# Request for Proposal (RFP)

## For
## the Saskatchewan
## Individual Digital ID Solution and Service Offering

Request for Proposal No.: SPS-RFP-0484

Issued Date: October 18, 2021

Submission Deadline Date: **December 6, 2021 at 2:00 p.m. local Saskatchewan time**

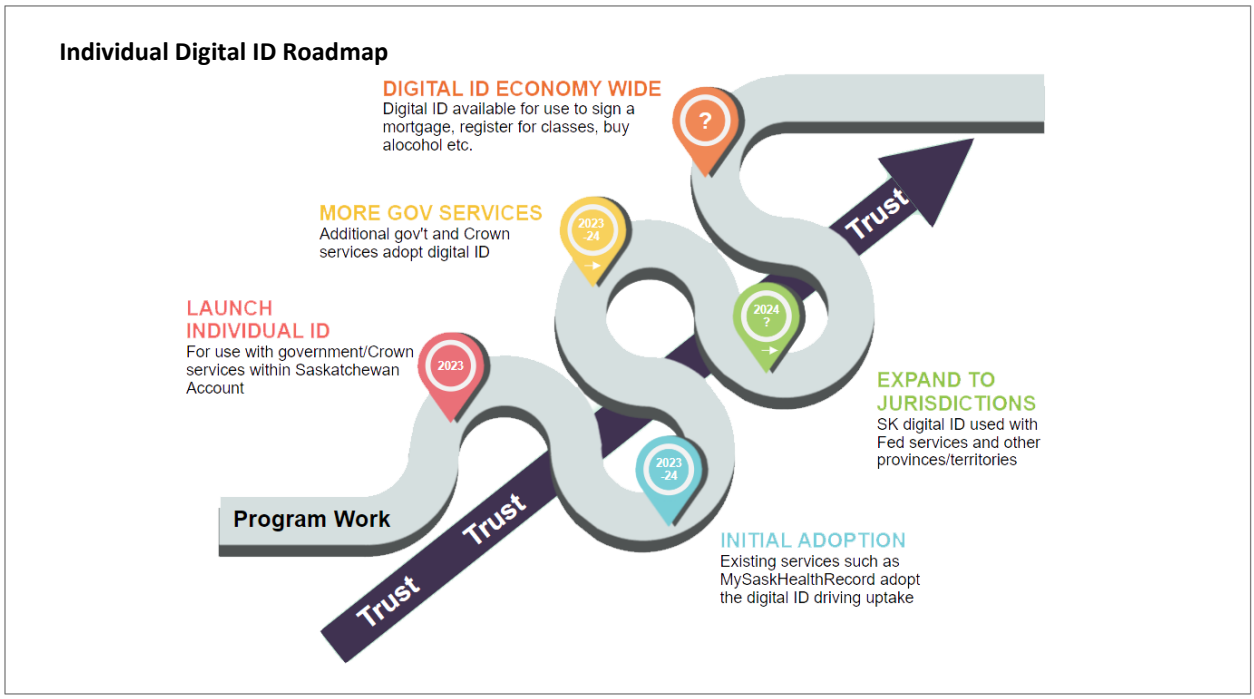
**TABLE OF CONTENTS**

# PART 1 - INVITATION AND SUBMISSION INSTRUCTIONS

## 1.1 Invitation to Proponents

This Request for Proposal (RFP) is an invitation by the Government of Saskatchewan (GOS) to submit proposals for the provision of the solutions and services encompassed in **the *Saskatchewan Individual Digital Identity Roadmap*[1], ** as further described in the RFP Particulars (Appendix A).

GOS is seeking a long-term partner to design, build, test, implement, roll out, and operate a level of assurance three (LOA3)[2] digital identity, in collaboration with the GOS digital partner network. This digital identity will be used by individuals residing in Saskatchewan to access online government services and eventually online transactions in the broader economy and other jurisdictions. Due to the broad nature of this RFP, consortium bids are welcomed and anticipated. Refer to Section 1.3 for further details on consortiums as it relates to this competition.




A digital ID is an online alternative to a physical ID, such as a driver's license or other government-issued photo ID. Today, governments and businesses rely on the presentation of an ID for many transactions, both in-person and online. In addition, many organizations request a copy of an ID for their records, either at the point of transaction, by mail or email. These practices are cumbersome for the user and create both fraud and privacy risks. In the case of a mailed or emailed ID, there is no way to connect the

[1] See A.1.1 – *Individual Digital ID Roadmap*

[2] As defined by the Digital Identity and Authentication Council of Canada (DIACC) Pan-Canadian Trust Framework (PCTF) (https://diacc.ca/trust-framework/pctf-overview/) and the Pan-Canadian Trust Framework-Public Profile (https://canada-ca.github.io/PCTF-CCP/)

copy back to the sender with certainty, and storage of the ID, whether submitted in-person or by mail/email, results in unnecessary storage of personal information, presenting a privacy risk.

With a digital ID, GOS is seeking to equip Saskatchewan residents and businesses with a key tool to move into the digital economy. It will empower residents to interact more online and it will also empower governments, organizations, and businesses to reduce the need for in-person or photocopy/email ID checks. Furthermore, a digital ID enables a self-serve option, making it simpler for citizens in terms of the time it takes, and the number of steps involved. The self-service option frees up government, Crown corporations, and eventually businesses and institutions, to focus their frontline resources on the people who truly need in-person support.

At the highest level, the scope of this RFP includes:

- Deliver the *Individual Digital ID Roadmap*'s first initiative: the *Individual Digital ID Foundations Initiative* (See A.1.2), under the direction and guidance of the GOS Project Manager and in adherence with GOS project standards and practices.
- Provide operational support for the *Individual Digital ID Roadmap* including but not limited to the development and delivery of the legislative and privacy frameworks, operational plans, and resources who will manage the service, technical citizen support, onboarding, the implementation of continuous improvement, and stakeholder support.
- Lead and/or support future initiatives relating to the *Individual Digital ID Roadmap* and the broader *Saskatchewan Digital ID Program* as requested.

The goals of the *Individual Digital ID Roadmap* are to:

1. Enable GOS to offer secure access to high-value and sensitive services online.
2. Enable Saskatchewan's digital economy by giving citizens tools to transact online with trust and security.
3. Deliver a foundational component in GOS' digital transformation, which is gaining importance in a virtual economy.

For more information on the delineation between the initiative, roadmap and program see Appendix A, Section A: Overview and Background.

This Competition, as well as any resulting agreement(s), may be utilized (but does not include any proprietary ownership of source code) for the broader public sector within the province of Saskatchewan. This includes, but is not limited to, non-government organizations (NGOS), crown corporations, government agencies, MASH sector, health districts, school boards, and municipal governments (cities and/or towns) (hereinafter the "Broader Public Sector Agency" or "BPSA"). GOS shall not be liable in any manner whatsoever to any Broader Public Sector Agency for its use of this Competition process or any of its associated agreements, and GOS shall not be liable to the Proponent for any Broader Public Sector Agency's use of this Competition process or any associated agreements.

## 1.2 RFP Contact

For the purposes of this procurement process, the "RFP Contact" will be:

**itprocurement@gov.sk.ca**

**Attention:** Shahlar Mammadov**,** SPS-RFP-0484

Proponents and their representatives are not permitted to contact any employees, officers, agents, elected or appointed officials or other representatives of GOS, other than the RFP Contact, concerning matters regarding this RFP. Failure to adhere to this rule may result in the disqualification of the Proponent and the rejection of the Proponent's proposal.

Inquiries and their responses may be posted on the website sasktenders.ca at the sole discretion of the GOS, without revealing the source of the inquiry.

## 1.3 Type of Agreement for Deliverables

The selected Proponent(s) will be requested to enter into direct contract negotiations to finalize an Agreement with GOS for the provision of the Deliverables. GOS expects the terms and conditions set out in the Form of Agreement in Appendix C to be included in the final negotiated Agreement with the selected Proponent(s). Proponents choosing to participate in this RFP process should be prepared to accept those terms and conditions, subject only to minor changes that may be mutually agreed upon in the negotiation process. It is GOS's intention to enter into an Agreement with one (or more) Proponents.

Where a consortium is responding to this RFP, the following shall apply:

a. one member of the consortium shall be the Proponent, and
b. the Proponent shall confirm that the Proponent shall assume full responsibility and liability for the work and actions of all consortium members (who are subcontractors to the Proponent) with respect to the obligations to be assumed pursuant to this RFP, provided that the Company shall be entitled to reject a subcontractor and may consent to a replacement.

The term of the Agreement is to be for a period of 5 years, with an option in favour of GOS to extend the Agreement on the same terms and conditions for an additional term of up to 2 years.

GOS has the right to negotiate a penalty clause with the Preferred Service Provider that will be included in the Agreement.

The Agreements(s) resulting from this RFP may include system software licensing, installation/configuration, data migration/implementation, identifiable program deliverables based on customer's needs, and yearly system infrastructure support and maintenance for the life of the solution.

**Proponents are asked to review Appendix C – Form of Agreement and respond to Mandatory 1 in Appendix D – Mandatory Requirements. Suppliers that hold an active Ministry of SaskBuilds and Procurement (formerly Central Services) Master Terms and Conditions are not required to review this Appendix.**

## 1.4 RFP Timetable

| | |
|---|---|
| Issue Date of RFP | **October 18, 2021** |
| Registration Deadline for Individual Proponent Conferences | **November 1, 2021** |
| Individual Proponent Conferences | **November 8 – 17, 2021** |
| Deadline for Questions | **November 19, 2021** |
| Deadline for Issuing Addenda | **November 24, 2021** |
| Submission Deadline | **December 6, 2021 2:00 p.m. local Saskatchewan time** |
| Rectification Period | **3 days after notification** |
| Anticipated Initial Ranking | **Week of January 17, 2022** |
| Proponents Presentation and/or Interview | **February 7, 2022 – February 18, 2022** |
| Proof of Concept | **February 28, 2022 - June 24, 2022** |
| Reference Checks | **As required** |
| Anticipated Deadline for Submission of Best and Final Offers ("BAFO") | **As required** |
| Anticipated Final Ranking | **July 31, 2022** |
| Anticipated Execution of Agreement | **August 31, 2022** |

The RFP timetable is tentative only and may be changed by GOS at any time.

### 1.4.1 Individual Proponent Conferences

Individual Proponent Conferences may be scheduled as follows:

Date: Between November 8th and 17th, 2021
Time: Between 9:00 a.m. and 4:00 p.m., Local Saskatchewan Time
Duration: Up to 55 minutes
Location: Microsoft Teams Meeting, or as otherwise directed by GOS

Individual Proponent Conferences are an opportunity to meet with Ministry staff in private, one-on-one sessions to learn more about the scope of this Competition. The Individual Proponent Conferences are optional. Proponents not requesting an Individual Proponent Conference may still submit a proposal. The conferences can be via phone or virtual meeting; they do not need to be attended in-person.

GOS will not reimburse any expense associated with participating in Individual Proposed Conferences.

If you are interested in an Individual Proponent Conference, your request should be directed, in writing, before the date mentioned on the Timeline to:

Contact: itprocurement@gov.sk.ca
Subject: Conference: SPS-RFP-0484

Your e-mail request should include:

1. Names and e-mail addresses of attendees from your organization.
2. A list of questions or agenda items you intend to table at the conference.

To ensure the quality of information, meeting minutes will be taken. Any questions and answers that clarify, change the requirements, or that are process related will be shared with all Proponents.

A Question and Answer amendment posted to SaskTenders, without revealing the source of the inquiry will be published listing topics discussed.

Steps may be taken to protect any proprietary information, if requested, in preparation of these materials. Verbal responses to an inquiry are not binding on either party.

## 1.5 Submissions of Proposals

### 1.5.1 Submissions

Proponents must submit by email only. GOS does not assume any responsibility for delayed or rejected Submissions. Proponents acknowledge that all risks associated with Submissions are the sole responsibility of Proponents, and that late Submissions, regardless of the reason, will be rejected.

**Submitting by email:**

One (1) electronic copy in .pdf, .doc or .docx, .xls and .xlsx., which includes the RFP reference number and closing date, are to be forwarded to:

response@gov.sk.ca

**The subject line of the email should contain the RFP reference number and competition title.**

One (1) email, including attachments, should not be larger than 25MB or it may not be successfully transmitted. It is recommended to send one (1) email. If a Proponent is sending multiple emails, provide clear instructions on how the Submission should be integrated.

Executable file formats such as .exe will not be accepted. The preferred file formats are .pdf, .doc, .docx, .xls and .xlsx.

The received time in the recipient's email inbox will be the recorded date and time of a Submission. GOS will provide confirmation of email receipt to Proponents via an automatic email message. If no confirmation email is received, please contact 306-787-6871.

Prior to closing, GOS will maintain confidentiality of e-mail Submissions subject to GOS officials opening an e-mail for the purpose of identification. If one or more files cannot be opened, because a file is corrupted, for example, the Proponent will not have an opportunity to resend such files after closing.

**For more information, refer to the document Guidelines for Proponent Submissions via Email on SaskTenders.**

### 1.5.2 Proposals to be Received on Time

Proposals must be received as set out above on or before the Submission Deadline. Submissions received after the Submission Deadline will not be accepted.

Proponents are advised to make Submissions well before the deadline. Proponents making Submissions near the deadline do so at their own risk.

### 1.5.3 Proposals to be Submitted in Prescribed Format

Proponents should submit electronic copies of their proposal via the email address provided above. Proposals should be prominently marked with the RFP title and number (see RFP cover), with the full legal name and contact information of the Proponent.

### 1.5.4 Amendment of Proposals

Proponents may amend their proposals prior to the Submission Deadline by submitting the amendment to the location set out above. Any amendment should clearly indicate the full legal name and return address of the Proponent, RFP title and number, and which part of the Submission the amendment is intended to amend or replace.

### 1.5.5 Withdrawal of Proposals

At any time prior to the execution of a written Agreement for provision of the Deliverables, a Proponent may withdraw a submitted proposal. To withdraw a proposal, a notice of withdrawal must be received by the RFP Contact and should be signed by an authorized representative of the Proponent. GOS is under no obligation to return withdrawn proposals.

[End of Part 1]

# PART 2 - EVALUATION AND NEGOTIATION

GOS will conduct the evaluation of proposals and negotiations in the stages described below.

## 2.1 Stage I – Requirements

GOS will review proposal components for administrative deficiencies and compliance with mandatory requirements.

**Administrative Deficiencies**

If GOS determines that a proposal fails to meet any of the mandatory or submission requirements, GOS may at its discretion offer a rectification process. If a proposal fails to satisfy any of the mandatory or submission requirements, GOS may issue the Proponent a rectification notice identifying the deficiencies and providing the proponent an opportunity to rectify the deficiencies. If the Proponent fails to satisfy those mandatory or submission requirements within the Rectification Period, the proposal will be rejected. The Rectification Period will begin to run from the date and time that GOS issues a rectification notice to the Proponent. The mandatory and submission requirements are set out in Appendix D and Appendix A, Section F respectively.

GOS may eliminate mandatory requirements unmet by all Proponents.

## 2.2 Stage II – Written Evaluation

GOS will evaluate each qualified proposal based on the rated criteria as set out in Appendix A.

The terms “requirement”, “shall”, “must” (or similar terms used in this RFP) are used for convenience only and are not intended to imply that any proposal that does not exactly match or meet such a “requirement” will necessarily be disqualified. Instead, as part of the evaluation process, Proponents, goods, and services will be evaluated based on the extent to which, and how well, they are able to satisfy the intent, fit for purpose and substance of the “requirements” or “specifications” contained in this RFP.

### 2.2.1 Pricing

Scoring of the submitted pricing will be in accordance with the price evaluation set out in Appendix A.

GOS reserves the sole right to reject any financial proposal that GOS deems to be materially deficient, through omission or unreasonable estimates of time or cost that are necessary to provide the Solution outlined in Appendix A including required maintenance and support.

**Pricing will be kept separate from the written proposal evaluation, accessible only after written proposals are evaluated.**

## 2.3 Stage III – Interviews/Presentations

Top-ranked Proponent(s) may be required to attend an interview or make a presentation to the Evaluation Team. The interview can include a presentation. Materials prepared by the top-ranked Proponent(s) for the interview/presentation shall be provided to the Evaluation Team prior to the interview/presentation.

The interview/presentation is intended to verify that the proposed approach meets all the requirements and provides the Evaluation Team exposure to the designated service team.

The interview/presentation may also be used to clarify any portion of the written proposal, if required. The Proponent may not alter the content of a proposal during the interview/presentation or provide any additional material.

