

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



**THE STATE OF ISRAEL
THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE -
THE GOVERNMENT IT AUTHORITY –
THE E-GOVERNMENT UNIT**



**PUBLIC RFI NUMBER – 001/2015
REQUEST FOR INFORMATION –
IDENTITY MANAGEMENT AND SINGLE SIGN-ON
APPLICATIONS
(IdM, SSO)**

**THIS DOCUMENT IS THE PROPERTY OF THE STATE OF ISRAEL
ALL RIGHTS RESERVED TO THE STATE OF ISRAEL**

**THE INFORMATION CONTAINED IN THE DOCUMENT SHALL NOT BE
PUBLISHED, DUPLICATED OR USED IN ITS ENTIRETY OR
PARTIALLY, FOR ANY PURPOSE WHATSOEVER APART FROM IN
REPLY TO THIS REQUEST FOR INFORMATION**

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



**REQUEST FOR INFORMATION (RFI) NUMBER 001/2015–
IDENTITY MANAGEMENT AND SINGLE SIGN-ON APPLICATIONS
(IdM, SSO)**

PART 1 – GENERAL/ADMINISTRATION

1. **GENERAL:** The E-Government Unit at the Government IT Authority at the Prime Minister's Office (hereinafter: "**the Requester**"), wishes, pursuant to the provisions of Regulation 14A of the Mandatory Tenders Regulations 5753 – 1993, to receive information from Israeli or foreign vendors, with local and international knowledge and experience (hereinafter: "**the Informants**"), about products for identity management (IdM) and single sign-on (SSO) applications (hereinafter: "**the Product/the Product**"), within the framework of an evaluation of the development and implementation of a technological infrastructure for use by citizens, residents and businesses that are in contact with the Government, receive services from it and interact with it, as well as for the Government employees (hereinafter: "**the Request**").

2. **SCOPE OF THE REQUEST:**

The Requester is requesting that the Informants shall submit a reply to the Request for Information (RFI). The reply should contain the following components:

- 2.1 Information with regard to the Products, including the hardware components, software, applications, communications and data security, for identity management and single sign-on applications and the use thereof (hereinafter: "**the Solution**").

- 2.2 A description of the Informants' capability and experience in providing the Solution.

- 2.3 Details regarding the method of providing the Solution.

- 2.4 **The possibility** of a demonstration – RFD (Request for Demonstration).

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



3. **CLARIFICATIONS:**

- 3.1 **This Request is a preliminary request to receive information only, and it does not constitute a phase in an engagement of one kind or another with any of the Informants replying to the Request. It should be emphasized that the Request does not constitute any undertaking of the Requester to continue in this process, in any way whatsoever, and it does not constitute a tender and/or invitation to submit bids and/or the establishment of a vendors' list. All the expenses involved in submitting the information shall be the sole responsibility of the Informant and the Informant shall not be entitled to any compensation or indemnity in respect of submitting the reply to the Request.**
- 3.2 **The Requester does not undertake to use the information, in its entirety or partially, for the purpose of preparation of the tender, or for any other purpose.**
- 3.3 **Conveying the information does not bestow upon the Informant any right vis-a-vis the Requester and does not impose any obligation whatsoever upon the Requester.**
- 3.4 The contents of this document do not constitute any undertaking to publish a tender in the matter as aforesaid, or any undertaking vis-a-vis the specification of the tender insofar as such may be published.
- 3.5 The Requester shall not be responsible for any payment or expense that the Informant may incur in respect of this Request and consequent upon the contacts with it, if any are held, within the context of evaluating the information, a demonstration or within any other context in this matter.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



3.6 The Requester shall be entitled to convey any information or datum connected to the information submitted to any person who is connected to the Requester and also to publish by way of a tender or in another way, specifications or characteristics that shall be based upon the information that may accumulate as a result of this process.

3.7 If a tender is published in connection with this Request, and without any undertaking to publish one as aforesaid, a reply to the Request shall not constitute a condition for participation in the tender, shall not grant any advantage to anyone who has replied to the Request merely due to the fact that it has replied to the Request, and shall not entail its participation in the tender or engagement with it in any other way.

4. **DEMONSTRATIONS:**

4.1 The Requester may, but is not obliged to, request that the Informant shall present the Products within the framework of a demonstration before a professional team on its behalf.

4.2 Demonstration of the Solution, if it will take place, shall constitute part of the Request and shall be subject to the contents thereof.

