



Ministry of Economy and Labour
Ministry of Economy Labour Headquarters

Request for Supplier Qualifications
For
Bermuda Digital Identity

Request for Supplier Qualifications No.: **BNDI2026**

Issued: **Monday October 5th, 2026**

Submission Deadline: **Friday November 27, 2026 10:00:00 AM Bermuda local time**

TABLE OF CONTENTS

PART 1 – INVITATION AND SUBMISSION INSTRUCTIONS	3
1.1 Invitation to Respondents.....	3
1.2 RFSQ Contact	3
1.3 Prequalification Process.....	4
1.4 RFSQ Timetable.....	4
1.5 Submission of Responses	4
PART 2 – EVALUATION AND SELECTION	6
2.1 Stages of Evaluation	6
2.2 Stage I – Mandatory Submission Requirements	6
2.3 Stage II – Evaluation	6
2.4 Ranking and Selection	6
2.5 Notification of Top-Ranked Respondents.....	6
PART 3 – TERMS AND CONDITIONS OF THE RFSQ PROCESS.....	8
3.1 General Information and Instructions	8
3.2 Communication after Issuance of RFSQ.....	9
3.3 Notification and Debriefing	10
3.4 Conflict of Interest and Prohibited Conduct.....	10
3.5 Confidential Information	12
3.6 Procurement Process Non-Binding	13
3.7 Governing Law and Interpretation	14
APPENDIX A – SUBMISSION FORM.....	15
APPENDIX B – RFSQ PARTICULARS	19
A. THE DELIVERABLES	19
B. MATERIAL DISCLOSURES	20
C. MANDATORY SUBMISSION REQUIREMENTS	21
D. MANDATORY TECHNICAL REQUIREMENTS.....	24
E. PRE-CONDITIONS OF AWARD	24
F. RATED CRITERIA	25
APPENDIX C – CERTIFICATE OF CONFIRMATION OF NON-COLLUSION	30
 ANNEX A - COMPANY PROFILE FORM	
 ANNEX B - SECURITY & PRIVACY MANDATORY TECHNICAL REQUIREMENTS QUESTIONNAIRE	
 ANNEX C - LOCAL BENEFIT FORM	

PART 1 – INVITATION AND SUBMISSION INSTRUCTIONS

1.1 Invitation to Respondents

This Request for Supplier Qualifications (“RFSQ”) is an invitation by the Government of Bermuda (the “Government”) to prospective respondents to qualify in accordance with Evaluation of Responses (Part 2) for eligibility to provide **Bermuda Digital Identity** as further described in Section A of the RFSQ Particulars (Appendix B) (the “Deliverables”).

The Government of Bermuda intends to procure a Digital Identity (DI) Platform through a single-provider Public-Private Partnership (PPP) model. The successful supplier will be responsible for the design, implementation, operation, maintenance, and ongoing support of the Digital Identity ecosystem, while the Government retains responsibility for policy, governance, regulatory oversight, and strategic direction. The programme is intended to deliver a secure, privacy-by-design digital identity capability for residents and support trusted access to public and private sector services. The procurement is being conducted on the basis that the solution will evolve through a phased implementation approach and may ultimately become a critical component of Bermuda's national digital infrastructure.

The procurement is for the design, implementation, operation, and ongoing support of Bermuda's Digital Identity (DI) Platform through a public-private partnership arrangement. The Government is seeking a qualified provider to deliver a secure, privacy-by-design digital identity ecosystem that enables residents to verify their identity and access public and private sector services through a trusted digital credential and digital wallet. The solution will support identity proofing, credential issuance, authentication, attribute sharing, fraud prevention, cybersecurity, and lifecycle management, while complying with Bermuda's legal, privacy, and cybersecurity requirements. The provider will also be responsible for establishing the supporting technical, operational, governance, integration, stakeholder engagement, and legislative enablement frameworks necessary to deliver a resilient, scalable, and inclusive national identity service that improves service delivery, strengthens regulatory compliance, and supports Bermuda's long-term digital transformation objectives.

1.2 RFSQ Contact

For the purposes of this procurement process, the “RFSQ Contact” will be:

Mark Neale mcneale@gov.bm

Respondents and their representatives are not permitted to contact any employees, officers, agents, elected or appointed officials or other representatives of the Government, other than the RFSQ Contact, concerning matters regarding this RFSQ. Failure to adhere to this rule may result in the disqualification of the respondent and the rejection of the respondent's response.

Prior to the Submission Deadline noted in the RFSQ timetable below, respondents that download this file and intend to respond are required to register their interest with the RFSQ Contact by emailing their company name and contact information to

Mark Neale mcneale@gov.bm

.

Amendment/addenda (If any) will be posted at <https://www.gov.bm/procurement-notices>. Respondents should visit the Government Portal on a regular basis during the procurement process.

1.3 Prequalification Process

Responses will be evaluated in accordance with the evaluation process set out in Part 2 of the RFSQ. Based on the evaluation of responses, certain respondents will be selected for inclusion on a prequalified supplier list of suppliers that are eligible to participate in an invitational second-stage competitive process for the potential provision of the Deliverables to the Government. Joint submissions are acceptable however if a joint submission is made, the submission must clearly indicate which party will act as the prime contractor.

1.4 RFSQ Timetable

1.4.1 Key Dates

Issue Date of RFSQ	Monday October 5th, 2026
No Pre-Bid / Site Meeting	
Deadline for Questions	Friday October 23, 2026
Deadline for Issuing Addenda	Friday November 6, 2026
Submission Deadline	Friday November 27, 2026 10:00:00 AM
Rectification Period	3 business days

All times listed are in Bermuda local time. The RFSQ timetable is tentative only and may be changed by the Government at any time. For greater clarity, business days means all days that the Government is open for business.

1.4.2 Site Visit / Pre-Bid Meeting

N/A

1.5 Submission of Responses

1.5.1 Responses to be Submitted at the Prescribed Location

Responses must be submitted to:

Electronic mail (E-Mail) submissions are accepted at mclineale@gov.bm.

If documents are larger than ten (10) MB please send them within a zip file.

In the subject line of the email, please state the RFP title. Please ensure to send a copy of your proposal in MS Word and/or Adobe PDF format.

1.5.2 Responses to be Submitted on Time

Responses must be submitted at the location set out above on or before the Submission Deadline. Responses submitted after the Submission Deadline will be rejected.