The Evaluation Team will ask questions about the contents of the proposal or presentation for clarification purposes. Clarifications made by the Proponent during the interview/presentation will become part of the Proponent's proposal and may be included in contract negotiations.

## 2.4 Stage IV – Proof of Concept

### 2.4.1 Proof of Concept Selection and Objectives

The top three ranked Proponents will be invited to participate in a technical proof of concept stage that will be conducted over three rounds. Each round will last three to four weeks, and the first round will be preceded by four weeks of preparation time. The proof-of-concept stage will last approximately four months.

1. Round #1 – Evaluate the capabilities of the proposed solution to capture a selfie and check for liveness, and to assess the user experience. The Proponent will be involved in a proof of concept that:
    a. Tests selfie capture capabilities using SGI's facial verification database and software, Cognitec. [1]
    b. Confirms the ability of the liveness checker to detect and reject presentation attacks from photos and masks.
    c. Assesses the user experience for the selfie capture and the check for liveness.

2. Round #2 – Evaluate the capabilities of the proposed solution to issue a set of predefined credentials that conform to the W3C Verifiable Credentials data model. (https://www.w3.org/TR/vc-data-model/)

3. Round #3 – Evaluate the capabilities of the proposed solution to issue a set of predefined credentials to three named third party wallets.

GOS recognizes the use of emergent technology for Rounds 2 and 3 and does not seek proof of an off-the-shelf product that is production ready. Rather, GOS seeks to understand the Proponent's current level of conformity and capabilities with regards to:

1. verifiable credential issuance and interoperability
2. awareness of the conformity gaps in the proposed solution
3. evidence of a roadmap that addresses identified gaps and demonstrates the proponent has a plan to stay current with evolving verifiable credentials and interoperability standards

The proof-of-concept stage is intended to:

1. verify that the proposed approach assessed in Stage II (2.2, Written Evaluation) and the presentations assessed in Stage III (2.3, Interviews/Presentations) functions effectively in the GOS ecosystem
2. confirm the Proponent's verifiable credential capabilities
3. confirm the Proponent's interoperability capabilities
4. provide both the Proponent and GOS teams with exposure for working together

**2.4.2 Proof of concept preparations and assessment overview**

Detailed technology and operational information will be available to Proponents as appropriate 60 days prior to the start of Round 1.

The proof-of-concept stage may also be used to demonstrate and/or clarify any portion of the written proposal or presentation, if required.

The Proponent may not alter the content of a proposal during the proof-of-concept stage, with the exception of changes (e.g., code changes or technical documentation required to complete a particular round) that improve the technical result of the proof of concept. Changes must be documented and submitted for review and approval prior to being incorporated. They must also align with the proposed solution submitted in Stage II.

The evaluation team will assess the effectiveness of the Proponents to complete the three rounds of the proof of concept. Clarifications and outcomes obtained during the proof-of-concept stage will become part of the Proponent's proposal and may be included in contract negotiations.

GOS reserves the right to:

1. adjust the proof-of-concept stage, including the structure or requirements of specific rounds, up to 60 days in advance of Round #1 of the proof-of-concept stage

2. increase or decrease the shortlist based on results of the previous rounds and the results of the previous stages; and/or

3. stop the proof-of-concept stage for any or all Proponents due to poor performance in a preceding round or if GOS feels it has attained necessary value.

    a. Proponents that receive less than 65% of the points in any round of the proof-of-concept stage or of the total points available may not proceed to the next stage of the evaluation process. The Evaluation Team will determine how many proponents, if any, will be further short-listed.

    b. Any proponents ranked at the lower end of the scale in any of the criteria may be rejected.

A $20,000 honorarium plus an in-kind contribution of the W3C conformance test (valued at $5000) will be provided to the three shortlisted Proponents. A copy of the conformance test results will be provided to Proponents for their own benefit.

For Rounds #2 and #3, interested Proponents will have the opportunity to pre-test and execute corresponding self-conformity tools. This includes issuing a series of dedicated and personalized credentials into three target wallets. This opportunity is available at the time of posting this RFP. It requires a sandbox subscription with the Digital Identity Laboratory of Canada (IDLab)

(https://idlab.org/) at a cost of $1000/month, with more robust subscriptions available. This cost is to be covered by the Proponent. See Appendix N for details.

**2.4.3 Round #1 - Demonstrate selfie capture, liveness, and user experience capabilities**

1. Objective
    a. A user, without intervention, can successfully take a selfie and complete a liveness check using a Proponent's software solution.
    b. 95% of the selfies taken are successfully matched with SGI's facial verification database:
        i. on average across a total 50-100 users
        ii. within pre-determined user segments; and
        iii. with a threshold of 0.9 on a scale of 0-1.
    c. The solution successfully detects and rejects presentation attacks including a photograph and a mask.

2. Resourcing
    a. The Proponent will be paired with SGI resources and user experience resources to execute the tests.
    b. 50-100 users will be recruited by GOS.

3. Approach
    a. Recruited users will take a selfie and complete a liveness check using a Proponent's solution. These selfies and liveness checks will be done consecutively by the user using each Proponent's solution to ensure effective comparison across Proponents.
    b. Negative matches (e.g., purposefully presenting the wrong user) and presentation attacks will be part of this test.
    c. The Proponents will then submit the resulting selfies to SGI for SGI to conduct facial verification using their Cognitec software.
        i. **NOTE**: for the production solution, this will be done via API. The manual intervention is for the proof-of-concept stage only.

4. Assessment
    a. Match score per user and overall average match score
        i. Segmented average match scores (e.g., based on visible minority users, indigenous users, age, etc.) should equal the overall average match score.
    b. Overall match rate, given the threshold of 0.9
    c. User experience of the capture tool as reported by the users during user experience testing
    d. Average speed for users to complete the selfie/liveness check; and
    e. Ability to detect and reject presentation attacks and incorrect matches.
    f. A report on this assessment will be issued to each Proponent.

5. Assessment Response
    a. Proponents will have the opportunity to respond to the assessment report to discuss gaps or concerns identified by the report.
    b. GOS recognizes this is a test environment and that elements like the match threshold may need revisiting ahead of production.

c. We are seeking to understand the Proponent's current level of conformity and capabilities within the test conditions and the Proponent's roadmap for addressing identified gaps.

**2.4.4 Round #2 - Ability to issue a verifiable credential in conformity with the W3C Verifiable Credentials data model**

1. Objective – Demonstrate technical conformity of the issued credentials to the W3C Verifiable Credentials data model. (https://www.w3.org/TR/vc-data-model/)

2. Resourcing
    a. Proponents will be asked to certify their proposed product/capabilities via the IDLab (https://www.idlab.org/).
    b. Detailed technology and operational information will be available to the Proponents as appropriate 60 days prior to the start of Round 1.

3. Approach
    a. The W3C | Verifiable Credential Conformance Test (https://w3c.github.io/vc-test-suite/implementations/) shall be carried out within the IDLab technology environment. It will be performed within a dedicated private sandbox set up for each Proponent's designated solution.
    b. The dedicated private sandbox will be at the Proponent's disposal, free of charge, for the duration of the proof-of-concept stage to a maximum of 10 weeks.
    c. The Proponent is responsible for:
        i. installing the solution into the sandbox
        ii. demonstrating to the IDLab that the installation is complete; and
        iii. providing written instructions to the IDLab to support the IDLab's assessment
    d. If applicable, a Proponent will need to identify and explain which components of the complete solution design can't be installed and operated from within the dedicated sandbox. In this explanation, reference the high-level architecture provided as a response to Appendix A - D.5.1 IT Requirements.

4. Testing methodology
    a. The W3C | Verifiable Credential Conformance Test will check that a Proponent's proposed solution generates Verifiable Credential Data Model documents to ensure conformance with the specification.
    b. The test will use the latest revision of the W3C testing framework for the Verifiable Credentials Data Model. The exact version of the W3C testing framework used for this test will be communicated to the appropriate Proponents 60 days prior to the start of the round.
    c. The test will be conducted by IDLab, on a Proponent's solution hosted at the IDLab, using a Proponent's written instructions.
    d. Deviation from the written instructions (e.g., to account for incomplete, incorrect or missing information) will not be allowed during IDLab's formal assessment of the solution.

5. Assessment
    a. Proponents will receive an assessment report that details the degree to which the solution conforms to the W3C Verifiable Credentials standard. The assessment will also

identify possible gaps that the Proponent must address before engaging into a formal W3C | Verifiable Credential certification process.

i. An example of a report is available: https://w3c.github.io/vc-test-suite/implementations/#conformance-testing-results

b. At GOS' discretion, and at any time after the solution is confirmed to be properly installed, Proponents may be asked to provide a walkthrough of the solution installed in the IDLab sandbox to enable GOS to compare the implemented solution to the previously submitted high-level architecture (Appendix A – D.5.1 IT Requirements) and seek further clarifications.

6. Assessment response
   a. Proponents will have the opportunity to respond to the assessment report to discuss gaps or concerns identified by the report.

### 2.4.5 Round #3 - Ability to issue a predefined credential to three named third-party wallets

1. Objective – The Proponent successfully issues a set of predefined credentials to three GOS designated third-party wallets (e.g., the Proponent will not pre-seed, or manually create wallet private key material outside the wallet). The primary goal of this test is to ensure interoperability of the proposed solution with arms-length wallet technologies.

2. Resourcing
   a. The Proponent will demonstrate this capability in a controlled environment hosted and operated at the IDLab (https://www.idlab.org/) using predefined credentials to be issued to the target wallets.
   b. IDLab will design and document the template and test data for each test credential.
   c. The issued credentials in the target wallets will be verified using IDLab test tools.
   d. IDLab will design, document and support "self-conformity" assessment steps and tools to be used by potential participants, at their discretion, in preparation for the round.
   e. IDLab will provide a "wallet-sandbox" for the duration of the round.
   f. Multiple conforming wallets will be made available. Three default designated wallets will be identified. Should one of these be from a short-listed Proponent, an alternate will be designated.
   g. Test data and related technology or operational information will be available to the appropriate Proponents 60 days prior to the start of Round 1.

3. Approach
   a. IDLab will design, operate, and report on Round #3
   b. The Proponent must leverage the sandbox and solution used in Round #2. If additional components are required for this round, they can be installed as part of Round #3.
      i. No changes can be made to the components already installed with the exception of technical changes (e.g., code and configuration changes) that improve the technical result of the proof-of-concept.
      ii. Any changes must align with the submitted solution design (Appendix A - D.5.1) and be documented and submitted for review and approval before being incorporated into the Proponent response. A Proponent may not alter the

content of a proposal during the proof-of-concept stage, with the exception of the above-mentioned changes.

iii. If adding components, Proponents will need to indicate what components from their high-level architecture (Appendix A – D.5.1) have been added to the sandbox or any other location.

c. Proponents will be required to provide detailed instructions to the IDLab on how to create a fresh new series of dedicated and personalized credentials, and how to issue the credentials into the three specified digital wallets.
d. The IDLab will follow the instructions provided by the Proponent and attempt to successfully deposit the Proponent's issued credentials into the three target digital wallets.
e. The interface method will be at the discretion of the Proponent. However, GOS envisions a preference for leveraging Aries Interop Profile (AIP) in the future. Therefore, leveraging published AIP methods with at least one of the designated wallets will be viewed favourably.

4. Assessment
   a. The IDLab will report on its ability to successfully deposit the credentials into the digital wallets.
   b. Final test results will be shared with GOS. Proponents will also obtain their own copy of the test results.
   c. At GOS' discretion, and at any time after the solution is confirmed to be properly installed, Proponents may be asked to provide a walkthrough of the solution to enable GOS to compare the implemented solution to the previously submitted high-level architecture (Appendix A – D.5.1 IT Requirements) and seek further clarifications.

5. Assessment response
   a. Proponents will have the opportunity to respond to GOS about the assessment report to discuss gaps or concerns identified by the report.

6. Additional Information
   a. Each Proponent will have to conclude an Evaluation Agreement with the IDLab before they can participate in Round #3 (See Appendix N). This Evaluation Agreement will include the Laboratory Terms and Conditions. The Terms and Conditions applicable are those applicable to Private Sandboxes with the exception that Proponents will not be able to deploy other solutions in their private sandbox from the IDLab catalogue of solutions.

**2.4.6 Proof of Concept Schedule**

| Item | Start Date | End Date |
|---|---|---|
| Preparation and briefing | February 28, 2022 | March 25, 2022 |
| Round 1 | March 28, 2022 | April 22, 2022 |
| Round 2 | April 25, 2022 | May 20, 2022 |
| Round 3 | May 24, 2022 | June 17, 2022 |
| Finalization | June 20, 2022 | June 24, 2022 |

The proof-of-concept schedule is tentative, and may be changed by GOS at any time.

## 2.5 Stage V – Reference Checks

Reference checks may be completed for the Proponent and/or their proposed resources and sub-contractors.

During reference checks, GOS reserves the right to contact any of the Proponent's customers who GOS believes may be able to provide information about the Proponent that would be pertinent to this RFP.

GOS reserves the right to conduct reference checks at any time during the RFP process.

Proponents who receive unfavourable references, in the opinion of the GOS, may have their proposal rejected.

## 2.6 Stage VI – Best and Final Offer (BAFO)

### 2.6.1 Initial Ranking of Proponents

After the completion of Stage III, scores from previous stages will be added together and Proponents will be ranked based on their total scores.

### 2.6.2 BAFO Process

GOS intends to invite the top-ranked Proponent(s) to participate in BAFO. During BAFO, GOS may provide each Proponent with additional information and seek further information and Submission improvements from each Proponent. After the expiration of the negotiation period, each Proponent may be invited to revise the initial Submission and submit a BAFO to GOS.

This process is typically used to address the following: confirming assumptions under which a Submission was developed; conducting whatever due diligence is deemed reasonable and necessary under the circumstances; proposing revisions to a Submission based on the results of any activities discussed previously; and provide more specific details in areas to be identified by GOS.

### 2.6.3 Evaluation of BAFO and Final Ranking of Proponents

Each BAFO will be re-evaluated and may be re-scored according to the evaluation criteria that will be provided in the BAFO process. A final ranking and decision may be made based on the new or additional information secured during this process. The top-ranked Proponent based on the evaluation of each BAFO will receive a written invitation to participate in a final round of negotiation to finalize the Agreement with GOS.

## 2.7 Stage VII – Contract Negotiations

### 2.7.1 Contract Negotiation Process

Any negotiations will be subject to the process rules contained in the Terms and Conditions of the RFP Process (Part 3) and will not constitute a legally binding offer to enter into an Agreement on the part of GOS or the Proponent and there will be no legally binding relationship created with any Proponent prior to the execution of a written Agreement. The terms and conditions in the Form of Agreement in Appendix C are intended to be included in the final negotiated Agreement with the selected Proponent. Negotiations may include requests by GOS for supplementary information from the Proponent to verify,

clarify or supplement the information provided in its proposal or to confirm the conclusions reached in the evaluation, and may include requests by GOS for improved pricing or performance terms from the Proponent.

### 2.7.2 Time Period for Negotiations

GOS intends to conclude negotiations and finalize an Agreement with the top-ranked Proponent. A Proponent invited to participate in direct negotiations should be prepared to provide requested information in a timely fashion and to conduct negotiations expeditiously.

### 2.7.3 Failure to Enter into Agreement

GOS may **at any time** at its sole discretion, discontinue negotiations with the top-ranked Proponent and may invite the next-best-ranked Proponent to participate in negotiations. This process will continue until an Agreement is finalized, until there are no more Proponents remaining that are eligible for negotiations, or until GOS elects to cancel the RFP process.

### 2.7.4 Notification to Other Proponents

Other Proponents that may become eligible for contract negotiations will be notified at the commencement of the negotiation process with the top-ranked Proponent. Once an agreement is finalized and executed by the Purchasing Entity and a Proponent, the other Proponents will be notified in accordance with the Terms and Conditions of the RFP Process (Part 3).

[End of Part 2]

# PART 3 - TERMS AND CONDITIONS OF THE RFP PROCESS

## 3.1 General Information and Instructions

### 3.1.1 Proponents to Follow Instructions

Proponents should structure their proposals in accordance with the instructions in this RFP. Where information is requested in this RFP, any response made in a proposal should reference the applicable section numbers of this RFP.

### 3.1.2 Proposals in English

All proposals are to be in English only.

### 3.1.3 No Incorporation by Reference

The entire content of the Proponent's proposal should be submitted in a fixed form, and the content of websites or other external documents referred to in the Proponent's proposal but not attached may not be considered to form part of its proposal. If Proponents wish to reference websites or external documents, they should obtain the approval of the RFP Contact prior to the Submission Date. Proponents are responsible for ensuring that all external content that is referenced is accurate, and are to provide notice to GOS of any changes that may arise after Submission. GOS may, at any time, require a Proponent to provide a hard copy of some or all of the external content referenced.