4.3 See the specification in Part 2 below.

5. **PUBLICATION OF THE REQUEST FOR INFORMATION DOCUMENTS:**

5.1 The documents shall be published on the website of the Government Procurement Administration at the Accountant General's Department (hereinafter: "**the Website**") at the address www.mr.gov.il under the heading: Tenders / (RFI) Number 001/2015 - Identity management and single sign-on applications (IdM, SSO).

5.2 The documents shall be available at the Website with effect from **Monday, 11/01/16.**

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



6. **CONTACT PERSON:** The contact person on behalf of the E-Government for the Request for Information, to whom all clarifications and questions should be addressed, is: Mr. Dov Horovitz, Telephone: 02-6664842, fax: 02-6664650, e-mail: dov@gov.il.

7. **PROCEDURE FOR SENDING CLARIFICATION QUESTIONS REGARDING THE REQUEST:**
 - 7.1 Interested Informants may refer questions and requests for clarification to the contact person's e-mail address, as aforesaid in Section 6.
 - 7.2 Questions that arrive before **Thursday, 21/1/16, at 14:00** shall be replied to.
 - 7.3 The Informant is requested to relate in the questions to the section number in Part 2.
 - 7.4 The Informant should ascertain that its questions have reached the contact person in their entirety.
 - 7.5 **A reply to the clarification questions shall be sent before Thursday, 28/1/16.**

8. **METHOD OF SENDING THE REPLY:**
 - 8.1 The Reply to the Request for Information should be sent by electronic mail, to the contact person's e-mail address, before Monday, **8/2/16** at **15:00**.
 - 8.2 The Reply shall contain documents in PDF format **and also in MS-WORD** or RTF.
 - 8.3 The Informant is requested to ascertain with the contact person that the Reply has been received.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



9. **CONTENTS OF THE REPLY:**

9.1 The details specified in Part 2 of the Request should be submitted.

9.2 The technical questions appearing in Part 2 of the Request, and all sub-sections thereof, should be addressed, and every sub-section should be answered in accordance with the Solution proposed by the Informant, whether they are explicit questions or a functional description.

9.3 Any material, documents and additional reply may be submitted, at the Informant's discretion.

10. **OWNERSHIP OF THE DOCUMENTS AND THE REPLY AND THE USE THEREOF:**

10.1 The Request document is the intellectual property of the Requester that is sent for the purpose of the Reply to the Request for Information.

10.2 The Reply document is the intellectual property of the Informant. Nevertheless, the Requester shall have the possibility of using the Information that is provided within the framework of the Reply for any purpose connected to its activity and the Informant shall have no claims in connection with the copyrights in the information.

THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT



REQUEST FOR INFORMATION (RFI) NUMBER 001/2015–
IDENTITY MANAGEMENT AND SINGLE SIGN-ON
APPLICATIONS (IdM, SSO)

PART 2 – SPECIFICATION OF THE
INFORMATION REQUESTED

1. **BACKGROUND:**

- 1.1 The E-Government Unit at the Government IT Authority at the Prime Minister's Office (hereinafter: "**the Requester**"), wishes to evaluate the possibility of purchasing and implementing Products for identity management and single sign-on applications (IdM, SSO) that comply with the requirements set out in detail below (hereinafter: "**the Solution**"), and hereby invites suppliers of Products in this field to submit a Reply to this Request for Information.
- 1.2 The Requester wishes to receive information from the Informants that have the appropriate knowledge and expertise regarding their experience in the development, marketing and implementation of Products for identity management and single sign-on applications (IdM, SSO).

2. **THE INFORMANT'S DETAILS:**

- 2.1 The Informant's name _____
- 2.2 Corporation's enrolment number _____
- 2.3 Place of corporation's enrolment: in Israel/abroad (state the name of the country):

- 2.4 Corporation's offices' address: _____
- 2.5 Corporation's offices' telephone: _____
- 2.6 Corporation's offices' fax: _____

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



- 2.7 Electronic mail address: _____
- 2.8 Website address (if any) _____
- 2.9 Year of foundation: _____
- 2.10 Details of representative/contact person for Reply to the Request for Information:
- 2.10.1 Name: _____
- 2.10.2 Position: _____
- 2.10.3 Mobile telephone: _____
- 2.10.4 E-mail: _____

