Chapter 2

Specification of the scope of the services

Note: The Ministry intends to translate this chapter as a service and for the convenience of the bidders/vendors. It is hereby clarified that in the event of any discrepancies between the Hebrew original and this translation, the Hebrew original shall take precedence. The Ministry is not responsible for the truthfulness and/or the accuracy of the translation and any reliance on the translation is solely under the responsibility of the bidder/vendor.

1. Required system specifications

1.1. General

A. As part of the provision of different services to the citizens by the government, and in particular in inter-ministerial work processes, the citizens or the government require to sign different electronic communications, including different documents and files.

B. The Government ICT Authority wishes to set up a central system that will issue electronic signatures that will serve both the citizens and the government ministries during the provision of the services to the citizen, with the intention to make accessible, in the best possible manner, the services to the citizens in online and digital form.

C. The following are the main types of the actions that the system is required to perform:

1) Signing different files and electronic messages – for the citizens, for the purpose of signing files and communications, for the purpose of their submission to the government ministries.

2) Signing with personnel keys or corporate e-seal – for the employees in the offices, the government ministries and administrative units that sign in the name of the organization where they work, in a specific signing procedure.

3) Machine signatures – for government ministries and the administrative units, for their signature in a corporate e-seal in a process that includes a collection of documents (batch) or a single document, without manual intervention or user's approval for each signature, however only for the entire task. For example – for the purpose of issuing signed certificates to the citizens.

4) Signatures of different representatives, such as of corporations – companies, associations etc. (that constitute a legal entity) and entities in the private sector, when the representatives can be lawyers, accountants, legal guardians, whoever received a judicial order or by delegation of authorities etc. vis-à-vis the different government ministries and its units.

D. The system is designated for digital signing on all file types, without using a smart card for the purpose of executing the electronic signatures itself, and with the option to execute electronic signatures in different mobile appliances, such as smartphones, tablets etc.

E. The vendor will supply the system, when the system includes all features, properties and components that are included in the answers the vendor provided in its bid, including the entire mandatory components listed hereunder and the entire quality components that the vendor declared that are included in the system in its response to the Tender.

F. The system will be based on an existing product. The system will be set up and will be integrated in the existing e-Government infrastructures in the Government ICT Authority including the government identification system, the information system, the CA services of e-Government, the private area, the information security infrastructures and the command and control infrastructures.

G. The system will allow the Ministry, the government ministries, the administrative units and other users, as the case may be, to receive as input electronic messages (such as – documents), both those represented in the government units as stated above and those received from citizens and representatives and that are transmitted and received in accordance with the legislation regarding electronic signatures (both in the Electronic Signature Law 5761-2001 (hereinafter: the "Electronic Signature Law") and the regulations promulgated thereunder, and specific laws referring to electronic signatures and to sign them electronically and enable the authentication of the signature.

H. The vendor will set up the system in such manner that the system will comply with the requirements of a secure signature in accordance with the Electronic Signature Law and in accordance with the guidelines of the Privacy Protection Authority in the Ministry of Justice (the "PPA"). For that purpose, the Ministry will make available the system for the inspection and approval of the PPA, in accordance with the provisions set forth in section 5.4 of this Chapter hereunder.

I. In addition, the Ministry intends to operate the system in a format of "approved signature" in accordance with the provisions of the Electronic Signature Law. The vendor will be required to assist the Ministry within the framework of this activity, as part of the services that will be provided within the framework of a tender, according to the requirements laid down by the Ministry, as stated in sub-section J hereunder.

J. In the event the Ministry acts for the purpose of obtaining certification by the PPA for the approval of the system in a format of "approved signature" the vendor will provide and assist in anything related to this matter, according to the guidelines set out by the Ministry.

K. According to the demands presented by the Authority or the Ministry, before starting production, the vendor will provide documents that describe the technology, including a certificate of conformance to the customary standard, if any, and an opinion of an information security expert regarding the reliability of the technology, in accordance with the requirements laid down in section 9(a) of the Electronic Signature Regulations (Secure Electronic Signature, Hardware and Software Systems and Review of Requests) 5762-2001.

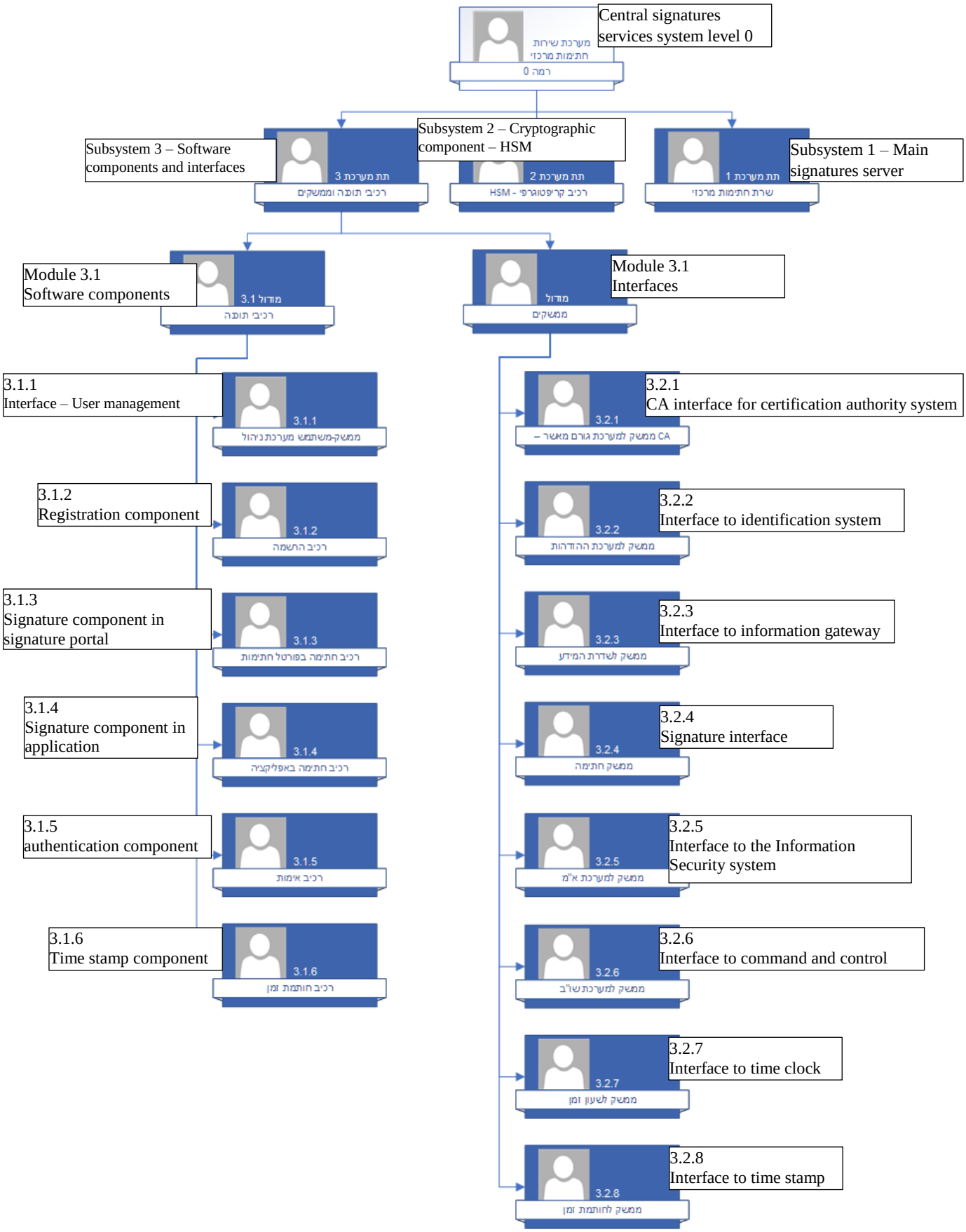
L. If, on the supply date of the system, during the acceptance tests or at any other stage during the term of engagement, it transpires that any of the mandatory components or the quality components in respect of which the vendor declared that they exist, and the Ministry did not disqualify the bid in accordance with the provisions set forth in the Tender documents, however demanded from the vendor to make good the missing materials, the vendor shall be obligated to complete the missing materials immediately or according to the demands made by the Ministry, in the facilities of the Ministry, in the development environment that the vendor will provide.

M. The Ministry estimates that the scope of use of the system will be gradual, when first the scope of use will be low and will increase over time. The Ministry cannot assess the period of time for the purpose of using the system, however according to its estimate the scope of use according to the reasonable number of users who are registered in the system at a certain point in time is as stated in the table in section 2.5 of Chapter 5.
It is clarified that the "**probable use**" will be used only for the purpose of setting a weighted price for a bundle, as stated in section 4.3.5 in Chapter 1 and the aforesaid shall not oblige the Ministry to commit to an actual scope of use.

1.2. Bill of materials and system components

1.2.1. System bill of materials

It is clarified that the bill of materials displayed hereunder is logical only. The vendor shall be entitled to offer a system with a different bill of materials provided that the system includes all the necessary components. It is necessary to present the response with respect to the structure of the bill of materials of the system in section 10, **Appendix B** in Chapter 3 of the Tender – "Affidavit regarding compliance with professional threshold conditions, mandatory requirements and quality requirements."


Central signatures services system level 0
מערכת שירות חתימות מרכזי
רמה 0
Subsystem 3 – Software components and interfaces
Subsystem 2 – Cryptographic component – HSM
Subsystem 1 – Main signatures server
3 תת מערכת
רכיבי תוכנה וממשקים
2 תת מערכת
HSM - רכיב קריפטוגרפי
1 תת מערכת
שרת חתימות מרכזי
Module 3.1 Software components
מודול 3.1
רכיבי תוכנה
Module 3.1 Interfaces
מודול
ממשקים
3.1.1 Interface – User management
3.1.1
ממשק-משתמש מערכת ניהול
3.1.2 Registration component
3.1.2
רכיב התשמה
3.1.3 Signature component in signature portal
3.1.3
רכיב חתימה בפורטל חתימות
3.1.4 Signature component in application
3.1.4
רכיב חתימה באפליקציה
3.1.5 authentication component
3.1.5
רכיב אימות
3.1.6 Time stamp component
3.1.6
רכיב חותמת זמן
3.2.1 CA interface for certification authority system
3.2.1
ממשק למערכת גורם מאשר – CA
3.2.2 Interface to identification system
3.2.2
ממשק למערכת ההזדהות
3.2.3 Interface to information gateway
3.2.3
ממשק לשדרת המידע
3.2.4 Signature interface
3.2.4
ממשק חתימה
3.2.5 Interface to the Information Security system
3.2.5
ממשק למערכת א"מ
3.2.6 Interface to command and control
3.2.6
ממשק למערכת שו"ב
3.2.7 Interface to time clock
3.2.7
ממשק לשעון זמן
3.2.8 Interface to time stamp
3.2.8
ממשק לחותמת זמן

1.2.2. System components

The following is a general description of the system components.

Architecture diagrams and additional information are attached hereunder in **Appendix 2-A** of this Chapter.

It is clarified that the description of the system components and the information provided in **Appendix 2-A** hereunder is logical only. During the detailed design it is possible that different processes, components etc. will be updated, provided that the requirements laid down in the Tender are fulfilled.

- **Subsystem for generation of keys and issuance of digital certificates** – the subsystem that is responsible for the key generation process and the issuance of digital certificates in an interface with the CA. The system will generate for each user a pair of keys – a private key for signing and a public key for authentication, will generate a CSR file (Certificate Signing Request) for the certification authority (CA) that will issue the private digital certificate that is requested for each of the users in the system. This subsystem will also handle the issuance of a corporate seal (e-seal).

- **Signatures subsystem** – the subsystem will handle receipt of the input for the signing process, the performance of the digital signing and the transfer of the deliverables to the application and interface subsystem.

- **Application components and applicative interfaces (API)** – these components will manage receipt of the identification information of users from the government identification system, will receive from the user the communications for signing, will send them to electronic signature in the signature subsystem, and will return the signed communication according to the interface, to the user, according to the usage scripts as stated in the Technology Appendix.

- **HSM (Hardware Security Modules) component** – an encryption component applied with protected software for the purpose of protecting the private signature keys in an optimal manner in terms of security and access control. If the vendor offers the required HSM component as a discrete and separate component compared to the other components listed above, i.e. – not in hard Appliance form but in a modular form by an external HSM or by the replacement/addition/upgrade of the HSM in the Appliance, the Ministry shall be entitled, at its discretion, to supply a proper HSM component independently, in lieu of the HSM component that was offered by the vendor. In such circumstances as said the costs of the HSM component will be offset from the system price accordingly. Even if the Ministry supplies the HSM component, in whole or in part, by itself, this shall not derogate from the liability of the vendor for the entire system.

2. Mandatory requirements

The vendor warrants that the offered product satisfies the mandatory requirements laid down in Appendix 1-A in Chapter 1 above on the bids' submission date. Without derogating from the aforesaid, the system will comply with the entire requirements laid down in section 2 hereunder during the entire term of engagement. To the extent that the offered product or the system do not comply with any of the aforesaid requirements, the vendor's bid will be disqualified. If, after signing the contract with the vendor it transpires that the system fails to comply with any of the mandatory requirements, the Ministry shall be entitled to terminate the contract forthwith.

2.1. System mandatory requirements

The vendor will supply the system when the system includes the following capabilities:

2.1.1. The execution of signatures transmitted to the system concurrently, and that include actions such as signing the information forwarded for signing, according to the load requirements laid down in this Tender.

