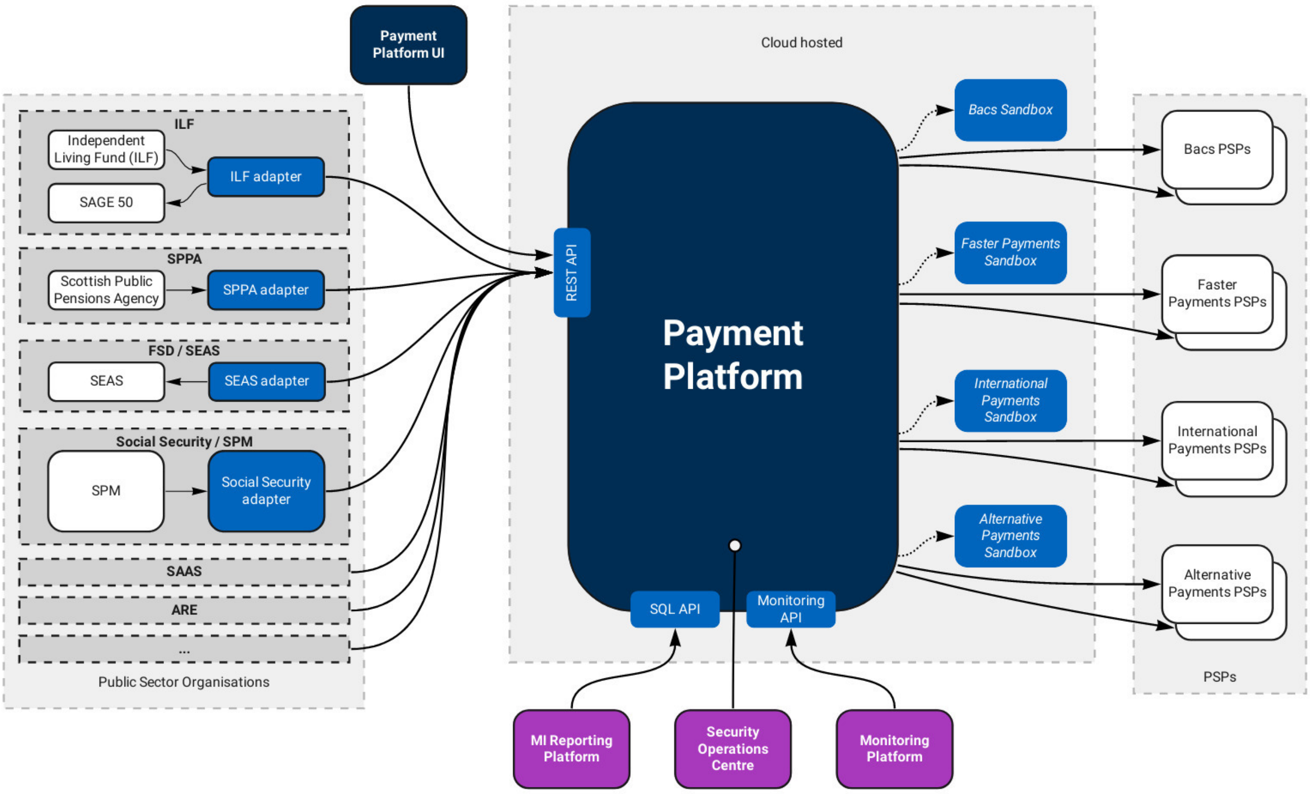
5.1. Payment schedule

The payment schedule for the project will be agreed during project initiation with the successful bidder. The payments will be linked to the desired project outcomes above and are expected to be paid quarterly in arrears.

Appendix A: High level architecture

A. 1. Components of the system

The following is a high level component diagram of the payment service which highlights significant parts of the overall service which will be required in Beta.



The **payment platform** (in the centre of the diagram) should be a cloud based platform with a standardised API. As a platform, its purpose is to provide a standard service that can be used by any public sector organisation that needs a payment service. Critically, the payment platform API should be well designed so that clients can be integrated by flexible use of the API rather than any bespoke changes to the core platform itself.

The **public sector organisations** (on the left hand side of the diagram) need to be integrated with the payment platform during beta. It is proposed that the integration is carried out by building and installing adapters into their platform environments that take existing payment requests and convert them into calls to the payment platform API.

It is crucial, in the early stages of moving into production, that the first organisations that move onto the payment platform have the reassurance of being able to switch back to their existing payment service. To test that the new service is behaving correctly, we would also like to be able to run the payment platform in parallel with their existing service, insofar as that is practically possible.

So, with respect the adapters:

- The adapters exist separately from the payment platform to ensure that the platform is standardised and does not require internal modification to accommodate new customers
- The adapters exist separately from the client systems during beta in order to limit modifications to client systems and preserve the existing methods of payment so that they can switch back during development if required
- Most existing integrations with payment providers involve the generation of a batch file which is sent by SFTP to a payment service. It is quite practical to intercept this file and convert it into calls to the payment platform API. However, to prevent payment requests being intercepted, we want to cryptographically sign payment requests before they leave the client system which prevents the use of an SFTP service hosted out with the client
- For some clients the adapters will just make payments. For others it will be necessary for the adapter to generate reports from the payment platform to match reports that are currently received from their existing payment service. The most complicated case is likely to be the various reporting requirements for Social Security, some of which feed into SEAS
- We expect that there will be a lot of common code between client adapters but some client environments may constrain technology choices and complicate the integration process

On the **right hand side of the diagram** there are a number of different PSPs. The payment platform will need to integrate with these in order to make payments. During beta SG will work with the commercial partner to evaluate which PSPs provide the necessary functionality at a competitive price whilst meeting any regulations or constraints imposed by the relationship of the payment service to the client organisations and to the government bank through the government banking contract.

The right hand side also shows a number of payment sandboxes. At the proof of concept stage, the Payments Project established that test sandbox environments provided by PSPs typically provide limited functionality and are insufficient for general testing. A BACS sandbox was developed during alpha and it is proposed that similar sandboxes are developed for all the PSP integrations in order to facilitate automated testing and the development of an ‘in production’ test environment for clients.

