Canada Revenue Agency   Agence du revenu du Canada

Request for Information

No. 1000436715

Enhanced Telephone Authentication

For

The Canada Revenue Agency

Closing Date and Time: February 28, 2023, 2:00PM

Disclaimer

Responding to this Request for Information (RFI) is not a prerequisite to receiving or being eligible to bid on any Request for Proposal (RFP) for this requirement. Any RFP will be advertised on the Government Electronic Tendering Service (GETS) commonly referred to as Buy and Sell (https://buyandsell.gc.ca/).

This RFI is not to be construed as a solicitation for tenders or proposals. No contract or other form of commitment will be entered into based on responses to this RFI. This RFI is not considered as authorization by the Canada Revenue Agency (CRA) to undertake any work that would result in costs to CRA.

Nothing in this RFI shall be construed as a commitment from CRA to issue an RFP for this program. CRA may use non-proprietary information provided in its review and/or in the preparation of any formal RFP. All responses will be held by CRA on a confidential basis (subject to applicable federal legislation) and remain the property of CRA once they have been received.

CRA may reproduce or photocopy or transcribe the response and any non-proprietary supporting documentation for the purpose of its review and/or inclusion in any resulting RFP document. Vendors responding to this RFI are advised to clearly identify which (if any) portions of their responses are proprietary and may be invited to a meeting to further clarify their responses to questions provided in Appendix A herein. The confidentiality of each vendor's response will be maintained.

CRA shall not be bound by anything stated herein. CRA reserves the right to change, at any time, any or all parts of the requirements as it deems necessary. CRA also reserves the right to revise its procurement approach, as it considers appropriate, either based upon information submitted in response to this RFI or for any other reason it deems appropriate.

Interactive Demonstration Sessions

CRA may at its sole discretion entertain presentations/demonstrations with interested vendors to provide them with the opportunity for a follow-up to their written response to present their capabilities in relation to this RFI.

Vendors that have expressed such interest and have demonstrated via their response to the RFI that their products(s) correspond sufficiently to the product questions as stated herein may be contacted within two weeks of the RFI closing date to schedule the demonstration.

The demonstration can utilize audio and/or video conferencing tools such as WebEx.or MS Teams. The time frame for each session will be a maximum of 75 minutes.

Responses and Enquiries:

Responses to questions must be submitted complete and in writing in the order shown. All requests for information in all sections of this document must be answered as concisely as possible while providing all information necessary to understand the proposed solution. Any deviation from the question or requirements that cannot be satisfied by the vendor must be clearly identified.

Any information of a confidential or proprietary nature contained in a Vendor's response should be clearly marked 'PROPRIETARY' or 'CONFIDENTIAL' by item or at the top of each page.

Responses to this RFI will not be used to pre-qualify or otherwise restrict participation in any future procurement process (e.g. an RFP). Responses will not be formally evaluated.

CRA will not reimburse any expenditure incurred in preparing responses and participating in the presentation sessions related to this RFI.

The Vendor must provide a contact name, email address and telephone number when submitting their response.

Vendors are requested to submit responses by February 28, 2023 2:00PM Eastern Daylight Time.

Electronic submissions are mandatory and should be submitted as one complete package.

Vendors are requested to submit responses to this RFI using the following e-mail

E-mail: val.wawrzynczak@cra-arc.gc.ca

All enquiries must be submitted via email to the attention of Val Wawrzynczak at val.wawrzynczak@cra-arc.gc.ca or by phone at (613) 614-9655

Summary of Canada Revenue Agency Requirements

The Contact Centre Services program is seeking to leverage Voice Authentication technologies to strengthen and modernize the way it verifies callers' identity in order to help protect Canadians and reduce the burden they have in identifying themselves when calling the CRA.