A respondent may, at its option, email the RFSQ Contact prior to the Submission Deadline with delivery details, including the anticipated arrival time of its response. If a response does not arrive on or before the Submission Deadline, the Government may provide those respondents who have

given such prior notice one additional business day to affect the delivery of their responses. The Submission Deadline will be deemed to be adjusted to the same time as specified in the Submission Deadline but on the following business day.

1.5.3 Responses to be Submitted in Prescribed Manner

Respondents shall submit 0signed original hard copies of their response or one (1) electronic copy (e-copy) in Microsoft Word or Adobe PDF format. If both a hard copy and an e-copy of the response are submitted and there is a conflict or inconsistency between the hard copy and the e-copy of the response, the hard copy of the response will prevail.

The original and all copies of the response shall be typed or written in indelible ink and shall be signed by a person duly authorized to sign on behalf of the Respondent. This authorization shall consist of a written authorization and shall be attached to the Submission Form included in (Appendix A). The name and position held by each person signing the authorization must be typed or printed below the signature. An Electronic Record of Signature will be accepted in the submission only in accordance with the requirements laid out in the Electronic Transactions Act 1999. Any interlineation, erasures, or overwriting shall be valid only if they are signed or initialed by the person signing the response.

Responses are to be submitted in a sealed package prominently marked with the RFSQ title and number (see RFSQ cover) and will not be opened until Friday November 20, 2026 10:00:00 AM. The full legal name and return address of the respondent should be marked on the package as well

1.5.4 Amendment of Responses

Respondents may amend their responses prior to the Submission Deadline by submitting the amendment in a sealed package prominently marked with the RFSQ title and number and the full legal name and return address of the respondent to the location set out above. Any amendment should clearly indicate which part of the response the amendment is intended to amend or replace.

1.5.5 Withdrawal of Responses

At any time throughout the RFSQ process, a respondent may withdraw a submitted response. To withdraw a response, a notice of withdrawal must be sent to the RFSQ Contact and must be signed by an authorized representative of the respondent. The Government is under no obligation to return withdrawn responses.

[End of Part 1]

PART 2 – EVALUATION AND SELECTION

2.1 Stages of Evaluation

The Government will conduct the evaluation of responses in the following two stages:

2.2 Stage I – Mandatory Submission Requirements

Stage I will consist of a review to determine which responses comply with all of the mandatory submission requirements. If a response fails to satisfy all of the mandatory submission requirements, the Government will issue the respondent a rectification notice identifying the deficiencies and providing the respondent an opportunity to rectify the deficiencies. If the respondent fails to satisfy the mandatory submission requirements within the Rectification Period, its response will be rejected. The Rectification Period will begin to run from the date and time that the Government issues a rectification notice to the respondent. The mandatory submission requirements are set out in Section C of the RFSQ Particulars (Appendix B).

2.3 Stage II – Evaluation

Stage II will consist of the following two sub-stages:

2.3.1 Mandatory Technical Requirements

The Government will review the responses to determine whether the mandatory technical requirements set out in Section D of the RFSQ Particulars (Appendix B) have been met. Questions or queries on the part of the Government as to whether a response has met the mandatory technical requirements will be subject to the verification and clarification process set out in Part 3.

2.3.2 Rated Criteria

The Government will evaluate each qualified response on the basis of the rated criteria as set out in Section F of the RFSQ Particulars (Appendix B).

2.4 Ranking and Selection

Based on the evaluation of the responses in Stage II,

The top 5 ranked respondents will be short-listed to participate in a potential invitational second stage competitive processes for the procurement of the Deliverables.

2.5 Notification of Top-Ranked Respondents

The top-ranked respondents selected by the Government to be included in the prequalified supplier list will be so notified by the Government in writing. Each selected respondent will be required to satisfy the pre-conditions of award listed in Section E of the RFSQ Particulars (Appendix B) within the timeframe specified in the selection notice. Failure to do so may result in the disqualification of the respondent and the selection of another respondent.

[End of Part 2]

PART 3 – TERMS AND CONDITIONS OF THE RFSQ PROCESS

3.1 General Information and Instructions

3.1.1 Respondents to Follow Instructions

Respondents should structure their responses in accordance with the instructions in this RFSQ. Where information is requested in this RFSQ, any response made in a response should reference the applicable section numbers of this RFSQ.

3.1.2 Responses in English

All responses must be written in the English language only.

3.1.3 No Incorporation by Reference

The entire content of the respondent's response should be submitted in a fixed form, and the content of websites or other external documents referred to in the respondent's response but not attached will not be considered to form part of its response.

3.1.4 References and Past Performance

In the evaluation process, the Government may include information provided by the respondent's referees and may also consider the respondent's past performance or conduct on previous contracts with the Government or other institutions.

3.1.5 Information in RFSQ Only an Estimate

The Government and its advisers make no representation, warranty or guarantee as to the accuracy of the information or empirical data contained in this RFSQ or issued by way of addenda. Any quantities shown or data contained in this RFSQ or provided by way of addenda are estimates only, and are for the sole purpose of indicating to respondents the general scale and scope of the Deliverables. It is the respondent's responsibility to obtain all the information necessary to prepare a response in response to this RFSQ.

3.1.6 Respondents to Bear Their Own Costs

The respondent will bear all costs associated with or incurred in the preparation and presentation of its response, including, if applicable, costs incurred for interviews, travel or demonstrations.

3.1.7 Response to be Retained by the Government

The Government will not return the response or any accompanying documentation submitted by a respondent.

3.1.8 No Guarantee of Volume of Work or Exclusivity of Contract

This RFSQ process will not result in any commitment by the Government to purchase any goods or services from any respondent. While the Government intends to conduct an invitational second-stage competitive process for the procurement of the Deliverables, it is under no obligation to do so and the Government may choose not to proceed with a second-stage

competitive process for the procurement of the Deliverables. The Government makes no guarantee of the value or volume of Deliverables that may be required. Any agreement entered into pursuant to an invitational second-stage competitive process will not be an exclusive contract for the provision of the described Deliverables. The Government may contract with others for goods and services the same as or similar to the Deliverables or may obtain such goods and services internally.