3. SPECIFICATION OF THE PROPOSED PRODUCT:

- 3.1 The Informant shall describe its involvement, expertise and experience in the development, marketing and implementation of Products in the field of identity management and single sign-on applications (IdM, SSO) (hereinafter: - the Product/ the Products).
- 3.2 Insofar as these are existing Products, the Informant shall confirm that it is the manufacturer and holder of the intellectual property, or present a confirmation from the manufacturer that the Informant is an authorized distributor of the Product it proposes.
- 3.3 The Informant should attach a comprehensive description of the Products.
- 3.4 It should be clarified that more than one Product relevant to this field may be proposed.
- 3.5 The following details should be specified **with regard to each** Product:
- 3.5.1 The Product's name: _____
- 3.5.2 The manufacturer's name: _____
- 3.5.3 The Product's present version/revision: _____
- 3.5.4 The year that the products' distribution commenced: _____

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



3.5.5 A brief description of the use of the Product (it is recommended to expand in a separate Appendix):

3.5.6 A list of countries and projects where the Product is implemented (it is recommended to expand in a separate Appendix):

3.6 A technical description of the Product: a technical description of the Product should be attached.

3.7 A description of the proposed Solution: An explanation regarding the proposed architecture and how it may be integrated into existing infrastructures on the basis of interfaces and standards, should be attached.

3.8 Supporting the standards: The Informant should state what are the Israeli standards, the international standards, the accepted protocols, and the standards of voluntary organizations (such as – the FIDO Organization standard), that the Product supports.

3.9 Standards compliance tests: Insofar as standards compliance tests have been conducted (according to the specification in Section 3.8 above), a specification of these tests should be attached for the purpose of proving compliance with the standards.

3.10 Data security tests: Subsequent to the previous section, in particular compliance with data security standards and penetration tests (PT) should be noted.

3.11 Performances: The Product's performances should be noted, according to relevant parameters and a referral to load tests conducted by competent bodies.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



3.12 Previous and existing applications in the Product: Examples of countries and projects where the Product is used should be specified, subsequent to the aforesaid in Section 3.5.6, specifying **the scale of the identities that the system** manages, the number of transactions per time unit, and the contact persons for the purpose of referral to these projects and reference to the use of the standards mentioned in Section 3.8 above.

3.13 Further details:

3.13.1 Further details may be provided, at the Informant's discretion.

3.13.2 In particular, details may be provided, at the Informant's discretion, with regard to the prices of the licenses for use of the Product, and the method of costing, also with regard to ranges of costs (e.g. – according to the number of users, according to actual usage, according to a "one-time organizational installation", quantities' discount, any other method).

3.14 Demonstration:

3.14.1 Insofar as a demonstration is required, specific guidelines shall be provided with regard to the location of the demonstration, the duration of the demonstration and the method of performing it.

3.14.2 The location of the demonstration may be at the Requester's offices, at the Informant's offices, or using a remote demonstration technique via video conference, at the Requester's discretion and after coordination with the Informant.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



3.14.3 The demonstration shall include at least three scenarios:

3.14.3.1 A scenario of the user's experience (UX) at the enrolment phase, at the issuance of the credentials phase and at the phase of the online authentication transaction itself.

3.14.3.2 A scenario of the operation of the Product by an administrator and the possibilities that the Product offers it.

3.14.3.3 A scenario of external interfaces with other systems.

3.14.3.4 Additional scenarios as proposed by the Informant at its discretion.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



4. THE REQUESTER'S REQUIREMENTS FROM THE PRODUCT:

4.1 OBJECTIVES AND TARGETS – GENERAL:

4.1.1 The Requester's objective is to evaluate a road-map towards the implementation of a system of identity management and single sign-on applications (IdM, SSO), in the E-Government unit, in particular for the citizens, residents and businesses, that apply for Government services, but also for Government employees, from different access channels to the services, including browsing on Internet sites, access from mobile devices in general and from "wearables" means in particular.

4.1.2 The Requester's intention is to develop a single sign-on infrastructure for citizens, residents and businesses, and also for government employees, for the purpose of delivering services. The intention is to enable the service provider to define the levels of assurance¹ that are required for each service in the authentication process, and subsequently to define authorization for users insofar as this is required.

4.1.3 An example of the authorization system is to allow access to a particular internal blog only to X particular users, or to allow data entry in a particular service only to whoever has previously specifically registered for this service.

4.1.4 The Informant should present how the authentication level of assurance is defined for each service, and also how the authorization module is operated.

¹ See also Section 4.3 below.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



4.1.5 One of the system's components shall permit the generation and/or the issuance of credentials on the basis of pre-defined parameters for access to the system, that are a derivative of the level of assurance. For example – a single password that will be permit authentication for all Government services.

