Reference: Clarifications – 1
Date: 28/1/16

To: Public RFI 001/2015 – participants

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

Attached are the clarifications to the RFI documents, as compiled by the e-gov unit.

It is hereby clarified that the clarifications in this document are a supplement to the RFI documents, unless otherwise stated.

1. Following is the detailed questions and clarifications table:

Clarification	Question	section	No.
As mentioned and clarified in the RFI documents, the system is intended primarily for the residents/ citizens of the country, but also for government employees themselves. The informant may present information regarding both sections and just one of them, if the proposed product supports only one section.	SSO solutions could be roughly divided into two categories: • Web SSO which is a solution for Web applications only, but is usually without an agent. It does not support other applications such as SAP, or 3270 Mainframe, but enables SSO from every device and location. • Enterprise SSO which is a solution that enables SSO execution for any kind of application such as Web, Client/Server, Legacy etc., but requires an agent at the end-point station, and therefore is implemented mainly for internal enterprise use. In order for us to know which solution to propose to you, could you clarify whether your intention is for an internal enterprise SSO for any kind of application by the employees, or perhaps Web SSO intended for citizens for external access? I'll appreciate if you could elaborate on this.	general	.1
The intention is to supply services for all of the citizens of the State of Israel.	Please could you elaborate on the quantity you would be looking at?	general	.2

Clarification	Question	section	No.
It means a potential of 6 – 8 million residents.			
See question 2 above.	How many users (identified as entities, users or companies) is targeted for the platform?	general	3
It is not possible for us to estimate this parameter at this stage.	How many connections are expected on a daily basis?	general	4
The intention is that all of the government applications and services for the citizens will be under SSO.	How many applications are available in the E-Government system? And how many would be subject to the SSO?	general	5
The RFI seeks solutions also for these kinds of SSO.	Are we expected to deliver other forms of SSO (web SSO, Web Service etc.)?	general	6
The reference is to wearables such as a "smart watch" that could be used for authentication, e.g. access control, or as long as these means make use of relevant operating systems and applications for authentication. This definition is general, it is not compulsory. The informant may relate to any wearables for which he has a relevant solution.	What is the meaning of "wearables computing" in relation to authentication and access control? Are there any specific wearables we should relate to?	4.1.1	7
It has not been decided yet. It is one the objectives of the RFI to look for such a product	An "identity provider" is mentioned (4.2.2), what product is it?	4.2.2	8
All types of tokens and smart cards compliant with ISO 7816 and specifically the new eID card.	Which token the client would like to use?	4.2.8	9
The intention in this section is to the definition of Level of Assurance (LoA), which is not "level of information security", but to the LoA in their common meaning, e.g. in a	The definition of the level of data security on which any organization may decide, is subject to the authentication standards.	4.3.2	10

Clarification	Question	section	No.
scale of 1 to 4 according to ISO 29115. The definition of the LoA for a specific service is done on account of the service provider. The credential will comply with the requirements of the respective LoA.	What is the intention? What is included under the header of "level of data security" in respect to the RFI?		
The requirements relate specifically to the new eID card, but there could be other means. The response could assume devices compliant with common standards such as ISO 7816, ISO 14443 etc.	We would like to find out what types of token the client would like to use? Also – what types of smart cards should be addressed?	4.4.1	11
It is a smart card compliant with ISO 7816.	What is the token type of the eID?	4.4.2	12
The requirement is functional and could be addressed in different ways. There is no preference to a specific solution at this stage.	Does the request relate to a response to the URL only in the workstation or also on the server side? Also, is it possible to identify the URL as different addresses?	4.5.1	13
This is definitely the intention.	Are all the Government website compatible (or will be) with proposed SSO standards (namely, SAML 2.0, OAuth or OpenID Connect, see 4.6.1)?	4.6.1	14
It is related to transfer of tokens between different environments, as "federation", including which could be government of commercial environments.	What is the meaning to "different environments"?	4.6.3	15
No extensions will be granted.	Is it possible to extend the date for questions and clarification?		16

Sincerely Yours

Dov Horovitz
Tender Committee Secretariat

This document is an integral part of public RFI 001/2015