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

PUBLIC RFI NUMBER – 002/2015
REQUEST FOR INFORMATION – ELECTRONIC AUTHENTICATION AND DIGITAL SIGNATURE APPLICATIONS IN MOBILE DEVICES

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THE INFORMATION CONTAINED IN THE DOCUMENT SHALL NOT BE PUBLISHED, DUPLICATED OR USED IN ITS ENTIRETY OR PARTIALLY, FOR ANY PURPOSE WHATSOEVER APART FROM IN REPLY TO THIS REQUEST FOR INFORMATION

REQUEST FOR INFORMATION (RFI) NUMBER 002/2015– ELECTRONIC AUTHENTICATION AND DIGITAL SIGNATURE APPLICATIONS IN MOBILE DEVICES

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 electronic authentication and digital signature applications for mobile devices (hereinafter: "**the Products/the Product**"), within the framework of an evaluation of the development and the 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. **CONTENTS OF THE REQUEST:**

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

2.1 Information with regard to the Products, including the hardware components, software, applications, communications and data security, for electronic authentication and digital signature and applications for mobile devices 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).

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 details 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 examining the information, a demonstration or within any other context in this matter.

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 it 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 present the Products within the framework of a demonstration before a professional team on its behalf.

4.2 Demonstration of the Solution, if it takes 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) 002/2015 - Electronic Authentication and Digital Signature Applications in Mobile Devices.

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

6. **CONTACT PERSON:** The contact person on behalf of the E-Government Unit 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 will 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.

9. **CONTENTS OF THE REPLY:**

9.1 The Informant details set out 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 transferred for the purpose of 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 intellectual property in the information.

REQUEST FOR INFORMATION (RFI) NUMBER 002/2015– ELECTRONIC AUTHENTICATION AND DIGITAL SIGNATURE APPLICATIONS IN MOBILE DEVICES

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 electronic authentication digital signature applications for mobile devices that comply with the requirements set out in detail below (hereinafter: "**the Solution**"), and hereby invites vendors 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 electronic authentication and digital signature applications for mobile devices.

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: _____

2.7 Electronic mail address: _____

2.8 Website address (if any) _____

2.9 Year of foundation: _____

2.10 Details of representative/contact person for the Reply to Request for Information:

2.10.1 Name: _____

2.10.2 Position: _____

2.10.3 Mobile telephone: _____

2.10.4 E-mail: _____

3. DETAILS OF THE PROPOSED PRODUCT:

3.1 The Informant should give details about its involvement, expertise and experience in the development, marketing and implementation of Products for electronic authentication and digital signature applications for mobile devices. The Reply should distinguish between mobile telephones and other mobile devices, such as tablets, i-pads, wearable computing etc.

3.2 Insofar as these are existing Products, the Informant should present confirmation that it is the manufacturer and holder of the IP/copyrights, or 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 Product it proposes, with reference to the Requester's demands and requirements from the Product as set out in detail in Section 4 below.

3.4 It should be clarified that more than one Product relevant to this field may be proposed/presented.

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: _____

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 applied (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 should be attached regarding the proposed architecture and how it may be integrated into existing infrastructures on the basis of interfaces and standards.

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 performance parameters and a referral to loads' tests conducted by competent bodies.

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, 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 regards to ranges of costs (e.g. – according to number of users, according to actual usage, according to a "one time organizational installation", quantities discount, or any other method).

3.14 Demonstration:

3.14.1 Insofar as a demonstration will be required, specific guidelines will 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 with coordination with the Informant.

3.14.3 The demonstration shall include at least three scenarios:

3.14.3.1 Conducting the enrolment process.

3.14.3.2 Conducting electronic authentication process from the mobile device.

3.14.3.3 Conducting the digital signature process from the mobile device.

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

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 deployment of electronic authentication and digital signature in mobile devices, in accordance with the existing technological alternatives in the market. The supreme objective is to provide a technological solution for smart phones, tablets, other field devices and "wearable computing" of one kind or another, for executing strong identification and authentication of the user, and creating digital signatures that complies with the State of Israel's common standards. Examples of implementation for government IT systems could be forms in the forms service, payments and in various websites.

4.1.2 The assumption is that smart eID cards will be issued for all citizens and residents of the State of Israel with an authentication certificate (already presently in effect and use) and digital signature certificate (in the course of realization); at the same time – "Tamuz" (computerized access and identification smart cards) containing an authentication certificate are issued for government employees and there will hold digital signature certificates (in the future). Likewise, there are authorized signatories in organizations who are identified by various methods, but this RFI will not deal with this population.

4.1.3 The Informant should specify separately its proposal with regard to mobile telephones, tablets, other end-user devices and "wearable computing".

4.1.4 The supreme objectives are to provide a solution for strong authentication of the user upon access to systems requiring strong authentication and to combine the digital signature capability in a mobile device, for example – to sign forms in the forms server, and on websites in general.