3.1.9 Equivalency

When proprietary names, brands, catalogues or reference numbers are specified in the Deliverables, they are intended to set a minimum standard, and preference for any particular material or equipment is not intended. The respondent may offer material or equipment of similar characteristics, type, quality, appearance, finish, method of construction and performance and if doing so must disclose any difference in the characteristics, type, quality, appearance, finish, method of construction or performance of the material or equipment.

3.2 Communication after Issuance of RFSQ

3.2.1 Respondents to Review RFSQ

Respondents should promptly examine all of the documents comprising this RFSQ, and may direct questions or seek additional information in writing by email to the RFSQ Contact on or before the Deadline for Questions. No such communications are to be directed to anyone other than the RFSQ Contact. The Government is under no obligation to provide additional information, and the Government will not be responsible for any information provided by or obtained from any source other than the RFSQ Contact. It is the responsibility of the respondent to seek clarification from the RFSQ Contact on any matter it considers to be unclear. The Government will not be responsible for any misunderstanding on the part of the respondent concerning this RFSQ or its process.

3.2.2 All New Information to Respondents by Way of Addenda

This RFSQ may be amended only by addendum in accordance with this section. If the Government, for any reason, determines that it is necessary to provide additional information relating to this RFSQ, such information will be communicated to all respondents by addendum. All Addenda will be published online at <https://www.gov.bm/procurement-notice>. Each addendum forms an integral part of this RFSQ and may contain important information, including significant changes to this RFSQ. Respondents are responsible for obtaining all addenda issued by the Government. In the Submission Form (Appendix A), respondents should confirm their receipt of all addenda by setting out the number of each addendum in the space provided.

3.2.3 Post-Deadline Addenda and Extension of Submission Deadline

If the Government determines that it is necessary to issue an addendum after the Deadline for Issuing Addenda, the Government may extend the Submission Deadline.

3.2.4 Verify, Clarify and Supplement

When evaluating responses, the Government may request further information from the respondent or third parties in order to verify, clarify or supplement the information provided in the respondent's response. The information may include, without limitation, clarification with respect

to whether a response meets the mandatory technical requirements set out in Section D of the RFSQ Particulars (Appendix B). The response received by the Government shall, if accepted by the Government, form an integral part of the respondent's response. The Government may revisit, re-evaluate and rescore the respondent's response or ranking on the basis of any such information.

3.3 Notification and Debriefing

3.3.1 Notification to Other Respondents

Once the Agreement is executed by the Government and a respondent, the other respondents may be notified directly in writing of the outcome of the procurement process.

3.3.2 Debriefing

Respondents may request a debriefing after receipt of a notification of the outcome of the RFSQ process. All requests must be in writing to the RFSQ Contact and must be made within sixty (60) days of such notification.

3.3.3 Procurement Protest Procedure

If a respondent wishes to challenge the RFSQ process, it should provide written notice to the RFSQ Contact in accordance with the Government's Complaints and Disputes procedures. The notice must provide detailed explanation of the respondent's concern with the procurement process or its outcome.

3.4 Conflict of Interest and Prohibited Conduct

3.4.1 Conflict of Interest

For the purposes of this RFSQ, the term "Conflict of Interest" includes, but is not limited to, any situation or circumstance where:

- (a) in relation to the RFSQ process, the respondent has an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including but not limited to (i) having, or having access to, confidential information of the Government in the preparation of its response that is not available to other respondents; (ii) communicating with any person with a view to influencing preferred treatment in the RFSQ process (including but not limited to the lobbying of decision makers involved in the RFSQ process); or (iii) engaging in conduct that compromises, or could be seen to compromise, the integrity of the open and competitive RFSQ process or render that process non-competitive or unfair; or
- (b) in relation to the performance of its contractual obligations under a contract for the Deliverables, the respondent's other commitments, relationships or financial interests (i) could, or could be seen to, exercise an improper influence over the objective, unbiased and impartial exercise of its independent judgement, or (ii) could, or could be seen to, compromise, impair or be incompatible with the effective performance of its contractual obligations.

3.4.2 Disqualification for Conflict of Interest

The Government may disqualify a respondent for any conduct, situation or circumstances determined by the Government, in its sole and absolute discretion, to constitute a Conflict of Interest as defined above.

3.4.3 Disqualification for Prohibited Conduct

The Government may disqualify a respondent or terminate any contract subsequently entered into if the Government determines that the respondent has engaged in any conduct prohibited by this RFSQ.

3.4.4 Prohibited Respondent Communications

Respondents must not engage in any communications that could constitute a Conflict of Interest and should take note of the Conflict of Interest declaration set out in the Submission Form (Appendix A).

3.4.5 Respondent Not to Communicate with Media

Respondents must not at any time directly or indirectly communicate with the media in relation to this RFSQ or selection of respondents pursuant to this RFSQ without first obtaining the written permission of the RFSQ Contact.

3.4.6 No Lobbying

Respondents shall not in relation to this RFSQ or the evaluation and selection process, engage directly or indirectly in any form of political action or other activity whatsoever to influence or attempt to influence Parliament, the Government, or to influence or attempt to influence any legislative or regulatory action, in the selection or evaluation of any respondent.

3.4.7 Illegal or Unethical Conduct

The proponent represents, warrants, and covenants that, in connection with activities performed under this Agreement or on behalf of the Government, the proponent has not and will not offer, promise, authorise, pay, or act in furtherance of an offer, promise, authorization, or payment of anything of value, directly or indirectly, to a Government Official (as hereinafter defined), political party or party official, candidate for political office, or official of a public international organisation, in order to obtain or retain business, to secure an improper advantage or benefit of any kind or nature to person(s) related, associated or linked to the Government Official, or to secure or influence discretionary action, inaction or a decision of a Government Official(s). For purposes of this proposal, the term "Government Official" shall mean and include any official, public officer or employee of the Government, as well as an official or employee in the judicial, legislative, or military, anyone acting in an official capacity for the Government, or any immediate family member of such persons. The proponent represents, warrants, and covenants that it has complied and will comply with *The Bribery Act 2016* and all other applicable laws of any relevant jurisdiction in connection with the performance of this Agreement. Without limiting the generality of the foregoing, the proponent represents, warrants, and covenants that it has not and will not take any action that would cause the Government or anyone acting on their behalf to violate or be subjected to penalties under *The Bribery Act 2016*, or the applicable anti-corruption laws of other countries.