The goal is to implement a flexible Voice Authentication solution, offering a full suite of identity proofing capabilities, which may include (but are not limited to):

- Active (Text Dependent) Voice Authentication – ability to authenticate a caller using a specific phrase that a caller has previously spoken.
- Passive (Text Independent) Voice Authentication – ability to authenticate a caller while the caller is talking with an agent using a previously recorded voice recording of the caller
- Semantic Fraud Detection – ability to perform speech to text conversion and to identify suspicious behaviour and patterns,
- Ongoing and tailored knowledge, expertise, recommendations, as well as access to advice on fraud strategies, case management, attack handling
- Watch List - Availability/maintenance of voiceprint databases of known bad actors. Ability to recognise call recordings and ongoing calls from known bad actors.
- ANI (Caller ID) validation – ability to detect potential unknown fraud cases by identifying calls coming from spoofed numbers.
- GEO location services – ability to determine if the call is from a known trusted device or a known fraudulent device.
- Business analytics/reporting – ability to perform statistical data analysis and to create reports on voiceprint enrolment rates, usage, trends, etc.

The solution must allow for integration with different telephony platforms concurrently and support multiple contact centers, to ensure integration with Government of Canada (GC) contact centres.

For the purposes of assisting vendors to respond to this RFI, CRA is considering the target solution to be divided into 2 sub-groups of related functions:

Subgroup1 – Functional requirements

- Active Voice Authentication
- Passive Voice Authentication
- Semantic Fraud Detection
- Watch List
- ANI validation
- GEO location services (low priority but future requirement)
- Business analytics/reporting
- Other Core Functionalities/Features

Subgroup 2 – Non-functional requirements

- Deployment options (public cloud, private cloud or on premise)
- Telephony platforms and contact centre applications supported
- Additional hardware/software requirements
- Documentation / Training
- Licensing/Costing models (deployment, pay-per-use, bulk pricing, etc)
- Solution costs
- Privacy & Security
- Other Non-functional Requirements

Vendors are encouraged to respond to this RFI if their solution can meet all or substantial portions of either subgroup 1 or of subgroups 1 and 2. Specific Questions for these subgroups can be found in Appendix A and B.

The purpose of this RFI is to:

1. Determine vendor capabilities in providing a suitable, secure Voice Authentication solution

2. Help CRA understand industry standards, best practices, and/or recommendations in terms of using Voice Authentication in a public service environment.

3. Provide an opportunity for industry to demonstrate and discuss its software functionalities, capabilities, and constraints.

4. Solicit feedback on options for integrating the solution with GC platforms and systems.

5. Solicit feedback on the cost, schedule, level of effort, hardware requirements, and technical architecture.

Constraints to be considered for the proposed solution

Official Languages - Must meet the Government of Canada standard under the Official Languages Act (accessible via the following hyperlink http://laws-lois.justice.gc.ca/eng/acts/o-3.01/). Specifically – user interfaces, functionality and documentation in English and Canadian French

Accessibility – Must meet the Government of Canada standard under the Accessible Canada Act (accessible via the following hyperlink https://laws-lois.justice.gc.ca/eng/acts/A-0.6/)

Privacy - Must meets the Government of Canada standard under the Privacy Act (accessible via the following hyperlink http://laws-lois.justice.gc.ca/eng/acts/p-21/)

Identity – Must meet/integrate with GC Enterprise Identity related Standards (Tell us Once, GC Digital Identity, etc.)

Data Communication/Residency – Any SaaS cloud hosted solutions must ensure data communication, and hosted destination falls within Canadian jurisdiction

User access – Must support limiting user access (user profiles) and configuration

Integration – Must provide support for document and records management either internally or externally and describe the integration required with existing Contact Centre platforms and the methods used

Retention – Must have flexible file retention rules

Appendix A – Subgroup 1 Questions (Functional requirements)

The following questions are representative of the type of information the CRA is seeking as it considers how to structure any RFP that might follow this RFI process.

Vendors must note that this list of questions is not exhaustive; vendors are invited to provide any additional information that might prove useful and/or beneficial to the CRA in preparing any subsequent RFP.