2.1.2. Support of a corporate signature, granting access to specific users in a specific organization to the e-seal of that organization.

2.1.3. Support of a number of signatures of different users on a document or in general – a specific electronic message.

2.1.4. Full support of the following standards:

1) Signature standards of eIDAS (PAdES, XAdES, CAdES)

i. ASiC - ETSI TS 103 174
ii. CAdES - ETSI TS 101 733
iii. XAdES - ETSI TS 101 903
iv. PAdES - ETSI TS 102 778

2) PDF - PDF Reference 1.7 (ISO 32000-1)
3) XML-Sig/XML-Dsig according to RFC 3075
4) 4) CMS\ PKCS#7 according to RFC 2315

2.1.5. The system will generate a pair of keys based on a customary standard for asymmetric signing, that uses the following specifications, in accordance with Israeli Standard 14888 Part 2 and the equivalent ISO/IEC standard and Israeli Standard 15946 and the equivalent ISO/IEC standard respectively, or an equivalent NIST standard:

1) RSA key at a length of 2048 bits as a minimum; and
2) ECDSA key at a length of 256 bits as a minimum.

2.1.6. Application and execution of a timestamp in the system, by interfacing with a time server/atomic clock, according to RFC 3161.

2.1.7. Support of review with CRL files and support of an online interface for review of the certificate status (OCSP) as part of the signature validation procedure.

2.1.8. A management interface enabling secure login that includes a 2-factor authentication for the system administrators, and that supports a separation of roles and definition of roles.

2.1.9. The management interface will have the option to define that certain sensitive actions will require identification of two different

users or more, for example: The System Admin will be able to execute a certain action but the said action will not be executed until the Security Admin logs into the system and approves it.

2.1.10. The compartmentalization of private keys will be possible in such manner that a specific authorized user will have access to a specific private key while another authorized user will be denied access to the private key of another user.

2.1.11. Support of a high availability work form – load balances and support of backup configuration, that includes as a minimum two (2) HSM components in the main site and one (1) in the secondary site in Active/Active configuration between the sites.

2.1.12. An HSM component (integrated in an Appliance or, alternatively – external) for the purpose of protecting the users' private keys, or for the purpose of encrypting the keys database.

2.1.13. The HSM component in the system will support numbers of users as ordered according to the user increments and will enable an upgrade and support of 15 million private keys as a minimum, whether directly in the HSM component and whether in an external database that constitutes an integral part of the system, and that is encrypted by the HSM component. For the avoidance of doubt, the total number of the HSM components that will support the storage requirements and the system performance will not be greater than 12 physical HSM components in the production environment in high availability (HA) unless otherwise stated by the Ministry.

2.1.14. The proposed HSM component complies with all of the cryptographic standards as stated hereunder:

1) Certification for Common Criteria in EAL 4 level or NIST – FIPS140-2 level 3 or another standard, as stated in section 2.1.5 in Chapter 1.
2) Modes of Operation of Validation System – SP 800-20
3) Random Number Generation – SP 800-90a;
4) Israeli Standard 10118 (ISO/IEC) – Encryption Algorithm;
5) Israeli Standard 18033 (ISO/IEC) – Hash Function.

2.1.15. In the event of an attack and/or damage caused to the network appliance, it will be required to assure that the entire sensitive information that is stored on the network appliance will be zeroed.

2.1.16. Ability to interface with **e-Government Certification Authorities (CA)** (including the government certification authority – GAMAM, CA, THAMMUZ and others to the extent defined) including interfacing capability with more than one certificate authority than in standard protocols (for example: CMP, PKCS10) for the purpose of issuing digital certificates to users.

2.1.17. Applicative interface (API) with which it will be possible to transfer the user information, the type of the signature that is required, and the information itself that is intended for signing. The signed communication will also be returned through this interface.

2.1.18. Applicative interface (API) for the purpose of managing the keys and the signature certificates – an interface for the setup and the deletion of users in the system, generation of pairs of keys for each user, the creation of request files for the issuance of digital certificates (CSR) and receipt of digital certificates that include the public keys of the said users, including everything required for the purpose of managing the keys and the signature certificates.

2.1.19. Migration/conversion/reception of users and the entire information about the said users (migration).

2.1.20. In the event the protection mechanism and the API consumption of the service requires identification, including access management, it will be necessary to provide support for the purpose of identification in the OAuth2 and SAML2. For the avoidance of doubt – the vendor will be required to perform integration with the vendor of the government identification system (the IDP) of the e-Government and with the information provider of e-Government.

2.1.21. The ability to monitor the entire system components, including the ability to send alerts by Syslog and SNMP protocols.

2.2. **Volumes, loads and performance**

2.2.1. The system will be able to generate pairs of new asymmetric keys for end users, and immediately afterwards to create a Digital Certificates Request that will be sent to CA that will be defined by the Ministry in a scope of 1,000 hours as a minimum.

2.2.2. The system will enable the execution of electronic signatures, at a rate of 100 electronic processes (transactions) per second as a minimum, that will be performed by 100 concurrent users as a minimum, with a signature in an RSA 2048.

2.2.3. It is clarified that:

2.2.3.1. The system will not limit the size of the files that can be signed by an end user or any applicative system. If necessary, the system will be able to produce an extract (HASH) from the source file and send the HASH for signing and not the source file itself. The system will return afterwards to the end user or the applicative system the signed file, in a standard data structure according to the electronic signatures standards defined in the Tender.

2.2.3.2. The provisions set forth hereinabove and hereunder do not constitute any undertaking regarding the actual scope of the operations in the system. The system will support expansion options as required, and in this regard with respect to the number of users as stated in section 1, sub-section M above.

2.2.3.3. The addition of servers, configuration and modifications that will be performed by the Ministry under the limitations set out in the license will not require additional costs.

2.2.4. Performance analysis will be performed in accordance with the provisions set forth in section 5.9.4 hereunder.

3. Quality requirements

For further information regarding the quality component requirements see section 4.3.4 in Chapter 1 and **Appendix 1-B** in Chapter 1.

The vendor undertakes that the system will comply with the entire quality requirements in accordance with the vendor's declaration in **Appendix B** of the vendor's bid (Chapter 3) during the entire term of engagement. To the extent that the system fails to comply with any of the quality requirements in accordance with the vendor's declaration, the Ministry shall be entitled to disqualify the vendor's bid. If, after the signing of the contract with the vendor it transpires that the system fails to comply with the quality requirements according to the vendor's declaration, the Ministry shall be entitled to terminate the contract forthwith or, alternatively, demand from the vendor to make the necessary completions, for no extra cost in such manner that the system will comply with the necessary requirements.

4. Information security requirements

The vendor and the system will comply with information security requirements and cyber protection requirements as set out in this section hereunder.

4.1. General

4.1.1. The vendor and anyone acting on its behalf, including its employees, service providers on its behalf, subcontractors and any other party involved in the installation of the system and/or any component thereof, including its setup and maintenance – will comply with the entire requirements and guidelines regarding information security and cyber protection, whether stated in the Tender documents and whether delivered by the Ministry from time to time at any stage during the performance of the project.

4.1.2. The vendor will assure to secure the entire information that reaches its possession as part of the fulfillment of its undertakings in accordance with the contract.

4.1.3. The system – including all components thereof – will not be based on cloud services.

4.1.4. Access to the entire solution components hosted in the e-Government will be granted from the e-Government facilities; no remote access to the system or any of its components.

4.1.5. According to the demands made by the Ministry, the vendor will present and describe the entire cyber protection features of the system, both in the information security layer and in the system protection layer including all its components, and in particular from the following aspects:

4.1.5.1. The information security architecture (including "information about the information" i.e. – information, monitoring and control), including the following aspects:

4.1.5.2. Confidential information in compliance with the requirements laid down in the law and privacy requirements.

4.1.5.3. Protection of data at rest, during processing and while in motion, including METADATA aspects.

4.1.5.4. Authentication, identification and electronic signature mechanisms.

4.1.5.5. Compliance with infrastructure and applicative compartmentalization and information access permissions.

4.1.5.6. Proposed cryptographic encryption/ compartmentalization mechanisms.

4.1.5.7. Adherence to the principles for the purpose of handling information while handling a cyber event (leak and/or vulnerability and/or handling malware).

4.1.5.8. Architectural description of high availability capabilities in the same physical site and in the during e-Government sites.

4.1.5.9. The vendor will provide a description of the proposed topology components, hardware, software, middleware and hardware (if any of these are proposed) from the aspects of functional systems, monitoring and control systems, identification systems and handling with cyber events.

4.1.5.10. The vendor is required to present a comprehensive threats analysis of the system and an analysis of specific threats for each technological component (a component can include more than one component), pointing to risks, while giving score to each risk and providing a proper solution accordingly.

4.1.6. According to the requirements made by the Ministry as said, the vendor is required to describe and concentrate on cyber protection aspects, the following points:

4.1.6.1. The entire information security mechanisms included in the system, in a level of each assembly and component. The description will refer specifically to each mechanism, compared to the functionality that is required in this Tender and the description of the threats as required above.

4.1.6.2. The entire security protocols that are supported and the sub-protocols in the system vis-à-vis the functionality that is required in this Tender and the description of the threats required as stated above.

4.1.6.3. The enforcement mechanisms that can be applied in addition to the ones integrated in the system (third-party entities) including the aspects of compatibility (interoperability) between them, and the level of feasibility for the inability to realize them, or a settlement in the manner of their realization, as a result of a technological conflict.

4.1.6.4. Built-in protection mechanisms against attacks including, if any, mechanisms for the purpose of adding dedicated capabilities of the vendor, both in a manner

that mandates reverse compatibility and forward compatibility with the manufacturer's updates for the full solution and mechanisms enabling customization only in the total solution (in the unit level and in the level of the total solution).

4.1.6.5. Secure development, including secure updates – will be described in detail, including proven methodology.

4.1.6.6. Maintenance mechanisms, updates, upgrades and the manner of their secure installation.

4.1.6.7. System support, if any, in assembly level of Secure Channel & Secure Payload (including a description). The vendor is required to describe the entire considerations for the purpose of this matter.

4.1.6.8. The vendor is required to refer to each of the points stated above and state how the system provides a solution to these threats, to the extent relevant.

4.2. **Security approach**

4.2.1. The vendor will supply and install the system in accordance with the cyber protection policy documents as updated from time to time, the information security policy, the secured systems development policy, the services gateway standard (ws.gov.il), the systems administration system policy, passwords policy, hosting policy of the e-Government Unit and the rules for the purpose of performing penetration tests (hereinafter: the "e-Government Documents") that will be delivered to the vendor, after the winning bidder signs the contract.

4.2.2. Third-party products: the use of a third-party code, such as a plug-in, auxiliary departments, supplemental products etc. requires the prior approval of the applications security department in the cyber protection system in e-Government.

4.2.3. The vendor undertakes to use updated operating systems for the servers (Windows or Linux) updated with the latest security

patches. The vendor will apply a periodic patches installation policy and an operating system upgrade policy in accordance with the instructions set forth by the Ministry.

4.2.4. The vendor will assist in defining the system protections, including a Firewall server, including setting the optimal configuration in terms of security, vis-à-vis the information security infrastructures and the access of e-Government.

4.3. Securing the solution in a physical level (under the responsibility of the e-Government Unit)

4.3.1. The physical security aspects will be defined based on the guidelines of the critical information infrastructures (CII) officer in e-Government.

4.4. Link to existing interfaces in e-Government

4.4.1. The system will enable full operational and security monitoring, command and control (CC) in all components. According to the demands made by the Ministry, the vendor is required to present and describe the system capabilities for the purpose of this matter – both self-CC (integrated in the product) and central (external).

4.4.2. The system will enable links to external systems (including monitoring systems, CC, services gateway – FW, XML, file upload system and systems such as Vmware, FW) by filtering components. The basic underlying assumption will posit realization by full filtering infrastructure.

4.4.3. The vendor will be required to integrate the system in accordance with the provisions set forth in the sections above, in the existing e-Government systems, including the cyber protection systems of e-Government.

4.5. Governance and compliance

4.5.1. The system will support Secure Payload & Channels. The vendor is required to present and describe the system capabilities for the purpose of this matter According to the demands made by the Ministry.

4.5.2. The vendor is required to present and describe the security standards that the system complies how such as HIPPA, SOX, PCI and the level of their compliance according to the demands made by the Ministry.

4.6. **Authentication**

4.6.1. Each component in the system such as – the operating system, API service and the like will be required to provide unique authentication for each of the components.

4.6.2. In an authentication process in API the system will use API Keys (Token) and not a username and a password.

4.6.3. According to the demands made by the Ministry, the vendor will describe the password management method for the purpose of granting access to the system administrators including with respect to following:

4.6.3.1. The manner of their internal storage in the system, for example by – a database, an operating system, a portal or an application. This will be done to the extent that an external system is not used.

4.6.3.2. The system will support password application capabilities for the purpose of granting access to the system administrators and that will include configuration of the following variables:

1) Password length: determining the password length of 9 characters or more.

2) Password complexity; enforcement of the use of characters that include uppercase and lowercase letters, digits and special characters.

3) Effect of the password: setting a period of time after which the user will be obligated to replace the password (X days).

4) Password history: configuration of a password history of at least 10 previous passwords.

4.6.3.3. The solution will support work with a central identity/password management system: for example – the use of an Active – Directory system.

4.6.3.4. The system will support control and prevention of failed identification attempts – including delivery of alerts regarding events as said – and locking users after a number of failed identification attempts, when it is possible to define the parameters constituting a condition for locking.