The proponent acknowledges and agrees that in the event that the Government believes, in good faith, that the proponent has breached this section, the Government shall have the right to immediately withdraw and terminate this opportunity and terminate any or all other agreements with the proponent.

3.4.8 Past Performance or Past Conduct

The Government may prohibit a supplier from participating in a procurement process based on past performance or based on inappropriate conduct in a prior procurement process, including but not limited to the following:

- (a) illegal or unethical conduct as described above;
- (b) the refusal of the supplier to honour submitted pricing or other commitments; or
- (c) any conduct, situation or circumstance determined by the Government, in its sole and absolute discretion, to have constituted a Conflict of Interest.

3.4.9 No Collusion

Respondents must not engage in any collusion and must sign the certificate as set out in the Certificate of Confirmation of Non-Collusion (Appendix C).

3.5 Confidential Information

3.5.1 Confidential Information of the Government

All information provided by or obtained from the Government in any form in connection with this RFSQ either before or after the issuance of this RFSQ

- (a) is the sole property of the Government and must be treated as confidential;
- (b) is not to be used for any purpose other than replying to this RFSQ and the performance of any subsequent contract for the Deliverables;
- (c) must not be disclosed without prior written authorization from the RFSQ Contact; and
- (d) must be returned by the respondents to the Government immediately upon the request of the Government.

3.5.2 Confidential Information of Respondent

- (a) A respondent should identify any information in its response or any accompanying documentation supplied in confidence for which confidentiality is to be maintained by the Government. The confidentiality of such information will be maintained by the Government, except as otherwise required by the *Public Access to Information Act 2010* ("PATI") or required by law or by order of a court or tribunal.
- (b) Respondents are advised that their responses will, as necessary, be disclosed on a confidential basis, to the Government's advisers retained to advise or assist with the RFSQ process, including the evaluation of responses. If a respondent has any questions about the collection and use of personal information pursuant to this RFSQ, questions are to be submitted to the RFSQ Contact.

- (c) The respondent is responsible to ensure that they comply with the *Personal Information Protection Act 2016* (“PIPA”), related to any information in the bidder’s custody, care or control.

3.6 Procurement Process Non-Binding

3.6.1 No Process Contract

This RFSQ is a request for responses only and participation in this RFSQ is not intended to create legal obligations between the Government and any of the respondents or their representatives. For greater certainty and without limitation:

- (a) Participation in this RFSQ will not give rise to any preliminary contract or collateral contract;
- (b) No respondent shall have any claim for any compensation of any kind whatsoever (whether in a contract, tort, law, equity or otherwise), as a result of participating in this RFSQ, and by submitting a response each respondent shall be deemed to have agreed that it has no claim against the Government;
- (c) The decision to award or not to award a contract to any respondent is at the discretion of the Government. The Government shall have no liability to any respondent with respect to the awarding of contract or the failure to award a contract to any respondent. Respondents acknowledge that the respondent that submits the response with the lowest price might not be awarded a contract.

3.6.2 No Legal Relationship or Obligation

No legal relationship or obligation regarding the procurement of any good or service will be created between the respondent and the Government by this RFSQ process.

3.6.3 Cancellation

The Government may cancel or amend the RFSQ process without liability at any time. Cancellation may occur, for example, if:

- (a) no qualitatively or financially worthwhile offer has been received or there has been no valid response at all;
- (b) the economic or technical parameters of the project have changed fundamentally;
- (c) exceptional circumstances or force majeure render normal implementation of the project impossible;
- (d) all offers exceed the financial resources available, or are otherwise inconsistent with the principles of economy, efficiency and effectiveness; or
- (e) irregularities require cancellation in the interest of fairness.

The publication of a procurement notice does not commit the Government to implement the programme or project announced.

3.7 Governing Law and Interpretation

The Terms and Conditions of RFSQ Process (Part 3)

- (a) are intended to be interpreted broadly and separately (with no particular provision intended to limit the scope of any other provision);
- (b) are non-exhaustive and will not be construed as intending to limit the pre-existing rights of the parties to engage in pre-contractual discussions in accordance with the common law governing direct commercial negotiations; and
- (c) are to be governed by and construed in accordance with the laws of Bermuda applicable therein.

[End of Part 3]

APPENDIX A – SUBMISSION FORM

1. Respondent Information

Please fill out the following form, naming one person to be the contact for this RFSQ response and for any clarifications or communication that might be necessary.

If the company is incorporated and registered, then a Certificate of Incorporation and a Certificate of Incumbency is required and must be submitted with the Submission Form.

Declaration of Interest: The respondent shall provide details of its ownership and/or managerial structure upon request from the Government. The respondent shall also provide a statement of whether or not it has any relevant and material interest relevant to the provision of Service. Such statement shall be provided at least annually or if there is any change in the interest of the respondent.

Full Legal Name of Respondent or Personal/Given Name:	
Representative Name (Person with Signing Authority) / Title:	
Any Other Relevant Name under which Respondent Carries on Business:	
Street Address:	
City, Province/State:	
Postal Code:	
Country:	
Phone Number:	
Respondent's Social Insurance Number issued by the Government of Bermuda:	
Respondent's Payroll Tax Number issued by the Government of Bermuda:	
Respondent's Registration Number issued by the Bermuda Registrar of Companies (if incorporated):	
Company Website (if any):	
Respondent Contact Name and Title:	
Respondent Contact Phone:	
Respondent Contact Fax:	
Respondent Contact Email:	

2. Acknowledgment of Non-Binding Procurement Process

The respondent acknowledges that this RFSQ process will be governed by the terms and conditions of the RFSQ and that, among other things, such terms and conditions confirm that this procurement process does not constitute a formal, legally binding bidding process (and for greater certainty, does not give rise to a Process Contract) and that no legal relationship or obligation regarding the procurement of any good or service will be created between the Government and the respondent unless and until the Government and the respondent execute a written agreement for the Deliverables pursuant to a subsequent invitational second-stage procurement process.

3. Ability to Provide Deliverables

The respondent has carefully examined the RFSQ documents and has a clear and comprehensive knowledge of the Deliverables required. The respondent represents and warrants its ability to provide the Deliverables in accordance with the requirements of the RFSQ.