### 3.1.4 References and Past Performance

In the evaluation process, GOS may consider information provided by the Proponent's references and may also consider information independently obtained by GOS about the Proponent or its proposal in the course of GOS's own due diligence, including any previous dealings or experience, if any, with a Proponent. GOS may contact any of the Proponent's customers who GOS believes may be able to provide information about the Proponent that would be pertinent to this RFP.

Proponents who have unfavourable past performance, in the opinion of the GOS, may have their proposal rejected.

The contractual performance of GOS's vendors is a matter of paramount importance to ministry and Crown organizations. Each organization may monitor and assess a vendor's contractual performance and reserves the right to take past contractual performance into account when evaluating future bids from the vendor.

### 3.1.5 Information in RFP Only an Estimate

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

### 3.1.6 Proponents to Bear Their Own Costs

The Proponent will bear all costs associated with or incurred in the preparation and presentation of its proposal, including, if applicable, costs incurred for interviews or demonstrations. Vendors who are shortlisted for the proof-of-concept stage will receive an honorarium of $20,000.

### 3.1.7 Proposal to be Retained by GOS

GOS will not return the proposal, or any accompanying documentation submitted by a Proponent. This includes reports generated by assessors during the proof-of-concept stage. The exception to this is the solution notes and solution implementation during the proof-of-concept rounds. The solution implementation remains the property of the Proponent and will not be kept by GOS.

### 3.1.8 Trade Agreements

Proponents should note that procurements falling within the scope of Chapter 5 of the Canadian Free Trade Agreement (CFTA) and/or the New West Partnership Trade Agreement (NWPTA) and/or the Agreement on Government Procurement are subject to those trade agreements, but that the rights and obligations of the parties will be governed by the specific terms of this RFP.

### 3.1.9 No Guarantee of Volume of Work or Exclusivity of Agreement

GOS makes no guarantee of the value or volume of work to be assigned to the successful Proponent. The Agreement to be negotiated with the selected Proponent will not be an exclusive contract for the provision of the described Deliverables. GOS may contract with others for goods and services the same as or similar to the Deliverables or may obtain such goods and services internally.

## 3.2 Communication after Issuance of RFP

### 3.2.1 Proponents to Review RFP

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

### 3.2.2 All New Information to Proponents by Way of Addenda

This RFP may be amended only by addendum in accordance with this section. If GOS, for any reason, determines that it is necessary to provide additional information relating to this RFP, such information will be communicated to all Proponents by addendum. Any information obtained in a method other than an addendum should not be relied upon. Each addendum forms an integral part of this RFP and may contain important information, including significant changes to this RFP. Proponents are responsible for obtaining all addenda issued by GOS.

### 3.2.3 Post-Deadline Addenda and Extension of Submission Deadline

If GOS determines that it is necessary to issue an addendum after the Deadline for Issuing Addenda, GOS may extend the Submission Deadline for a reasonable period of time.

### 3.2.4 Verify, Clarify and Supplement

When evaluating proposals, GOS may at its sole discretion request further information from the Proponent or third parties in order to verify, clarify or supplement the information provided in a proposal. The response received by GOS shall, if accepted by GOS, form an integral part of the Proponent's proposal.

GOS may consider information independently obtained by GOS about the Proponent or its Submission in the course of GOS's own due diligence, including any previous dealings or experience by it or others, if any, with a Proponent.

### 3.2.5 Time Disputes

In the event of a dispute regarding time, GOS's time clock will govern.

## 3.3 Notification and Debriefing

### 3.3.1 Notification to Other Proponents

Once an Agreement is signed by GOS and a Proponent, the other Proponents will be notified. Proponents may be notified by public posting in the same manner that this RFP was originally posted of the outcome of the procurement process.

### 3.3.2 Debriefing

Proponents who submitted a proposal may request a debriefing after receipt of a notification of the outcome of the procurement process. All requests must be in writing to the RFP Contact within thirty (30) days of such notification. The intent of the debriefing information session is to aid the Proponent in presenting a better proposal in subsequent procurement opportunities. Any debriefing provided is not for the purpose of providing an opportunity to challenge the procurement process or its outcome.

## 3.4 Conflict of Interest and Prohibited Conduct

### 3.4.1 Conflict of Interest

GOS may disqualify a Proponent or take any other action it deems appropriate in its sole discretion, for any conduct, situation or circumstances, determined by GOS, in its sole and absolute discretion, to constitute a Conflict of Interest.

For the purposes of this RFP, "Conflict of Interest" includes any situation or circumstance where, in relation to a GOS procurement competition, a participating Proponent has an unfair advantage, a perception of an unfair advantage or engages in conduct, directly or indirectly, that may give it an unfair advantage, including:

(a) having, or having access to, information in the preparation of its proposal that is not available to other Proponents, but such does not include information a Proponent may have obtained in the past performance of a contract with a public entity, including GOS, that is not related to the creation, implementation or evaluation of this or a related procurement competition;

(b) communicating with any person with a view to influencing preferred treatment in this procurement competition (including but not limited to the lobbying of decision makers involved in this procurement competition); or

(c) engaging in conduct that compromises, or could be seen to compromise, the integrity of the open and competitive procurement competition or renders that competition non-competitive, less competitive, or unfair.

All Proponents should advise GOS in writing whether it has any actual, potential or perceived Conflict of Interest, and if so, the nature of each Conflict of Interest. A Proponent may, in the sole discretion of GOS, be disqualified from this RFP process if a Proponent is found to have a Conflict of Interest.

### 3.4.2 Disqualification for Prohibited Conduct

GOS may disqualify a Proponent, rescind an invitation to negotiate or terminate a contract subsequently entered into, or take such other action it may deem appropriate if GOS, in its sole and absolute discretion, determines that the Proponent has engaged in any conduct prohibited by this RFP.

### 3.4.3 Prohibited Proponent Communications

Proponents should not engage in any communications that could constitute a Conflict of Interest.

### 3.4.4 Proponent Not to Communicate with Media

Proponents should not at any time directly or indirectly communicate with the media in relation to this RFP or any Agreement entered into pursuant to this RFP without first obtaining the written permission of the RFP Contact.

### 3.4.5 No Lobbying

Proponents should not, in relation to this RFP or the evaluation and selection process, engage directly or indirectly in any form of political or other lobbying whatsoever to influence the selection of the successful Proponent(s).

### 3.4.6 Employee Submissions

GOS employees (as a Proponent or a proposed resource) may be ineligible to enter into an Agreement.

### 3.4.7 Illegal or Unethical Conduct

Proponents are not to engage in any illegal business practices, including activities such as bid-rigging, price-fixing, bribery, fraud, coercion, or collusion. Proponents are not to engage in any unethical conduct, including lobbying, as described above, or other inappropriate communications; offering gifts to any employees, officers, agents, elected or appointed officials or other representatives of GOS; deceitfulness; submitting proposals containing misrepresentations or other misleading or inaccurate information; or any other conduct that compromises or may be seen to compromise the competitive process provided for in this RFP.

### 3.4.8 Past Performance or Past Conduct

GOS may prohibit a Proponent from participating in this or future procurement processes 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 Proponent to honour its submitted pricing or other commitments

(c) any conduct, situation or circumstance determined by GOS, in its sole and absolute discretion, to have constituted an undisclosed Conflict of Interest

## 3.5 Confidential Information

### 3.5.1 Confidential Information of GOS

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

(a) is the sole property of GOS and must be treated as confidential;

(b) is not to be used for any purpose other than replying to this RFP and the performance of any subsequent Agreement for the Deliverables;

(c) must not be disclosed without prior written authorization from GOS; and

(d) must be returned by the Proponent to GOS immediately upon the request of GOS.

### 3.5.2 Confidential Information of Proponent

Proposals will be accepted in confidence, as they contain financial, commercial, scientific, technical and/or labour relations information, except as may be otherwise provided herein. The confidentiality of such information will be maintained by GOS, except as otherwise required by law or by order of a court or tribunal, or by regulatory order of the Government of Saskatchewan, including but not limited to, the Crown Investment Corporation of Saskatchewan and other agencies or ministries of government including its boards, commissions, or panels. Proponents are particularly advised that GOS is subject to legal requirements that may require disclosure of Submission information including, without limitation, under *The Freedom of Information and Protection of Privacy Act* (Saskatchewan). Notwithstanding the foregoing, GOS reporting requirements may result in the public disclosure of dollars paid to the successful vendor from any Agreement awarded.

Proponents are advised that their proposal will, as necessary, be disclosed, on a confidential basis, to advisers retained by GOS, and/or to Crown corporations (as defined in The Crown Corporations Act, 1993) and GOS agencies or ministries, including its boards, commissions, or panels, to advise or assist with the RFP process, including the evaluation of proposals. If a Proponent has any questions about the collection and use of personal information pursuant to this RFP, questions are to be submitted to the RFP Contact.

## 3.6 Procurement Process Non-binding

### 3.6.1 No Contract A and No Claims

This procurement process is not intended to create and will not create a formal, legally binding bidding process and will instead be governed by the law applicable to direct commercial negotiations. For greater certainty and without limitation:

(a) this RFP will not give rise to any Contract A – based tendering law duties or any other legal obligations arising out of any process contract or collateral contract; and

(b) neither the Proponent nor GOS will have the right to make any claims (in contract, tort, or otherwise) against the other with respect to the award of a contract, failure to award a contract or failure to honour a proposal submitted in response to this RFP.

### 3.6.2 No Contract until Execution of Written Agreement

This RFP process is intended to identify prospective Proponents for the purposes of negotiating potential Agreements. No legal relationship or obligation regarding the procurement of any good or service will be created between a Proponent and GOS by this RFP process. A legal relationship will not arise until the successful negotiation and execution of a written Agreement.

### 3.6.3 Non-Binding Price Estimates

While the pricing information provided in proposals will be non-binding prior to the execution of a written Agreement, such information will be assessed during the evaluation of the proposals and the ranking of the Proponents. Any inaccurate, misleading or incomplete information, including withdrawn or altered pricing, could adversely impact any such evaluation or ranking or the decision of GOS to enter into an Agreement for the Deliverables.

### 3.6.4 Effect of this RFP

This RFP process does not in any way restrict or limit GOS's pre-existing rights to engage in commercial negotiations with any vendor or to procure the Deliverables from any vendor through any other process. Without limiting the generality of the foregoing, GOS may:

(a) choose whether to evaluate any proposal;
(b) modify this RFP or RFP process, including any technical, commercial or contractual terms;
(c) re-issue this RFP, either in the same form, or with modifications;
(d) begin or end negotiations with any Proponent for some or all of the Deliverables;
(e) reject any proposal;
(f) abandon its plans to obtain any of the Deliverables;
(g) invite anyone (including any Proponent) to give it an offer to provide some or all of the Deliverables under any terms;
(h) at any time before awarding the Agreement, GOS may do the following:
- require the Proponent to submit further information not requested in this RFP to verify the Proponent's ability to perform the Agreement, including financial data, references to support assertions of past relevant experience, information about the Deliverables, and proof of the Proponent's legal capacity to perform the Agreement;

- inspect the Proponent's equipment and facilities that will be used to perform the Agreement to verify the Proponents' technical or commercial capacity to perform the Agreement; and

(i) cancel the RFP process without liability at any time.

## 3.7 Governing Law and Interpretation

These Terms and Conditions of the RFP Process (Part 3):

(a) are intended to be interpreted broadly and independently (with no particular provision intended to limit the scope of any other provision);

(b) are non-exhaustive and must 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 the Province of Saskatchewan and the federal laws of Canada applicable therein.

[End of Part 3]

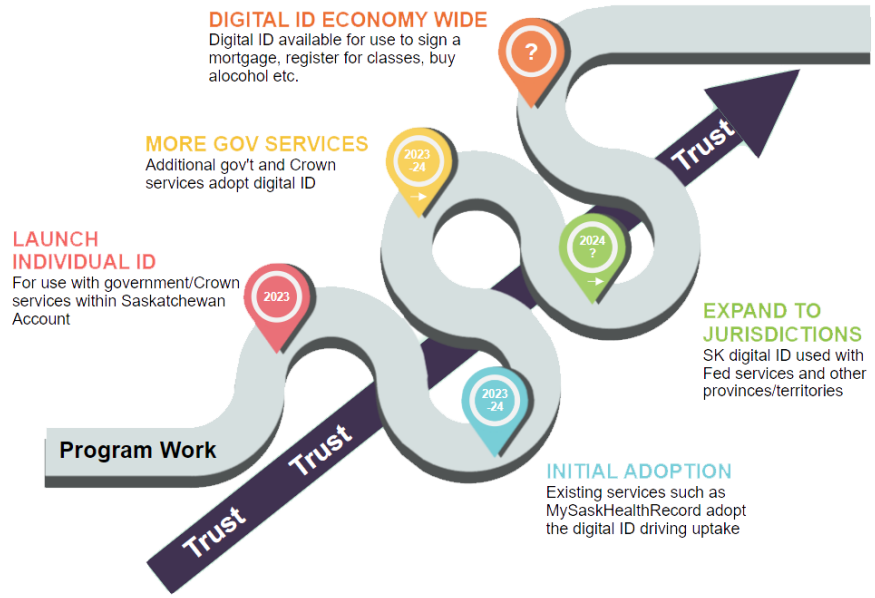
# APPENDIX A - RFP PARTICULARS

## A. OVERVIEW AND BACKGROUND

### A.1 Individual Digital ID Overview

Developing and delivering individual digital identification for Saskatchewan residents is a significant undertaking. As depicted in the following roadmap, individual digital ID will be designed, delivered, and implemented in phases that span several years. The focus starts small by first enabling government services. Over time, GOS will enable digital ID for use across jurisdictions, and into the wider economy, for transactions such as signing a mortgage, writing online exams, accessing rental housing, and age-gated retail purchases like alcohol.

**Individual Digital ID Roadmap**




#### A.1.1 Individual Digital ID Roadmap

The *Individual Digital ID Roadmap* (above) is the focus of this RFP. Responsibility for the roadmap lies with the *Digital Identity Program* which is managed by the *Digital Strategy and Operations Branch* (DSO) within the *Ministry of SaskBuilds and Procurement* (SBP). The *Roadmap* is a forward-looking view of the major milestones for issuing digital IDs to Saskatchewan residents. This *Roadmap* will be broken up into multiple initiatives. The first initiative, *Individual Digital ID Foundations*, will focus on Milestones #1, Launch Individual ID and #2, Initial Adoption.

### A.1.2 Individual Digital ID Foundations Initiative

The *Individual Digital ID Foundations Initiative* is the first initiative that the successful Proponent will deliver. It results in a production ready centralized ID for use by the defined target audience (A.2). It will be used with government services and Crown corporations via Saskatchewan Account (A.4.1).

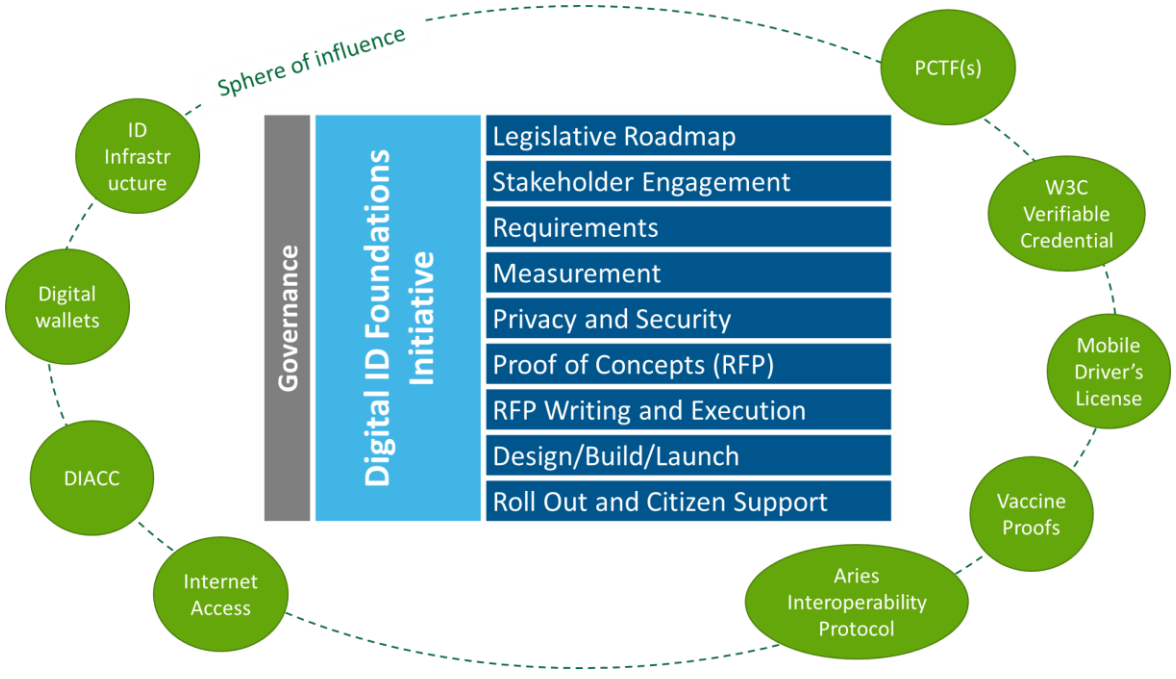
This centralized ID must be built as a foundation for verifiable credentials. In other words, the work to deliver a verifiable credential, following this centralized ID, would be iterative, not net new.