4.6.3.5. In any event, the passwords will not be saved in a HARD CODED in any application, and will not be saved as CLEAR TEXT.

4.6.4. Any deviation from the authentication policy or its disruption will create a record that will be forwarded in a digital and online form to the monitoring hierarchy in a format recognized by the SIEM system.

4.7. **Authorizations and permissions management**

4.7.1. The use of Shared Credential in operating systems, applications, system administrators etc. is prohibited. The implementation will be performed by way of procedures and controls.

4.7.2. The system will support "role segregations" that is hierarchical and decentralized, i.e. – inside the organization and between different organizations.

4.7.3. The vendor is required to describe the integrated permissions management mechanisms in the system and interfacing with the external identity management system such as Active-Directory & LDAP. The vendor is required to describe the entire Roles in the system and the permission levels existing for each of the roles.

4.7.4. The system will support RBAC (Role-Based Access Control).

4.7.5. The system will support a central permissions mechanism according to the requirements of the system and that will support the following principles:

4.7.5.1. The minimal permission principle: each system and each system component will grant access only to authorized entities and with minimal permissions as may be required.

4.7.5.2. The system will support access limitation policy to the system resources (files, folders, registry keys etc.) as set out by the Authority).

4.7.5.3. Minimal permissions for a database user; when accessing the database for the purpose of performing authentication, retrieval and update of data, the system will support the permissions granted for Store Procedure only or as minimal as possible.

4.7.6. The system will support granting of permissions based on users that are system administrators/groups in an identity management system such as AD.

4.7.7. The system will support the granting of access permissions to the management interfaces based on IP addresses (ACL).

4.7.8. Deviation from the permissions policy or its disruption will create a record that may be forwarded in a digital format and online to a defined monitoring hierarchy, in a format recognized by the SIEM system.

4.8. **Logical protection**

4.8.1. The system interfaces will be modular. The separation of interfaces will be enabled, such as – full separation between the user interface and the management interface, and the management interfaces themselves.

4.8.2. The inspection of the system and the customizations will be performed in a separate network environment and all as stated in section 5.9.5.

4.8.3. The operation and services systems of the system will be hardened in accordance with the procedures of the e-Government Unit. The e-Government Unit, together with the assistance and support of the vendor, will perform the necessary works.

4.8.4. Critical software updates: the vendor will deliver to the Ministry updates of the operating systems and security updates for the system and for each of its components, immediately after the publication of each update by the manufacturer of the system or the component, as the case may be, or immediately after detecting a vulnerability.
The system will support the download of updates not in a direct connection to the internet (Offline).

4.8.5. The system – including all components thereof – except for the components that are exposed in a secure manner to the end user for the purpose consuming the services – will not enable or require a direct connection to the internet.

4.8.6. The e-Government Unit shall be entitled to install on the system servers monitoring software for the purpose of providing protection and monitoring of the e-Government Unit and protection software changing from time to time as may be required and according to the requirements laid down by the protection unit in cyber when the vendor will accompany the e-Government Unit upon demand.

4.8.7. The system will support a White List component on the servers.

4.8.8. The system will enable the implementation of a multiple-requests mechanism in any part of the system in which information was created and/or authenticated (including multiple requests for uploading files).

4.8.9. The vendor undertakes to notify the Ministry regarding any defect/weakness/vulnerability detected and repair them according to the requirements made by the Ministry.

4.8.10. Any deviation from the logical protection policy or its disruption will create a record that may be transferred in a digital and online manner to the monitoring hierarchy in a format recognized by the SIEM system.

4.9. Protection of transmitted messages (Message Security)

4.9.1. According to the demand made by the Ministry, the vendor is required to describe the manner of protection of the messages that are transmitted in the system.

4.10. Smart card

4.10.1. The system will support identification with a smart card for the purpose of accessing the management interfaces. The required manner of identification – 2FA or a smart card, will be set out by the Ministry.

4.11. Encryptions

4.11.1. According to the demands made by the Ministry, the vendor is required to describe the encryption mechanisms, whether integrated and/or external that are supported/planned to be supplied in all system components.

4.12. Access control

4.12.1. The system will support ACL management (Access Lists) that can be applied with respect to different populations (for example, limitation of access and involvement of developers in the production environment).

4.12.2. The system will support (Quota) rate limit for the user, the service, the organization etc.

4.12.3. The system will apply an Anti-Throttling mechanism.

4.13. Protection in the application level

4.13.1. The system will support the application of input tests according to the principle of constrain → reject → sanitize:

4.13.1.1. Constrain: the use of a White List – verification of input according to type, length, format and range.

4.13.1.2. Reject: use of a Black List – blocking an input known to be used for recognized attacks.

4.13.1.3. Sanitize: sanitizing and isolating the input – convert an input with a potential of becoming malicious into a safe input.

4.13.2. In addition to the aforesaid, the system will also verify the format of the request received for API. For example, in the event the request that is received for an API is in XML format, then the system will also verify the XML structure by a Schema, according to its definition.

4.13.3. The system will apply Session Timeout mechanisms and additional protections against Session attacks, such as – Session Hijacking, CSRF etc.

4.13.4. The system will support Schema Validation (description of the features, standards and protocols).

4.14. **Data & Information**

4.14.1. The system will support the separation of its components and the definition of the protection levels that are required for the purpose of accessing the information according to the classification of the information.

4.14.2. Data at Rest:

4.14.2.1. The entire data stored in the system and that is private, will be stored with encryption.
The encryption mechanism will be based on recognized and standard algorithms. The encryption keys will be under the exclusive control of e-Government and encryption keys that were generated separately can be imported to the system. The vendor shall be entitled to perform maintenance works without knowing the encryption keys.

4.14.2.2. The system will enable the encryption of a disc and basic database encryption up to the cell level in it.

4.14.2.3. The system will not enable storage of sensitive information in the Cache mechanisms.

4.14.2.4. The system will not enable the storage of confidential information in open format. Any information that is defined as confidential will be encrypted.

4.14.2.5. The system will support the encryption of sensitive immovable data by the use of customary encryption protocols (AES 256 bit as a minimum).

4.14.2.6. The passwords of local users will be kept in a secure manner while using customary and secure encryption protocols such as SHA512 together with the Salt values.

4.14.3. Data in Motion:

4.14.3.1. The entire data transmitted in the network will be transmitted in an encrypted manner in the data level itself, irrespective of network encryptions such as TLS1.2 and above. It is clarified that Base 64 is an uncustomary encryption method.

4.14.3.2. Data that includes usernames and passwords must be encrypted in the network traffic.

4.14.4. When setting up an interface for the information network, the interface will be set up according to the API REST standard of e-Government and in compliance with the e-Government information security procedures that will be provided to the vendor.

4.15. **Network**

4.15.1. The entire traffic will be encrypted with commercial encryption protocols such as IPSEC, AES, 256bit and the like.

4.15.2. The Server Side to the public internet: no access to the services on the internet will be allowed from the server side.

4.16. **Monitoring, logs (log files) and alerts**

4.16.1. The system will log any action in a secure file that will be sent to the events management center (SIEM) of the e-Government Unit.

4.16.2. The system will enable the system administrators, according to their permissions, to define the components in which the actions will be recorded in the log files.

4.16.3. The system will enable data transfer capabilities to SIEM according to the customary standards, such as Syslog.

4.16.4. According to the requirements made by the Ministry, the vendor is required to describe the entire system monitoring capabilities, including – an application, database, services, links, queries, information security violations (Security Violations, Queries, Connections, Services, DB). The vendor is required to specify and describe the entire logs that are recorded in the system and that can be integrated in the system information system (including activities that were successful – Success).

4.16.5. The system will support alerting capabilities such as – sending emails, SMS, instant messaging – by central systems – or the display of a message in the administrator console in the event of a violation and extraordinary events.

4.16.6. The system will enable the display and analysis of trends and usage over time.

4.16.7. The system will enable receipt of alerts from the users regarding suspected improper/incorrect use of the account.

4.16.8. The system will enable "to enrich" the data in the log such as: machine type, operating system type, User Agent etc.

4.16.9. The system will enable the documentation of any change in an organized log file, or access to such a file according to the policy settings in the system.

4.16.10. The log files in the system will be protected against unauthorized access (viewing, modification, deletion); and the system will enable identification of unauthorized access.

4.16.11. Any modification in the information that was collected after it was recorded will not be allowed (anti-repudiation).

4.16.12. According to the demands made by the Ministry, as part of the detailed design stage, the vendor will deliver detailed design for the purpose of defining the cyber monitoring and the correlations that are required in the cyber monitoring systems existing in the cyber

protection center of the e-Government Unit, for the purpose of monitoring all actions that are required for the purpose of conducting investigations for the detection and analysis of suspicious activities. These systems will include SIEM and Big Data. The design will include customized alerts and screens for the purpose of conducting full research and monitoring and in accordance with the requirements of the cyber protection system of the e-Government Unit.

4.16.13. The system will keep historical data of any action for a parametric period that will be set for the purpose of providing across-the-board monitoring and providing answers to legal issues.

4.17. Response to information security events and/or threat of an outbreak of an information security event

4.17.1. The vendor undertakes to respond immediately to such an event and/or a threat of an outbreak of such an event as said and solutions within the period of time defined in the SLA table and according to the definition of the malfunction, in the event of detection of data breaches, or against information security threats.

4.17.2. The vendor undertakes to report and notify immediately the e-Government Unit regarding any security failure and/or data breach – or a suspected of a defect and/or data breach – that exists or that is detected in the system and/or in the infrastructures with which the system was developed and present the ability for the purpose of mitigating the vulnerability or the risk of vulnerability until the full repair of the defect and after the vulnerability is eliminated.

4.18. Managing information security events

4.18.1. According to the demands made by the Ministry, the vendor is required to provide a description of the manner of conducting information security events in the system.

4.18.2. According to the demands made by the Ministry, the vendor will provide a description of the tools supporting the events management in the system. It is clarified that the meaning is not to an internal SIEM system but to additional tools for the purpose of detecting and conducting local inquiries. The vendor will participate, as may be required, in the analysis and the investigation of information security events in the system.

4.18.3. According to the demands made by the Ministry, the vendor will provide a description of the management procedures for defensive failure events.

4.19. General guidelines

4.19.1. In the event of alleged conflicting information security requirements, the vendor is required to notify the representatives on behalf of the Ministry for the purpose of this matter, and comply with the requirement that is the strictest out of the different requirements, unless the Ministry waived in advance and in writing any demand as said.

4.19.2. The signature of the vendor on the declarations in the Undertaking of Confidentiality is a condition for the delivery of the e-Government documents referred to in this section.

5. Implementation

5.1. General

5.1.1. The vendor will install the system, including all the environments as stated in section 5.8, in the server farm in the e-Government premises (On premise) and in a Cluster configuration for the purpose of maintaining survivability and redundancy in the production environment (duplication of components), and in the secondary site (in the DR facility or in any other site as ordered by the Ministry), without any geographic limitations, in Active/Active configuration, and all in accordance with the instructions set forth by the Ministry.

5.1.2. The vendor will install the system, and in particular will provide proper definitions, in accordance with the Tender documents and in accordance with the Ministry guidelines, and will integrate the system in the Ministry sites based on the communication infrastructure and the systems existing and operating in each and every site up to the full and proper operation in production, to the satisfaction of the Ministry, and in compliance with the acceptance tests and the entire requirements set forth in the Tender, and all in accordance with the guidelines set out by the Ministry.

5.2. Staff members provided by the vendor

5.2.1. The vendor will appoint a permanent project manager on its behalf. The project manager will act as the representative on behalf of the vendor and will concentrate all the vendor's tasks and the requirements of the Ministry during the term of engagement. The project manager will be responsible for the coordination of the

performance of the services among the different entities on behalf of the vendor and the management team on behalf of the Ministry.

5.2.2. In addition to the project manager, the vendor undertakes to allocate regular staff for the purpose of performing the services (hereinafter: the "**Staff Members**").

5.2.3. The Ministry shall be entitled to reject the placement of the project manager or any of the Staff Members or demand their replacement without giving any reasons.

5.2.4. The vendor shall not be entitled to replace out of its own initiative the project manager or any of the Staff Members without obtaining the prior and written approval of the Ministry.

5.2.5. The vendor undertakes to make available the Staff Members, including the project manager, that will have proper security clearance. Each of the Staff Members on behalf of the vendor that engages in the performance of the services will have security clearance required by the Ministry and will undergo a security check as decided by the Ministry. The project manager and any other person and entity acting on behalf of the vendor will be required to sign an Undertaking of Confidentiality according to the decision made by the Ministry.

5.3. Stages for the purpose of implementing the project

After making the announcement of the winning bidder, signing the contract and issuing an order as stated in the Tender documents, the vendor will supply and install the system, until its operation in production, according to the following stages:

A. Preparation of work plans and a design document and their delivery to the Ministry, as stated in section 5.6 hereunder.

B. Performance of a detailed design as stated in section 5.7 hereunder.

C. Supply and installation of the system, as stated in section 5.8 hereunder.

D. Inspection of the system until its operation in production, in accordance with the provisions of section 5.9 hereunder.