4. Addenda

The respondent is requested to confirm that it has received all addenda by listing the addenda numbers, _____ to _____ (if applicable) issued by the Government, or if no addenda were issued by the Government write the word “None”. The onus is on respondents to make any necessary amendments to their responses based on the addenda. The respondent confirms it has read, received and complied with these addenda. Respondents who fail to complete this section will be deemed to have received all posted addenda.

5. No Prohibited Conduct

The respondent declares that it has not engaged in any conduct prohibited by this RFSQ.

6. Conflict of Interest

Respondents must declare all potential Conflicts of Interest, as defined in section 3.4.1 of the RFSQ. This includes disclosing the names and all pertinent details of all individuals (employees, advisers, or individuals acting in any other capacity) who (a) participated in the preparation of the response; **AND** (b) were employees of the Government within twelve (12) months prior to the Submission Deadline.

If the box below is left blank, the respondent will be deemed to declare that (a) there was no Conflict of Interest in preparing its response; and (b) there is no foreseeable Conflict of Interest in performing the contractual obligations contemplated in the RFSQ.

Otherwise, if the statement below applies, check the box.

- ☐ The respondent declares that there is an actual or potential Conflict of Interest relating to the preparation of its response, and/or the respondent foresees an actual or potential Conflict of Interest in performing the contractual obligations contemplated in the RFSQ.

If the respondent declares an actual or potential Conflict of Interest by marking the box above, the respondent must set out below details of the actual or potential Conflict of Interest:

7. Disclosure of Information

Any information collected or used by or on behalf of the Government under this solicitation document is subject to the Public Access to Information Act 2010 (“Act”). The information belongs to a class of information that might be made available to the general public unless it is contained in a record that is exempt from disclosure under the Act. Any questions regarding the collection, use, or disclosure of the information should be directed to the public authority that issued this solicitation document.

Signature of Witness

Signature of Respondent Representative

Name of Witness

Name of Respondent Representative

Title of Respondent Representative

Date

I have the authority to bind the respondent.

SAMPLE CERTIFICATE OF INCUMBENCY

The undersigned being the Secretary of the company as named below (the "Company"), a company duly organised and existing under the laws of the Islands of Bermuda and having it's registered office as set out below DO HEREBY CERTIFY that the following is a true and correct listing of the Directors and Officers of the Company in full force and effect as of the date hereof.

DIRECTORS

List

ALTERNATE DIRECTORS

List

OFFICERS

List

IN WITNESS WHEREOF I have hereunto set my signature in accordance with the Bye-Laws of the Company.

Company Name:

Date:

Secretary/Director

APPENDIX B – RFSQ PARTICULARS

A. THE DELIVERABLES

The Government is seeking information from qualified suppliers with proven experience in delivering national-scale digital identity ecosystems. The future procurement is expected to include the design, implementation, operation, support and continual enhancement of a Digital Identity Platform, Digital Wallet capability, and associated governance, security and integration services. Suppliers should consider the anticipated future-state digital identity ecosystem described below when preparing their responses.

Hardware and Software Procurement

The Supplier shall provide all hardware, software, licences, subscriptions, tools, and supporting components necessary to deliver, operate, and maintain the Bermuda National Digital Identity Platform and associated Digital Wallet solution. This includes all infrastructure, identity management components, integration tools, monitoring solutions, and supporting technologies required for a fully functional production environment.

Installation, Configuration and Implementation

The Supplier shall design, install, configure, integrate, test, and deploy the Digital Identity Platform, Digital Wallet, and associated services. This includes identity proofing capabilities, credential issuance, authentication services, relying party integrations, API configuration, migration activities, operational readiness activities, user acceptance testing, training, knowledge transfer, and transition into production support.

Security, Privacy and Operational Assurance

The Supplier shall implement and maintain all cybersecurity, privacy, fraud management, business continuity, disaster recovery, monitoring, reporting, and compliance controls necessary to support a secure and resilient Digital Identity service. This includes security architecture, privacy-by-design controls, incident response capabilities, security testing, audit logging, fraud detection and identity repair processes, and compliance with applicable legal and regulatory requirements.

Stakeholder Enablement and Adoption

Provide stakeholder engagement, public education, relying-party onboarding, training materials, user support documentation, and adoption activities necessary to support successful implementation and uptake of the Digital Identity ecosystem.

Operational Support and Managed Services

Provide ongoing operation, maintenance, support, monitoring, reporting, service management, performance management, platform upgrades, incident management, and lifecycle support for the Digital Identity Platform throughout the contract term.

B. MATERIAL DISCLOSURES

Prospective suppliers should be aware of the following material matters, each of which may impact solution design, implementation methodology, contractual obligations, pricing, and ongoing operational responsibilities:

- The Digital Identity Programme is intended to be delivered through a single-provider PPP model, under which the selected supplier will be responsible for the delivery and operation of the platform.
- The Government anticipates that the Digital Identity Platform will be designated as Critical National Information Infrastructure (CNII)
- Government will complete a formal information classification assessment prior to the subsequent procurement stage. The resulting classification will determine minimum cybersecurity, cryptographic, resilience, availability, logging, monitoring and recovery requirements. Suppliers must demonstrate capacity to operate solutions in accordance with Government-defined classification controls.
- A Government-led information classification assessment will establish the minimum security controls, availability targets, recovery objectives, monitoring requirements, cryptographic standards, and incident response obligations applicable to the solution.
- The solution will rely on integration with authoritative Government registers and source systems for identity proofing, verification, and attribute validation, including, where applicable, immigration, civil registration, corporate registry, taxation, and other authoritative government systems. The readiness and quality of these data sources may affect implementation activities and timelines.
- Legislative, regulatory, and policy changes may be required to support implementation of the Digital Identity Programme. The successful supplier will be expected to assist with legislative gap analysis, regulatory enablement, and related advisory activities.
- The solution must comply with Bermuda's Personal Information Protection Act 2016 (PIPA), including requirements relating to privacy by design, data minimisation, consent management, transparency, retention, and cross-border data transfers.
- Government will establish mandatory requirements relating to hosting arrangements, data residency, cross-border transfers of personal information, and Transfer Impact Assessments (TIAs), which suppliers will be required to satisfy.
- The successful supplier will be required to undergo and successfully complete independent security assessments and assurance reviews prior to contract award and production deployment.
- The contract will include requirements for data portability, knowledge transfer, transition support, secure data destruction, exit management, and Government step-in rights to ensure continuity of service and minimise vendor lock-in.