Vendors that provide written feedback may be invited to a one-on-one consultation session with CRA representatives. This session would allow vendors to provide additional feedback pertaining to this RFI as well as to explain comments made in their written submission.

A.1 – Active and passive voice biometrics, fraud detection/prevention, ANI validation, GEO location services, business analytics and reporting	
A.1.1	Does your product support Active (Text Dependent)Voice Authentication? If yes, describe.
A.1.2	Does your product support Passive (Text Independent Voice Authentication? If yes, describe.
A.1.3	Can a voiceprint be created from historical voice recordings? If yes, what are the supported format(s)?
A.1.4	Does your product have a noise cancellation feature to account for external/outside noise?
A.1.5	Does your product have the ability to detect artificial voice on a call during the enrolment and authentication processes?
A.1.6	Does the product have the capability to remove silence and non-speech signals during enrollment to arrive at a the proper SUS (seconds of useable speech)
A.1.7	Does the concept of updating/replacing a user's voiceprint exist in the product, or is each voiceprint enrolment a new user? Does your solution allow users to update/maintain their voiceprints?
A.1.8	Over the product's lifecycle, as you make improvements to the techniques used to create a voiceprint, will it be necessary to create a new voiceprint for users that are already enrolled?
A.1.9	Does the product have the capability to identify voiceprints that were created by the same speaker? In other words, given some target False Acceptance Rate (FAR) (which may be different from that used for normal authentication), an identity claim represented by one voiceprint could be verified by comparing against other voiceprints. The problem that we are trying to solve with this question/capability is that one individual creates voiceprints for multiple identities, which would indicate fraud.
A.1.10	Verify Speaker against Black List – does the product provide a 1 to many matching process to detect in real time that current caller is on Black List. If yes, how is this handled?
A.1.11	Describe the process of ANI validation employed by your solution and the impact it has on the determination of caller identification.
A.1.12	Describe the process of GEO location services employed by your solution and the impact it has on the determination of a user’s identification validity.
A.1.13	Is it possible to disable the use of GEO location services within your solution suite if required due to legal/privacy concerns?
A.1.14	Is call metadata available for use as report parameters and what call metadata is required?
A.1.15	Describe your reporting system with respect to: • whether it is part of an industry standard platform, or is it a propriety in-house developed product • the “out of the box” reports • scheduled running times or ad-hoc • ability to export and in what formats (for example, .csv, .xls, and .pdf) • additional software not provided with existing solution for standard or custom reports text and graphic results on standard and custom reports
A.1.16	Can your reports and the data underlying them be exposed via an open/industry standard data layer and in what formats?
A.1.17	Describe how your system would provide results and reports for English and French.
A.1.18	Does your product have a purchase or licensing structure that is not based on usage/volume; for example, initial purchase price, fixed monthly fee, etc..
A.1.19	Does your product support storing the voiceprint external to your product (in a Government of Canada data centre), and not storing the voiceprint in your product, with the voiceprint

	being provided at the same time as it is to be used (for example, provided with audio for authentication; provided with other voiceprints as described in A.1.9).
A.1.20	What False Acceptance Rate (FAR) can your product achieve when configured to have a False Rejection Rate (FRR) of at most 10%?
A.1.21	What False Rejection Rate (FRR) can your product achieve when configured to have a False Acceptance Rate (FAR) of at most 0.002%?
A.1.22	How does your solution mitigate potential issues in the form of bad actors using deep-fake or equivalent subversive technologies?

A.2 – Other Functional Requirements	
A.2.1	What Platforms does your solution support?
A.2.2	What integration options are available out of box?
A.2.3	How does your solution support multi-tenancy and scalability?
A.2.4	How are new features/functionality requests supported on your product/solution roadmap?
A.2.5	What Interface modes are supported between Call Centres (CC) and Enhanced Telephone Authentication (ETA), i.e. synchronous voice stream and/or asynchronous voice sample? If your product does not support voice stream, then for Passive Authentication & Semantic Fraud Detection, does CC need to create voice sample using a software tool and forward to ETA?
A.2.6	Does Integration with CC require integration software in the CC (e.g. create sample from stream) as well as its subsequent support?