E. Provision of documentation and source code, as stated in section 5.10 hereunder.

F. Training, as stated in section 5.11 hereunder.

G. Support – warranty and maintenance, as stated in section 5.12 hereunder.

5.4. Approval of the system for signing in "secure" level by the Privacy Protection Authority

5.4.1. Following the guidelines set out by the Ministry and with the support of the Ministry, and in accordance with the instructions set forth in the work plan, the system shall comply with the requirements laid down by the Privacy Protection Authority (the "PPA") for the purpose of providing a secure signature, and in this regard the requirements laid down in section 8 of the Electronic Signature Regulations (Secure Electronic Signature, Hardware and Software Systems and Review of Requests) 5762-2001. The vendor will provide to the Ministry, as may be required, all necessary approvals and documents, for the purpose of complying with the requirements laid down in the aforesaid regulations. It is clarified that in the event an expert opinion is required pursuant to section 9(a)(1) of the Regulations, the vendor will provide, at its expense and under its responsibility, an expert opinion as required in the regulations.

5.4.2. The request will be submitted in accordance with the "Submission of a request by a certificate authority for the issuance of signing means on network appliance (HSM) (hereinafter: the "**Procedure**") hereby attached. (In addition, the Procedure was published in the procurement director website – in the tender publication page as stated in section 1.5 in Chapter 1).

נוהל הגשת בקשה
ל גבי התקן רשתי.pdf

5.4.3. It is emphasized that the registrar shall be entitled to demand any other information it requires for the purpose of reviewing the request for approval of issuance of electronic signature on a network appliance. The vendor will be required to provide such information as said, to the extent required, to the Ministry.

5.5. Work documents – General

5.5.1. The following documents shall be referred "**work documents**": the work plan (as stated in section 5.6 hereunder), the detailed design

document (as stated in section 5.7 hereunder), the testing document that includes the different testing scripts, including scripts according to the system usage scripts, for the different testing stages – the delivery tests by the vendor, the acceptance tests by the Ministry, performance tests and strength/penetration tests (as stated in section 5.9 hereunder), documentation (as stated in section 5.10) and any other document delivered within the framework of the project.

5.5.2. After the vendor delivers to the Ministry any of the work documents, the Ministry will deliver written notice to the vendor, at its sole discretion, whether it approves the said work document proposed by the vendor (in whole or under conditions) or whether it rejects the said document.

5.5.3. In the event the Ministry rejected any of the work documents or approved it under conditions, the vendor will amend the document according to the demand made by the Ministry and at its expense, and will submit to the Ministry any of the work documents when the said document is amended, according to the reservations and/or the comments made by the Ministry in its notice.

5.5.4. The Ministry will deliver to the vendor its response to the amended document, *mutatis mutandis*, and so on and so forth, until obtaining the full and final approval of the Ministry for the said document of the work documents.

5.5.5. The guidelines and/or the requirements that the Ministry will deliver to the vendor in connection with any of the work documents including a rejection/amendment/revision/approval etc. as stated in this section: (a) shall not give rise to grounds for a delay and/or withholding of the fulfillment of any of the undertakings of the vendor in accordance with the contract and (b) impose on the Ministry any liability and/or derogate from the liability of the vendor for the quality, validity and effect of the said document of the work documents and the services provided in accordance with the said document and (c) derogate from the other undertakings of the vendor in accordance with the contract.

5.5.6. Without derogating from the generality of the aforesaid, the vendor shall be held solely liable for any error, omission, non-conformance, ambiguity and/or any other defect of any kind, to the extent that such a defect is found in any of the work documents. As part of the said actions the vendor will perform, at its expense, any revision and/or amendment that are required in any of the work documents and/or the system itself and/or in any part of the services, and all for the purpose causing them to be in conformance

to the requirements laid down in the technical specification and the contract.

5.6. Schedules, work plan and detailed design

It is emphasized: meeting the schedules is a material part of the engagement. The Government ICT Authority regards the successful completion of the project within the shortest period of time as highly important.

5.6.1. The vendor will provide to the Ministry, in 10 workdays as of the date of receiving the order from the Ministry, a work plan for the purpose of implementing the project in stages, a Gantt chart based on PERT method and that includes binding schedules for the performance of all the activities that are described and a risk management plan in the project, and documents regarding work procedures in the project, including the quality assurance procedure, the project management procedure, the layout management procedure, the variations procedure and the documents management procedure.

5.6.2. The following are the primary milestones that are required from the vendor in the performance of the project and the work plan.

5.6.3. **It is emphasized: the duration of the milestones stated hereunder might vary (shortening/extension) according to the requirements laid down by the Ministry and according to the requested changes in the milestones that the vendor is entitled or the submit during the preparation stage of the work plan for the approval of the Ministry**.

5.6.4. Work on part of the deliverables will be performed simultaneously, as stated in the table, and according to the decision of the Ministry.

5.6.5. The schedule will commence as of the date the Ministry delivers the order to the vendor.

5.6.6. The table is defined according to workdays (and not calendric years).

5.6.7. The vendor shall be responsible for the implementation of the milestones described in the following table:

#	**Milestones according to deliverables**	**Stage commencement time**	**Stage duration (in workdays)**
1.	Submission of work plan and work procedures by the vendor to the Ministry	Receiving the order	10 days
2.	Submission of a detailed design document (DDD) by the vendor to the Ministry	Approval of the work plan and the work procedures by the Ministry	25 days
3.	Submission of a testing script document as described in the Tender	Approval of the detailed design document by the Ministry	20 days
4.	Setting up a development and testing environment in accordance with the entire requirements laid down in the Tender and according to the instructions of the Ministry	Approval of the detailed design document by the Ministry	45 days
5.	Performance of delivery tests for the development environment and testing	Completion of setup of the development and testing environment	10 days
6.	Setting up a pre-production and production environment in accordance with the entire requirements laid down by the Ministry and according to the guidelines	Approval of the acceptance tests for the development and testing environment	40 days
7.	Performance of delivery tests for the pre-production and the production environment	Completion of setup of the pre-production and the production environment	10 days
8.	Performance of load tests and performance as defined in the Tender and obtaining approval regarding compliance with performance and performance of information security testing according to the	Completion of approval of acceptance tests in the pre-production and the production environment	15 days

	demands made by the Ministry		
9.	Active service for end-to-end electronic signature, for 3 initial services in the pre-production and in the production environment	After approval of the load testing in the pre-production and the production environment by the Ministry	30 days
10.	3 services for the signature of the employees of active government ministries in the pre-production and the production environment	After completion of the setup of the end-to-end electronic signature service and obtaining the approval of the Ministry for the tests that were defined	30 days
11.	An active signature service for citizens in the pre-production and the production environment	After completion of setup of the signing service for government employees in structured signing procedures. And after obtaining the approval of the Ministry for the tests that were defined.	50 days
12.	Performance of delivery tests for every service separately from the services described above (electronic, Ministry procedures, citizens)	Completion of setup of active signature services in the pre-production and the production environment: For: 3 electronic signature services 3 Ministry signing services Citizens' signatures Respectively	15 days
13.	Operation in production	Approval of acceptance tests	1 day
14.	Setup of a DR environment according to the requirements laid down by the Ministry	Completion of approval of the acceptance tests in the pre-production and the production environments	15 days
15.	Active signature service for company representatives and office holders in the pre-production and the	After completing the acceptance tests and the operation in production for the signing services	25 days

	production environment, including the entire testing stages as described above	described above (machine, ministries, citizens)	

5.7. Detailed design

In 25 days as of the date of approval of the work plan and the project work procedures, the vendor will provide to the Ministry a detailed design document that will present the entire technical definitions that are required for the purpose of implementing the functionality that is required by the Ministry and/or anyone acting on its behalf. For the purpose of preparing the detailed design document the vendor will hold professional meetings with the representatives of the Ministry and/or anyone acting on its behalf, and at the end of such meetings the vendor will deliver to the Ministry a detailed design of the system and everything required for its installation in the Ministry sites, including technological and infrastructure planning, including hardware and software requirements, in accordance with the information security requirements, and including a backup mechanism.

5.8. Supply and installation of the system

The vendor will install the system in each of the environments as stated hereunder, in accordance with the requirements and the work plan.

5.8.1. General – in all environments

The installation of the system in all environments will include the following, *inter alia*:

5.8.1.1. **Hardware and software**:

- In the event the system that was proposed by the vendor also includes virtual implementation components, the installation of the said components will be performed by the vendor on a virtual infrastructure manufactured by Vmware that will be supplied by the Ministry.

- The installation will include the installation of the operating system, auxiliary software, communication settings and required interfaces to the e-Government systems by API for the purpose of exporting and importing data according to the requirements laid down by the Ministry, and all according to the detailed design that will be made in accordance with the provisions set

forth in section 5.6 above and in accordance with the entire requirements laid down in the Tender.

- In the event the vendor's bid is based on an appliance (including the HSM component), the vendor is required to perform the installation including all components thereof, including hardware and software updates, communication settings and required interfaces.

- The vendor will supply and install the required hardware and software for each level of users that will be ordered. The installations will be performed by the vendor and in accordance with the instructions of the Ministry.

A. <u>Infrastructure software</u>

- The vendor will provide any infrastructure software that is required for the purpose of operating the system and for which the Ministry has no licenses, including – communication software, statistical software, development tools, operation software etc. In addition, the vendor will provide the entire licenses for the operating system as required according to its bid, unless the Ministry supplied the systems independently and all in accordance with its instructions.

B. <u>Applicative software</u>

- The vendor will supply the entire applicative software and the development customizations that are required for the live operation of the system, according to the detailed design prepared in accordance with the provisions set forth in section 5.6 above.

- The vendor will provide all tools and services that are required for the current update of the system by the Ministry.

- The vendor will provide any additional component that is required for the purpose of fulfilling its entire undertakings for the full operation of the system in accordance with the Tender documents and the contract.

C. <u>Software development kit (SDK)</u>

- The vendor will provide any tool or software development kit for the product (SDK) to the extent that such a tool or a kit exists for the proposed product, including an SDK for the development of applications in mobile devices.

5.8.1.2. **Interfaces and integration** –

It is clarified that the vendor will perform integrations in all the following environments. The integration will be performed between the signatures server that will be set up and the e-Government systems, including:

1) The government identification system (a system with which an authentication process of the user will be performed in an attempt to consume a service in the signatures server) and identification with the MERKAVA system.

2) The information gateway (API-gateway with which the services will be externalized) for all applicative services that are required (including MERKAVA).

3) The CA components as defined by the Ministry.

4) In addition, the vendor is required to provide an API interface including integration with the information gateway as may be required, for the creation and documentation of the keys management/certificates management process in all life cycle stages, as described in Appendix A-2, sections 3 and 4.

5.8.2. **Development environment**

The vendor will install the development environment in the main site or, alternatively, in the cloud, according to the instructions set forth by the Ministry. The development environment will grant access to the system API for the purpose of developing processes that require interfacing with the main signatures system. There is no need that the configuration of the development environment will be identical to the production environment, and it can be based on simulators as long as the environment provides identical functionality that includes all logical components that are required for the operation of the system and the interfacing between the systems. The environment will include the following, *inter alia*:

- Simulator for the HSM that will enable development without HSM hardware.
- Simulator for testing the interfaces with the e-Government systems.

5.8.3. **Testing environment**

The vendor will install the testing environment on the main site. The testing environment will allow access to the system's API to perform acceptance tests to processes that require interfacing with the central signature system. It is not necessary for the test environment configuration to be identical to the production environment, and it is not required to withstand loads, but all interfaces must be identical to the production environment. The vendor undertakes to supply and install the system in the testing environment, within 60 calendar days at the latest, from the date of approval of the detailed design by the Ministry as aforesaid, or at another date, as set out in the work plan, including all components required for the establishment and operation of the system and in accordance with the system configuration settings and system setup up to its full operation, and after correcting deficiencies following the findings of the acceptance tests, to the Ministry's satisfaction.
In addition, at the installation stage in the testing environment, or at any other time, in accordance with the Ministry's requirements, compliance with the requirements of the Privacy Protection Authority, as stated in section 5.4 above, will be examined.

5.8.4. **Pre-production environment**

After successfully completing acceptance testing and their approval by the Ministry, the vendor will install the system in the pre-production environment on the main site in accordance with the work plan and characterization, in the same configuration as the production environment, except for the withstanding of loads, which will allow the execution of delivery tests and acceptance tests prior to the going online. The environment will have the capacity to withstand only the first-class loads – 100,000 users, to meet the load of 50 users simultaneously performing 50 operations per second (less than the requirements in the production environment).

5.8.5. **Production environment**

After successfully completing the delivery and acceptance tests set in the pre-production environment and approval of system integrity by the Ministry, the vendor will install the system in the production

environment on the main site and secondary site, according to the work plan and characterization. All system components in the main site production environment will be installed in dual configuration to maintain system survivability. The installation of the production environment will also include installation on the secondary site, in Active/ Active configuration for synchronous backup of all system components, with the system in good working order in the production environment and secondary site as stated below, including:

5.9. Tests

5.9.1. General – The test document

5.9.1.1. At the time specified in the work plan, the vendor shall submit the test document, including the delivery test scenarios (hereinafter: the "**Delivery Test Scenarios**") and the acceptance test scenarios (hereinafter: the "**Acceptance Test Scenarios**") (the delivery test scenarios and the acceptance test scenarios will be referred to together: the "**Test Scenarios**") for the Ministry's written approval, in accordance with the tender instructions.

5.9.1.2. The vendor undertakes to submit the Test Scenarios to the Ministry for approval at the time specified in the work plan. The vendor shall specify in the Test Scenarios the description of the tests to be carried out, the components and elements tested and the processes to be carried out in each of the tests, the tools for conducting, executing and managing the tests (including details of the tools to be used for the performance tests); The objectives, metrics and standards and other conditions whose fulfillment constitutes a condition for the success of the delivery tests, in accordance with the Ministry's requirements in the tender documents, including and without prejudice, the rules of assessment and formulas used by the vendor to examine the results and/or success of each delivery test.