The **Payment Platform UI** (to the top left of the diagram) represents a standardised user interface for all users of the platform: client users and users who are providing customer service for the payment service as a whole. However, there is no obligation for this to be a single shared interface as long as it meets user needs.

Below the platform are three components:

- The **MI reporting platform** will need to be a highly configurable tool so that clients can generate real-time and periodic reports on payment types, values and volumes. It is anticipated that this will be an off-the-shelf system. Given the existing use of, and future need for, MI Platforms within SG, it is possible that the MI platform choice may be influenced by wider stakeholders
- The **monitoring platform** represents a single monitoring capability spanning all of the systems that the payment service is responsible for with the probable exception of the client adapters. It is anticipated that this will provide tools for monitoring system state and performance as well as provide mechanisms for tracing calls through the system for the purposes of debugging, support and fraud detection. There are wider stakeholders within SG for a standardised monitoring platform and this may influence technology choices made in partnership with the commercial partner
- The **security operation centre** (SOC) is critical to monitoring the security of the payment platform. Whilst the commercial partner will be required to design and build a secure system that can be monitored by the SOC, the commercial partner will not be responsible for setting up or running this

The high level separation of components reflects design decisions that have been made in partnership with the commercial partner for alpha. Whilst the aim of beta is to build on that work, that is not at the exclusion of alternatives. It is also possible that more detailed work with client organisations will introduce complications that we are currently unaware of.

A. 2. The design of core payment platform

The core payment platform has been designed with the following principles and design choices. We do not anticipate significant changes to these in beta but are open to well-argued proposals that deviate from these.

Immutable transaction log	Transactions are stored as a series of events that cannot be deleted. This facilitates high speed and robust storage and retrieval of transactions. It also simplifies distributed processing, backup and recovery. Note that, the exception to this rule is the mass deletion of all records after seven years.

Event sourcing	The fundamental record is not of the current state but the events from which the state of the system can be projected.
Command Query Responsibility Segregation (CQRS)	Mechanisms for storing and retrieving information are individually tuned and tailored for their use. So the processing of transactions uses queues whereas the handling of reporting uses SQL queries on a relational store with a materialised view of the linear event stores.
Containerised deployment	Components of the system are deployed as pre-built immutable containers that, for security reasons, cannot be logged in to or modified in production.
Microservices	The system is broken into components that can be individually scaled out to respond quickly to changes in demand. Although commonly referred to as microservices, the division into components should focus on loose coupling and the separation of concerns rather than on each component having a small single function.
Zero downtime deployments	The platform should be designed so that deployments do not require downtime and the service could be delivered 24 hours a day, 7 days a week even if this is not the initial requirement of the service.
Convention over configuration	Prefer being opinionated about how a particular task or feature is delivered and provide sensible defaults. Limit the amount of configuration available to instances where real value is delivered.

Self-serve over Centralised administration	Prefer giving clients the ability to self-serve using the platform, rather than require actions to be performed by a central team. The self-service capabilities should be made available through the API as well as the UI, so that the capabilities can be integrated into client systems rather than requiring users to switch between systems to complete their work.
Automate all payment platform processes were possible	Prefer automated operation and integration of the platform over requiring human intervention through the payment platform UI. Encourage client systems to use the payment platform API to build functionality into their own systems that simplify process flow. For example, if a client system is the place where payment details are entered, then it is probably the best place to be notified that the payment details were incorrect to provide the same user with the ability to rectify the situation without having to log into the payment platform.
Keep customer specific functionality outside the platform	The payment platform exists to be a consistent focused service that reliably and consistently operates for all customers. Customers migrating from existing payment solutions may rely on specific functionality that is not built into the payment platform. To facilitate the migration of such systems without forcing customers to adapt their own systems, this customer specific functionality is pushed out into ‘customer adapters’ that sit between the existing customer systems and the standardised API of the payment platform. The strategic aim of the payment platform is to encourage customers to directly integrate with the API (see below).

Encourage customers to directly integrate with the API and use the platform to drive process improvement	Whilst the customer adapters provide an interface between customer systems and the payment platform, the target architecture is one where customer systems connect directly to the payment platform API without any adapters. The payment platform API will enable functionality in customer systems. For example, customer systems could add live payment status information into their systems and allow staff to cancel payments directly within the time window where this is technically possible. Account detail entry screens could validate the account details directly with the payment platform and return immediate feedback where account details are clearly incorrect.

Appendix B: Functional requirements

The following functional requirements are broken down into the same high level capability groupings as presented in section 3 (Overall requirements). Each requirement describes a conceptual component of the system and the functionality required and includes a MoSCoW (Must Should Could Won't) rating. For the purposes of estimating the work of the Beta phase (this procurement) you should account for all of the "must" and "should" requirements as work to be done and the "could" requirements as future capabilities that the design must accommodate but not implement.

Each functional requirement has a reference code at the beginning of the function title. This reference forms no purpose in this document other than providing a consistent way of identifying a specific requirement should you need to do so in any communications.

Please note that this is an agile project and whilst this list reflects our best understanding of the critical components of the payment platform, this list of requirements will most likely be subject to change and may not be exhaustive.

B. 1. Capability grouping: Integration

FR053 The Integration API must accept payment files uploaded by SFTP

Currently SFTP is used by many customers as a mechanism for securely uploading payment files. The requirement to support this is only there to facilitate integration. However, due to additional security measures that will require payment files to be signed before they are transmitted, it may be more practical to integrate an adapter into the customer system and then transmit messages directly to the Payment API.

FR063 The Integration common code must automate the generation and flow of customised reports from the payment platform into customer specific formats and systems

Any customisation of these reports should take place in the adapter sitting outside the core platform. All requests should be made through standard platform APIs. There should be no special APIs or privileged ways of connecting into the payment platform to deliver this functionality.