For example: the solution should be able to issue a centralized digital ID to a user via Saskatchewan Account when the centralized ID is first available. When the verifiable credential becomes available, the user should be able to login to Saskatchewan Account and issue that same centralized digital ID to a digital wallet of their choosing as a verifiable credential.

The scope of the *Individual Digital ID Foundations Initiative* is defined in detail in B.1. The target delivery date of the *Individual Digital ID Foundations Initiative* is September 2023.

Scope and schedule for future initiatives will be determined closer to their start dates.

**Individual Digital ID Foundations Initiative Scope**




### A.1.3 Individual Digital ID Foundations Initiative Partners and Collaborators

The *Individual Digital Identity Foundations Initiative* is sponsored by three parties:

1. **GOS** has the mandate to provision and deliver a Saskatchewan ID program.
2. **SGI** provides drivers' licences (and photo ID cards) for Saskatchewan residents and is the owner of the province's widely used biometric database (a facial verification database covering ~93% of

the population). SGI is the primary individual validator and verifier for an individual Saskatchewan ID. For more on facial verification, see A.4.3 SGI facial verification database.

3. **eHealth** is the proverbial anchor tenant of the individual Saskatchewan ID with its MySaskHealthRecord accounting for nearly 400,000 users registered with Saskatchewan Account (A.4.1). eHealth is also accountable for vital statistics in Saskatchewan.

The primary bodies for national collaboration are the Jurisdictional Experts on Digital Identity Committee (JEDI) and the Digital Identity and Authentication Council of Canada (DIACC). The first is a federal/provincial/territorial working group that collaborates on national issues and information sharing to advance the concept and practice of using digital identification. The second is a non-profit group of public and private sector leaders who are developing a Canadian framework for digital identification and authentication.

## A.2 Target audience

### A.2.1 Target audience definition

The target audience is <u>all</u> individuals who:

1. are residents of Saskatchewan
2. desire to access government services and more broadly use a digital ID online (minors included); and
3. are entitled to be in Canada (e.g., possess a birth certificate, permanent residency card or other Canadian Citizenship and Immigration Canada documentation). This entitlement includes temporary residents of Saskatchewan.

Temporary residents are individuals who are legally authorized to enter Canada for temporary purposes and/or temporarily reside in Saskatchewan. Criteria and categories include:

1. Individuals who have a temporary resident visa, are an international student, a temporary worker and/or have a temporary resident permit; and/or
2. file Saskatchewan income tax (if required); and/or
3. don’t hold a driver's licence from another jurisdiction; and/or
4. normally live in any of the following in Saskatchewan:
    - lodging provided by an employer (including motels, hotels, and work camps)
    - dormitories

### A.2.2 Target audience considerations

A default online issuance may not be achievable for 100% of the target audience. For example, there will be individuals in the target audience that cannot or will not use facial verification (see Appendix L and M) and/or do not have a Saskatchewan driver’s licence or an SGI-issued photo ID card. Best estimates suggest that 93% of the Saskatchewan population aged 14 and up have either a Saskatchewan driver’s licence or an SGI-issued photo ID card (see Appendix O).

In addition, stakeholder engagement research conducted by GOS with residents of Saskatchewan (see Appendix L), highlighted the importance of accounting for specific needs in terms of access and usability

across various communities. These communities include but are not limited to rural and remote communities, seniors, indigenous communities, people with disabilities, the 2SLGBTQ+ community, newcomers to Canada in the last five years, people in low-income brackets, people who struggle with and/or are at the crossroads of mental illness, addictions and homelessness, and people who struggle with digital technology (digital literacy), etc. For full findings, see Appendices L and M.

## A.3 High-level Scope and Timelines

The scope of the RFP is focused on the issuance and maintenance of a digital ID in two contexts:

1. The first is the issuance of a digital ID to be used within the context of Saskatchewan Account (A.4.1). This is the primary focus of the *Individual Digital ID Foundations Initiative* (A.1.2). It will provide access to government services, and it will not require a digital wallet. Users will use it solely within the context of Saskatchewan Account.

   For this first initiative, GOS is targeting a start date of September 2022 and a completion date of September 2023. Completion is defined as:
   1. The requirements outlined in B.1 are met;
   2. At least one government service is connected to and using the digital ID; and
   3. A defined roll-out period, to be determined in consultation with the successful proponent, is concluded.

2. The second context is a decentralized ID or verifiable credential. It will be used in conjunction with a digital wallet to access services in other jurisdictions and in the broader economy. The wallet, however, is not in the scope of this RFP. Wallets will be left to user choice. As stated in A.1.2, the decentralized ID should be an iteration on the first context, not net new work. The target date for the delivery of the decentralized ID is not yet known. However, GOS anticipates a pilot of the decentralized ID could be in scope for the September 2023 deadline or shortly thereafter.

In both contexts, the digital ID must meet the deliverables outlined in *B. Deliverables* including strategies and frameworks that support and contextualize the technical solution.

## A.4 Existing Capabilities

The following existing capabilities are available for the Proponent's consideration in the Proponent's response.

### A.4.1 Saskatchewan Account – Enterprise Single sign-on platform (Vendor: Vivvo Application Studios, Product: CitizenOne)

As part of the One Government Strategy, Saskatchewan Account is the enterprise approach for Single Sign On. Saskatchewan Account provides citizens and organizations/businesses a simple and secure way to access Government of Saskatchewan online services with a single account. It offers authentication, profile management and rule-based access to Government of Saskatchewan services. The Saskatchewan Account is managed and supported by the *Digital Strategy and Operations Branch* within the *Ministry of SaskBuilds and Procurement*. It is built using the CitizenOne product from Vivvo Application Studios.

At creation, Saskatchewan Accounts are LOA1 – self attested. Through Saskatchewan Account's existing validation capabilities (A.4.4) an individual's account can be upgraded to a roughly LOA2 status (See A.4.4) because GOS can prove that the person is a legitimate person, but not that the person is the right person or a real person behind the computer. It is envisioned that a digital ID would be issued through Saskatchewan Account, levelling up a users' account from the original LOA1 or LOA2, to an LOA3. In the context of the *Individual Digital ID Foundations Initiative*, which focuses on issuing a centralized ID, Saskatchewan Account likely plays the role of holder for the digital ID. The precise relationship between Saskatchewan Account and the digital ID issuance, maintenance and continuous validation processes will need to be determined in design to ensure a streamlined user experience.

At the end of August 2021, Saskatchewan Account had over 400,000 users, or nearly 40% of Saskatchewan's population. The majority of these users have access to their MySaskHealthRecord and are therefore SGI validated (~LOA2) (A.4.4). Proponents should anticipate that most of these users will adopt a digital ID either proactively or through the five-year driver's license renewal cycle, which could force an upgrade from an LOA2 account to an LOA3 account at the time of renewal.

### A.4.2 Enterprise Integration Services (Software: Azure Integration Services)

The Enterprise Integration Services Platform facilitates the transfer of information between systems (both GOS systems and external parties) via API calls. The API management, authorization, and authentication via this platform protects GOS resources and decouples point-to-point connections, providing secured access to GOS Information Assets.

In the context of digital identity, we are most concerned with the transfer of information from Saskatchewan Account to a connected government service (aka a relying party) and the transfer of information from claim providers to Saskatchewan Account. See Appendix D - Mandatory Requirements for more information.

Information currently transferred includes:

1. Saskatchewan Account to connected service (relying party)
    a. Profile information (name, email address, mailing address, phone numbers)
    b. Confirmation of consent; and
    c. Shared secrets, PINs, or other unique identifiers that link a Saskatchewan Account to the user's record for the connected service.

Saskatchewan Account capabilities include:

2. Synchronous and asynchronous services with publish/subscribe capability which can publish changes made on Saskatchewan Account (e.g., profile information) to subscribed GOS systems (e.g., connected services) while respecting consent status indicated by the citizen or business.
3. Capturing Service Access and Profile Changes: Saskatchewan Account (CitizenOne Platform) generates an activity GUID related to a citizen or business ID upon any changes to a citizen/business profile.
4. Alerting support tiers of integration downstream point issues
5. Providing API abstraction to protect GOS resources and to prevent system compromise.
6. Can identify Citizen / Business GUIDs affected by outage and potential impacts to downstream GOS Systems
7. Breach support from the enterprise integrations services (EIS) platform:
    a. If the relying party (connected government services) product is breached, the enterprise integration services platform can assist in managing traffic flow to integrated systems.

b. If the identity and access management product (CitizenOne – Saskatchewan Account) is breached, the EIS platform can determine the level of impact to citizens/businesses accessing GOS services via Saskatchewan Account, which ministries are affected, and manage traffic flow with integrated systems.
c. If the identity provider product (subject of this RFP) is breached, the EIS platform can determine the level of impact to citizens/businesses and manage traffic flow with integrated systems.

### A.4.3 SGI facial verification database

SGI, which issues driver's licences and identification cards to Saskatchewan residents, has the only biometric database in the province that captures a significant portion of the population (estimated at ~93%). This database uses Cognitec software for facial verification, although the software has potential to change with procurement cycles. Leveraging this database is preferred over an issuance process that scans and verifies against the physical credential only.

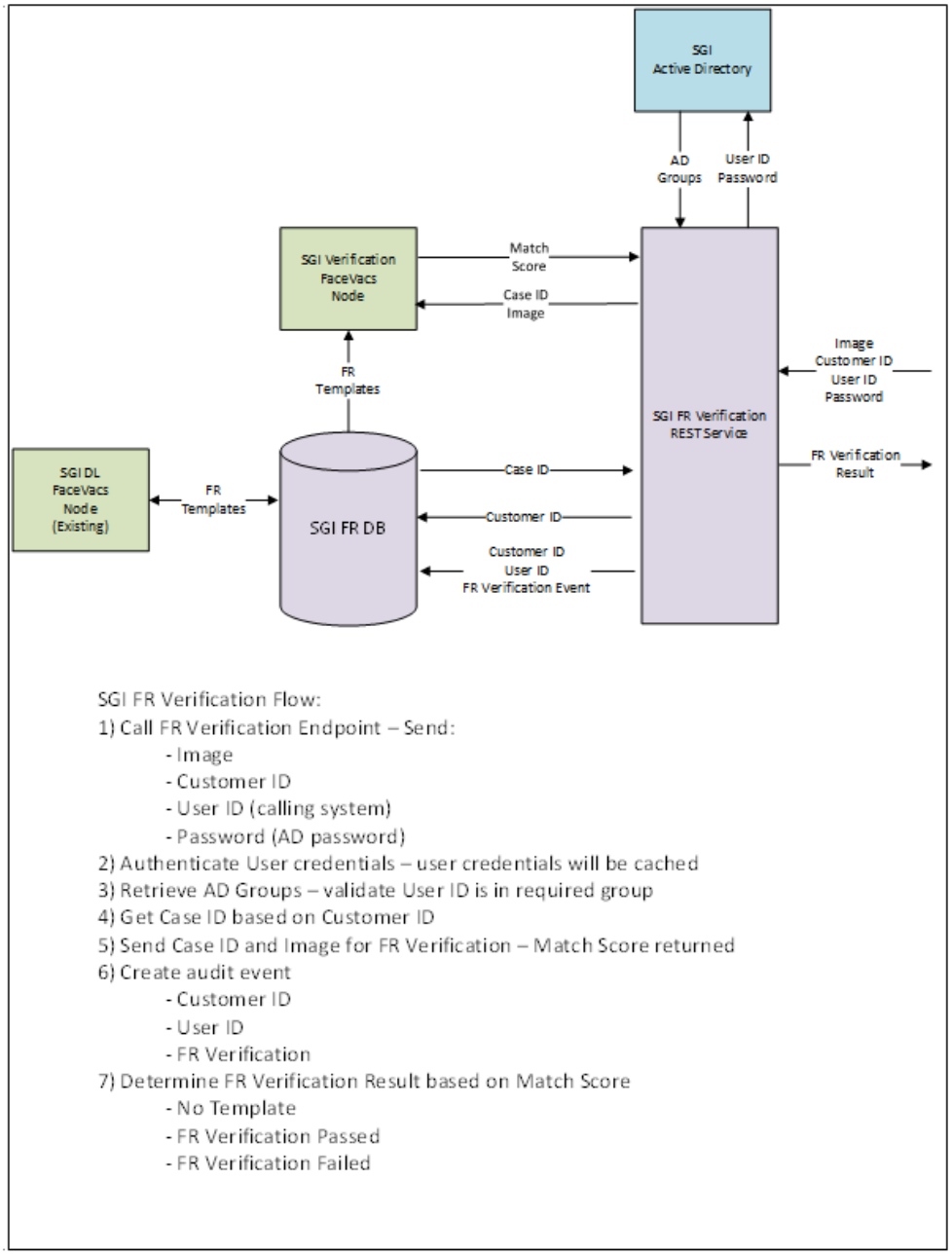
SGI will be responsible for facial verification. However, how this facial verification is achieved, is still under exploration. GOS is currently considering two options:

1. The Proponent passes a photo to SGI and the photo is matched against the SGI database using the Cognitec software.
    a. Option 1 is the minimum requirement that all Proponents must be able to meet (See Appendix C mandatory requirement #14). In the case of option 1, SGI's Cognitec technology cannot ingest facial blueprints/faceprints/templates.

2. The Proponent passes a facial blueprint/faceprint/template to SGI and installs its own facial verification software behind the SGI firewall to run the facial verification against the SGI database. The photo does not leave the user's device.

GOS is also open to additional options, provided these proposals align with Mandatory #11 (SGI will not pass raw photos outside its firewall) and clearly demonstrates how the proposed option best mitigates privacy and security risks.

The figure below provides a high-level diagram of how option one would work, if that option is pursued.




SGI FR Verification Flow:
1) Call FR Verification Endpoint – Send:
- Image
- Customer ID
- User ID (calling system)
- Password (AD password)

2) Authenticate User credentials – user credentials will be cached
3) Retrieve AD Groups – validate User ID is in required group
4) Get Case ID based on Customer ID
5) Send Case ID and Image for FR Verification – Match Score returned
6) Create audit event
- Customer ID
- User ID
- FR Verification

7) Determine FR Verification Result based on Match Score
- No Template
- FR Verification Passed
- FR Verification Failed

### A.4.4 Existing validation capabilities with SGI that enable GOS to ask SGI yes/no questions

GOS has an LOA2-ish verification in place today premised on REST API validations with SGI and managed via Saskatchewan Account. Currently the APIs confirm:

- if the person exists in the database;
- if the person is a resident of Saskatchewan;
- if the person is 18 or over; and
- if the user entered name matches the name on record.

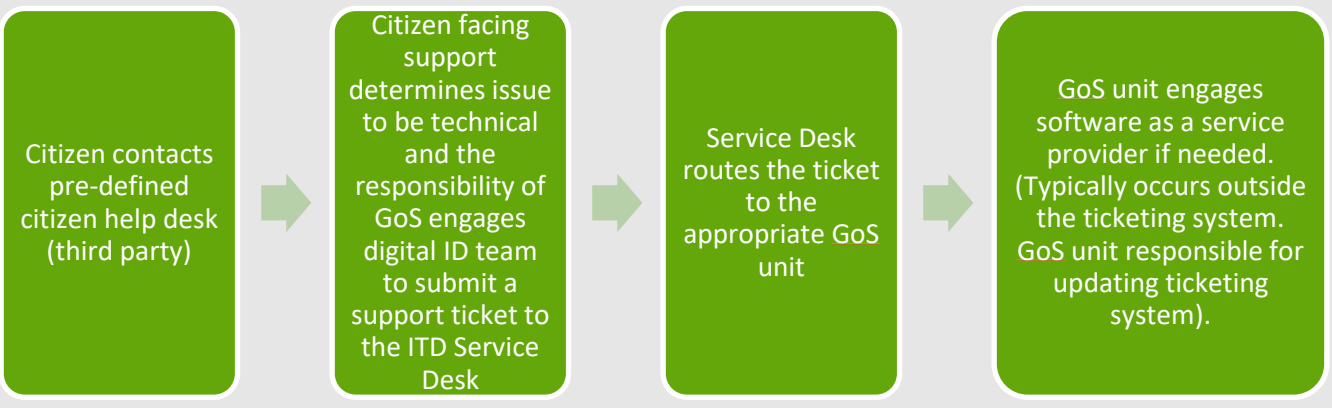
The questions are posed by Saskatchewan Account, routed through the Enterprise Integration Services platform, and passed to SGI's identity hub, which then responds. If a positive response is received from SGI, Saskatchewan Account generates a token confirming that response. This process and the production solution are available to be leveraged.