4.1.5 The Product shall support the Hebrew language.

4.2 **METHOD OF WRITING THE DIGITAL CERTIFICATE ONTO THE MOBILE DEVICE:**

4.2.1 The method of using the remote enrolment module ("Mobile RA").

4.2.2 The proposed method of communication between the Certificate Authority (CA) and the mobile device.

4.3 **METHOD OF STORING THE PRIVATE KEY AND THE DIGITAL CERTIFICATES IN THE MOBILE DEVICE:**

4.3.1 Storage in a Secure Element.

4.3.2 Storage on a USIM.

4.3.3 Storage by an application (HCE).

4.3.4 Storage on a detachable device (e.g., USB stick, secured memory card).

4.3.5 Storage on a server/ HSM (or in another remote hardware component).

4.3.6 Storage by another method.

4.4 **A POSSIBLE CONNECTION BETWEEN A DIGITAL CERTIFICATE ON A MOBILE DEVICE AND THE NEW NATIONAL eID CARD OR "TAMUZ" CARD:**

4.4.1 The State of Israel has begun to issue smart eID cards, based on smart cards, that contain, inter alia, an electronic authentication certificate and a digital signature certificate that are installed on the chip in the smart card (at this stage only electronic authentication certificates are issued).

4.4.2 Concurrently, "Tamuz" cards are issued to government employees on which an electronic authentication certificate and a secured digital signature certificate are issued.

4.4.3 Authentication and digital signature may be executed by the smart cards – both the new eID card and the "Tamuz" card.

4.4.4 The Informant, if the Solution it proposes relates to such a connection, should relate to the question of how it is possible to connect between the electronic authentication certificate and the digital signature certificate, respectively, on the new eID card or on the "Tamuz" card, and digital certificates of the same person in his mobile device (when a person may have more than one mobile device). For example – by "derived credentials".

4.4.5 The Informant should propose the solutions it proposes for this issue, both on the logistical level and on the physical level, for example – by external card readers connectable to the mobile device, by a secured process including at first identification via the smart card, by a repeated physical appearance at kiosks, or by other solutions.

4.5 **A SPECIFICATION OF THE PRODUCT'S CHARACTERISTICS FOR ELECTRONIC AUTHENTICATION:** Please specify the following details:

4.5.1 What operating system is used?

4.5.2 Standards' support;

4.5.3 The system current version;

4.5.4 Use cases.

4.5.5 Please note the number of previous versions of the Product;

4.5.6 What are the main issues of the changes between the different versions?

4.5.7 What are the considerations and requirements for issuing new versions?

4.5.8 The time period between issuing new versions;

4.5.9 Backwards version support policies.

4.6 **CHARACTERISTICS OF THE DIGITAL SIGNATURE PRODUCT:** Please specify the following details:

4.6.1 What operating system is used?

4.6.2 Standards' support;

4.6.3 The system current version;

4.6.4 Use cases.

4.6.5 Please NOTE the number of previous versions of the Product;

4.6.6 What are the main issues of the changes between the different versions?

4.6.7 What are the considerations and requirements for issuing new versions?

4.6.8 The time period between issuing new versions;

4.6.9 Backwards version support policies.

4.7 **MODE OF INTERFACING TO THE INTERNET INFRASTRUCTURE:** There is a requirement for systems that are based upon strong identification via a smart card, for example – protected Internet systems in MICROSOFT environment. A solution to this should be presented.

4.8 **PAYMENTS BY MOBILE DEVICES:** Insofar as there is support in the Product to electronic payments, independent of authentication and digital signature, the Informant should note the use of payments using a secured electronic wallet.

4.9 **SUPPORT FOR MOBILE OPERATING SYSTEMS:** The Informant should specify the extent of support of the leading mobile operating systems on the market, such as – iOS, Android, Windows etc.

4.10 **REQUIREMENTS FOR THE END USER DEVICE:**

4.10.1 The Informant should note hardware requirements from the end user devices, and any additional requirements from the end user device, for the purpose of operating the proposed system.

4.10.2 The Informant should relate to the physical protection of the certificate storage component, or any kind of monitoring of tampering to the physical component, for example – when the device is repaired by a technician etc.

4.11 CRYPTOGRAPHIC REQUIREMENTS:

4.11.1 The Informant should specify the types of enciphering supported.

4.11.2 The Informant should specify support of hashing. Support of SHA2 or equivalent is required.

4.11.3 The Informant should note the maximum RSA key length and support for RSA 1024, 2048 and 4096.

4.11.4 The Informant should note the maximum ECC key length.

4.12 ARCHITECTURE:

4.12.1 The Informant should present support for a local solution on the device that does not require cloud infrastructures for operation, and also supports offline operation.

4.12.2 The Informant should present support for a central solution based upon cloud infrastructures (if relevant).

4.13 **OPERATIONAL AND MONITORING PROCESSESS:**

4.13.1 The Informant should present support for a "life cycle" of a digital certificate, from the issuance through support of CRL and OCSP, or an equivalent method of revoking/cancelling a revoked certificate, when this is required.

4.13.2 The Informant should present the method of monitoring the issuance process at the device level, including accesses to the certificates, creation and revocation.

4.13.3 The Informant should note whether there is a connection to MDM systems for the management of certificates on the organization devices.