FR061 The Integration common code must convert different formats of customer payment files into platform API calls

The conversion should take place in adapters that sit outside of the core platform so that the platform itself is always dealing with standardised data. All requests should be made through standard platform APIs. There should be no special APIs or privileged ways of connecting into the payment platform to deliver this functionality.

FR065 The Integration common code must ensure that payment requests from customers are electronically signed before they leave the client system

To prevent fraud, the payment platform should only make payments for requests that have been electronically signed by the customer system. To do this it may be necessary to place the customer adapter within the bounds of the customer system and provide code within the adapter to sign the requests it receives.

FR081 The Adapter for ILF must integrate ILF and SAGE 50 with the payment platform API

The ILF adapter, running alongside ILF systems, must be able to take existing batch payment instruction files and issue secure, signed payment requests to the payment platform API. This adapter must also be able to produce transaction reports (using the platform API) that can be fed into the ILF instance of SAGE 50.

FR082 The Adapter for SPPA must integrate SPPA with the payment platform API

The SPPA adapter, running alongside SPPA systems, must be able to take existing batch payment instruction files and linked international payment account details and issue secure, signed payment requests to the payment platform API.

FR083 The Adapter for Social Security must integrate Social Security with the payment platform API

The Social Security adapter, running alongside Social Security systems, must be able to take existing batch payment instruction files and issue secure, signed payment requests to the payment platform API. This adapter must also be able to automate the generation of a range of custom reports designed to replicate existing reports currently generated by their existing payment service.

FR084 The Adapter for SEAS must integrate SEAS with the payment platform API

The SEAS adapter, running alongside SEAS (the SG accounting system), must be able to integrate with SEAS to record transactions or summary transactions for those organisations that integrate with SEAS. This requirements currently covers SPPA and Social Security. Where possible, this adapter should be common to all organisations that integrate with SEAS and should not have to be modified to accommodate new customers of the payments service that require this functionality.

FR085 The Adapters for other public bodies (to be determined) could integrate those organisations with the payment platform API

Additional adapters will be required to integrate with other public sector organisations over time. These adapters should reuse code from existing adapters. Where possible customers should be encouraged to integrate directly with the payment platform API to remove the need to maintain separate adapters.

B. 2. Capability grouping: MI

FR054 The MI API must support integration with external MI systems to allow read-only queries on the structured transaction history

This will most likely be with a SQL interface which must be secured to ensure that no personal or customer confidential data is exposed through it.

B. 3. Capability grouping: Monitoring

FR039 The Monitoring must provide real-time information about system load

There should be time series data showing critical data like memory usage and processor load that gives enough data to monitor that the systems are performing within their reasonable capacity.

FR040 The Monitoring must provide real-time information about scaling state

There should be time series data showing when the platform has scaled up or down.

FR038 The Monitoring must provide real-time information about processing times

There should be time series data, categorised by request type, indicating the time taken to process each request. Where valuable, this might also break down that processing time to indicate how much time is spent in different components of the system. In particular, the data must include itemised entries showing the time taken by third party services to process requests.

FR037 The Monitoring must provide real-time health checks for all components

All separate components and instances of those components should be designed to respond to health checks so that system failures can be monitored and recorded.

FR041 The Monitoring should provide real-time information on service performance

The payments service will be required to transparently report key performance indicators (KPIs) to monitor and manage its operation. The final KPIs will be determined during Beta but are likely to include information reflecting the cloud running costs and environmental impact as well as transaction volumes, values and success rates.

B. 4. Capability grouping: Platform Core

FR015 The Platform Core transaction processor must enforce payment limits per file / batch

Different limits on the maximum overall value of payments in a batch must be able to be configured for each product of each customer. If a limit is breached then the payments will require authorisation to proceed. Authorisation could be either through the UI of the payment platform or through the API.

FR051 The Platform Core API must be primarily an HTTPS REST API interface

The API should, unless explicitly agreed, conform to the API technical and data standards laid out here: https://www.gov.uk/guidance/gds-api-technical-and-data-standards

FR060 The Platform Core infrastructure must be capable of being redeployed into a new cloud region with full data recovery

This process must be fully scripted so that, whilst the decision to redeploy will probably be a manual one, the actual process is fully automated.

It will need to be possible to test this process on a live system.

FR080 The Platform Core monitoring must provide information about traffic

There should be time series data showing the number and type of requests hitting the system and providing summary statistics on the payment types and highlighting failure cases.

FR016 The Platform Core API must validate that payment files are syntactically and semantically correct

The payment API must do all it can to immediately reject any transaction requests that cannot be fulfilled. The payment platform cannot check that every destination account is valid (particularly for international payments) but there are substantial process cost improvements and benefits to recipients if the platform can reject an invalid payment immediately rather than on a future date.

FR011 The Platform Core PSP integration must be able to make payments using Faster Payments

The payment platform must be able to make Faster Payments payments through one or more PSPs. Social Security rely on a service referred to as "short term contingency" provided by DWP CPS which takes late dated BACS payments and pays them using Faster Payments to ensure that they are paid on time. The payment platform needs to address the same needs through the combination of Faster Payments and automatic routing of payments to a suitable network based on payment due date.

The selection of suitable PSPs will be part of the work of delivering this functionality.

FR010 The Platform Core PSP integration must be able to make payments using BACS

The payment platform must be able to make BACS payments through one or more PSPs.

The selection of suitable PSPs will be part of the work of delivering this functionality.

FR014 The Platform Core transaction processor must be capable of enforcing payment limits per individual transaction

Different limits on the maximum value of payments must be able to be configured for each product of each customer. If a limit is breached then the payment will require authorisation to proceed. Authorisation could be either through the UI of the payment platform or through the API.

FR008 The Platform Core transaction routing and scheduling must automatically change the payment route to satisfy the date requirements of a payment that cannot otherwise be made on time

Within each payment instruction there should be the option to specify which payment networks can be used to make the payment and some order of fallback preference. In the event that the payment cannot be fulfilled through the intended payment network, the payment platform should attempt to make the payment through one of the other approved routes. Only if none of these routes are possible should the payment be rejected.

FR012 The Platform Core PSP integration must be able to make international payments

The payment platform will need to be able to be able to make payments to the vast majority of beneficiaries of SPPA.