### A.4.5 ITD Service Desk (Software: Service Now)

The ITD Service Desk is GOS' central point for internal, technical support for GOS operated systems and will need to be considered in the context of technical support for the individual digital ID solution. It also provides some ticketing support for GOS' external vendors. However, this requires a GOS intermediary. External vendors do not have direct access to the ITD Service Desk ticketing system.

Any issue identified by a vendor must be flagged with a GOS primary contact for a ticket to be filed. Conversely, an issue identified by another stakeholder related to an external vendor will be routed to the GOS primary contact. It is the primary contact's responsibility to engage the external vendor. Incident management and problem management are also managed through the ITD Service Desk. The SLA for the ITD Services Desk is attached as Appendix K.

Below is an example diagram of a support call and parties involved. This diagram is generic, not specific to the digital ID use case.




### A.4.6 Relationship with the Digital Identity Laboratory of Canada

The partnership in place with the Digital Identity Laboratory of Canada for 2.5 Stage IV – Proof-of-concept could be extended to support design, build, test and any pilots of decentralized ID etc. Proponents should indicate their intention to leverage the IDLab in their responses, if desired.

### A.4.7 SGI driver's licence and photo ID card issuance process

To support the fully online issuance of a digital ID, GOS assumes a reliance on SGI's in-person process for the Saskatchewan driver's licence or the SGI photo ID card. In this way, an in-person verification process is part of the overall digital ID issuance, but GOS does not need to create a new in-person process specifically for digital ID.

For more on SGI's in-person issuance, see SGI's Identity and Residency Verification information: https://www.sgi.sk.ca/identity-and-residency-verification#your-identity

In circumstances, where another physical credential may be relied upon for digital ID issuance, it would need to meet the same or higher issuance standards as the SGI issuance process.

## A.5 Material Disclosures

This procurement is limited to enabling the Government of Saskatchewan as an ID issuer. The role of holder and verifier are out of scope of this procurement.

### A.5.1 The role of holder and associated products such as digital wallets is out of scope

GOS will not be provisioning a wallet. Rather it is expected that the solution will (eventually) be able to issue a verifiable credential to a wallet.

### A.5.2 The role of verifier and associated products is out of scope

1. In the case of the digital ID issued and used via Saskatchewan Account (A.4.1), Saskatchewan Account is the verifier of the digital ID, prior to a user gaining access to a connected service.
2. In the case of the verifiable credential pilot (part of the *Individual Digital ID Foundations Initiative* A.1.2) the verifier is likely to be another Canadian jurisdiction or a single organization with a compelling presence in Saskatchewan to drive adoption.
3. In the case of verifiable credentials adopted more broadly (future state (A.3(2)) GOS anticipates the private sector will ultimately provide the technology required to verify IDs (e.g., in the same way Moneris et al provision point of sales options in the context of credit cards).

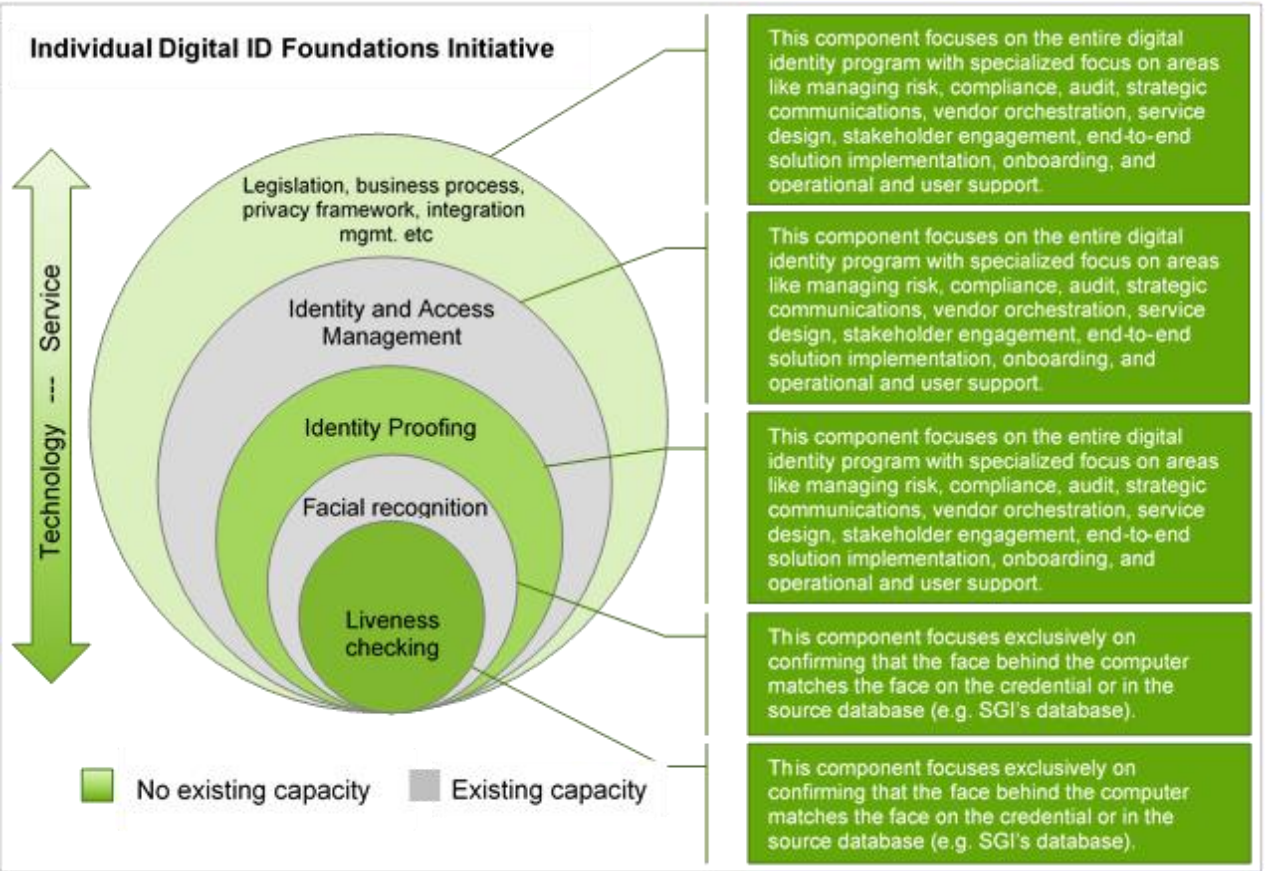
### A.5.3 Identity and Access Management System is out of scope

An identity and access management system is not in scope for the Proponent's proposal. However, GOS' identity and access management system, Saskatchewan Account, will form part of the overall solution. As explained in A.4.1 Saskatchewan Account, it is anticipated that the individual ID delivered through the *Individual Digital ID Foundations Initiative* will be issued and used via Saskatchewan Account.

# B. DELIVERABLES

## B.1 Individual Digital ID Foundations Initiative Implementation Services

The diagram below illustrates the complexity of implementing a digital ID technical solution in the context of the *Individual Digital ID Foundations Initiative*. Under the direction and guidance of the GOS Project Manager – in adherence with GOS project standards and practices, and in partnership with existing GOS vendors – the proponent is expected to deliver the full scope of the *Individual Digital ID Foundations Initiative*.




### B.1.1 Implementation Services for the Individual ID Foundations Initiative

The Proponent is required to deliver an LOA3[3] digital ID that, at a minimum:

1. Is issued entirely online by default (e.g., no mailed out PIN, no in-person visit)
2. Is issued and used first as a centralized ID through Saskatchewan Account (see A.4.1)
3. Is built with the intention that the same ID can be shared as a verifiable credential to a wallet to support:
    a. the decentralized digital ID pilot (requirements 21 – 26) and
    b. the overall *Individual Digital ID Roadmap* (A.1.1).
4. Has optical character recognition (OCR) or equivalent functionality to scan the government-issued ID, to reduce user error and support people with visual impairments.
5. Offers alternate LOA3 processes to support edge cases (see appendices M and N).
6. Proves the person behind the computer is a legitimate person (they legally exist).
7. Proves the person behind the computer is the right person (not an imposter).
8. Proves the person behind the computer is a real person (e.g., not a photo).
9. Confirms that the verification is happening in real time (e.g., not a video).
10. Can be issued and used by users who have EITHER a mobile device with a camera (e.g., phones, tablets etc.), a computer with a camera (e.g., desktop, laptop), OR both.

[3] As defined by the Digital Identity and Authentication Council of Canada (DIACC) Pan-Canadian Trust Framework (https://diacc.ca/trust-framework/pctf-overview/) and the Pan-Canadian Trust Framework-Public Profile (https://canada-ca.github.io/PCTF-CCP/)

11. Is available to and accessible by the target audience defined in A.2.
12. Can securely share personal attributes with a relying party when needed (e.g., on a case-by-case basis to ensure data minimization wherever possible).
13. Is aligned to the program and project goals as defined in PART 1 – 1.1.
14. Is aligned and assessed to be in conformance with the Pan-Canadian Trust Framework (PCTF) - (https://diacc.ca/trust-framework/pctf-overview/) and the PCTF Public Profile (https://canada-ca.github.io/PCTF-CCP/).
15. Is modular by design and maximizes portability of data, applications, and interoperability.
16. Is aligned to a digital identity privacy framework (See B.1.4).

The Proponent is required to develop and execute the following:

17. A detailed overall initiative design document including items like detailed scope, timelines, stakeholder engagement, off-ramps, resourcing structure, responsibilities, and accountabilities across GOS and vendor resources, etc.
18. A service design strategy and implementation plan including user experience testing in collaboration and with oversight from the GOS Service Design team.
19. A testing strategy and implementation plan that:
    a. includes regression, performance, load and UAT testing
    b. ensures no impact to other existing integrated services or components
    c. accounts for full solution end-to-end system integration testing
    d. accounts for GOS, eHealth and SGI testers for user acceptance testing
20. A plan to onboard any existing services that use the existing LOA2 validation (see A.4.4). The exact number of services that need to be onboarded will be refined through the course of the initiative. An onboarding process, and documentation to support onboarding future services, will be a required outcome of this activity.

    **NOTE:** For the purposes of pricing, Proponents can anticipate that 3 - 5 services will require onboarding as part of the *Initiative.*

The Proponent is required to design and execute a pilot for the issuance of decentralized individual digital ID (e.g., a verifiable credential) that:

21. Builds on the centralized ID rather than starting from scratch. In other words, the pilot must not require the issuance of a new digital ID but rather focuses on issuing the existing centralized digital ID delivered in requirements 1-15 as a verifiable credential.
22. Is wallet agnostic.
23. Is interoperable as contemplated in the Pan-Canadian Trust Frameworks (e.g., with third party wallets and other jurisdictions).
24. Is modular by design and maximizes portability of data, applications, and interoperability.
25. Accounts for, and at a minimum, cautions against, bad actors both in the wallet context and the verifier context (e.g., entities requesting to "see" the ID).
26. Conforms to the W3C Verifiable Credential standard, the PCTF (https://diacc.ca/trust-framework/pctf-overview/) and the PCTF-Public Profile (https://canada-ca.github.io/PCTF-CCP/).

**NOTE:** this pilot is likely to be with another Canadian jurisdiction or a single organization that would drive uptake in Saskatchewan. It may ultimately be descoped from the *Individual Digital ID Foundations Initiative* and scheduled for a later date. However, for the purposes of responding to

this RFP, and for pricing, assume that the pilot is part of the *Individual Digital ID Foundations Initiative*.

### B.1.2 Initiative Management

1. **Governance**
   Governance of the *Individual ID Foundations Initiative* is a critical component to *Initiative* success. Members of governance comprise a Steering Committee that provides oversight, guidance and critical decision making. The final authority for critical decisions is the Steering Committee.

   The Proponent will participate in governance by identifying members from the Proponent's organization who can speak with detailed understanding of the Proponent's performance and demonstrate how the Proponent's organization is providing support for Proponent delivery and success. The Proponent will deliver performance reports that align with standards and processes established by the GOS Project Manager for the *Initiative*, and these reports will be used as an input to report integrated *Initiative* performance to the Steering Committee.

2. **Project and Relationship Management**
   The Proponent will assign a Project Manager who is accountable to the GOS Project Manager for complying with GOS project processes and reporting project performance for all aspects of the solution, regardless of whether the Proponent is a consortium or a single organization.

   Working in a government organization requires an appreciation for the complex relationships that arise from working across different departments and at different levels of the hierarchy. Working groups will be multi-disciplinary and multi-interest. Within this context, the Proponent will be required to establish strong relationships among all parties, developing trust by working from a position of honesty and adopting a non-defensive outlook. The Proponent will be required to demonstrate flexibility and fair play, particularly when working collaboratively on deliverables that emerge in definition with time and understanding.

3. **Stakeholder Engagement**
   In collaboration with the GOS Senior Digital ID Business Analyst, the Digital ID Program Director, and the GOS Project Manager, the Proponent is required to develop and support the execution of a stakeholder engagement plan.

   In addition to the three sponsoring organizations (A.1.3 *Individual Digital ID Foundation Initiative* Partners and Collaborators), the *Digital ID Program* will be expected to engage various stakeholders during the design and delivery of the *Initiative* to ensure usability, uptake, and responsible/ethical design. These stakeholders include but are not limited to:
   a. Citizens – users of digital ID with specific focus on those who may find it difficult to access or use a digital ID. See Appendices M and N.
   b. Service providers/Relying parties - GOS ministries and Crown corporations
   c. Architecture and security review committees
   d. The Office of the Information and Privacy Commissioner
   e. The Jurisdictional Experts on Digital Identity (JEDI), the Digital Identification and Authentication Council of Canada (DIACC) and the broader digital ID community

4. **Individual Digital ID Foundations Initiative Resourcing**
   In collaboration with the GOS Project Manager, the Proponent is required to design the resourcing structure that will ultimately manage the *Individual Digital ID Foundations Initiative*.

   For the *Initiative,* GOS will provide the following resources/capabilities:
   a. End-to-end Project Manager
   b. Privacy lead
   c. Solution, integration, and security architects
   d. Standards assessment for:
      i. Privacy
      ii. Security
      iii. Architecture
      iv. Service Design
      v. Project Management

### B.1.3 Multi-tier citizen support model

In collaboration with the Digital ID Program director, the GOS Project Manager and subject matter experts, the Proponent is required to develop a multi-tier citizen support model for use once the *Individual Digital ID Foundations Initiative* is in production. The support model must, at a minimum:

1. ensure citizens can complete the digital ID registration process.
2. account for the target audience including the use cases in Appendices M and N.
3. Account for multi-stakeholder tiers 2 and 3 support (e.g., SGI, GOS, Saskatchewan Account vendor and Proponent resources) while ensuring a streamlined user experience for citizens.
4. Account for the default LOA3 issuance process.
5. Facilitate as required, any alternative LOA3 issuance processes developed to address A.2.2 Target Audience Limitations.
6. Account for manual review of facial verification checks that don't pass the match threshold.
7. Provide for 24/7 monitoring of service availability, including degradation.
8. Provide for extended citizen support hours. For the purposes of pricing, assume 8AM – 8PM, 7 days a week.
9. Leverage the GOS' IT Division (ITD) Service Desk and existing ITD support, incident management and problem management capabilities where relevant (A.4.5).

### B.1.4 Development of Service Management and Policy Framework

In collaboration with the Digital ID Program director, the GOS Project Manager and subject matter experts, the Proponent is required to develop the following plans and frameworks to support the *Individual Digital ID Foundations Initiative* once in production.

1. Develop a resourcing structure to manage the resulting individual digital ID service offering, including recommended functions/roles and responsibilities that can then be used by the Program Director to determine staffing and partnership requirements.