5.9.1.3. The Test Scenarios will be subject to the Ministry's approval and any changes made thereto by the Ministry or per its instruction.

5.9.2. **Performance of delivery tests**

5.9.2.1. As a condition of approval for the installation of the system in the production environment, and as an integral part of the fulfillment of its obligations according to the tender documents, the vendor shall carry out, in the presence of the Ministry representatives, at its responsibility and expense, at the stages and times stipulated for this purpose in the work plan, the delivery tests (including compliance with the information security requirements, as detailed below), in accordance with the Delivery Test Scenarios approved by the Ministry. It is hereby clarified that the presence of the Ministry representatives and/or an instruction given by them shall not impose any responsibility on the Ministry and/or derogate from the vendor's responsibility according to the tender documents for the delivery tests as well as to correct the findings of the acceptance tests as set out below.

5.9.2.2. The delivery tests of the system will be carried out in accordance with the Delivery Test Scenarios defined by the vendor and approved by the Ministry.

5.9.2.3. The Delivery Tests will be performed in each of the requested environments in available government facilities, as determined by the Ministry.

5.9.2.4. The vendor will immediately act to correct, rewrite, modify in accordance with any finding/ defect/ comment that may be discovered during the delivery tests.

5.9.3. **Performance of acceptance tests**

5.9.3.1. The Ministry may, at its discretion, conduct acceptance tests for the system itself and/or through a third party on its behalf and the vendor will be required to cooperate fully with the Ministry or such third party. Notwithstanding the foregoing, the Ministry may, at its sole discretion, waive the acceptance tests, in whole or in part.

5.9.3.2. The system's acceptance tests will be conducted in accordance with the Acceptance Test Scenarios prepared by the vendor, in accordance with the Ministry's guidelines and approval. The vendor

undertakes to submit Acceptance Test Scenarios to the Ministry for approval of the system at a time specified in the work plan. The Acceptance Test Scenarios will include, at a minimum:

- Compliance with the tender requirements and the Ministry's conditions in accordance with the terms of the tender.
- Definition of reasonable response times, describing the mechanism for testing and specifying computerized tools for conducting the tests.
- The results of the delivery tests performed by the vendor before delivery for acceptance tests.

5.9.3.3. Acceptance tests will be conducted at the e-Government facilities, in the requested environments, as determined by the Ministry.

5.9.3.4. The Ministry may at any time during the contract period, inspect the system in any way it deems appropriate, including conducting a code review, data testing, information and penetration testing, performance testing, and the like, as required. The vendor will assist the Ministry and/or whoever it instructs when performing these tests.

5.9.3.5. Handling of the test findings: The vendor undertakes to handle all the findings that will be revealed in the tests, both those carried out by it and those carried out by the Ministry, and in accordance with the instructions given to it by the Ministry and to correct all that is required to reach compliance with the acceptance tests accordingly.

5.9.4. **Performance tests**

5.9.4.1. Should it be required by the Ministry, the vendor will perform a load and performance test on the system, during which the system's ability to meet the load and performance requirements as specified in section 2.2 of Chapter 2 above (hereinafter: "**Performance Tests**") will be tested.

5.9.4.2. The Performance Test will be performed in the production environment or another environment as determined by the Ministry.

5.9.4.3. The vendor shall provide scenarios describing the test to be performed by it, and shall use, and make available to the Ministry, a testing tool approved by the Ministry for the performance test, both by the vendor and the Ministry. The test tool will support tests for different loads at the same time.

5.9.4.4. The vendor will provide the results of the performance test as proof of the system's compliance with the load.

5.9.4.5. The Ministry's representative and/or someone on its behalf will be present at the performance test by the vendor.

5.9.4.6. In the performance test by the Ministry, a representative of the vendor will be present, as per the Ministry's invitation.

5.9.4.7. Handling of the test findings: The vendor undertakes to handle all the findings that will be revealed in the performance tests, both those carried out by it and those carried out by the Ministry, and in accordance with the instructions given to it by the Ministry and to correct all that is required to reach compliance with the acceptance tests accordingly.

5.9.5. **Information security tests**

5.9.5.1. The vendor will provide all system components for information security tests, including penetration tests and code review for developments made for the Ministry and a report on code review and penetration tests performed on the proposed product, all in accordance with the Ministry's requirements and the tender requirements in general and section 4 of Chapter 2 in particular. The actual tests will be performed by the e-Government information security team on the e-Government website.

5.9.5.2. The tests will be carried out at a time as determined by the Ministry prior to the system's launch and will be attended by a representative of the Ministry and/or someone on its behalf. The test will be performed in the production/ pre-production environments and/or otherwise, as determined by the Ministry.

5.9.5.3. Handling of the test findings: The vendor undertakes to handle all the findings/ defects and in accordance with the instructions given to it by the Ministry and to correct anything required for the purpose of obtaining approval for launch.

5.9.5.4. The system will meet all the requirements of the Information Security Commissioner as well as the information security procedures and e-Government procedures, including penetration tests and periodic code reviews. The vendor must prevent any security breaches and address them as soon as they are discovered, including removing from the system any information security threats and repairing any deficiencies.

5.10. **Documentation**

5.10.1. The vendor will provide the documentation required for the system as stated below in accordance with and on time as per the Ministry's requirements:

- The detailed design document.
- The tests document includes documentation of the test scenarios and their results, including documentation of tests and certifications of the system and its components.
- Technical documentation for all hardware and software tools, including product book, SDK documentation if any, system configuration on its various components including servers and file structure on servers.
- User guide according to roles as well as a guide for the infrastructure team – operation of the application; Detailed includes screen shots – for those in charge of system operation and those in charge of operating system infrastructure as well as a briefing document for the government service center.
- Documentation regarding developments and adjustments made to the system, **for the Ministry**, including programming files and source code.
- Any documentation that will be required in the future for ongoing operations, infrastructure and conversions.
- The vendor undertakes to update the technical documentation, documentation and system guides and programming files in accordance with any change in any of

the components of the system, including version management and changes.

5.10.2. The vendor may add to the required documentation list.

5.10.3. The documentation can be provided in Hebrew or English, depending on its source.

5.11. **Training**

5.11.1. **Training of managers and users** – the vendor undertakes to provide the Ministry and its representatives (up to 35 functionaries) with training on the system. The training will include everything required so that the Ministry's representatives can manage, operate and maintain the day - to - day operation of the system independently by the Ministry's personnel. The training will include training on how to make adjustments so that the Ministry can do so independently if it so desires. Initial training will be conducted until the end of the system's acceptance tests or at another time according to the Ministry's instructions. In addition, depending on the Ministry's order, the vendor will provide periodic training once a year accordingly. Training on the system and periodic training will be performed as part of the vendor's obligations and without any additional payment beyond the payment for the cost of the system.

5.11.2. **Training for developers/ courses** – Without detracting from the generality of the aforesaid, in accordance with the requirement of the Ministry, the vendor will conduct courses for the purpose of training developers and implementers of the system (approximately 10 developers and implementers). The scope of training and scope of users and trainees listed is an assessment only and is not binding upon the Ministry. The course will include everything required so that each participant according to his role can perform his role in the system fully, properly and as required. Payment for this course will be made in accordance with the vendor's proposal in the quote section.

5.11.3. **Manufacturer course** – In addition to the above, the bidder will price in the additional items the cost of a manufacturer course for one participant on the product infrastructure. The Ministry will be entitled to order this course in accordance with the quote and the procedure for purchasing changes and improvements, as detailed below in section 6.

5.12. Support Services – Warranty and Maintenance

5.12.1. Warranty period

A) The warranty period will be 12 months starting from the Ministry's approval for the operation of the system in production (hereinafter: the "**Warranty Period**").

B) During the said Warranty Period, the vendor will provide, free of charge, support services for the system and everything in accordance with the definitions and detailing in sections 5.12.3 and 5.12.4 below.

5.12.2. Maintenance period

A) At the end of the Warranty Period, and subject to the issuance of an order signed by the Ministry's authorized signatories and subject to the terms of the order, the vendor will provide support services to the system, until the end of the contract as defined in the contract (the maintenance period).

B) The maintenance will be provided according to the consideration and the rest of the terms and conditions specified and defined in the tender and contract, and to the Ministry's full satisfaction.

5.12.3. Support services

The vendor will provide the services listed below (hereinafter: the "**Support Services**") during the Warranty Period, as defined in section 5.12.1 above, without any additional consideration. The vendor will also provide the Support Services during the maintenance period, as defined in section 5.12.2 above, should these be requested by the Ministry.

A) Maintenance of the system, in all environments, including investigating and locating the source of faults, fault repairs and preventive maintenance of hardware, software (bug fixes), and internal and external documentation.

B) Preventive maintenance – proactive service, and periodic preventive care in accordance with the manufacturer's instructions.

C) Replacement of defective system components with normal components manufactured by the manufacturer, with a corresponding or improved technical specification than the defective component.

D) Supply and installation of new editions, and provision of training and full documentation about them, all until their full proper operation in the required environment(s), including updates, including the level of vitality for updating, to the system for adaptation to end device versions, operating systems, new standards, document types, as well as the provision of new editions and versions, updates, patches, etc. of the system and the fulfillment of its obligations in the event that the production of the system or any of its components is stopped (as detailed below in section 5.13.2).

E) Installing patches – Installing fixes, changes and updates regularly received from the software manufacturer. The vendor will install the patches in the Ministry's testing environment. Essential patches (such as fault repairs) will be installed by the vendor, in accordance with the Ministry's guidelines, immediately after compliance with the tests. Other patches will be installed as needed and in accordance with the Ministry's decision and work plan. The patches will be installed in pre-production and/or production environments, according to the Ministry's decision.

F) Firmware updates – Installing patches and firmware updates that are regularly distributed by the manufacturer. Essential updates (such as bug fixes) will be installed immediately. Other patches will be installed as needed and in accordance with the Ministry's decision and the work plan.

G) Arriving at the site and providing accompaniment by a technician to deal with faults and complex initiated works.

H) Consultation in problem solving and proper implementation of the systems and assistance in providing solutions to problems arising from faults by providing repairs of the manufacturer or bypass solutions, until a perfect solution is provided by the manufacturer, including accompaniment and support of the Ministry's application team, as required by the Ministry and telephone support of the Ministry's application team, if required.

I) Technical support in the Ministry in the establishment of services in offices/ external services for citizens in accordance with the Ministry's requirement.

J) Operation of a service center as specified in section 5.12.4.2 below.

K) Making future changes and improvements as required from time to time by the Ministry.

L) For the avoidance of doubt, the vendor will be required to adapt the system and the product of the signature, to future versions of the operating system and/or to future versions of standards and/or to future versions of documents.

M) Monitoring and control of the service (reporting and monitoring) as specified in section 5.12.4.5 below.

5.12.4. **Support services will be provided as needed as follows**:

5.12.4.1. Service times

A) The vendor will provide support services during business hours, Sunday to Thursday from 8:00 to 18:00 (hereinafter: the "Business Hours").

B) In cases of disabling/ critical malfunctions, as required by the Ministry, the service times will be for 24 hours, 7 days a week (24/7), and the response times for the service will be in accordance with the provisions below in section 7.1.4.

5.12.4.2. **Call center and telephone/ remote support**

5.12.4.2.1. **General**

A) During the Warranty and Maintenance Period, the vendor will provide the Ministry with a telephone line, email address and contact information via WhatsApp (hereinafter: "**Call Center**") to which to report any malfunctions (it should be clarified that there is no intention of establishing a dedicated call center for services under this tender beyond what is stated in the section).

B) The operating hours of the Call Center and telephone support shall be as specified in section 5.12.4.1 above.

C) Response to service and support calls – The vendor will be required to meet the response times listed below in section 7.1.4.

D) The Call Center will handle fault inquiries, problems and questions reported by authorized

users of the Ministry as well as inquiries for telephone/ remote guidance.

E) Telephone/ remote guidance and support will be provided by a suitable staff member of the vendor for the purpose of troubleshooting the system.

F) If the fault has not been resolved by telephone instruction, the fault will be referred to a staff member for physical support at the site as detailed below in section 5.12.4.3.

G) The Call Center will provide response in Hebrew.

H) The vendor, in accordance with the Ministry's requirement, will provide the Ministry with the procedure for handling faults, including the manner of handling if an escalation is required for handling a fault (such as transferring the handling of the fault from the Call Center, to the Call Center manager, a team leader, etc.)

I) The vendor will issue, once a month, a summary report of inquiries to the Call Center.

5.12.4.3. **Physical support on site and supply of replacement equipment**

A) To the extent that a malfunction cannot be resolved via telephone support as aforementioned, support will be physical at the site itself, in accordance with the Ministry's instructions, through an appropriate vendor and/or manufacturer staff member. Remote connection will not be allowed.

B) Support hours shall be as specified in section 5.12.4.1 above.

C) The response times required for the arrival of the staff member and supply of replacement equipment are detailed below in section 7.1.4 below.

D) For any malfunction that requires physical support on the Ministry's site, the vendor must

ensure that a staff member with the appropriate clearance level is sent to the site.

E) In accordance with the type of fault as defined in section 7.1.4 below, the staff member will remain on site until the fault is rectified to the Ministry's satisfaction.