The selection of suitable PSPs will be part of the work of delivering this functionality.

There may be an opportunity during the Beta phase to roll out direct international payments to the Single Euro Payments Area (SEPA) first and test this with Social Security.

FR023 The Platform Core transaction processor must automatically reconcile return messages with originating payments

Reconcile ARUCS and AWACS message from BACS with the originating payment request so that the original payment status is updated to reflect this information.

FR045 The Platform Core customer configuration must allow customers to configure a separate payment account for each product

Customers must be able to use different bank account configurations for different products. For any one product it must be possible to either configure a single account or two accounts, where one account is for making payments and the other for receiving payment returns.

Note that customers are not obliged to make payments for different products from different accounts so the system must not rely on that.

FR019 The Platform Core transaction processor must be able to cancel a payment submitted to the payment platform but not yet submitted to payment networks

This functionality must be available both through the payment UI and through the API.

FR035 The Platform Core transaction store must delete payment data for a customer or user in compliance with regulations

It may be that General Data Protection Regulation (GDPR) 'right to be forgotten' rules could require that some data associated with payments may need to be deleted from immutable transaction records. The system will need to be designed to address this.

FR020 The Platform Core transaction processor must be able to recall a payment that has been submitted to payment networks but can still be recalled

This functionality must be available both through the payment UI and through the API. The API should also provide a mechanism to obtain updates to the status of any recall (e.g. success/failure).

FR022 The Platform Core UI must allow authorised users to approve or reject payments that exceeded limits

If a payment exceeds set limits per payment or per batch then the payment should be put on hold requiring user intervention. The Platform UI should provide the necessary features to allow an authorised user to approve or reject these payments. Depending on the customer configuration, in some cases this might need multiple authorised users to approve the action. An API should also be available to approve such payments without using the UI.

FR001 The Platform Core transaction processor must maintain a history of transaction events including transactions that are successful, unsuccessful or in mid-processing

This transaction history must be immutable so that it can act as an auditable record of every transaction that has gone through the payment platform.

FR007 The Platform Core transaction routing and scheduling must hold back the submission of rapid payments to facilitate fraud detection and prevention

Payment mechanisms that allow payments to be made rapidly, such as Faster Payments, open up particular fraud risks because they limit the time window between the potential identification of unusual behaviour and the resulting transfer of funds. The payment platform should provide a mechanism so that all rapid payments can be delayed to provide a time window for identifying and acting on security alerts.

FR047 The Platform Core security should meet the Cyber Resilience Framework target level

General details about the Cyber resilience framework can be found here: https://www.gov.scot/publications/cyber-resilience-framework/. The Cyber Resilience Strategy document states that public sector organisations should be required or encouraged to achieve “target” level, on a risk-based and proportionate basis. The payment platform will be a target for cyber-crime and so security requirements will be proportionately higher than most public sector services.

FR005 The Platform Core transaction routing and scheduling should accept future dated payments and schedule them at the right time

The payment platform needs to be able to accept payments before they are due to be paid. For some payment networks like BACS, there is a three day processing time which means that the payments need to be received at least three days before they need to be paid. In some cases customers may want to issue the payment instructions to the payment platform ahead of time in order to provide contingency in case of system failure.

FR009 The Platform Core transaction routing and scheduling should individually route payments to the best commodity based on business rules

Speed of delivery, cost of delivery and the preferences of individual recipients are all considerations that should factor into routing decisions made by the payment platform. Customers should be able to configure business rules for individual products to determine how to route payments. As long as there is room for future enhancement, the beta implementation only needs to provide the flexibility required by the known set of initial users of the payment platform.

FR013 The Platform Core PSP integration should be able to make payments to citizens who cannot receive payments into a bank account

A decision needs to be made, in collaboration with Social Security, on the mechanism to be used for making payments to citizens who cannot receive payments into a bank account. These are commonly referred to as “alternative payments”.

There will also need to be significant service design to establish the role of the payment platform if the chosen mechanism requires the physical distribution of cards or the provision of direct telephone support to recipients.

Whilst the requirements for implementing this functionality are as yet unknown, the architecture of the payment platform must not prevent the introduction of the functionality that is likely to be required to implement a solution like the one currently operated by the Department for Work and Pensions (DWP) using i-Movo.

The choice of a suitable PSP will be part of the work of delivering this functionality.

FR024 The Platform Core transaction processor could notify the end user that a payment has been made

Directly message recipients of funds that the funds have entered the payment network and are due to be lodged into their account on a given date. Also notify recipients in the event that a payment is returned or fails after entering the payment networks.

Implementing this feature will require payment messages to include sufficient contact information and information regarding the payment to enable the payment platform to compose a suitable message and send it to the intended recipient.

FR078 The Platform Core API could validate IBAN and BIC numbers provided with international payments

There are certain rules around the construction of IBAN and BIC numbers which enable a level of verification without access to actual account details. This requirement covers the provision of an API by the Payment Platform so that customers can build in validity checks in the user interfaces of their own systems.

FR006 The Platform Core transaction routing and scheduling could hold back the submission of payments to PSPs before the submission date so that subsequent cancellation is easier

Many payment networks and PSPs allow payments to be submitted in advance of the required submission date. However, depending upon the payment network and/or the PSP, this changes and sometimes complicates the process of cancelling a payment that has not yet been made. The payment platform should be able to hold back the submission of payments until close to the final submission date to increase the likelihood that a request to cancel a payment can be fulfilled quickly and simply.

FR017 The Platform Core API could validate UK bank account sort codes

Using the Extended Industry Sort Code Directory (EISCD) and documented rules around the construction of sort codes and account numbers (including modulus check) to check that sort codes are valid and are capable of receiving payments by the payment mechanism being proposed. See Vocalink number validation rules

FR036 The Platform Core transaction store must automatically delete data after seven years

The immutable store of transactions should be capable of deleting records after seven years without breaking any functionality such as recovery after a major infrastructure failure. The deletion process should be automatic and should genuinely release storage space to address the environmental impact of maintaining a growing data store.