2. Participate as a subject matter expert in the design and implementation of a citizen onboarding plan and mass-market campaign to drive uptake.

**3.** Develop and implement a maintenance and continuous improvement strategy (see B.2.2) that accounts for standard public sector budget cycle planning, continuous improvement, external and internal stakeholder engagement, user-centred design, and user experience testing.

**4.** Support the development of the Digital ID Privacy Framework. This will be established by GOS (and may evolve over time).

a. This privacy framework will require inputs from the successful Proponent, such as vendor business processes to integrate with, or support, GOS privacy-related business processes. This could include (but is not limited to) processes related to:

i. privacy/security incidents
ii. privacy impact assessments
iii. information access requests (such as by an individual for their own information or for more information about privacy-related policies, procedures, and practices)
iv. privacy compliance challenges

b. The digital identity initiative must, at a minimum:

i. be consent-based
ii. reflect privacy principles in the Canada Standards Association Model Code for the Protection of Personal Information
iii. reflect privacy best practices
iv. comply with all applicable legislation (i.e., all applicable legislation, including applicable provincial, federal, and international legislation).

c. The digital ID initiative must uphold the concept of "data minimization" with respect to the collection, use, disclosure, retention, and other handling of personal information.

d. The successful Proponent will be expected to contribute to GOS privacy impact assessments of GOS digital ID technology offerings and associated business processes.

e. The successful Proponent will be expected to complete (or have completed) and maintain privacy impact assessments on any technology and business processes that support GOS digital ID technology offerings and associated business processes.

f. The successful Proponent's privacy impact assessments will feed into GOS privacy impact assessments. The successful Proponent will be expected to maintain, and complete as required, privacy impact assessments at their own cost.

**5.** Develop and implement a records management plan that ensures all digital ID program records (including but not limited to documentation, digital ID account records, API requests etc.) are maintained in accordance with The Archives and Public Records Management Act (APRMA)

**6.** Develop and implement a change management strategy, in line with industry best practice, for the delivery and launch of the *Individual Digital ID Foundations Initiative*.

7. Develop a documented onboarding process for ministry and Crown services (relying parties) that, at a minimum:
    *a.* is grounded in the experience of onboarding existing services as part of the *Individual Digital ID Foundations Initiative* (B.1.1 (20))
    b. is grounded in stakeholder engagement of relying parties to ensure buy-in and uptake (e.g., ministries and Crown corporations)
    c. provides requirements and instructions for relying parties to consume the digital ID via Saskatchewan Account

8. Develop a legislative, regulatory, and policy roadmap that ensures, at a minimum:
    a. the Individual Digital ID service offering is appropriately safe guarded
    b. can rely on appropriate sources of truth
    c. can be accepted by government programs with the same ease a physical ID is accepted today

    The desired outcome is a roadmap that indicates what legislation, regulation or policy needs to change, what the changes are, and an implementation plan to achieve this change.

    Based on the current analysis of existing legislation, and the time required to enact legislative change, there is not an urgent pressure to have this roadmap fully executed ahead of launching the *Individual Digital ID Foundations Initiative*, nor is it realistic to expect it. The legislative roadmap will necessarily be a highly collaborative, multi-stakeholder process with significant oversight and direction from the Program Director and GOS Project Manager. A legislative jurisdictional analysis and strategic direction will be provided to support the development of this roadmap.

9. Develop and implement an auditing process, in line with industry best practice, that enables the Digital ID Program to respond to auditors and assessments (internal or third party) with regards to conformity to the Pan-Canadian Trust Frameworks, W3C Verifiable Credential, and privacy and security audits.

10. Develop and implement a fraud management framework, in line with industry best practice, for the delivery and launch of the *Individual Digital ID Foundations Initiative*.

11. Develop and implement a risk management framework, in line with industry best practice, for the delivery and launch of the *Individual Digital ID Foundations Initiative*.

12. Develop and implement a risk management framework, in line with industry best practice, for the operation of the individual digital ID.

## B.2 Individual Digital ID Roadmap Management and Support

### B.2.1 Support the execution of the *Roadmap* management

The Proponent is required to participate in the *Individual ID Roadmap* management including operations, support, maintenance, enhancements, and continuous improvements.

The following responsibilities include:

1. Ongoing maintenance and continuous improvement
2. Transitioning the decentralized ID pilot to a full-scale production solution
3. Reoccurring user experience testing and stakeholder engagement to inform the roadmap
4. Onboarding services
5. Supporting the onboarding of citizens, especially in high-volume scenarios
6. Participating in governance
7. Supporting privacy and security management, investigations, compliance, and audit efforts
8. Maintaining records in accordance with the Archives and Public Records Management Act (APRMA)
9. Delivering change management
10. Supporting the execution of the legislative roadmap
11. Continued relationship management

### B.2.2 Research and Development

As part of the support for the *Individual Digital ID Foundations Initiative* and GOS' overall *Individual Digital ID Roadmap*, the Proponent is expected to provide reporting and presentation on research and development findings. This regular reporting will create opportunity for innovation, throughout the length of the contract, and enable proof-of-concepts, pilots, new features, etc. It will also ensure the *Digital ID Program* remains responsive to changing standards and technology, emerging policy, user needs and trends, etc.

At a minimum, research and development findings shall be reported on an annual basis, timed to support the budget submission cycle. Budget submissions are due at the beginning of September each year.

Report/presentation requirements:

1. The report/presentation must include, at a minimum:
    a. the Proponent's technology roadmap (short, medium, and long term)
    b. emerging trends in technology and standards
    c. anticipated technology and standards changes
    d. high-level costs, risks, benefits, and impacts

    This is necessary to make informed decisions and benefit from the development of newer technologies.
2. Upon Ministry request, the Proponent shall provide detailed benefit, risk, and impact analysis including a detailed estimate, complexity, and a roadmap of how the advancement would be introduced and integrated without disruptions to the digital ID service or its integrations.
3. Continuous improvements and enhancements will be determined, subject to Ministry approvals, following this reporting exercise, and ahead of budget submissions.

### B.2.3 Multi-tier citizen support

Deliver the multi-tier citizen support model developed in B.1.3, in line with industry best practice and in partnership with the ITD Service Desk (A.4.5).

## C. MANDATORY REQUIREMENTS

The mandatory requirements are listed in Appendix D – Mandatory Requirements and Submission Form.

## D. RATED CRITERIA

The following is an overview of the categories and weighting for the rated criteria of the RFP.

| **Rated Criteria Category** | **Weighting (Points)** | **Percentage %** |
|---|---|---|
| D.1 Proponent Profile | 10 | 1 |
| D.2 Proponent Experience and Qualifications | 110 | 11 |
| D.3 Proposed Approach | 150 | 15 |
| D.4 Information Technology Requirements | 80 | 8 |
| D.5 Information Security Requirements | 80 | 8 |
| D.6 Initiative Implementation and Transition | 30 | 3 |
| D.7 Risk Management Plan | 30 | 3 |
| D.8 Proposed Team and Resources | 30 | 3 |
| D.9 Value Add-ons and Innovation | 30 | 3 |
| D.10 Local Knowledge | 100 | 10 |
| D.11 Community Benefits | 100 | 10 |
| D.12 Pricing | 250 | 25 |
| **Total Points** | 1000 | 100 |

Proposals that receive less than 65% of the points in any of the above categories or of the total points available may not proceed to the next stage of the evaluation process. The Evaluation Team will determine how many Proposals, if any, will be short-listed.

Any Proposal ranked at the lower end of the scale in any of the criteria may be rejected.

### D.1 Proponent Profile

Each Proponent should provide a brief introduction and overview of the company(ies) and partnerships as they are related to this RFP. In addition, GOS is seeking the following information:

**D.1.1** Capability and qualifications to provide the Deliverables. Refer to A. Overview and Background and B. The Deliverables.

**D.1.2** Location of head office and any sub-offices.

**D.1.3** Details of any and all subcontracting, partnership or consortium arrangements proposed by the Proponent specifically relating to the provision of Services as described herein including but not limited

to software licencing relationships that may support the final solution. Outline the nature of the proposed involvement and the nature of the relationship.

**NOTE:** The information asked for above must be provided for all consortium partners, partners of the Proponent, and sub-contractors included in the submission.

## D.2 Proponent Experience and Qualifications

Each Proponent should provide the following in the Submission:

**D.2.1** Describe, in detail, similar successful engagements of similar size, scope and complexity as described in this RFP. For each project, provide, at a minimum**:**

1. An overview of the engagement including client details such as name, contact information, and client industry.
2. A description of the roles and responsibilities that your firm, and any partner organizations, had in the engagement.
3. An overview of how the engagement aligns with the scope and scale of the requirements outlined in this RFP.
4. Project timelines and key milestones including rollout and transition to a steady state.
5. A list of the deliverables and acceptance criteria.
6. A description of the challenges experienced, and key learnings gained by your firm from involvement in the engagement.

   **NOTE:** Projects that represent a similar approach/structure as that proposed by the Proponent are desired. If, for example, the Proponent is proposing a consortium response or to engage a specific organizational unit or supplier partner in the proposed approach, it is preferred that project examples provided in response to this section include similarly structured engagements.

   Top-ranked Proponents may be asked to provide or confirm client references (including contact name and e-mail address) for each project.

**D.2.2** Describe, in detail, your experience with initiative governance involving multiple organizations as initiative sponsors (A.1.3 and B.1.2(1)). Provide lessons learned and 1-3 examples from initiatives of equivalent complexity.

**D.2.3** Describe, in detail, your experience with relationship management involving multiple organizations as initiative sponsors (B.1.2 (2)). Provide lessons learned and 1-3 examples from initiatives of equivalent complexity.

**D.2.4** Describe, in detail, your experience with stakeholder engagement involving multiple external stakeholders, including but not limited to users, in the design and delivery of a complex initiative (B.1.2 (3)). Provide lessons learned and 1-3 examples from initiatives of equivalent complexity.

**D.2.5** Describe, in detail, your experience with designing and delivering solutions where the solution is informed by multiple pieces of legislation, and the legislation, regulation, and policy are evolving (B.1.4 (4b) and Mandatory #9). Provide lessons learned and 1-3 examples from initiatives of equivalent complexity.

**D.2.6** Describe, in detail, your experience with developing and executing legislative and regulatory changes (B.1.4 (8)). Provide lessons learned and 1-3 examples from initiatives of equivalent complexity, in particular, where you have had to lead changes across multiple pieces of legislation and regulations for a common purpose.

**D.2.7** Describe, in detail, your experience with designing and delivering solutions that address privacy considerations during early stages of design and delivery. In particular, describe your experience upholding the concept of "data minimization" with respect to the collection, use, disclosure, retention, and other handling of personal information (B.1.4 (4)). Provide lessons learned and 1-3 examples from initiatives of equivalent complexity.

**D.2.8** Describe, in detail, your experience with integrating your business processes with client privacy and security-related processes, such as privacy/security incident investigation and response, privacy oversight body investigations and security audits, resolution of privacy complaints and compliance challenges, and assessment of privacy impacts (B.1.4 (4), B.1.4 (9), and Mandatory #2. Provide lessons learned and 1-3 examples from initiatives of equivalent complexity.

**D.2.9** Describe, in detail, your experience with supporting mass-market marketing campaigns for digital service uptake (B.1.4(2). Provide 1-3 examples of equivalent complexity where you have worked as a subject matter expert supporting and executing communications.

**D.2.10** Describe, in detail, the programs, or initiatives you have in place to promote diversity, inclusion and/or equity within your organization and the outcomes of these programs to-date. Clearly articulate which of the three elements (diversity, inclusion, equity) your programs target and include any written policy or certifications you have in this space.

**D.2.11** Describe, in detail, and provide examples of how you account for bias, discrimination, low levels of digital literacy, multilingual target audiences and accessibility in the solutions you offer.

## D.3 Proposed Approach

In many of these rated criteria, you will see a request to clearly describe, in detail, your approach for both the centralized ID (A.3 (1)) and the decentralized ID (A.3 (2)). It is not expected that your responses are fully matured as they relate to decentralized ID. Where gaps exist, acknowledge the gaps, and provide commentary on how you plan to address them through your roadmap. Where the approach does not change from one context to another, simply state no change. To this end, each Proponent should provide the following in the Submission:

**D.3.1** Describe, in detail, how your proposed approach will meet each of the Mandatory Requirements in Section C, Mandatory Requirements.

**D.3.2** Describe, in detail, your overall approach to deliver the *Individual Digital ID Foundations Initiative* as described in A, Overview and Background and B, The Deliverables. Clearly indicate:

1. the value of the approach and how the approach will enable GOS to realize its desired business outcomes listed in 1.1 Invitation to Proponents
2. how your proposed approach will align with the *Individual Digital ID Roadmap* (A.1.1)
3. any intention to leverage the IDLab (if desired) and describe how it would be used

**NOTE:** A detailed response against each requirement in B.1 and B.2 is not necessary for this response. Subsequent rated criteria will delve into the detail of each requirement listed in sections B.1 and B.2.

**D.3.3** Describe, in detail, how your proposed approach will meet requirements 1 – 4 (see B.1.1): issuing an LOA3 digital ID fully online, for use through the Saskatchewan Account.

**D.3.4** Describe, in detail, how your proposed approach will meet requirements 6 – 9 (see B.1.1), proving the person is legitimate, the right person, a real person and that the verification is happening in real time.

**D.3.5** Describe, in detail, how your proposed approach will handle facial verification and liveness checking (B.1.1 (7-9)). Detail how your approach will**:**

1. Achieve option 1 in A.4.3 – leveraging SGI's existing capabilities for facial verification – while maintaining data minimization, and ensuring privacy and security are not compromised. State your assumptions.

And, if applicable, detail how:

2. Your approach will achieve option 2 in A.4.3 – using Proponent provided software for facial verification behind SGI's firewall – while maintaining data minimization, ensuring privacy and security are not compromised and not permitting the photo to leave a user's device in order to generate a facial blueprint/faceprint/template.
    a. State your assumptions.
    b. State how you currently account for bias in your facial verification algorithm.
    c. State how you can evolve your algorithm to address underrepresented populations, specifically indigenous populations, to meet the needs of Saskatchewan residents.

3. You will deliver an alternative approach that still meets Mandatory #11 and will maintain data minimization, ensuring privacy and security are not compromised, while not permitting the photo to leave the user's device in order to generate a facial blueprint/faceprint/template.
    a. State your assumptions.
    b. State how you currently account for bias in your facial verification algorithm.
    c. State how you can evolve your algorithm to address underrepresented populations, specifically indigenous populations, to meet the needs of Saskatchewan residents.

And:

4. State your preferred approach from above. Include your rationale and assumptions.

**D.3.6** Provide a roadmap for your liveness checking and genuine presence confirmation (B.1.1 (8-10)). Include plans for continuous improvement. Speak specifically to how you plan to evolve your solution to stay current and responsive to bias and evolving presentation attacks.

**D.3.7** Describe, in detail, how your proposed approach will comply with the DIACC Pan-Canadian Trust Framework (https://diacc.ca/trust-framework/pctf-overview/) and the Pan-Canadian Trust Framework-Public Profile (https://canada-ca.github.io/PCTF-CCP/), including the various privacy and security considerations (B.1.1 (14)). In circumstances where one or more requirements are not met or based on the Proponent's expertise, are not feasible or applicable, Proponents should:

1. articulate their position,

2. indicate if this deviation relates to the individual digital ID used via Saskatchewan Account and/or the verifiable credential,
3. state their assumptions,
4. detail the work arounds (if any),
5. describe how the potential risk from not meeting the requirement(s) will be mitigated by the Proponent to the satisfaction of GOS.

**D.3.8** Describe, in detail, how you will deliver a digital ID to the target audience (described in section A.2 Target Audience) that will meet requirement #5 in B.1.1 and:

1. have alternate processes to support edge cases that meet LOA3 (see Appendices M and N for use cases) and maintains equitable access (e.g., alternate processes remain timely and easily accessible);
2. accommodate individuals not represented or partially represented in the SGI database or other selected source of truth database(s).

Describe how your approach would change (if at all) from issuing a centralized ID to later issuing a decentralized ID.

Proponents will need to explain how they will maximize participation in the Saskatchewan Individual Digital ID, bearing in mind these limitations. LOA3[4] approaches other than the use of facial verification will be required in addition to facial verification. Potential alternatives could be:

1. Use of an issuing process with offline steps, that prioritizes accessibility and risk-management
2. Acceptance of a range of credentials, weighing risk profile and potential gain in uptake (e.g., health card, treaty card, passports etc.)
3. Use of video call verifications

We encourage Proponents to see the above as examples only and to bring their creativity to bear to solve this problem in a way that addresses user needs. See Appendix L and M for stakeholder engagement findings and user stories that illustrate limitations and pain points with existing or potential identity issuance processes.