- The supplier will be required to provide ongoing managed services and operational support, including 24/7 support for security-critical incidents, cybersecurity monitoring, incident response, fraud management, and service restoration activities.
- The programme is expected to be implemented in phases, initially focusing on a priority first use case of immigration with a particular emphasis on work permits and residents permits, before expanding to additional public and private sector services.
- It is a Government requirement that residents will not be charged for access to essential digital identity services. Suppliers must therefore propose a commercial model that supports this objective while ensuring long-term sustainability of the service.
- Government anticipates requiring support for open standards including OpenID Connect, OAuth 2.0, SAML and applicable Credential Standards.
- Government expects the future solution to include digital wallet functionality supporting identity and attribute credentials across mobile and web channels.

Government intends that the Digital Identity Platform will serve as, or directly underpin, the Government Identity Provider (IdP) supporting the One Stop Shop (OSS) programme and associated authentication services. Suppliers should consider integration, federation and authentication requirements necessary to support Government-wide identity and access management capabilities.

C. MANDATORY SUBMISSION REQUIREMENTS

1. Submission Form (Appendix A)

Each response must include a Submission Form (Appendix A) completed and signed by an authorized representative of the respondent.

2. Certificate of Confirmation of Non-Collusion (Appendix C)

Each response must include a Certificate of Confirmation of Non-Collusion Form (Appendix C) completed and signed by an authorized representative of the respondent.

3. Company Certificate of Incorporation

A signed copy of the Certificate of Incorporation must be included for respondents that are companies/corporations.

4. Certificate of Incumbancy

A copy of the Certificate of Incumbancy must be included for respondents that are companies/corporations.

5. Other Mandatory Submission Requirements

Stakeholder Engagement

Proponents should describe their indicative approach/plan to how they will maximise stakeholder engagement throughout the initial stages of the project.

Company Profile

Proponents must submit sufficient information to demonstrate their organisational capability, relevant experience, and suitability to participate in the procurement process. At a minimum, submissions must include a corporate profile identifying the legal entity and ownership structure of the proponent, details of relevant experience delivering digital identity, identity verification, or other high-assurance digital services, and a minimum of three comparable project references. Submissions must also include details of the proposed delivery team and key personnel, a description of the proponent's cybersecurity, privacy, and risk management capabilities, and a high-level overview of the proposed approach to delivering Bermuda's Digital Identity programme. Proponents must disclose any actual, potential, or perceived conflicts of interest and confirm their ability to comply with Bermuda's Personal Information Protection Act 2016 (PIPA) and other applicable legal and regulatory requirements. Failure to provide the required information may result in the submission being deemed non-compliant and excluded from further consideration.

See Annex A - Company Profile Form

Local Benefits

Each Proposal must include the completed Local Benefit Form - Social, Economic, and Environmental.

Security and Privacy Requirements

Proponents are required to complete and submit the attached Security & Privacy Mandatory Technical Requirements Questionnaire.

See Annex B - Security & Privacy Mandatory Technical Requirements Questionnaire

Digital Identity Solution Capability and Technical Readiness

To proceed to detailed evaluation, proponents must demonstrate, on a pass/fail basis, that they possess the technical capability and experience necessary to deliver the proposed solution. Proponents must demonstrate experience designing, implementing, or operating digital identity, digital credential, identity verification, or comparable trusted digital services. The proposed solution must be capable of providing secure digital identities and digital wallets, supporting identity proofing and verification, and integrating with government and private-sector relying parties. Proponents must demonstrate a privacy-by-design approach, support for data minimisation, and the use of open standards that promote interoperability and avoid unnecessary vendor lock-in. The proposed solution must include robust cybersecurity, risk management, fraud management, audit logging, monitoring, reporting, and identity lifecycle management capabilities, including enrolment, credential issuance, update, suspension, recovery, and revocation processes. Proponents must also demonstrate their ability to support data portability, transition,

and exit arrangements to ensure the long-term resilience and continuity of Bermuda's Digital Identity ecosystem.

Digital Identity Production Experience

Respondents are required to submit a detailed reference case study for at least one named production Digital Identity implementation currently, or previously, operated by the respondent. The submitted case study must include the client name, number of enrolled users, years in operation, current operational status, service availability achieved, regulatory frameworks supported, and the scope of identity services delivered. Respondents should also describe their specific role in the deployment, key challenges addressed, operational outcomes, and any measurable performance indicators demonstrating the success and maturity of the solution.

Identity Proofing and Verification

Proponents must describe their identity proofing and verification capabilities including document verification, biometric and non-biometric options, assurance levels and fraud controls.

Selective Disclosure and Consent Management

Proponents must describe capabilities relating to selective disclosure, consent management and attribute sharing.

Privacy Compliance Capability

Proponents must describe how the proposed solution supports compliance with PIPA and privacy-by-design principles.

Security Operations Capability and Availability and Resilience

Proponents must describe security monitoring, Security Operations Centre capability, incident response arrangements, service availability targets and disaster recovery capability.

Technical Support and Operational Staffing

Proponents must provide information regarding key operational, cybersecurity and technical resources available for delivery and ongoing support.

Digital Identity Trust Framework Assessment

Suppliers must demonstrate experience assessing solutions against recognised Digital Identity trust frameworks. Suppliers must agree to perform a gap assessment against the UK Digital Identity and Attributes Trust Framework and provide recommendations for future alignment.

Identity Repair Services

The supplier must demonstrate the existence of documented identity repair procedures including re-proofing, credential re-issuance, relying party notification, fraud case management and user support.

D. MANDATORY TECHNICAL REQUIREMENTS

Proven Digital Identity Solution

The supplier must have successfully implemented and operated at least one production digital identity or equivalent high-assurance digital credential solution for a government, regulated industry, or national-scale programme. The solution must currently be in live operation or have been operational within the last five years. Evidence must be provided through a named client reference.

Cybersecurity Certification and Controls

The Supplier must maintain ISO/IEC 27001 certification or an equivalent independently audited information security certification demonstrating the implementation and ongoing operation of a comprehensive Information Security Management System (ISMS). Evidence of certification and scope of accreditation must be provided. The Authority reserves the right to determine whether any proposed equivalent certification provides an appropriate level of assurance.