F) In the event of a hardware malfunction whose repair has not been completed by the date specified in section 7.1.4 below, the vendor undertakes to provide replacement equipment. The vendor will install on the replacement equipment all the software that was installed on the replaced equipment. The form of connection to the network of the replacement equipment will be that of the replaced equipment. The vendor will transfer, at the request of the Ministry, all the basic software, settings and data stored in the replaced equipment to the replacement equipment. This transfer can be done by transferring the data only or by transferring the media between the replaced equipment and the replacement equipment, in accordance with the Ministry's requirement.

G) In the event of a software malfunction whose repair has not been completed on the date specified in section 7.1.4 below, the vendor undertakes to provide a temporary alternative solution, in accordance with the Ministry's requirement.

5.12.4.4. **Manufacturer Support**

If necessary, and in accordance with the Ministry's requirement, the vendor must ensure the manufacturer's support. If necessary, direct contact with the manufacturer will be made by the vendor, as well as contact with the manufacturer's help desk.

5.12.4.5. **Service monitoring and control**

A) Every service call and fault handling will be documented by the vendor in real time. The

vendor will produce a "fault report" after its solution which will include the call/ fault description, description of the handling, solution description and any relevant information.

B) At the request of the Ministry, and at least once a quarter, even if it is not required to do so by the Ministry, the vendor shall submit a report detailing the service calls handled by it – as well as the call/ fault description, description of the handling, solution description and any relevant information.

C) Such reports shall contain the data to be defined by the Ministry and submitted in a format to be determined by it.

D) The reports will be submitted to the contact person on behalf of the Ministry, signed by the authorized signatories on behalf of the vendor and, in addition, also on a magnetic device in a format to be determined by the Ministry.

5.13. **Continuity of service**

5.13.1. **General**

A) The vendor must commit to the continuous retention of knowledge, including the system capabilities, adaptations, architecture and infrastructure required in the detailing of this request for proposals.

B) If the vendor is an authorized vendor of the product, it is clarified that the vendor undertakes to provide the support services for the product regardless of the continuation of the current and normal business activities of the product manufacturer. In the event that the manufacturer decides to discontinue support for the product component, it shall not relieve the vendor from the responsibility of providing at its own expense a component and/or support identical in nature and quality to the product component which has been manufactured and/or supported by the product manufacturer.

C) The Ministry reserves the right to perform the support services or any part thereof independently. If it has done so, the vendor will not be entitled to any payment in respect thereof.

5.13.2. **Technological update of the system/ equipment components**

A. The vendor undertakes that in the event of a version update, the release of a new model, the replacement of a series of equipment items, the vendor will notify the Ministry of innovations and updates.

B. In the event of the release of an updated/ improved version of any software components integrated in the system (including a major release), the vendor will offer the Ministry to update the existing version without any additional consideration for the software and/or its installation. Should the Ministry instruct the vendor to install the update accordingly, the software/ version installation will be performed according to the Ministry's instructions, even at unusual times and for no additional charge.

5.13.3. **A halt in the production of system/ equipment components**

A. In the event of discontinuation of the system production and/or any of its components and/or equipment included in the vendor's offer, or in the case of a planned cessation of production, the vendor shall contact the Ministry immediately upon being informed of the fact and shall update the Ministry on the innovations and updates. In such a case, the Ministry will have the option of choosing one of the following courses of action:

1) Subject to the Ministry's prior written approval, the vendor shall provide, in lieu of the discontinued system, components and equipment, a system, components and equipment whose features are identical or exceed – according to the Ministry's inspection and determination – the features of the system and equipment in the vendor's proposal, at no additional cost. The alternative system, components and equipment will undergo a characterization, testing, installation and implementation process and are adapted to the characterization, testing, installation and implementation process undergone by the original product; or

2) Stop the engagement with the vendor, in whole or in part, and purchase such products through a new tender, or in any other way the Ministry deems appropriate.

5.13.4. **Separation Plan**

5.13.4.1. In accordance with the Ministry's directive, the vendor will prepare and provide the Ministry with a separation plan. The separation plan defines the processes that will be activated in the event of termination or end of the contract between the parties (in whole or in part) for any reason, and at any stage of the provision of services, both in the implementation, operation or warranty stages, and during the maintenance period, should it be exercised.

5.13.4.2. The purpose of the separation plan is to transfer the services (including the data), in whole or in part, to the Ministry or anyone on its behalf, in an orderly manner that will prevent any damage and/or malfunctions to the Ministry during and after the separation, and in full cooperation of all parties, as stated below.

5.13.4.3. In the event the Ministry decides to stop receiving some of the services, the level of service with regard to the other services that the Ministry has chosen to continue receiving will not be affected. Without derogating from the provisions of the separation plan or contract, the vendor undertakes to do everything in its power, and to perform every action, in order to achieve the aforementioned goal, and to refrain from performing any action that may frustrate or harm the aforementioned goal.

5.13.4.4. The vendor undertakes to act in good faith, to cooperate fully, comply with all Ministry requests and help implement the separation successfully and quickly. The vendor undertakes to follow the separation plan even if it has any arguments against the Ministry and including against the Ministry's decision to separate or financial claims. The parties agree that in any case of litigation between the parties regarding the Ministry's decision to separate, the vendor will refrain from seeking remedy in the form of an enforcement order or injunction, and will be satisfied with a remedy of compensation.

5.13.4.5. Separation stages:

(1) "**Preparation period**" – from the date of the Ministry's notification of the termination of the contract until the Ministry's approval of the end of the preparation period. During the preparation period, the vendor will provide training to the Ministry's representatives, as well as to the representatives of the new vendor (s), in the event the Ministry has contracted other vendor/s. The beginning of the training will be immediately upon the start of the preparation period, or immediately upon the selection of another vendor(s). The vendor must take steps so that within one month of the Ministry's notice of the termination of the contract, all information, data, and other materials will be transferred to the new vendor(s) in a manner that allows the continuation of services without harm.

During the preparation period, the vendor will continue to be obligated to all sections of the contract, including all the details of the level of service in the contract, and at the same time – to carry out the separation plan in this section.

If required, for the purpose of training, the vendor undertakes to provide employees from among the staff members, as selected by the Ministry at its absolute discretion. These employees will work jointly with the representatives of the new vendor(s) as well as with the Ministry and/or someone on its behalf, to transfer the services as quickly and correctly as possible.

(2) "**Support period**" – from the date of completion of the preparation period until 12 months thereafter. During the support period, the vendor's employees and/or those on its behalf who participated in the provision of services (and who will be selected by the Ministry at its absolute discretion), will provide the new vendor(s) or the Ministry representatives or

anyone on their behalf, telephone assistance and, if necessary, assistance in the Ministry facilities, in the scope of monthly hours required, and in accordance with the changes and improvements procedure.

5.13.4.6. The Ministry will state in its notification whether this is the termination of all services provided by the vendor and transfer to a new contracted vendor (termination of the contract in its entirety, or leaving some of the services with the vendor and transferring some of them to a new contract.

5.13.4.7. In both cases the vendor is obliged to abide by the separation plan in respect of those parts of the contract which have been terminated. In the event of termination of some of such services, the consideration due to the vendor from the Ministry will be adjusted according to the extent of the services left to it. The vendor will continue to provide the services, as required to provide such services before the separation plan was initiated. These services will be provided until the end of the engagement period or until the Ministry expressly notifies in writing that it wishes to discontinue them before the end of the engagement period.

5.13.4.8. Subject to the Ministry's notification of the separation as aforesaid, the vendor must specify all the steps required in order to maintain the level of service in case the Ministry elects to use the services of another vendor. The vendor will describe, during the preparation period, the order of steps that must be taken in order to transfer services with a minimum of malfunctions, and all the steps so as to allow the Ministry to transfer the services to another party.

5.13.4.9. The separation plan will contain, among other things, what is required according to the following details: Transfer of up-to-date documentation; Transfer of inventory management files (hardware, software, licenses, etc.); Completing tasks in execution, converting existing data in the vendor's systems and exporting it including user information, content and all required, assignment of maintenance agreements,

support and assistance of vendors or subcontractors providing services to this tender; Maintaining confidentiality and destroying data after transferring it to the Ministry or to anyone on its behalf.

5.13.4.10. Any product and any information that exists and any information that will be accumulated, and relates to the vendor's services to the Ministry, is and will remain the sole property of the Ministry. The Vendor may not use and/or allow another to use any data and/or document and/or input and/or output of this information, directly or indirectly, for itself and for any other party, on its behalf or not, for consideration or not for consideration.

5.13.4.11. The assignment of the vendor's agreements with the subcontractors as specified in section 14.8 of the engagement contract will be carried out at the responsibility of the vendor during the preparation period.

5.13.4.12. The vendor shall return to the Ministry all documents, documentation, clarifications or any other detail, on any media (paper, magnetic or optical media, etc.), relating to the provision of the services. The vendor will transfer all components of the services (data and documents, etc.), in such a way that no detail remains in its hands that was not in its hands before this contract.

5.13.4.13. The vendor warrants that, at the end of the separation period, it will not leave any material, information or documentation pertaining to the Ministry and/or its related parties (subject to the law), and that it will document the process of destroying the data in its possession.

6. Additional services and products – changes and improvements ("C&I")

6.1. Ordering additional services – changes and improvements

6.1.1. For the purpose of additions, ongoing developments, related services and products, consulting, integration, changes and improvements to the system as well as professional tasks required for proper and ongoing operation of the system that are not included in the other vendor obligations under the tender documents (hereinafter: "**C&I**"), the Ministry may order from the vendor, from time to time and at its sole discretion, the performance

of such services and the vendor is obliged to perform them in accordance with the Ministry's instructions.

6.1.2. The vendor represents that it has the necessary knowledge to perform C&Is, and it undertakes that the C&Is it performs will be carried out in accordance with the manufacturer's instructions and guidelines and will not infringe on the vendor's and manufacturer's obligation for warranty for the system, equipment and services under the tender, and that these C&Is will be integrated in the system in such a manner that they do not impair is quality and operation once done.

6.1.3. The Ministry will be entitled to order C&Is from time to time under the C&Is ordering procedure as detailed in section 6.3 below.

6.1.4. The vendor will provide the C&Is through staff members (as defined in section 5.2 above), but the Ministry may request that the vendor provide additional and/or other service providers for the execution of the C&Is.

6.2. **Ordering additional products and services**

6.2.1. The Ministry reserves the right, in accordance with the quote in the tender or alternatively in accordance with the C&Is procedure detailed in section 6.3 below and all according to the Ministry's decision, to order items such as:

6.2.1.1. Duplication of the system as specified in section 6.2.3.

6.2.1.2. A signature portal as specified in section 6.2.4.

6.2.1.3. Certificate authority service as specified in section 6.2.5.

6.2.1.4. Additional products and services within the framework of the tender, as specified in section 6.3.

6.2.2. It is clarified that the Ministry has sole and absolute discretion to purchase the additional products, and that this right is a unilateral right that does not bind the Ministry in any way and the Ministry may publish a different and separate tender for each such product or group of products.

6.2.3. **System duplication**

6.2.3.1. The Ministry reserves the right to set up the system to meet both the requirements for a secure signature and the unique requirements for a certified signature, subject to technological feasibility and subject to obtaining approvals from the Ministry of Justice's Privacy Protection Authority.

6.2.3.2. Should the Ministry require for this purpose (or for any other reason) the duplication of the system into two separate systems – one for a secure signature and the other for a certified signature – the Ministry will pay the vendor as specified in the quote chapter and in accordance with the provisions below:

A. The price includes all the components required for the duplicate system, including its supply, installation, implementation of interfaces and adjustments, if required, in the production environment, all according to the Ministry's instructions.

B. The price for the number of users will depend on the price of a package of users that will be used **cumulatively** for both systems.

6.2.4. **The Signatures Portal**

6.2.4.1. **General**

A. The Signatures Portal will allow end users to perform through an Internet interface, signatures on files as well as verify the correctness of signatures of existing files in all protocols supported by the Ministry (hereinafter: "**Signatures Portal**"). Through the portal, registered users will be able to sign files without installing local software on their computers.

B. The Signatures Portal will allow the Ministry to maintain the signature software without distributing versions and ensure signature integrity online and without installing local software. For a signature according to standards that are not supported in PDF, this will be an available option to verify the signature and extract the original signed files.

C. Users – For the purposes of this section, any user registered on the system who has a certificate and keys in the Central Signature System. In accordance with the Ministry's requirement, the Signatures Portal will be defined as an identified service through the government identification

system. On the other hand, for the purpose of verifying and validating the signature (authentication), no identification will be required and the service will be open to anyone who is required to verify the correctness of a signature.

D. Development Technology – If the vendor develops the portal as required, the vendor will be allowed to use any technology that enables the development of a web application. On the client side, the implementation will be in HTML + Javascript and on the server side any relevant technology (c#, Java, JavaScript, etc.) and provided that it can interface with the government identification system.

E. Environments: The vendor will provide at least three environments – development, testing and production.

F. Maintenance – The vendor will be required to maintain the Signatures Portal and make necessary repairs (bug fixes, security vulnerability fixes and any other flaws), in accordance with the schedules set forth below in section 7.1.4. Also, in the event that additional requirements are added in the future, the vendor will be required to provide development services according to the rates specified in its offer. In any event, the vendor will provide the Ministry with the source code for the developments performed by it so that the Ministry will be able to maintain the Signatures Portal itself.

G. End Device Support – The Signatures Portal will run optimally on any end device that allows running an up-to-date browser, including mobile devices – phones, tablets and PCs.

H. The portal display layer will be accessible in accordance with the accessibility requirements and regulations at AA level, at least.