FR077 The Platform Core API could validate UK bank account numbers

Extend the internal checking of UK bank account numbers into an API that customers can used to enhance the checking of account details as they are entered into their systems. See FR017 for more details of the underlying checking.

B. 5. Capability grouping: Platform UI

FR069 The Platform UI must allow authorised users to view data required to allow them to provide support to end users of the payment platform

Payment platform support staff will need to be able to access customer data in order to support users of the platform. This access will need to be logged and design decisions are still to be made about whether or not platform staff will have any ability to action any changes to payments on behalf of customers.

FR067 The Platform UI could allow users to make one-off payments

This is a mechanism that allows approved users to make one-one payments through the UI. As well as controlling who can initiate a one-off payment the system must require separate approval and there may need to be a number of additional security controls including additional-factor authentication and controls around times of the day when these can take place. By default this mechanism should be disabled for all users and customers.

Appendix C: Non-functional requirements

The following non-functional requirements (NFR) define cross-cutting constraints on the platform and service that apply across multiple functional requirements.

Each non-functional requirement includes a MoSCoW (Must Should Could Won't) rating. For the purposes of estimating the work of the Beta phase (this procurement) you should account for all of the "must" and "should" requirements as constraints on the work to be done and the "could" non-functional requirements as future constraints that should be considered for the target architecture.

Each non-functional requirement has a reference code at the beginning of the title. This reference forms no purpose in this document other than providing a consistent way of identifying a specific requirement should you need to do so in any communications.

Please note that this is an agile project and whilst this list reflects our best understanding of the critical non-functional requirements of the payment platform, this list will most likely be subject to change and may not be exhaustive.

C. 1. Category: SLA

NFR034 The service *must* be able to recover, within 24 hours, from the failure of multiple availability zones

This platform will most likely be hosted continuously across multiple availability zones and be capable of being automatically deployed to another region in the unlikely event that all of the availability zones in a region are compromised. This critically impacts the approach for distributing data across zones and regions, which must be able to recover without data loss.

NFR037 The service *must* provide telephone support between 09:00 and 17:30 Mon-Fri excluding bank holidays

Telephone support should be available during operating hours and 30 minutes after the system has processed its last payments for the day.

NFR004 The platform *must* process payments between 09:00 and 17:00, Mon-Fri excluding bank holidays

Any payment instructions received outside of these hours should be validated immediately but then queued for further processing within the service operating hours listed. This constraint exists to remove a critical need for out of hours telephone support and to enhance security.

NFR035 The platform *must* prevent any actual payments being transmitted to PSPs or payment networks outside of the hours of 09:00 and 17:00, Mon-Fri or on bank holidays

This constraint exists to enhance security.

NFR011 The platform *must* be operational for payment administration, reporting and monitoring, between 05:00 and 23:00, seven days a week

To address the needs of automated out of hours batch processing and organisations that may need to work out of normal working hours in order to address peak demands or failures in their own systems, all payment platform APIs must be fully operational within these platform operation hours.

C. 2. Category: compliance

NFR006 The platform *must* maintain transaction records for 7 years and then automatically delete them

The payment platform should be designed to be able to automatically manage the retention of data, automatically deleting data that should no-longer be maintained by the platform.

NFR005 The platform *must* comply with GDPR

The design of data stores must account for any GDPR ‘right to be forgotten’ in balance with any requirements to maintain business records for seven years. This particularly relates to additional metadata that may be attached to payments which may fall under the right to be forgotten but not be required for business records.

C. 3. Category: design

NFR027 The platform data model *must* transmit customer specific attributes alongside each transaction

The model should clearly define which attributes should be recorded in the transaction log and which contain sensitive information that might need to be deleted to conform with GDPR.

NFR021 The platform *must* use data storage techniques that allow schema changes without breaking historical records

If upgrades to the platform require changes to the structure of data then the platform must be able to continue to read historical records which are immutable by design.

NFR022 The platform *must* use a data model that gives the freedom for customers of the platform to attach additional metadata to payments that can be queried and output with transaction reports

There are clear cases where the integration of the payment platform will be far enhanced if customers can attach additional fields of data to payments in order to facilitate downstream processing or integration. However, whatever mechanisms are used must account for the potential need to delete that data separately from the underlying transaction record if GDPR rules apply specifically to the additional data.

NFR038 The platform data model *must* maintain data relating each payment back to the original batch

There are numerous aspects of the process of handling payments that require knowledge of the batch that a payment belongs to, so this information must be part of the metadata of a payment that is understood by the core platform.

NFR026 The platform data model *must* accommodate accounting ledger codes as a standard field

Whilst the core payment platform does not understand these codes, it may need to transmit these codes with transaction reports in order to fulfil integration requirements.

NFR033 The platform *should* limit the use of vendor specific technologies or standards to prevent lock-in

All technology choices, including cloud hosting, should aim to avoid a situation where the payment platform is ‘locked-in’ to a single vendor product which could constrain future development and reduce value for money. This does not preclude the use of off-the-shelf products that may provide good value for money. However, such products should be selected because they interface with the platform in a loosely coupled way which enables them to be swapped out for alternative products in the future. In keeping with the Digital First strategy this promotes the use of open source solutions.

NFR019 The platform *should* use a standardised representation of payments and payment processing events that abstracts away the distinctions between individual payment mechanisms

The more the payment platform can provide an abstraction layer from the underlying payment mechanisms, the more the platform is free to change the underlying mechanism it uses to make those payments and the easier it will be for customers of the payment platform to accommodate changes to the payment networks.

C. 4. Category: fraud

NFR003 The platform *must* transmit and store the necessary data to support fraud investigation

The design of APIs and messages should carefully consider the inclusion of additional information that may facilitate the identification of fraud.

NFR008 The platform *could* support the implementation of Confirmation of Payee

The payment API should accommodate the immediate or future implementation of Confirmation of Payee for Faster Payments and BACS. Architectural design consideration should be taken for the possibility of adding a separate API for Confirmation of Payee checking and for caching results to accelerate checking and/or reduce cost.