4.2 **THE ANTICIPATED USER EXPERIENCE (UX):**

4.2.1 The user shall access any Government website, for the purpose of receiving any service, by clicking on the appropriate web link.

4.2.2 The service shall examine the user's level of assurance. If he is not yet enrolled into the system, he shall be referred to the enrolment process. Thereafter the user's identity shall be examined against the identity provider. Likewise the user's level of assurance shall be examined by the service in accordance with its level of assurance.

4.2.3 If there is conformity between both levels of assurance, and the identity is authenticated, it will be possible to proceed to the service itself.

4.2.4 The intention is that it shall be possible to route any user, in accordance with the processes to be specified (e.g., work flow and a so-called "logical constitution"), in accordance with the input data.

4.2.5 In the enrolment process, the solution provided for the record management for each resident for his identification and authentication to the Government should be presented, including a solution for the possible management of user names and passwords in the Government, in a centralized mode.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



- 4.2.6 The system shall allow interfaces to external information systems for the purpose of ascertaining the user's attributes (such as against other Government databases, subject naturally to appropriate legal authorization).
- 4.2.7 The system shall permit a particular user's details/attributes to be deleted, upon a user's initiative and/or by the system manager.
- 4.2.8 The system shall support all levels of assurance, and the use of appropriate credentials, including user name and password, OTP, smart card or other token, based upon the enrolment process, and in accordance with the directives and procedures prescribed.
- 4.2.9 The applicant should note what is the system's support to determine a password's strength, or its' ability to test it, in case the user selects a password.

4.3 **AUTHENTICATION LEVELS OF ASSURANCE:**

- 4.3.1 The intention is that there shall be a generic definition of the authentication levels of assurance within the framework of a national secure identification policy.
- 4.3.2 Every service provider/ministry shall be responsible for defining the authentication level of assurance for the services it provides.
- 4.3.3 At the same time, there shall be a definition of the technological solutions that comply with every authentication level of assurance, within the context of the enrolment processes, credentials management and the authentication transactions themselves.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



4.4 **CREDENTIALS:**

- 4.4.1 A Solution shall be required for the various types of smart cards, tokens, and also for access from mobile / wearable devices (e.g., a "smart watch").
- 4.4.2 The Informant should relate in particular to the support for an electronic identity card (eID) and a public key infrastructure system (PKI).
- 4.4.3 It should be clarified that the solution is not confined to services and websites that shall be hosted in the server farm in the E-Government Unit, but also to services that shall be hosted in an external infrastructure, and in this use-case the Informant should present how the trust relations between them will be formed.

4.5 **SPECIAL REQUIREMENTS – GENERAL:**

- 4.5.1 "CONTINUED AUTHENTICATION": "Continued authentication" shall be possible during a transaction, that is to say – beyond the authentication at the beginning of a transaction, authentication could also take place at certain time points during the course of the transaction, such as – in a transition to a nested transaction, or according to another profile.
- 4.5.2 WORK FLOW: It shall be possible to define the work flow of the enrolment process, the issuance of credentials and the online authentication transaction itself.

**THE STATE OF ISRAEL – THE GOVERNMENT OF ISRAEL –
THE PRIME MINISTER'S OFFICE
THE GOVERNMENT IT AUTHORITY – THE E-GOVERNMENT UNIT**



4.6 **SSO – SPECIAL REQUIREMENTS:**

4.6.1 Full support of SAML 2.0 is required. Informants should relate to other protocols such as OAuth and Open-ID Connect.

4.6.2 Credential federation is required, namely – the possibility of transition between domains during the course of the SSO process even though they are not physically hosted in the E-Government Unit servers farm.

4.6.3 The issuance of the token with the credentials to the user, so that it will be possible to transfer the token between different environments.

4.6.4 Multi-platform support on the service providers' side, for the purpose of transferring credentials/tokens.

4.6.5 **PRODUCTION OF REPORTS AND CONTROL:** The option of obtaining detailed reports with regard to system performance and its operation, such as – which service was delivered, which user had access to the service, the service's availability hours, loads, failed authentication attempts (data security aspects).

4.6.6 **DATA SECURITY:** Reporting on data security events including information and logs transfer to an external SIEM system.

4.6.7 **AVAILABILITY AND RECOVERY:**

4.6.7.1 High availability and redundancy support.

4.6.7.2 Support for data back-up and recovery (DR) site, including decentralization into several physical sites, in an ACTIVE-ACTIVE mode.