Hosting and Cross-Border Data Transfer Compliance and Accessibility Requirements

The supplier must confirm its ability to comply with Government-defined hosting, data residency, cross-border transfer and Transfer Impact Assessment requirements.

Acceptance of Government Security Requirements

The supplier must formally accept Government security, cybersecurity, incident reporting, information classification, CNII and regulatory requirements as may be applicable to the programme.

Security and Privacy Requirements

Proponents are required to complete and meet the requirements of the attached Security & Privacy Mandatory Technical Requirements Questionnaire.

E. PRE-CONDITIONS OF AWARD

1. Financial Checks

Prior to awarding a contract to the selected respondent, the contracting department will perform financial checks to confirm whether the respondent is delinquent in making payments to the Government for Social Insurance contributions, Payroll Tax or any other debt recorded by the Accountant General's Debt Collection Section, and will perform a check with the Bermuda Registrar of Companies to confirm whether the respondent is a proper legal entity that is in good standing.

Cybersecurity & Privacy Assessment

The successful Proponent and solution will be required to complete and pass the Government's vendor assessment, including, but not limited to, Cybersecurity and Privacy assessments and issuance of an Interim Authority to Operate by the Ministry of National Security before contract award. If required by Government, the Proponent, upon request, shall provide any requested information, documents, certification and other materials required to facilitate such assessments.

Such costs associated with the provision of such materials will be the responsibility of the Proponent.

F. RATED CRITERIA

The following sets out the categories, weightings and descriptions of the rated criteria of the RFSQ. Respondents who do not meet a minimum threshold score for a category will not proceed to the next stage of the evaluation process.

Proponents who are shortlisted may be invited to present oral presentations for the purpose of introducing key members of the project team and allowing the Government to fully understand the prospective Proponent's ability to meet the evaluation criteria and deliverables. Oral presentations will not be scored separately. Instead, the Government may modify scores and resulting ranking based on the oral presentations of those prospective proponents.

#	Category	Weighting (%)	Threshold
1	Relevant Experience and Capability	25	15/25
2	Technical & Architectural Solution	10	6/10
3	Security, Privacy & Fraud Management	10	6/10
4	Delivery Approach & Implementation Plan	10	N/A
5	Legal & Regulatory Readiness	5	N/A
6	Stakeholder Engagement, Adoption & Reporting	10	N/A
7	Local Benefits	30	N/A
Total Points		100	

1. Relevant Experience and Capability

The following questions will be considered when each proposal is evaluated:

- Does the respondent clearly demonstrate the ability to meet the Government's requirements?
- Does the respondent have the support capability required?
- Does the respondent demonstrate relevant experience leading and developing Digital Identity programmes of comparable scale, complexity and scope.
- Do the persons who will be working on the project have the necessary skills and experience?
- Does the respondent demonstrate that they have the structure, experience, resources, and capabilities demonstrate its ability to successfully deliver, operate, and support the proposed Digital Identity solution?
- Does the proposed project team demonstrate the qualifications, experience, and capacity required to successfully deliver and support the Services?
- Does the respondent demonstrate experience successfully managing subcontractors, implementation partners, technology providers, and other third parties, when necessary, in comparable Digital Identity programmes?
- Does the respondent's experience delivering and operating Digital Identity solutions in live production environments demonstrate its ability to meet the Government's requirements?
- Does the respondent demonstrate experience in operating and supporting Digital Identity solutions in live production environments comparable to the Government's requirements.

- Does the respondents case studies and client references demonstrate successful delivery and operation of solutions comparable to the Government's requirements in terms of scope, scale, complexity, and outcomes?
- Were the respondent's referees positive about their experience of working with the contractor/vendor/supplier, and would they use the Proponent again?
- Has the proponent performed well on previous Government Projects?

2. Technical & Architectural Solution

The following questions will be considered when each proposal is evaluated:

- Does the respondent demonstrate that its Digital Identity platform is capable of alignment with recognised industry standards, best practices, and modern Digital Identity principles?
- Does the solution support interoperability through recognised standards and protocols, including OpenID Connect (OIDC), OAuth 2.0, SAML, Verifiable Credentials, Decentralised Identifiers (DIDs), and other applicable standards?
- Does the respondent demonstrate that its Digital Identity platform is capable of supporting identity proofing, identity verification, authentication, credential issuance, credential lifecycle management, and digital wallet functionality?
- Does the respondent demonstrate that its Digital Identity platform is capable of supporting privacy-enhancing capabilities, including selective disclosure, consent management, data minimisation, and user control of personal information to meet the Government's requirements, regulations and legislation?
- Does the respondent demonstrate that its Digital Identity platform is capable of the flexibility and scalability required to support future services, additional relying parties, new credential types, and evolving legal, regulatory, and business requirements?
- Does the respondent's proposed API architecture, developer tools, integration capabilities, and onboarding processes support adoption and integration by government entities, regulated organisations, and other relying parties?
- Does the respondent demonstrate that its Digital Identity platform is capable of minimising vendor lock-in and support portability of identity data, interoperability, and transition to alternative providers or operating models?
- Does the respondent demonstrate that its Digital Identity platform is capable of providing resilience, scalability, high availability, disaster recovery, and business continuity capabilities sufficient to support critical Digital Identity services as required by the Government?
- Does the respondent demonstrate that its Digital Identity platform is capable of ensuring accessibility, usability, and a positive user experience for residents, businesses, government entities, and other stakeholders?
- Does the respondent demonstrate they are capable of supporting the ongoing monitoring, maintenance, management, and support of the solution throughout its operational lifecycle in line with the Government's requirements?
- Does the respondent demonstrate that its Digital Identity platform has been implemented in compliance with applicable legal, regulatory, privacy, security, and trust framework requirements?