C. 5. Category: integration

NFR024 The platform *should* be able to be integrated with new customers without enforcing process change upon them

Whilst the payment platform should encourage a transition to the use of more efficient payment processes, it should also provide the flexibility to integrate with existing processes so that customers are not forced to change their processes in order to integrate. However, to do so may require substantial work in bespoke customer adapters.

NFR025 The platform *should* only support functionality that meets the needs of multiple customers

As a general rule, the core payment platform should not have any specific functionality that is designed for only one customer. In most cases the particular needs of individual customers should be addressed in the customer adapters rather than through the implementation of core payment platform functionality.

C. 6. Category: performance

NFR014 The service *must* respond to 95% of customer queries in four hours within the working hours of the telephone support service

A separate NFR specifies the working hours of telephone support. Where a query is raised near the end of a day's support hours the expectation is that the clock stops at the end of the support hours and restarts at the beginning of the support hours on the next working day.

NFR012 The platform *must* never lose data

All instructions accepted and acknowledged by the payment service must be retained and processed without data loss, corruption or duplication.

NFR017 The platform *must* automatically handle 99% of all process exceptions and provide sufficient information to manually support those that cannot be handled

Whilst the payment platform should aim to automate all processes, there will be some exception cases that cannot be handled automatically. The platform needs to be able to alert support staff to those cases and provide sufficient information so that the support staff can investigate the issue and address the problem. All unhandled exceptions must be documented and added to the development backlog for potential automation.

NFR013 The platform *must* be able to recover from 99% of individual component failures within one hour of the failure

Most individual component errors should be automatically detected and recovered by killing and redeploying the component. This NFR does not cover systemic failures of a cloud hosting availability zone.

NFR031 The platform *should* automatically switch off or scale down services in low-load conditions to reduce environmental impact

The design of the platform should consider maximum and minimum load conditions, trying to limit the number of services that need to be running when there are few if any users. Consideration could be given to starting components on demand when usage is low.

NFR030 The platform *should* process up to 10 million BACS payments in a single day

Whilst the current anticipated load on the payment platform should be much lower than this, there are conceivable situations where this volume of payments could be issued on a single day.

C. 7. Category: policy

NFR015 The platform *must* be hosted in the cloud

In line with the Scottish Government cloud first policy, the payment platform must be hosted in the cloud. This does not apply to customer adapters that, for security reasons, will typically be hosted within the cloud hosting environment of the customer system which may or may not be in the cloud. The payment platform must be capable of being hosted in the UK as some public sector organisations may require their data to be maintained in the UK.

NFR016 The platform *must* document all APIs and base them on industry standard protocols, message formats and data types

To facilitate integration and avoid vendor lock-in, all APIs should be fully documented with examples and should be based on standard practices for API design.

C. 8. Category: security

NFR036 The platform *must* prevent sensitive data from being exposed in logs or tracing data

Rather than assuming that staff looking at logs have sufficient security clearance to do so, sensitive data should not be written to the logs in the first place.

NFR009 The platform *must* encrypt all data in transit and at rest

Encryption of data in transit applies not just to external APIs but also to all internal APIs including monitoring and logs. All data file storage including log files and databases should be on encrypted storage devices. Any encryption techniques used must be considered secure by NCSC.

NFR001 The platform *must* authenticate all API calls

There should be no exposed interfaces to the platform that can be accessed without authentication regardless of whether or not they are intended only for internal use.

NFR010 The platform *must* record transaction events in an immutable store

There should be no way that transaction records can be amended after the fact to hide unauthorised activity.

NFR029 The platform *must* delay the processing of payments by two hours

Two hours is an intentional delay in order to provide time for fraud issues to be addressed and to allow customers to cancel payments before they have entered the payment network. This means that payments made less than two hours before any daily cut-off time for the underlying payment network will be delayed until the next working day.

NFR002 The platform *must* check the permissions of the external user before fulfilling a request

Components of the system that perform critical operations should ensure that the underlying request was initiated by a user with the necessary permissions to perform the operation. In other words, the platform should not contain internal APIs which perform critical operations and assume that permissions have been checked before they are called.

C. 9. Category: validation

NFR007 The platform *must* validate payment instructions at the boundaries of the payment platform or before

Many existing payment systems leave checks on the validity of payment instructions to the payment networks themselves. Payment instructions such as BACS payments with lower case text are accepted for delivery but then fail at a later point in time when upstream processes fail. The payment platform should validate all payment instructions immediately upon receipt and reject requests immediately for any instructions that cannot be actioned.

Appendix D: Transitional requirements

Alongside the work of design, development and support of the payment service, the supplier will be required to plan and carry out the necessary transitional activities to ensure that SG, or a third party designated by SG, can provide continuity of service beyond the term of the contract.

Those transitional requirements will include:

- Transitioning the management and ownership of cloud hosted services.
- Transitioning all customer facing support services.
- Transitioning all customer integration functions and knowledge.
- Transitioning ongoing development work and knowledge including all the source code, source graphic files and any other materials produced as part of the work.
- Transitioning of all passwords and permissions required to access or control systems and services.

Appendix E: Service delivery and support

During the contract and any agree extension period, the supplier will be expected meet all of the support needs of the payment service and help with the transition of support to the organisation that takes over this role.

The full extent and scale of the support will depend upon the extent to which the payment platform automates the services of the payment service, and the scale of the roll-out of the service within the period of the contract.

For the purposes of estimating the work of the Beta phase bidders should assume that the support function will need to operate during the hours specified in Appendix C: Non-functional requirements. For the purpose of calculating support costs, bidders should also assume that there will be no support required within year 1 of the contract and that support for the following customers will be required as described below:

- ILF making one payment run per week for 12 payrolls per month from the start of year 2 of the contract
- SPPA ramping up to 50 payrolls per month spread out throughout the month from month 15 into the contract
- Social Security on-board one benefit from 18 months into the contract. This support may include bank liaison

Suppliers should be clear that the support goes beyond the support of the technical platform delivery and covers the full support needs of users of the service.