I. Data Security -

1) The system will support a secure file upload process that includes policy mechanism support such as: file types, size, black list, white list.
2) The system will support an API connection to the e-Government scan and content disarm systems, the file scans will be performed by sending the file by the system to the e-Government content disarm system using API access.

6.2.4.2. **Supply of the Signatures Portal and its implementation and installation**

A. Upon the Ministry's order, the vendor will provide and install the Signatures Portal on the e-Government website or alternatively in a cloud configuration as directed by the Ministry. It is the Ministry's responsibility to interface it to e-Government systems (such as – to the government identification system).

B. The vendor will be required to integrate the Signatures Portal in accordance with the e-Government requirements including the information security requirements as set out in section 4 respectively, and adaptation to changes mandatory under the requirements set out above, if any.

C. The vendor will be required to allow user interface modification as per e-Government requirement. The GUI components themselves will be written as needed by the e-Government development teams.

D. Upon completion of the integration, as required by the Ministry, and in coordination, the vendor will provide e-Government with the source code of the Signatures Portal, including appropriate documentation so that it can continue to maintain and develop the portal independently.

E. The exercising of the Signatures Portal will be done within 45 working days from the date of the

order, or alternatively according to the work plan that will be determined, all according to the Ministry's decision and according to the fulfillment requirements as stated above.

F. The fee for the portal, as specified in the quote section, will include all costs for all required activities, including licenses, analysis, planning, design, establishing the infrastructure and management interface, detailed characterization, development, installation, project management, testing, documentation and any other cost, until the operational activation of the portal inclusive.

6.2.5. **Certificate authority service**

6.2.5.1. At the request of the Ministry, and if the vendor has a "certificate authority" solution, the vendor will be required to provide any document, characterization, and detail on the service offered in accordance with the Ministry's requirements, including details of the protocols required to submit requests, the manner of saving of the keys, and any other relevant details required.

6.2.5.2. According to the Ministry's order, and if the vendor has such a solution, the vendor will provide a certificate authority service, which will be able to issue certificates for signature for the entities/ some of the entities that will be created in the signature server.

6.2.5.3. Can provide the certificate authority service either as an internal module (as part of the system) or as an external service that the signature server can utilize – according to the bidder's proposal.

6.2.5.4. The vendor shall, should the service be commissioned, provide and install any component and interface necessary between the signature system and the certificate authority service, as well as have the service undergo tests in general and information security tests in particular, and correct their findings in accordance with the Ministry's requirements and specified in this tender.

6.2.6. **Cloud environment**

The requirement in this tender is for the establishment of the infrastructure at available e-Government sites. The Ministry will examine in the future the possibility of transferring the system, in whole or in part, to a cloud environment, should it become relevant and at the Ministry's discretion only.

6.3. **C&Is ordering procedure**

C&Is will be ordered in accordance with the following procedure:

6.3.1. The contract manager on behalf of the Ministry, as defined in the contract, will ask the vendor to submit a proposal for the execution of C&Is. The proposal will be submitted within the time set by the Ministry. The proposal will be detailed and included the characterization required for execution, an assessment as to the total estimated hours, a financial estimate based on the number of estimated hours, multiplied by the relevant tariff for those professionals and net of the discount specified in the vendor's proposal, detailing the professional service providers, the schedule for the C&Is, expected and possible effects of the C&Is on the system and the performance of other vendor obligations, and anything else that may be requested by the contract manager.

6.3.2. The C&Is will be executed in accordance with the Ministry's decision and at its sole discretion, in one of the following ways: either at a cost per hour, in accordance with actual hours, or alternatively – at a total price in accordance with the vendor's proposal in the above section. In case of a total price, the milestones for payment will be agreed upon.

6.3.3. The vendor's proposal will be submitted to the contract manager on behalf of the Ministry.

6.3.4. The Ministry will be entitled to contact the vendor regarding any component included in its proposal and request clarifications/ completions/ updates/ changes regarding it. It will be clarified that at any stage, the Ministry may approve or reject the vendor's updated proposal, conduct further negotiations in relation thereto, or change the method of engagement – all at its sole discretion.

6.3.5. Only after the contract manager's written confirmation of the vendor's proposal (original or updated) will the Ministry issue a suitable order duly signed by the authorized signatories empowered to bind the Ministry.

6.3.6. The vendor acknowledges that it is aware that the commencement of the C&Is by it is conditional upon the issuance of an appropriate

order duly signed for the C&Is and upon compliance with the other provisions of this section and that the Ministry will have no obligation to accept the vendor's proposal.

6.3.7. Once the order for C&Is has been issued, the vendor will update any documentation that needs to be updated in accordance with the order, including the work plan, which will include, among other things, the work to be performed, and how the plan meets the Ministry's requirements, work steps, schedule (including start and end dates of the performance of the C&Is), all the changes and impacts (if any) on the system, and any other such impact on the services (hereinafter: the "C&Is Plan").

6.3.8. The vendor will keep a detailed work log in which it will document all the actions performed by it as part of the provision of the C&Is to the Ministry.

6.3.9. In the event the C&Is were performed at hourly rates, as part of the vendor's monthly report in relation to the services the subject of the contract provided by it, the vendor will submit to the contract manager on behalf of the Ministry, for inspection and approval, a detailed report that includes a monthly concentration of these hours, including details of business hours and components, if any. This report will be submitted for review and approval by the Ministry's contract manager as part of the vendor's ongoing conduct regarding reporting and payment of consideration for the contracted services, all as set out in sections 7-9 of the contract.

6.3.10. Payment for C&Is at a total price will be done in accordance with the agreed milestones.

6.3.11. Each C&I will be submitted to the Ministry's tests in accordance with the testing procedures described above, or as agreed between the parties. Each task will undergo a series of delivery tests by the vendor in a testing environment. After the delivery tests, the vendor will deliver the C&I to the Ministry for the purpose of conducting acceptance tests, which will be performed at the Ministry's discretion. The C&I will be installed in a production environment only after receiving written approval from the Ministry.

6.3.12. Payment to the vendor will be made after the written approval of the contract manager on the execution of the C&I to his satisfaction and approval of the report and in accordance with the payment procedure customary in the Ministry.

6.3.13. It is clarified that the Ministry may carry out tasks independently through staff members on behalf of the Ministry, or through any

other party whom the Ministry elects to engage, and that the said procedure does not oblige the Ministry to turn to the vendor with a request for proposals.

7. Service Level Agreement (SLA)

7.1.1. The Service Agreement is a tool in the hands of the Ministry to define policies and priorities for delivery, liability and to carry out supervision over the vendor for the fulfillment of the vendor's obligations under the contract.

7.1.2. The Vendor undertakes to comply with the response times set forth below in the Service Level Agreement for service calls and/or operations calls, and accordingly, the vendor undertakes continuous, ongoing and strenuous work within the work day, while allocating the appropriate and necessary personnel to resolve the problem.

7.1.3. The call window for receipt of service, the response time for handling faults, the manner of handling the products and equipment and the nature of the coverage, will be in accordance with what is detailed below, as well as in accordance with all the conditions specified in the technical specifications and the contract.

7.1.4. The vendor must meet the following response times for service calls. The service call times themselves are listed above in section 5.12.4.1:

Type of malfunction	**Description of the malfunction type**	**Service window**	**Response time/ handling time – Tender requirements**
Waiting time for a human response at the call center			Up to five minutes.
Critical	Disables the system	7*24	Start of handling of the malfunction within a maximum of 10 minutes during business hours from the time the call is opened at the call center and within 30 minutes when the call is not opened during business hours.

Type of malfunction	**Description of the malfunction type**	**Service window**	**Response time/ handling time – Tender requirements**
			In the event that professionals on behalf of the vendor need to arrive at the Ministry's facility, arrival time at the Ministry site will be within 2 hours of the call opening. The handling will be carried out continuously until the malfunction is resolved, in any way required both during business hours and outside business hours, including, if necessary, hardware replacement by the next day (NBD).
Severe	Disables a service or component in the system or several of them or use of the system capabilities	Business hours	Start of handling of the malfunction within a maximum of 1 hour from the time the call is opened at the call center. In case of reporting after 18:00, the handling of the malfunction will begin on the next business day, by 09:00 at the latest. In the event that professionals on behalf of the vendor need to arrive at the Ministry's facility, arrival time at the Ministry site will be within 4 hours of the call opening. The handling will be carried out continuously during business hours depending on the level of maintenance until the malfunction is resolved.

Type of malfunction	**Description of the malfunction type**	**Service window**	**Response time/ handling time – Tender requirements**
Ordinary	Is not critical or severe/ non-compliance with the tender requirements	Business hours	Start of handling of a malfunction reported until 12:00 will be on the same day until 18:00. If a malfunction is reported after 12:00, handling will begin on the following business day until 12:00 noon. In the event that professionals on behalf of the vendor need to arrive at the Ministry's facility, arrival time at the Ministry site will be within 8 hours of the call opening. The handling will be carried out during the entire business day until the malfunction is resolved.
Worsening			In the event that professionals on behalf of the vendor need to arrive at the Ministry's facility, arrival time at the Ministry site will be according to the agreement with the vendor.
Information Security Event	An information security event and/or threat of such an event will be classified as a "critical malfunction", unless the Ministry's classification, at its discretion, is of a lesser degree of severity.		Solutions for the event will be provided within a time frame defined for a **critical malfunction**, or otherwise in accordance with the prescribed classification.
Non-compliance with	Failure to meet performance requirements will be classified as a "critical		Solutions for the event will be provided within a time frame defined for a **critical malfunction**, or otherwise in accordance with the

Type of malfunction	Description of the malfunction type	Service window	Response time/ handling time – Tender requirements
performance requirements	malfunction", unless the Ministry's classification, at its discretion, is of a lesser degree of severity.		prescribed classification.

7.2. **Liquidated damages for breach of the Service level Agreement**

7.2.1. If the vendor does not meet the service levels defined in the table above, the vendor will pay liquidated damages as detailed in the table below.

7.2.2. The realization of the liquidated damages by the Ministry can and will be done by way of offsetting an invoice under process of signing and approval of an authorized signatory on behalf of the Ministry and/or by the Ministry in any other way.

7.2.3. The damages specified in the table do not prevent the Ministry from exercising any other sanction against the vendor, including filing a claim for all of its actual damages and/or forfeiting the performance guarantee.

Topic	Liquidated damages for non-compliance with the tender requirements
Waiting for a response to opening a call at the call center	NIS 100 compensation for every 5 minutes of delay in human response
Response time for a critical malfunction or non-handling according to the Ministry's requirements	NIS 500 compensation for every 15 minutes delay at the beginning of handling a malfunction and/or the arrival of the professionals at the Ministry facility and/or failure to handle in accordance with the tender requirements
Response time for a severe malfunction or non-handling according to the Ministry's requirements	NIS 500 compensation for every 1-hour delay at the beginning of handling a malfunction and/or failure to handle in accordance with the tender requirements

Topic	Liquidated damages for non-compliance with the tender requirements
Response time for an ordinary malfunction or non-handling according to the Ministry's requirements	NIS 250 compensation for every 1-hour delay at the beginning of handling a malfunction and/or failure to handle in accordance with the tender requirements
Delay in excess of 7 business days in the delivery of the service or equipment and its installation.	NIS 1,500 compensation for every day of delay
Delay in meeting milestone schedules set in a work plan or in the Ministry's order.	NIS 1,000 compensation for each day of late delivery of a milestone in the work plan or order. NIS 5,000 compensation for each day of late delivery of the system in a production environment.

7.3. **Fundamental breach of the Service Level Agreement (SLA)**

Without prejudice to any other right or remedy conferred on the Ministry under the contract and/or by any law, the following is a list of breaches of the Service Level Agreement (SLA) which will constitute a fundamental breach of the contract for which the Ministry may terminate the contract:

A. The vendor does not provide a solution to a critical malfunction within 7 days.

B. Delay in delivery of the systems and/or equipment in excess of 7 business days from the date set for delivery in the order.

C. Violation of terms of the SLA as set out below:

Quality of service component	Description of the breach
Response time and handling of the malfunction	Over 30% deviation in response time to malfunctions (critical, severe, or ordinary) and/or in their treatment, according to a documented record of the Ministry representatives.
Providing a service that does not	5 times or more of deviation, within a period of six months,

Quality of service component	**Description of the breach**
meet the tender requirements on all its appendices and parts	in the delivery of service that does not meet the tender requirements, according to documented complaints of the Ministry.
Deviation in performance	5 times or more of deviation, within a period of six months, of a decrease of more than 10% in the system performance (minimum and maximum), according to the tender requirements.
Information security events	5or more information security events, within a period of six months.

Appendix 2-A

Description of the Central Signature Service System Architecture

1. **General**
   - 1.1 This appendix presents the architectural concept of the Central Signature Service System.
   - 1.2 The final architecture will be determined according to the principles listed below, and according to the vendor's proposal, within the framework of the design phase – the detailed design.
   - 1.3 The product tree of the system is presented above in section 1.2 of Chapter 2.
   - 1.4 The architecture is presented in a number of use cases that the system is supposed to support.
   - 1.5 The architecture is presented as follows:
     - 1.5.1 Description of system components – in Section 2.
     - 1.5.2 Scenarios of key generations and issuance of an initial digital certificate – in section 3.
     - 1.5.3 Signature scenarios – in section 4.
     - 1.5.4 Authentication scenarios – in section 5.