**D.3.9** Describe in detail how the proposed approach will actively incorporate a diversity of perspectives to mitigate biases in the design and build process.

**D.3.10** Describe, in detail, how the proposed digital ID will be made available to users who have EITHER a mobile device with a camera (e.g., phones, tablets etc.), OR a computer with a camera (e.g., desktop, laptop), OR both (B.1.1 (10)). Describe how your approach would change (if at all) from issuing a centralized ID to later issuing a decentralized ID.

**D.3.11** The solution is expected to conform to all applicable legislation including but not limited to:

1. The Freedom of Information and Protection of Privacy Act
2. The Health Information Protection Act

[4] As defined by the Digital Identity and Authentication Council of Canada (DIACC) Pan-Canadian Trust Framework (https://diacc.ca/trust-framework/pctf-overview/) and the Pan-Canadian Trust Framework-Public Profile (https://canada-ca.github.io/PCTF-CCP/)

3. The Traffic Safety Act
4. The Vital Statistics Act
5. Data Matching Agreements Act (not yet in force but still applicable)

As well, the solution is expected to allow future digital identity ecosystem participants to comply with all applicable legislation. For example, when a GOS decentralized ID is made available to the broader economy in future, commercial organizations subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) must be able to use the digital ID in compliance with PIPEDA.[5] Similarly, where a digital ID is issued to a digital wallet offered by a commercial organization subject to PIPEDA (and not offered by GOS), the organization offering the wallet must be able to receive and manage the digital ID in compliance with PIPEDA.

Describe, in detail, in line with mandatory requirement #10, how the solution is expected to conform to all applicable legislation. Where/if your proposed solution would ideally differ from legislation/ regulation, state what the non-conformance would be, the rationale for non-conformance and any assumptions made.

**D.3.12** Describe, in detail, how the proposed approach will uphold the concept of "data minimization" with respect to the collection, use, disclosure, retention, and other handling of personal information (B.1.4 (4c)).

**D.3.13** Provide a roadmap for your verifiable credential offering in the context of issuer. Include plans for continuous improvement (B.1.1 (21-26) and B.2.1 (2)). Speak specifically to:

1. How this roadmap supports the overall *Individual Digital ID Roadmap* (A.1.1)
2. How you plan to evolve your solution to conform with the Aries Interop Profile 2.0 (AIP) and stay current as AIP continues to evolve
3. How you plan to stay current with the W3C Verifiable Credential Data Model
4. How you plan to leverage the Research and Development requirement (B.2.2) to ensure the GOS technology solution remains current

**D.3.14** The digital identity landscape remains relatively immature as it relates to standards and GOS requires flexibility to adapt to the ever-changing standards landscape (Mandatory #8). Describe in detail:

1. the relevant digital ID standards with which the proposed solution currently conforms,
2. the degree to which it conforms,
3. the rationale for non-conformance if gaps exist,
4. how you plan to stay current and in conformance with the wide range of relevant digital ID standards,
5. the approach for leveraging the Research and Development requirement (B.2.2) to ensure the GOS digital ID solution remains current.

[5] Under the Digital Identity and Authentication Council of Canada (DIACC), Pan-Canadian Trust Framework (PCTF), they may play the role of "verifier" or "relying party".

**D.3.15** Describe, in detail, how the proposed approach will deliver a verifiable credential pilot that builds off the initial delivery of a centralized ID and meets requirements 21 – 26 of B.1.1. Pay specific attention to how this pilot will build on the work done for the centralized ID as opposed to being net new work.

With regards to requirement B.1.1 #23 Interoperability, describe in detail how your proposed approach will leverage blockchain (or other innovative solutions that provide for credential portability and verification) including identifying the technology choice. Clearly state your rationale, assumptions and how the proposed approach meets the interoperability requirement.

**NOTE** A blockchain based solution may ultimately be required but GOS is open to alternatives, at least in the short term, recognizing that the space continues to evolve.

**D.3.16** Indicate what privacy impact assessments, if any, have been conducted on the technology and associated business processes that are proposed in your response (B.1.4 (e)). Please note that further evidence of your privacy impact assessment work (e.g., copies of reports; summaries of reports) may be requested as part of the evaluation of your proposal.

### D.3.17 Fraud Management

Fraud management requires elements such as fraud monitoring, policies, and procedures, including fraud and dispute resolution processes, fraud reporting, fraud analysis, etc.

Describe, in detail, which industry standard framework you will use for fraud management and if you are certified for conformance (B.1.4 (10)). If there are circumstances where you do not conform to a particular requirement from your selected framework, and/or a requirement is not feasible or applicable, Proponents should:

1. articulate their position
2. indicate if this deviation relates to the centralized ID, the decentralized ID, or both
3. state their assumptions
4. detail the work around (if any)
5. describe how the potential risk from not meeting the requirement(s) will be mitigated by the Proponent to the satisfaction of GOS

## D.4 Information Technology (IT) Requirements

Each Proponent should provide the following in the Submission:

### D.4.1 Proposed Technical Solution

Describe, in detail, how your proposed technical solution will meet the business and IT requirements specified in this RFP. Provide a detailed description of any IT components for any aspect of the delivery of your proposed solution. The information should include:

1. A high-level diagram and conceptual layout of the solution components regarding the recommended system architecture;
2. An overview of the network illustrating how the solution will be accessed and secured for GOS employees, GOS citizens and/or businesses;
3. An indication of how interfaces to applications outside of the solution are facilitated;

4. A detailed description on how the solution complies with section **D.4.2 Required GOS Enterprise Services and Standards**. Also indicate any proposed use of additional GOS services outlined in section **D.4.3 GOS Enterprise Services Leverage Opportunities**;
5. Details regarding the proposed hosting environment and supporting infrastructure from which this solution will be provided. Provide an acknowledgement and compliance with the applicable computing environment expectations outlined in Appendix H – Infrastructure Architecture (refer to "Appendix Contents and Instructions" within this document for further detail);
6. An indication of the recommended technical environments to support the initial and on-going development, testing, training and production requirements. Explain the licensing requirements and cost implications for each environment;
7. A description on how the production environment will be monitored for performance, and how the solution can be scaled up or down;
8. An overview of patching, maintenance and lifecycle management strategies to keep the solution in a supported and secured state. Describe the ability to accommodate a mandatory change requiring a promotion into production outside the regular release schedule.

**D.4.2 Required GOS Enterprise Services and Standards**

GOS' guiding framework for IT investments focuses on a One Government, citizen-centric approach towards program and service delivery. Achieving this vision requires a consistent approach for digital identities, integrated platforms, increased re-use of common services, common platforms, and common data. As new solutions are introduced into GOS' IT portfolio, existing enterprise services must be considered. As outlined and further described in **Appendix H – Infrastructure Architecture,** GOS requires the Proponent to utilize, integrate or comply with these enterprise services and standards. Proponents are required to describe in detail how their proposal will meet the requirements below:

Application Authentication

All solutions that are dependent on user identities and authentication are required to utilize or integrate with the existing Government of Saskatchewan application authentication standards for employees, citizens and businesses. These include:

- Government Employee Identities and Authentication – Single Sign On with GOS Microsoft Azure Active Directory.
- Citizen and Organizations Identities and Authentication – Single Sign On with GOS Saskatchewan Account (A.4.1). The solution must leverage Saskatchewan Account to manage citizen and organization profiles. All updates to profile will be complete in Saskatchewan Account and populated in the solution (Mandatory #5).
- Government Partner Organizations - Applications or functionality that are targeted for organizations providing services to the Government of Saskatchewan are required to use the GOS Azure AD Business to Business (B2B) delegation with their identity provider.

GOS Enterprise Integration Services (EIS)

The solution must leverage the GOS EIS Platform (A.4.2) to access any government informational assets needed for the solution. EIS Platform is used to integrate public entity profiles created in Saskatchewan Account with service provider applications using a secured, consistent and repeatable process. The EIS Platform may also provide APIs to access partner services.

Web Application Firewall Service

To mitigate risks for cyber threats against the GoS's public facing and internal applications, all new solutions are to include the GOS Web Application Firewall as a Service solution. This service will be incorporated into all new public facing or internal application solutions.

IT Service Management

In support of providing a "one number to call" approach for Government employees, and services being proposed, proponents are required to indicate how their service management processes and systems can integrate with the GOS Enterprise IT service management operations (incident, problem, change, release, and knowledge management).

We understand that given the emerging nature of this technology, some of the solution blocks may not adhere to GOS standards. In circumstances where one or more requirements are not met or based on the Proponent's expertise, are not feasible or applicable, Proponents should:

1. articulate their position
2. indicate if this deviation relates to centralized ID (A.3 (1)), the decentralized ID (A.3 (2)) or both
3. state their assumptions
4. detail the work around (if any)
5. describe how the potential risk from not meeting the requirement(s) will be mitigated by the Proponent to the satisfaction of GOS

### D.4.3 Open Source

Remaining nimble to respond to changes as they come is paramount. The solution built should be modular by design and maximize portability of data, applications and interoperability (B.1.1 (15)). An open-source approach allows GOS to evolve quickly in a technology space where standards have yet to solidify. Describe, in detail, how your proposed solution will leverage open-source software where possible. Identify your stack and provide your rationale for the use of this stack. Alternatively, describe in detail how the solution could be made available to other jurisdictions looking to leverage Saskatchewan's progress.

### D.4.4 Public-Facing Online Services

GOS has undertaken focused efforts to standardize how citizens and organizations conduct online transactions with government. The full policy and standards for public-facing online services, as well as those specific to the proponent (enterprise tool requirements, user interface requirements and development requirements), are outlined in **Appendix J** and required by Mandatory #7. Describe, in detail, how your proposal will meet the requirements outlined below:

- configuration of UI elements to meet GOS design styles and branding;
- incorporating user experience methods into user interface design;
- mobile first solutions;
- browser testing; and
- building responsive user interfaces that comply with the World Wide Web Consortium's Web Content Accessibility Guidelines 2.0 Level AA or higher.

## D.5 Information Security Requirements

Proponents are required to conform with Appendix G - Information Security including a Threat Risk Assessment (TRA) of the solution. This is performed by GOS with inputs from all project participants. The final TRA is required prior to the solution going live and with every significant change thereafter.

Each Proponent should provide the following in its Submission:

### D.5.1 General Information Security Requirements

Describe, in detail, the extent to which the proposed Solution and/or Service aligns with each of the requirements listed in Appendix G – Information Security, Section 1.1, General Information Security Requirements. Further describe in detail how security-related service level metrics will align to both the DIACC Pan-Canadian Trust Framework (https://diacc.ca/trust-framework/pctf-overview/) and the Pan-Canadian Trust Framework - Public Profile (https://canada-ca.github.io/PCTF-CCP/).

### D.5.2 Data Classification Security Requirements

GOS Information Assets for this system contain highly sensitive data and have been classified by the Information Owner as Class A. Additional information pertaining to this Information Classification is contained in Section 2 of Appendix G, Information Security.

Describe, in detail, the extent to which the proposed Solution and/or Service aligns with each of the requirements listed in Section 1.2, Data Classification Security Requirements, of Appendix G, Information Security.

In circumstances where one or more data classification security requirements are not met or based on the Proponent's expertise, are not feasible or applicable, Proponents should:

1. articulate their position
2. indicate if this deviation relates to centralized ID (A.3 (1)) or decentralized ID (A.3 (2)) or both
3. state their assumptions
4. detail the work arounds (if any)
5. describe how the potential risk from not meeting the requirement(s) will be mitigated by the Proponent to the satisfaction of GOS

### D.5.3 Overarching Information Security Policy

GOS desires engagement with Service Providers who can demonstrate a strong information security posture and maturity. Review Appendix G, Information Security, Sections 2 and 3, and state your understanding of the information presented in the policy.

### D.5.4 Security Objectives and Control Statements

Review Appendix G, Information Security, Section 3, Security Objectives and Control Statements, and state your understanding. In your response, articulate the extent to which the Service Provider's established information security policy aligns with that established by the Government of Saskatchewan. Service Providers should append and reference a copy of their established information security policies or, at a minimum, provide an outline of their policies and confirm the industry standard framework(s) to which they align.

In circumstances where one or more security objectives and control statements, based on the respondent's expertise, either do not align to the PCTFs or are not feasible or applicable, respondents should articulate their position and describe how the potential risk from not meeting the requirement(s) will be mitigated by the Service Provider to the satisfaction of GOS.

## D.6 Initiative Implementation and Transition

With the desire for the *Individual Digital ID Initiative* (B.1) to be in production by September 2023, each Proponent should provide the following in its submission:

**D.6.1 Provide a detailed plan that describes:**

1. the deliverables that you will deliver during the Initiative implementation and transition to operations phase of the engagement
2. the anticipated work packages (see A.1.2 scope figure for guidance) including:
    a. estimated start and end dates for each work package
    b. an indication of the deliverables and milestone dates associated with each work package
    c. an indication of the resource allocation for each work package
3. the method of initiative and project monitoring and reporting that will be provided
4. an indication of the expectations and support required from GOS
5. how you will coordinate across the three partner organizations (GOS, eHealth and SGI) and the provided resources to deliver to B. The Deliverables
6. how you will work under the direction and guidance of the GOS Project Manager

**D.6.2** Describe, in detail, how you will design and implement a testing strategy that meets requirement B.1.1 (19).

**D.6.3** Describe, in detail, how you will design and deliver, in collaboration and with oversight from the Saskatchewan Account Team, an onboarding strategy to connect government services to the digital ID via Saskatchewan Account (B.1.4 (7)) The documentation should provide both requirements and instructions for government services to consume the digital ID. The response should also detail your approach to onboard services currently leveraging the LOA2 identity in Saskatchewan Account. These services range in user volumes from 1000s to 100,000s (B.1.1 (20)).

Services not already leveraging Saskatchewan Account will be onboarded over time, and based on the needs of the government service, once the initiative is fully operational. The Proponent is not expected to provide a roadmap for onboarding new services.

**D.6.4** Describe, in detail, how you will develop and execute a multi-tier citizen support model that meets the requirements set out in B.1.3. Include the types of service level targets and support offerings you will provide.

**D.6.5** Describe, in detail, how you will develop and execute a maintenance and continuous improvement strategy and implementation plan that meets requirement B.1.4 (3).

**D.6.6** Describe, in detail, how you will design and deliver a records management policy and implementation plan that meets requirement B.1.4 (5).

**D.6.7** Describe, in detail, how you will design and deliver a change management policy and implementation plan, that meets requirement B.1.4 (6).

**D.6.8** Describe, in detail, how you will design and deliver an auditing process that meets requirement B.1.4 (9).

## D.7 Risk Management Plan

Each Proponent should provide the following in the Submission:

Describe your approach to risk management for the *Individual Digital ID Initiative* and its operations. The risk management plan should outline potential risks, the risk owners, and plans for capturing, assessing, scoring, and ultimately managing risks for the following categories:

**D.7.1 *Individual Digital ID Foundations Initiative* Risk Management Plan (B.1.4 (11)).**

1. **People Risks:** Risks related to the capability / capacity of resources as well as risks associated with management control changes.
2. **Initiative Risks:** Risks related to the initiative management (scope, schedule budget), governance, and transition to operations and establishing operational of obligations.
3. **Technology Risks:** Risks that threaten the performance of the seamless transition to operations including any risks related to technology operations.
4. **Stakeholder Risks:** Risks related to all parties involved in the initiative, delivery of goods or services (Internal, External, Community organizations etc.).
5. **Privacy, Information Security and Fraud Risks:** Risks that threaten the privacy of individuals and groups/communities, identity integrity, as well as the confidentiality, integrity, and/or availability of Government of Saskatchewan Information Assets.

**D.7.2 Risk Management Plan – operations (B.1.4 (12))**

1. **People Risks:** Risks related to the capability / capacity of resources as well as risks associated with management control changes.
2. **Technology Risks:** Risks that threaten the performance of technology operations.
3. **Stakeholder Risks:** Risks related to all parties involved in the initiative, delivery of goods or services (Internal, External, Community organizations etc.).
4. **Operational Risks:** Risks related to the product management (budget, support, continuous improvement, maintenance), and governance of other operational of obligations.
5. **Privacy, Information Security and Fraud Risks:** Risks that threaten the privacy of individuals and groups/communities, identity integrity, as well as the confidentiality, integrity, and/or availability of Government of Saskatchewan Information Assets.