The successful bidder will work in partnership with SG and public sector partners to finalise the terms of service which establish exactly what support will be provided.

Appendix F: Testing and static analysis

This project has a significant scope of development and delivery which will need to be carried out by coordinated teams. In this context, extensive automated testing is critical to project success and cannot be retrofitted at the end of the project.

The supplier will be expected to:

- produce automated unit tests alongside every completed code submission
- automate the running of all units tests on at least a daily basis and make the acceptance of code into production a dependent upon full test completion
- automate static code analysis and reporting on test coverage and test performance with tooling that maintains a time-series record of these analyses throughout the contract period
- Carry out manual usability tests to guide and validate user design choices
- Set up automated integration tests of all external API functionality against sandbox PSP adapters
- Carry out automated monthly performance and load tests against critical API calls within a controlled environment and report variation throughout the contract period.
- Put in place the necessary metrics to record and monitor the performance of critical components of the platform in production
- Provide support for security testing of the platform on development and production environments throughout the course of the contract. Security testing, including penetration testing, will be conducted by a third party arranged by SG

Appendix G: Working together

G. 1. Agile delivery

The SG Payments project team use agile methodology for project delivery. Whist bidders are being asked to provide an estimate based on the concrete requirements supplied in this document, we expect the successfully bidder to work in an agile way, collaboratively shaping the project as it iteratively delivers increasing functionality into a secure live service.

The Digital First Service Standard defines the phases of an agile project and more information about the agile phases can be found on the mygov.scot resources website.

The payments projects has already been through Discovery and Alpha phase. This document describes the procurement for the Beta phase: delivering a working service and putting it into production.

G. 2. SG payments team

The SG project team, presented in the table below, will form the core multidisciplinary team with responsibility for overseeing the complete payment service including: the design, build and test of the payment platform; and defining and managing standards for user research, service design, data and security.

This team will scale gradually from the beginning of the Beta phase in September 2020 and be supplemented by the supplier's team. Given the breadth and scope of the work we anticipate that this large team will break down into sub-teams focused on parallel work streams.

SG Payments Beta phase – Scottish Government team			
Role	Current team	Scaling to (by end March 2021)	Anticipated SG team for Beta year 2
Transformation Lead	1	1	1
Product Owner	1	1	1
Delivery Manager	1	1	1
Business Analyst	0	1	2
Enterprise Architect	1	1	1

Project Support	1	1	2
Service Designer	1	1	2
Associate Delivery Manager		1	2
Payments SME		1	1
Data Analyst		1	1
Security Analyst		1	1
User researcher		1	2
Content Designer		0.5	1
Associate Product Owner		2	3
Technical architect			1
Commercial lead		1	1
Total FTE	6	15.5	23

The success of the project will be dependent upon close working with the integration partners. This list will grow, but at the beginning of Beta it will include: Independent Living Fund Scotland (ILF), the Scottish Public Pensions Agency (SPPA), Social Security Scotland and SG's Financial Services Division (FSD), and Information and Technology Services (iTECS).

The team will be supported by input from the wider organisation, including Financial Management, Procurement & Commercial, Office of the Chief Designer and links into the wider technical practice within Digital Directorate.

They will regularly call upon expertise from SG's Digital Commercial Service, as well as seeking expert external support in areas such as cyber-security.

Appendix H: The technology foundation

Two stages of research, design and development have taken place prior to this bid. All the materials from that work will be made available to the successful bidder after they have onboarded.

The source code of both the proof of concept and alpha stage software developments were coded in the open and can be found on GitHub (see the links in Appendix J: below).

H. 1. Alpha technology choices

The following technology choices were made for the Alpha implementation and are presented here as an indication of the codebase of alpha which is available to be taken forward into Beta. None of these previous technology choices are a constraint on the design and development of the Beta, however, we do expect the successful bidder to make full use of all of the research and development work proceeding Beta and to build on lessons learned.

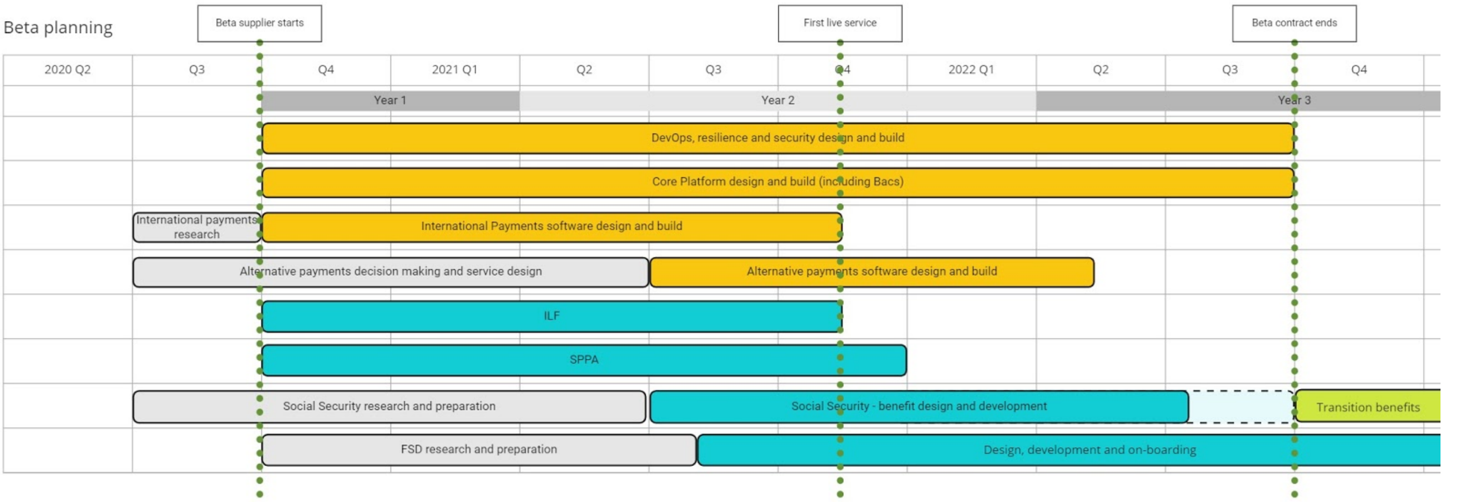
Cloud provider	AWS
CI/CD orchestrator	GitLab
Container orchestrator	Kubernetes
Container orchestrator deployment	AWS EKS
Container runtime	Docker
Infrastructure monitoring	AWS Cloudwatch
Event store and event bus	Kafka
Event store and event bus implementation	Confluence cloud Kafka
Object store	AWS S3
Container registry	GitLab registry
Service mesh	Istio
SFTP Gateway	AWS SFTP Transfer
Application monitoring	Prometheus, Kubernetes dashboard, Confluence dashboard, Cloudwatch