2. **Description of the system components**
   - 2.1 Internal components of the system:
     - 2.1.1 Central Signature Server: delivery under the vendor's responsibility:

Central Signature Server

שרת חתימות מרכזי

     - 2.1.2 HSM: Can be included in the central signature server, as part of the appliance or as a separate component. delivery under the vendor's responsibility:

     - 2.1.3 Management Components and Application Interfaces:
       Below is a table of the division of responsibilities for the management components and interfaces, according to the above product tree diagram, including the responsibility for the supply, and whether the

component is an integral part of the system supply or is optional (optional components will be handled according to the C&I ordering procedure as specified in section 6.3 above):

Component number	**Component name**	**Under the responsibility of**	**Mandatory/ optional**
Sub-system 1	Central Signatures Server	The vendor	Mandatory
Sub-system 2	HSM component	The vendor	Mandatory
Sub-system 3	Software component and interfaces	According to the detailing below	
Module 3.1	Software component	According to the detailing below	
3.1.1	User interface and management system	The vendor	Mandatory
3.1.2	Registration component	The vendor	Optional – according to the Ministry's decision
3.1.3	Signature component in the signatures portal	The vendor	Optional – according to the Ministry's decision
3.1.4	Signature component in the application	The vendor	Optional – according to the Ministry's decision
3.1.5	Authentication component	The vendor	Mandatory
3.1.6	Timestamp component	The vendor	Mandatory
3.2	Interfaces	According to the detailing below	
3.2.1	Interface to the certificate authority system	The vendor	Mandatory (in accordance with the provisions of section 5.8.1.2)
3.2.2	Interface to the identification system		
3.2.3	Interface for information gateway		
3.2.4	Signature interface	The vendor	Mandatory

3.2.5	Interface to the information security system	The vendor	Mandatory
3.2.6	Interface to the C&C system	The vendor	Mandatory
3.2.7	Time clock interface	The vendor	Mandatory
3.2.8	Timestamp Interface (TSA)	The vendor	Mandatory

2.2 **System interfaces (direct and indirect) in different scenarios**:

2.2.1 The responsibility for the external systems is with the Ministry.

2.2.2 The vendor is responsible for the implementation of the interfaces for these systems, in accordance with the specifications for each interface in the technical requirements of the tender.

2.2.3 The Government Identification System:

2.2.4 The information gateway:

2.2.5 Applied Web server (including MERKAVA, or other non-hosted systems available in e-Government):

2.2.6 CA GAMAM (Optional – Other CA):

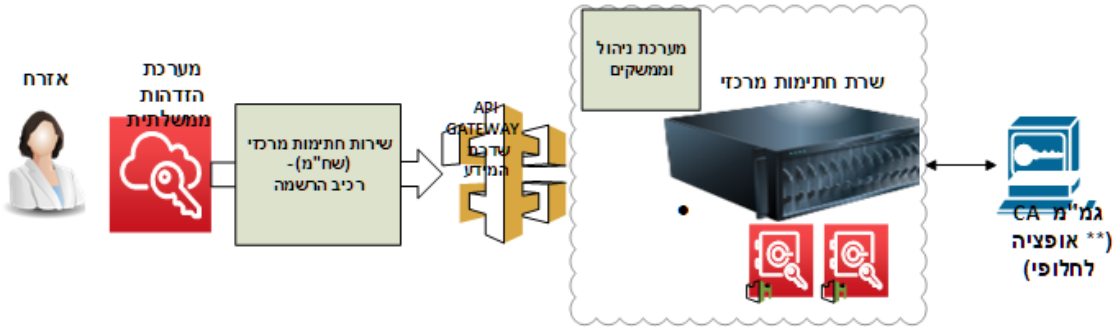
CA גמ"מ

2.2.7 CA THAMMUZ:

CA תמו"ז

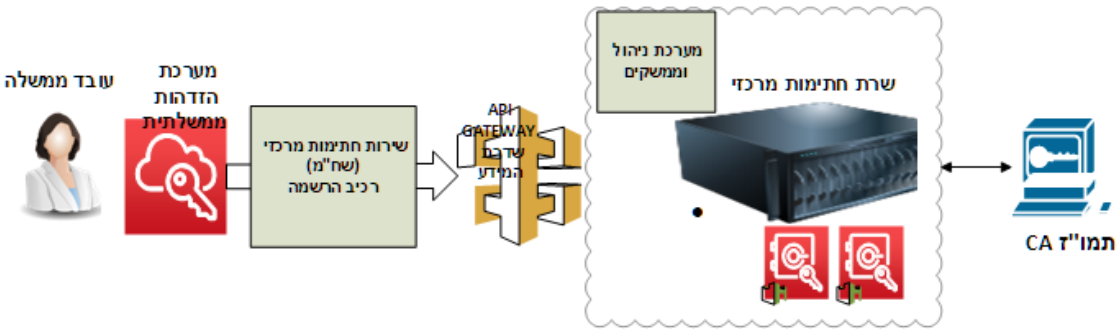
3. **Key generation scenarios and issuance of an initial digital certificate**:

3.1 **Citizen**



*CA GAMAM (** option for an alternative)*	*Central signatures server*	*Management system and interfaces*	*API gateway*	*Central signatures services – registration component*	*Government identification system*	*Citizen*

3.2 **Government employee**:



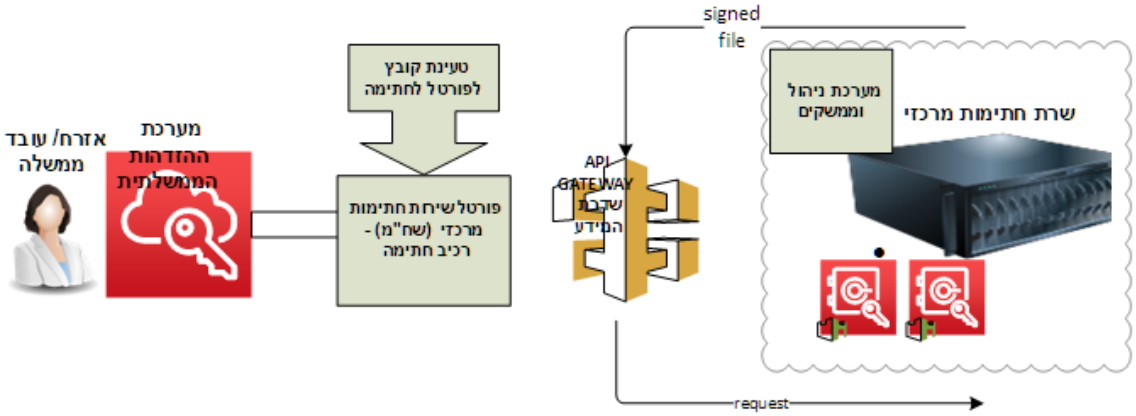
CA THAMMUZ	*Central signatures server*	*Management system and interfaces*	*API gateway*	*Central signatures services – registration component*	*Government identification system*	*Government employee*

3.3 **<u>Organizational seal</u>**:

Signature server	*Management interface for the generation of a certificate for the machine*

4. **<u>Signature</u>**:

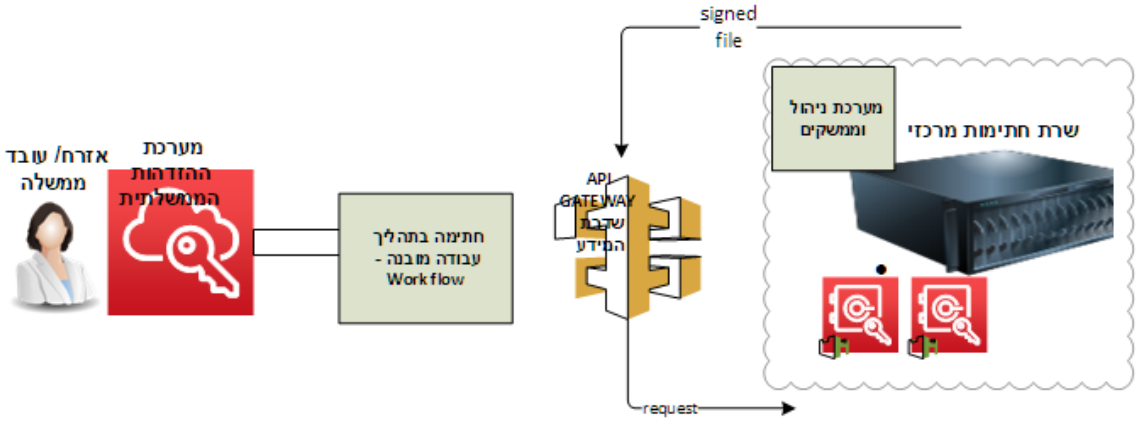
4.1 **<u>Signature process using WEB application interface (for citizen/ government employee from an office system)</u>**:



Central signatures server	*Management system and interfaces*	*Signed file*	*API gateway*	*Loading a file to the portal for signature*	*Government identification system*	*Citizen/ Government employee*
				Central signatures services –		

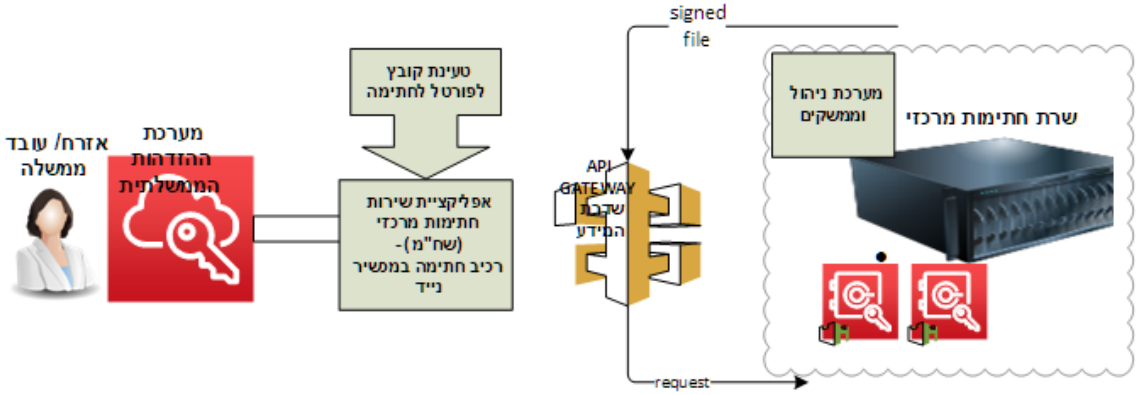
				registration component		

4.2 **Signature in a structured work process**



Central signatures server	*Management system and interfaces*	*Signed file*	*API gateway*	*Signature in a structured work process – work flow*	*Government identification system*	*Citizen/ Government employee*
		Request				

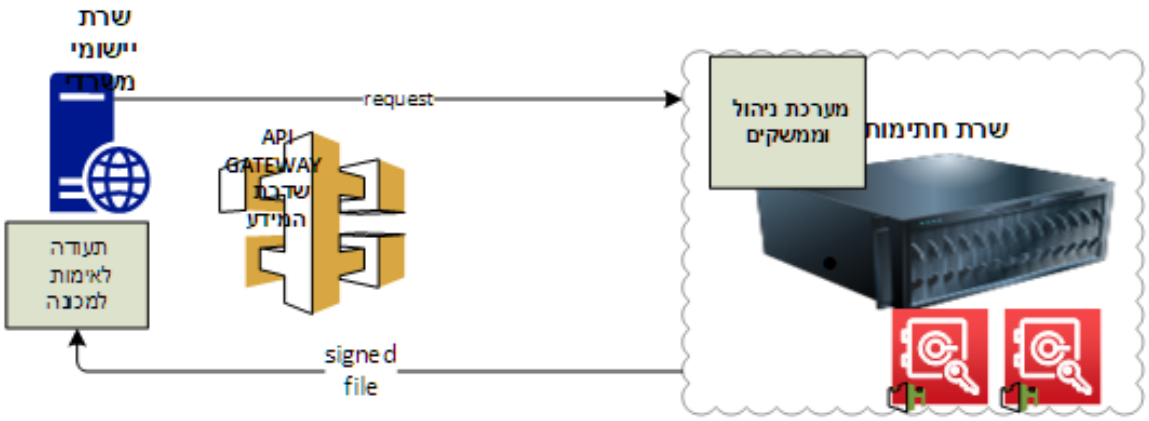
4.3 **Signature using mobile application interface**:



Central signatures server	*Management system and interfaces*	*Signed file*	*API gateway*	*Loading a file to the portal for signature*	*Government identification system*	*Citizen/ Government employee*
		Request		*Central signature service app*		

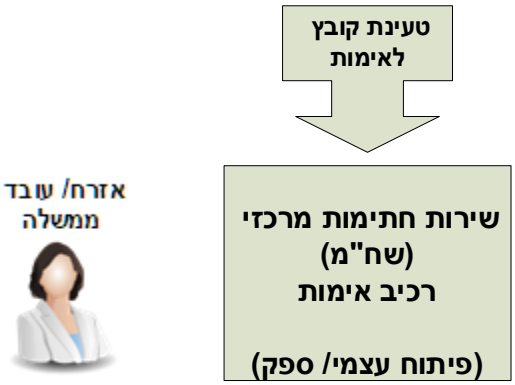
				– signature component in a mobile device		

4.4 **Organizational seal (machine signing)**



Central signatures server	*Management system and interfaces*	*Request*	*API gateway*	*Certificate for machine authentication*
		Signed file		

5. **Authentication**



Loading a file for authentication	
Central signature service app – authentication component (self-development/ vendor)	*Citizen/ Government employee*