## D.8 Proposed Team and Resources

For the *Individual ID Foundations Initiative,* the Proponent, at a minimum, is expected to provide lead resources (and teams where relevant) in the following areas (B.1.2 (4)):

1. Project Manager(s) – recognizing all proponent project management will be under the direction and guidance of the GOS Project Manager and must be in adherence with GOS project standards and practices
2. Security
3. Privacy (GOS will provide a Privacy Lead – the Proponent is expected to have privacy resources who, at a minimum, can liaise with the Privacy Lead)
4. Service Design
5. Architecture
6. Development
7. Testing (regression, performance, load, UAT etc.)

8. Operations (support and continuous improvement)
9. Subject matter expertise to support a mass-market marketing campaign at launch
10. Change Management
11. Records Management
12. Legislation, regulation, and policy management expertise
13. Risk management and auditing process development

**D.8.1 Team Information**

- Describe the proposed team(s) structure(s) and roles for both *the Individual Digital ID Foundations Initiative*.
- Explain how this composition and structure will provide effective service delivery and achievement of performance standards.

**D.8.2** Provide a detailed description of your succession plan for the replacement of a team resource(s) (if required) once the Proponent is working under a contract with the GOS (B.1.2 (4) and B.2.1). Describe your approach to the assignment of resources, including how the Proponent proposes to deal with vacation, illness, resignations, training, onboarding of new resources (including new GOS resources) and other absences, without impact to service delivery.

Proponents may be asked to provide client references (including contact name and e-mail address) for each resource.

## D.9 Value Add-ons and Innovation

Each Proponent should provide the following in the Submission:

**D.9.1** Identify value add-ons in the proposed solution that may assist GOS when implementing *Initiative* and *Roadmap* targets as identified in Appendix A. These are value add-ons not otherwise referenced when responding to other Mandatory or Rated requirements.

**D.9.2** GOS wants to be recognized for taking steps to realize the importance of protecting our environment. Proponents should indicate if they participate or are involved in "Green", environmental and/or sustainable initiatives. If so, provide descriptions of the initiatives.

**D.9.3** Detail capabilities to support relational ID (e.g., elder care, parent/guardians on behalf of minors, power of attorney etc.). Indicate roadmap for capabilities and status of capability (e.g., is production ready, under development, exploratory, etc.).

**D.9.4** Detail capabilities for organizational ID (e.g., corporations, sole proprietors, NGOs, schools, hospitals etc.). Indicate roadmap for capabilities and status of capability (e.g., is production ready, under development, exploratory etc.)

**D.9.5** Detail experience with conceptualizing, designing and/or onboarding verifiers (e.g., small business, large corporations, and institutions) to a verifiable credential ecosystem. Proofs of concepts are acceptable examples but must be indicated as such.

**D.9.6** Detail experience with conceptualizing, strategizing and/or initiative planning for expanding to a verifiable credential ecosystem, accounting for issuers, holders, and verifiers.

**D.9.7** Detail any capabilities or partnerships you may have to support users who have English as a second language (e.g., speakers of Dene, Cree, Tagalog, Urdu, German, Yoruba, Igbo, etc.)

## D.10 Local Knowledge

The GOS and its Ministry stakeholders are interested in understanding the Service Provider's experience with the Government of Saskatchewan, or comparable entity, as it relates to the technical and business landscape.

## D.11 Community Benefits

Describe how you can provide a maximum positive impact to the Saskatchewan community. GOS is interested in supporting regional economic development and enhancing quality of life across the province. Generating local community benefits and economic activities are considered objectives of this competition and the Proponent's ability to offer these benefits will be assessed in this competitive process. Proponents are required to clearly describe how they will be committed to addressing and maximizing local employment opportunities for Saskatchewan residents, supporting Saskatchewan industry, and generating economic development, including but not limited to percentage of Saskatchewan resources to be involved, and engaging local partners and sub-contractor companies if applicable.

Additionally:

- Describe how, through service implementation and ongoing service delivery you have contemplated local capacity building as a key feature of your proposed team and resourcing strategy.
- Describe how the local composition of your team and identified key individuals will contribute to the successful delivery.
- Provide an overview of the anticipated level of local resources (on a percentage basis) that will be involved in delivering the services both through service implementation and ongoing service delivery.

Alignment to Saskatchewan's Growth Plan

Describe how your Team's overall approach and/or team strategy align with Saskatchewan's Growth Plan, with specific emphasis on how all elements:

- Support the transformation of Saskatchewan's economy through innovation and technology and support the growth of Saskatchewan's technology sector.
- Increase efficiency, effectiveness and productivity of government programs and services.
- Identify any other linkages that your approach, team strategy or other components of your submission have for supporting or addressing other stated goals and objectives of Saskatchewan's Growth Plan specifically how it can support the goal to triple the growth of Saskatchewan's technology sector by 2030.

## D.12 Pricing

**Pricing will be kept separate from the written proposal evaluation. It will only be accessed after written proposals are completed.**

Pricing will be scored based on a relative pricing formula using the rates set out in the Pricing Form. Each Proponent will receive a percentage of the total possible points, which will be calculated in accordance with the following formula:

$$lowest\ price \div proponent's\ price\ \times\ weighting = proponent's\ pricing\ points$$

# E. OTHER RATED CRITERIA

| Optional Rated Criteria Category (See PART 2) | Weighting (Points) |
|---|---|
| E.1 Interviews/Presentations/Demonstrations | 200 |
| E.2 Proof-of-concepts | 200 |
| E. 3 Reference Checks | 150 |
| **Total Points** | |
| E.3 BAFO | To Be Determined |

Details for Other Rated Criteria will be provided to top-ranked Proponents as outlined in PART 2 of this RFP.

# F. SUBMISSION GUIDELINES

**Submissions should include all the information requested, and be presented in the order described below:**

### F.1 Table of Contents

A listing of the Submission contents with reference to the appropriate page number. Page numbering and tabs are beneficial.

### F.2 Letter of Introduction

One page of introduction which should be dated and signed by an official authorized to negotiate, make commitments and provide clarifications with respect to the Submission on behalf of the Proponent.

### F.3 Executive Summary

Provide a summary of the key features of your Submission.

### F.4 Forms

**Mandatory Requirements and Submission Form**

Each Submission must respond to the Mandatory Requirements and include a Submission Form (Appendix D), or a document containing the information requested by the Submission Form, completed, and signed by an authorized representative of the Proponent.

**Pricing Form**

Each Submission should include a Pricing Form (Appendix B), or a document containing the information requested by the Pricing Form, completed in accordance with the instructions contained in the form.

### F.5 Rated Criteria

Each Submission should include a response to each of the rated criteria (Section D of this Appendix) completed according to the instructions contained in the form.

## APPENDIX B – PRICING FORM

Refer to Appendix B – Pricing Form, a separate document.

## APPENDIX C - FORM OF AGREEMENT

*Proponents are asked to review Appendix C – Form of Agreement and respond to Mandatory 1 in Appendix D – Mandatory Requirements.*

# APPENDIX D - MANDATORY REQUIREMENTS & SUBMISSION FORM

**1. Mandatory Requirements** Proponents should complete the following table:

| **The Proponent agrees to the following:** | **Yes** | **No** | **Pg.#** |
|---|---|---|---|
| **Mandatory #1 -** Service Providers are required to review Appendix C, Form of Agreement and agree to one of the following:<br>1.Yes, you accept the terms and conditions as outlined in the Appendix, or<br>2.You provide a markup with requested changes to the Appendix, or<br>3.You advise that you have a current SaskBuilds and Procurement (formerly Central Services) Master Terms and Conditions and agree that it will used for any engagement resulting from this competition. | | | |
| **Mandatory #2** - The Proponent confirms it has established Information Security Policies, Standards, and Specifications which align with ISO 27002:2013, or a similar/equivalent industry recognized code of practice for information security controls. These are outlined in Appendix G - Information Security | | | |
| **Mandatory #3 -** The Proponent confirms that its proposed approach to Services and Solution delivery will ensure that all sensitive data, containing Personally Identifiable Information, at-rest, including data backups, remain in Canada. | | | |
| **Mandatory #4 -** The Proponent confirms that its proposed approach to Services and Solution delivery will ensure that all sensitive data, containing Personally Identifiable Information, in-transit, including data backups, is end-to-end encrypted at all times. | | | |
| **Mandatory #5 -** The proponent confirms that its proposed solution will integrate with the Government of Saskatchewan's single sign-on platform, Saskatchewan Account (A.4.1). This platform provides account creation, authentication, profile management, and allows citizens/organizations to access government online services.<br>The Proponent agrees to leverage SAML2 for account authentication. | | | |

| | | | |
|---|---|---|---|
| **Mandatory #6 -** The prospective solution must meet the GOS accessibility standard defined for World Wide Web Consortium, Web Content Accessibility Guidelines 2.0 Level AA (W3C WCAG 2.0 AA) or higher. | | | |
| **Mandatory #7–** All services must be responsive in design to ensure that they function and are user friendly on the browsers defined in the browser standard. These are outlined in Appendix J – Developing Public Facing Services. | | | |
| **Mandatory #8 –** The Proponent recognizes the digital identity environment is evolving and commits to staying current, and conforming as needed, to ensure the digital ID remains compliant with Level of Assurance 3 (LOA3), is interoperable, secure and privacy protecting.<br>At a minimum, the Proponent must comply with the standards below:<br>• the DIACC Pan-Canadian Trust Framework (https://diacc.ca/trust-framework/pctf-overview/)<br>• the Pan-Canadian Trust Framework - Public Profile (https://canada-ca.github.io/PCTF-CCP/).<br>• W3C Verifiable Credentials Data Model https://www.w3.org/TR/vc-data-model/<br>Other anticipated standards for compliance include:<br>• Aries Interop Profile 2.0 https://aries-interop.info/aries-interop-intro.html<br>• The forthcoming Standards Council of Canada National Trust standard<br>• Mobile Driver's Licence https://www.iso.org/standard/69084.html<br>The Proponent may identify others to which the Proponent complies. | | | |

| | | | |
|---|---|---|---|
| **Mandatory #9 -** The solution must conform to applicable legislation, including but not limited to the list below. Where the solution may exceed the boundaries of current legislation, the Proponent must identify the ways in which legislation may be amended.<br>• The Freedom of Information and Protection of Privacy Act<br>• The Health Information Protection Act<br>• The Traffic Safety Act<br>• The Vital Statistics Act<br>• Data Matching Agreements Act (not yet in force but still applicable). | | | |
| **Mandatory #10 –** The solution must have capabilities for a selfie capture, facial verification, liveness checking and genuine presence detection in line with global best practices. | | | |
| **Mandatory #11** - As explained in A.4.3 SGI Facial Verification Database, the facial verification responsibility must lie within the SGI firewall. SGI will not pass raw photos outside the firewall.<br><br>The Proponent's solution must enable facial verification behind the SGI firewall or must be able to pass a raw photo to SGI via encrypted RESTful APIs. | | | |

## 2. Proponent Information

| Please fill out the following form, naming one person to be the Proponent's contact for the RFP process and for any clarifications or communication that might be necessary. | |
|---|---|
| Full Legal Name of Proponent: | |
| Any Other Relevant Name under which Proponent Carries on Business: | |
| Street Address: | |
| City, Province/State: | |
| Postal Code: | |
| Phone Number: | |
| Fax Number: | |

| Please fill out the following form, naming one person to be the Proponent's contact for the RFP process and for any clarifications or communication that might be necessary. | |
|---|---|
| Company Website (if any): | |
| Proponent Contact<br>Name and Title: | |
| Proponent Contact Phone: | |
| Proponent Contact Fax: | |
| Proponent Contact Email: | |

The Proponent acknowledges the RFP process will be governed by the terms and conditions of the RFP, 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 Contract A bidding process contract), and that no legal relationship or obligation regarding the procurement of any good or service will be created between GOS and the Proponent unless and until GOS and the Proponent execute a written Agreement for the Deliverables.

_____ _____

Signature of Proponent Representative Title of Proponent Representative

_____ _____

Name of Proponent Representative Date

## APPENDIX E - DEFINITIONS

Throughout this RFP, the following definitions apply:

**"Agreement"** means the written contract between the top-ranked Proponent and Her Majesty to provide the services contemplated by this RFP.

**"Client"** (referring to ministry) means Her Majesty the Queen in the right of the Province of Saskatchewan, as represented by the Ministry of SaskBuilds and Procurement.

**"Desirable" "Rated" "Should"** means requirements that may have a degree of importance to be objectives of this RFP and may be rated.

**"Deliverables"** means the functions, duties, tasks and responsibilities to be provided by the Proponent as described in this RFP.

**"Delivered Duty Paid"** refers to a transaction where the seller pays for the total costs associated with transporting goods and is fully responsible for the goods until they are received and transferred to the buyer. This includes paying for costs, export and import duties, insurance and any other expenses incurred during shipping of the goods. The risks and charges are with the seller of the goods until delivery is made in the buyer's country at an agreed-upon location.

**"Entity"** refers to the Government of Saskatchewan, the province or ministries are used for administrative purposes and mean Her Majesty the Queen in Right of the Province of Saskatchewan, as represented by the Minister of SaskBuilds and Procurement.

**"Evaluation Team"** means the individuals who will evaluate the Submissions on behalf of the Government of Saskatchewan.

**"GST"** means Goods and Services Tax (currently at 5%).

**"Level of Assurance"** (LOA1, LOA2, LOA3) While there are differing views on levels of assurance, this RFP relies on the definition of LOA as defined by the Digital Identity and Authentication Council of Canada (DIACC) Pan-Canadian Trust Framework (https://diacc.ca/trust-framework/pctf-overview/) and the Pan-Canadian Trust Framework-Public Profile (https://canada-ca.github.io/PCTF-CCP/)

**"Mandatory"** means requirements that are imperative and must be met in order for the proposal to receive consideration.

**"RFP"** means Request for Proposal.

**"PST"** means Saskatchewan Provincial Sales Tax (currently 6%).

**"Proponent"** means an individual or a company that provides, or intends to provide, a Submission in response to this RFP.

**"Saskatchewan Time"** means Local Saskatchewan Time as verified by the time clock located at 1855 Victoria Avenue, Regina, SK.

**"Single Procurement Service"** means the Purchasing Branch under *The Purchasing Act, 2004*.

**"Submission"** means the bid, proposal, or document provided by a Proponent in response to the RFP.

**"Successful Supplier"** means the organization responding to this RFP who is determined to be successful in this competition and has signed an Agreement.

## APPENDIX F - ITD ENVIRONMENT

Appendix F may be found as an attached document to this Competition. It describes the technology information environment and should be taken into consideration while building your submission.

## APPENDIX G - INFORMATION SECURITY

The above mentioned Appendix may be found as an attached document to this Competition. It lists ITD's information security requirements and should be taken in consideration while building your submission.

## APPENDIX H - INFRASTRUCTURE AND ARCHITECTURE

The above mentioned Appendix may be found as an attached document to this Competition. It describes ITD's considerations in regards to the Solution's Infrastructure and Architecture requirements and should be taken in consideration while building your submission.

## APPENDIX I - NOT APPLICABLE

## APPENDIX J - DEVELOPING PUBLIC-FACING ONLINE SERVICES POLICY

The above-mentioned Appendix may be found as an attached document to this Competition. It describes ITD's considerations with respect to creating and developing solutions that interact with the public through online platforms. As described throughout the document, those requirements should be taken in consideration while building your submission.

## APPENDIX K - SERVICE LEVEL AGREEMENT

The above-mentioned Appendix may be found as an attached document to this Competition. It describes the service level agreement for the ITD Help Desk.

## APPENDIX L – STAKEHOLDER ENGAGEMENT REPORTS

The above-mentioned Appendix may be found as an attached document to this Competition. It includes:

1. Detailed survey results from a (nearly) representative sample of 802 Saskatchewan residents on the subject of digital ID
2. A report that covers both the survey finding and findings from our one-on-ones with organizations representing communities that have access concerns as it relates to digital ID.

## APPENDIX M – USER STORIES

The above-mentioned Appendix may be found as an attached document to this Competition. It includes user stories that detail access concerns as it relates to digital ID and should be taken into consideration while building your submission. It is expected that your submission account for both happy-path digital ID issuance and the edge cases explored in these user stories.

## APPENDIX N – IDLAB AGREEMENTS

The above-mentioned appendix may be found as an attached document to this competition. It includes the two agreements that will need to be signed by the Proponents shortlisted for the proof-of-concept stage

## APPENDIX O - PENETRATION OF DRIVERS LICENCES & ID CARDS IN SASKATCHEWAN

The above-mentioned appendix may be found as an attached document to this competition. It includes the detailed breakdown by age of Saskatchewan residents that hold a Saskatchewan driver's licence or SGI-issued photo ID card.