Authentication	AWS Cognito
Log management	AWS Cloudwatch
Configuration and secret management	Kubernetes
Scheduler	Kubernetes
Programming Language	Java (back-end) TypeScript (front-end)
Language Runtime	Open JDK 11
Application server	Reactor-Netty
Application framework (core)	Sprint and Spring Boot
Application framework (streaming)	Kafka streams and Spring Cloud Kafka streams
Application framework (web)	Spring-webflux
Message Codec (internal)	Avro
Message Codec (external)	Json (Jackson)
Messaging Protocol (internal)	Kafka
Messaging Protocol (external)	Http + WebSocket and STOMP
Configuration management	Spring Boot and Spring Cloud Kubernetes
Authentication and authorisation	OAuth(Spring Security and Spring Security OAuth)
Scheme evolution	Confluence schema registry

Appendix I: Milestone plan

The following milestone plan presents the desired schedule of development and delivery for Beta and beyond. Please note that the years listed as “Year 1”, “Year 2” are financial years but the quarters “Q1”, “Q2” are calendar years. The project is scheduled to start in Q4 2020.

In this diagram the orange bars represent core platform development tasks and the blue and grey/green bars represent integrations with public sector clients. SG will revise this plan and work with the appointed commercial partner to plan out and schedule the work and the beginning of the contract.



Appendix J: Links to further information

Scottish Government Digital Strategy	https://www.gov.scot/publications/realising-scotlands-full-potential-digital-world-digital-strategy-scotland/
Digital First Service Standard	https://resources.mygov.scot/standards/digital-first/
Scottish Approach to Service Design (SAtSD)	https://www.gov.scot/publications/the-scottish-approach-to-service-design/
Cyber resilience framework	https://www.gov.scot/publications/cyber-resilience-framework/
NCSC Security guidance	https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles
Digital Directorate blog	https://blogs.gov.scot/digital/
Github repository	https://github.com/sg-payments

Appendix K: Definition of terms

Term	Definition	Comment
ARUCS	(BACS) Automated Return of Unapplied Credits Service	-
AWACS	(BACS) Advice of Wrong Account for Automated Credits Service	-
BIC	Bank Identifier Code	-
Capability	Something the service can do – the 'what'	-
Common or Shared	Technology or processes that are designed to be used across multiple organisations	-
Component	Technology that realises a capability – the 'how'	-
CQRS	Command Query Responsibility Segregation	-
DR	Disaster Recovery	The set of policies, tools and procedures to enable recovery or continuation of vital technology infrastructure and systems following natural or human-induced disaster.
EISCD	The Extended Industry Sort Code Directory	-
FSD	Financial Services Division	A Scottish Government division responsible for the operation and development of SEAS.
HSM	Hardware Security Module	A physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.
IBAN	International Bank Account Number	

Term	Definition	Comment
ILF	Independent Living Fund Scotland	An organisation whose mission is to enable disabled people to achieve their independent living outcomes by the dignified assessment of needs and the distribution of discretionary awards.
Incremental development	Each successive version builds on the previous to add usable functionality	-
iTECS	Information and Technology Services	The Scottish Government's ICT operation, responsible for supporting and developing the core platforms used across the Scottish Government and its shared service community.
ITT	Invitation To Tender	The formal publication and invitation to suppliers to bid to supply products or services.
Ledger	A collection of financial accounts	-
MI	Management Information	Information extracted and processed from IT systems. It is used to better inform decision making in an organisation and maximise business value.
MVP	Minimum Viable Product	A version of a product with just enough features to satisfy early customers and provide feedback for future product development.
Payment system	An underlying mechanism for making payments such as BACS, CHAPS, Faster Payments, etc.	Sometime referred to as "commodity service" or a PSP (Payment Service Provider).
Payment system broker	A third party organisation that provides a service for accessing one or more underlying payment systems	-
Payments service or platform	The proposed Scottish Government payments service	Sometimes referred to as "the service". The payments service is intended to provide a service but also act as a platform to support additional services or integrations.

Term	Definition	Comment
PCI	Payment Card Industry	The organisations which store, process and transmit cardholder data, most notably for debit and credit cards.
Platform	Service components produced once and used multiple times across a government	-
PoC	Proof of Concept	A short project/phase to test ideas and validate assumptions.
POCa	Post Office Card Accounts	-
PSP	Payment Service Provider	A PSP provides online services for accepting electronic payments by a variety of payment methods including credit card, direct debit, bank transfer etc. They provide a single payment gateway to multiple payment methods.
Reconciliation	The process of comparing two different accounting records to ensure that the figures are accurate, consistent and traceable	In particular, this term is often used to refer to the process of associating payment instructions with their corresponding returns and failure responses from banking networks.
SaaS	Software as a Service	-
SEAS	Scottish Government Enterprise Accounting System	-
SEPA	Single Euro Payments Area	-
SFTP	Secure File Transfer Protocol	-
SG	The Scottish Government	-
SLA	Service Level Agreement	-
SOA	Service Oriented Architecture	A style of software design where services are provided to the other components by application components, through a communication protocol over a network.

Term	Definition	Comment
SOC	Security Operations Centre	-
SPPA	Scottish Public Pensions Agency	-
SSA	(Scottish) Social Security Agency	-