3. Security, Privacy & Fraud Management

The following questions will be considered when each proposal is evaluated:

- Does the respondent demonstrate that its proposed Digital Identity solution is supported by an appropriate security architecture and privacy-by-design framework, including cryptographic controls, key management and safeguards aligned with Bermuda's Personal Information Protection Act (PIPA), sufficient to protect identity data and meet the Government's requirements?
- Does the respondent's proposed identity proofing controls, fraud prevention measures, fraud detection capabilities, and identity recovery processes demonstrate its ability to maintain trust and integrity within the Digital Identity ecosystem?
- Does the respondent's proposed use of cryptographic controls, encryption mechanisms, and key management arrangements demonstrate its ability to protect identity data and maintain system integrity?
- Does the respondent demonstrate experience providing security monitoring, threat detection, vulnerability management, incident response, and ongoing cybersecurity management for comparable Digital Identity environments?
- Does the respondent's proposed approach to data minimisation, consent management, audit logging, transparency, accountability, and user control of personal information demonstrate its ability to protect privacy and support the responsible use of identity data?
- Does the respondent demonstrate established business continuity, disaster recovery, and operational resilience capabilities for comparable Digital Identity services?
- Does the respondent demonstrate that its proposed solution maintains trust in the Digital Identity ecosystem through appropriate governance, risk management, security controls, privacy protections, fraud management measures, and ongoing compliance arrangements?

4. Delivery Approach & Implementation Plan

The following questions will be considered when each proposal is evaluated:

- Does the respondent demonstrate an understanding of the Government's objectives, requirements, and desired outcomes for the Digital Identity programme?
- Does the respondent demonstrate a high-level methodology for implementing a Digital Identity programme of comparable size and complexity?
- Does the respondent demonstrate experience managing programme risks, assumptions, dependencies, constraints, and issues in comparable implementations?
- Does the respondent demonstrate the ability to mobilise appropriately qualified and experienced personnel for delivery?

The following questions will be considered when each proposal is evaluated:

- Does the respondent demonstrate an understanding of Bermuda's legal, regulatory, and policy environment and its ability to support the successful implementation and operation of the Government's Digital Identity Programme?
- Does the respondent demonstrate experience conducting legislative and regulatory assessments to support Digital Identity or comparable programmes?
- Does the respondent's proposed solution and delivery approach demonstrate its ability to support compliance with the Personal Information Protection Act (PIPA), anti-money laundering and anti-terrorist financing (AML/ATF) obligations, cybersecurity requirements, and other applicable legal, regulatory, and governance requirements?

- Does the respondent's experience supporting legislative reform, regulatory implementation, or policy development for Digital Identity initiatives or comparable programmes demonstrate its ability to meet the Government's requirements?
- Does the respondent demonstrate experience managing legal, regulatory, stakeholder, and implementation risks associated with Digital Identity programmes?
- Does the respondent's understanding of Digital Identity trust frameworks, assurance models, and international best practices demonstrate its ability to support the development, implementation, governance, and operation of the proposed solution and meet the Government's requirements?

6. Stakeholder Engagement, Adoption & Reporting

The following questions will be considered when each proposal is evaluated:

- Does the respondent demonstrate experience engaging government entities, industry participants, citizens, businesses, regulated organisations, and other stakeholders during comparable Digital Identity programmes?
- Does the respondent demonstrate experience supporting public education, awareness, trust-building, and adoption activities for Digital Identity programmes?
- Does the respondent's proposed approach to accessibility, inclusivity, and equitable access demonstrate its ability to ensure that Digital Identity services are available and usable by all users and meet the Government's requirements?
- Does the respondent demonstrate experience establishing performance measurement, monitoring, reporting, and service management arrangements for comparable Digital Identity programmes?
- Does the respondent's proposed approach to supporting vulnerable, digitally excluded, underserved, or at-risk populations demonstrate its ability to ensure equitable access to, participation in, and adoption of the Digital Identity ecosystem and meet the Government's requirements?
- Does the respondent demonstrate experience using stakeholder feedback, user satisfaction data, and continuous improvement processes to enhance Digital Identity services?

7. Local Benefits

The Government has established the minimum evaluation weight regarding Local Benefits for this procurement at 30% of the total points.

The local benefit considerations will be given to each of the following factors when proposals are evaluated:

- Is the proponent a local specified business? (See the Code of Practice for Project Management and Procurement on the Government's Portal for the definition of "Specified Business")
- Local Workforce Utilization
 - Number of Bermudians employed by the proponent.
 - Engagement of Bermudian employee (%) during the project.
 - Use of local specified businesses in the proponent's supply chain.
 - Use of local specified business as subcontractors (if applicable).

- Safety and Health record of the proponent for the three immediately preceding years of reporting
- Operational Environmental considerations and policy for their working site and projects. (each proponent to provide a copy)

See Annex C - Local Benefit Form

APPENDIX C – CERTIFICATE OF CONFIRMATION OF NON-COLLUSION

Notes for the respondents

The essence of Open Tendering is that the Government of Bermuda shall receive bona fide competitive response from suitably qualified persons or entities. In recognition of this principle, each person or entity that submits a response will be required, by way of the signature of a duly authorized representative of the company, to confirm that the response has been submitted without any form of collusion.

All respondents must complete and sign a Certificate of Confirmation of Non-Collusion. Any proposals submitted which do not include a signed copy of the Certificate will be wholly rejected and will not be included in the evaluation process.

If it is later found that the undertakings made below have been breached at any stage of the procurement process, then the respondent will be expelled from the process immediately. In the event that this is discovered after a contract award, legal action may be taken against the respondent and/or any party involved in the matter.

Any respondent that submits false information in response to this Request for Supplier Qualifications (RFSQ), and any other person or entity involved in collusion, may be excluded from competing for future contracts tendered by the Government of Bermuda.

Confirmation of non-collusion

I/We certify that this is a bona fide proposal, intended to be competitive and that I/We have abided by the terms and conditions related to this tender and that I/We have not fixed or adjusted the amount of the proposal or the rates and prices quoted by or under or in accordance with any agreement or arrangement with any other person.

I/We confirm that we have not received any information, other than that contained within the RFSQ pack, or supplementary information provided to all respondents.

I/We also certify that I/We have not done and undertake that I/We will not do at any time any of the following acts:

- (a) communicating to a person other than the RFSQ Contact the amount or approximate amount of my/our proposed response (other than in confidence in order to obtain quotations necessary for the preparation of the response for insurance);
- (b) entering into any agreement or arrangement with any other person that he shall refrain from competing or as to the amount of any proposal to be submitted; or
- (c) offering or agreeing to pay or give or paying any sum of money, inducement, gift /hospitality or valuable consideration directly or indirectly to any person in relation to this procurement.

By signing this document, I/we have read and agree to its terms and conditions.

(1) _____ Title _____ Date _____

(2) _____ Title _____ Date _____

for and on behalf of _____