Appendix B – Subgroup 2 Questions (Non-functional requirements)

The following questions are representative of the type of information the CRA is seeking as it considers how to structure any RFP that might follow this RFI process.

Vendors must note that this list of questions is not exhaustive; vendors are invited to provide any additional information that might prove useful and/or beneficial to the CRA in preparing any subsequent RFP.

Vendors that provide written feedback may be invited to a one-on-one consultation session with CRA representatives. This session would allow vendors to provide additional feedback pertaining to this RFI as well as to explain comments made in their written submission.

B.1 – Solution universality, additional requirements, documentation and training, licensing models and solution costs	
B.1.1	Is any aspect of your solution platform dependent, or are there other hard dependencies upon which it's use is predicated?
B.1.2	Is any aspect of your solution hardware dependent, or are there hard dependencies upon which it's use is predicated?
B.1.3	Provide two examples where your solution was implemented. Include implementation time, common success factors, and obstacles in implementing this solution.
B.1.4	What type of technical documentations do you provide for your application (e.g. white paper, installation and configuration instruction, release notes, etc.)?
B.1.5	Does your solution include 3rd party or open source software? If so, please list them
B.1.6	What are the licensing models currently in place for your solution?
B.1.7	Including all hardware and software requirements, what is the pricing model for a complete voice authentication solution and fraud detection/prevention solution, including upfront deployment and ongoing maintenance costs and your average professional services and upgrade costs over 5 years? Example 1000 agents
B.1.8	What are the minimum PC system requirements for call centre agents using your solution?
B.1.9	How long is typical implementation (including developing, deploying, and customizing the solution to meet the business needs)? Does this time vary based on the scale of the implementation, and if so how?

B.1.10	Describe the different types of training you provide for this type of solution (initial / long term).
B.1.11	Are the training services available in English and French?
B.1.12	In general, how much time would it take for a user to become self-sufficient in using the system?
B.1.13	What are the activities and the type/level of expertise required to maintain the solution on an on-going basis?
B.1.14	Where do you see the future of biometric authentication?
B.1.15	How do you see the future of contact centre authentication evolving in the next 5 years?
B.1.16	Can you offer a performance model of your potential solution (number of voice prints that can be created as original enrolments per minute, validations per minute, etc.)?
B.1.17	With which contact centre platforms has your product been integrated?
B.1.18	Are you able to name other clients who have successfully implemented your solution into their process? Could you describe their onboarding considerations and what you did to alleviate pain points?
B.1.19	Can your product be deployed on-premises in a Government of Canada data centre?
B.1.20	Please describe or demonstrate the agent-facing side of the solution.

B.2 – Other Non-Functional Requirements	
B.2.1	How many solutions have you implemented for GC or Similar large organizations?
B.2.2	Is your company the Developer of the Product?
B.2.3	How many Templates, Design Patterns, Guidelines, been developed by your company. and evolved over time, for Development, Configuration, Operations of Voice Authentication solutions?
B.2.4	What is your implementation process including? • What are the roles in the Development, Implementation, Migration, and Operations of the ETA solution? • How many Subject Matter Expert resources you have?
B.2.5	What information do you need to effectively scope and provide cost estimates of your ETA solution? • Predictable: Concurrent Licence-Based Model • Usage-Based: Per Minute; Per User, Per transaction, ... • Additional Details for more accurate pricing: o Integrations (IVR, Screen pop, DB Lookups, ..) • Custom Programming and Addons
B.2.6	What are the key cost categories involved in implementation? • What is your implementation costing model? • What are the drivers for implementation costs?
B.2.7	What are the costs for the following different Voice Authentication service offerings?: • Active Voice Authentication different from • Passive Voice Authentication different from • Semantic Fraud detection • Historical Fraud Detection • Black listing, • ANI • Other