RFP for Supply, Installation, Implementation, Integration and Maintenance of Hardware Security Module (HSM) Technology solution for Digital Signatures and Key Management solution for Encryption

Tender Reference No.: OICL/HO/ITD/HSM/2022/01 Dated 19/04/2022

Response to Pre-Bid Queries

Sl. No.	RFP Page No.	Point / Section #	Existing Clause	Query Sought	OICL Reply
1	17	1.6 Project Timelines	1. Supply and delivery of Appliance, Software and Hardware at DC and DR - Deliver at OICL respective locations within 6 weeks from the date of issuance of Purchase Order 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations - Within 8 Weeks from the date of issuance of purchase order 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) - Within 10 Weeks from the date of issuance of purchase order 4. Trainings - All the trainings to be completed within 1 week from the date of request for training from OICL 5. Disaster Recovery Drill - Within 2 weeks from the date of request from OICL	In view of the global shortage of chips which has resulted in the built-up stress in the supply chain of all IT equipment and other COVID-19 related restrictions we would request OICL to kindly amend the delivery timeline as suggested below: 1. Supply and delivery of Appliance, Software and Hardware at DC and DR - Deliver at OICL respective locations within 12 weeks from the date of issuance of Purchase Order 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations - Within 14 Weeks from the date of issuance of purchase order 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) - Within 16 Weeks from the date of issuance of purchase order 4. Trainings - All the trainings to be completed within 2 weeks from the date of request for training from OICL 5. Disaster Recovery Drill - Within 4 weeks from the date of request from OICL	**Revised Timelines :** 1. Supply and delivery of Appliance, Software and Hardware at DC and DR = Deliver at OICL respective locations within **10 weeks** from the date of issuance of Purchase Order, 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations= Within **12 Weeks** from the date of issuance of purchase order, 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) = Within **14 Weeks** from the date of issuance of purchase order , 4. Trainings = All the trainings to be completed within 1 week from the date of request for training from OICL , 4. Disaster Recovery Drill = Within 2 weeks from the date of request from OICL
2	17	2.1 Scope for Digitally Signing of Documents using HSM technology	These documents (namely Policy Schedule, Collection Receipt, Terms & Conditions Document, etc.) that are generated on a real time basis by the OICL's Core Insurance System (INLIAS) are required to be digitally signed in real time as these are shared with customers.	Please clarify if there will be SSO between the existing INLIAS system and the signing solution?	**Clarification:** As of now there is no SSO between INLIAS system and signing application.
3	18	7/2.2 Scope for key Management Solution	To ensure optimal data protection, solution provided must support the 'Bring Your Own Key (BYOK)' model or "Host your own Key (HYOK)" and take end-to-end responsibility of securely storing and managing the encryption keys used by its "Cloud Service Providers(CSPs)" during the encryption process on-premise on a FIPS 140-3 or above certified Key Management appliance	Since the Key Management appliance is backed up with HSM which FIPS 140-2 level 3 , we would request OICL to kindly change the clause to reflect the same as suggested here - "*during the encryption process on-premise on a FIPS 140-2 Level 3 or above certified Key Management appliance.* "	**Revised Clause:** To ensure optimal data protection, solution provided must support the 'Bring Your Own Key (BYOK)' model or "Host your own Key (HYOK)" and take end-to-end responsibility of securely storing and managing the encryption keys used by its "Cloud Service Providers(CSPs)" during the encryption process on-premise on a FIPS 140-2 Level 3 or above certified Key Management appliance.
4	20	2.3 General Scope	xx. The Bidder will have to provide full operational, maintenance and technical support during the entire period of the contract.	Please confirm if OICL will allow remote access to the solution setup for providing technical support from our centralized help desk.	**Clarification:** Bidder needs to provide full operational, maintenance and technical support during the entire period of the contract with remote access but in case it is required to visit any of the data centers/head office then bidder must send the competent resources to the designated site for any kind of troubleshooting. Further bidders are requested to visit clause 2.4 and 2.5 for more clarity.
5	23	2.5 Facility Management Services	1) Bidder shall provide 24 x 7 on call support for regular maintenance of the systems and overall solution for complete duration of contract. These resources should be field engineers of L1 & L2 level with ability to resolve any severity issues that may arise during the period. Resources are responsible for both sites.	Under Scope of work, OICL has mentioned that L1 & L2 resources are required **on call basis**, i.e. bidder needs to provide the required support (L1 & L2) as and when support is required basis any issue being faced by OICL. However, OICL has asked commercials to be submitted as FMS Services in Appendix 2 : Bill of Material. Request for clarity whether the resources are to be deployed onsite for 24 x 7 or resources would be required on call basis.	**Clarification:** Bidder needs to provide full operational, maintenance and technical support during the entire period of the contract with remote access but in case it is required to visit any of the data centers/head office then bidder must send the competent resources to the designated site for any kind of troubleshooting. Further bidders are requested to visit clause 2.4 and 2.5 for more clarity.
6	78 / 80/ 88	10.2 Appendix 2: Bill of Material	Summary of Total Cost FM Manpower Cost	In case resources are to be deployed onsite, please share the no. of L1 & L2 resources to be deployed.	**Clarification:** Bidder needs to provide full operational, maintenance and technical support during the entire period of the contract with remote access but in case it is required to visit any of the data centers/head office then bidder must send the competent resources to the designated site for any kind of troubleshooting. Further bidders are requested to visit clause 2.4 and 2.5 for more clarity.
7	28	3.1.9 Payment Terms	AMC/ATS The AMC/ATS shall commence on completion of the warranty period. The AMC & ATS will be treated as a part of the total cost of the project. - Quarterly in arrears	We would request OICL to kindly amend the AMC / ATS related payment term as suggested below to align with the industry standard: AMC/ATS The AMC/ATS shall commence on completion of the warranty period. The AMC & ATS will be treated as a part of the total cost of the project. - Annually in advance	Please be guided by RFP
8	28	OICL RFP : 3.2 Other RFP Requirements GEM RFP : 1.2 other RFP requirement	b. Technical Inspection and Performance Evaluation - OICL may choose to carry out a technical inspection/audit and performance evaluation of products/services offered by the Bidder. The Bidder would permit OICL or any person / persons appointed by OICL to observe the technical and performance evaluation / benchmarks carried out by the Bidder. Any expenses (performing the benchmark, travel, stay, etc.) incurred for the same would be borne by the Bidder and under no circumstances the same would be reimbursed to the Bidder by OICL.	As per the said clause, we understand that the successful bidder will have to permit OICL or any person/ persons appointed by OICL for carrying out technical and performance evaluation / benchmarks. However, in case any expenses (like benchmarking, travel, stay, etc..) are incurred, the same shall be borne by bidder for their employees and OICL will bear the expenses for their employees / persons appointed by them. Please clarify.	**Revised Clause:** Technical Inspection and Performance Evaluation - OICL may choose to carry out a technical inspection/audit and performance evaluation of products/services offered by the Bidder. The Bidder would permit OICL or any person / persons appointed by OICL to observe the technical and performance evaluation / benchmarks carried out by the Bidder. Any expenses (performing the benchmark etc.) incurred for the same would be borne by the Bidder and under no circumstances the same would be reimbursed to the Bidder by OICL.
9	74	10.1 Appendix 1: Technical and Functional Specifications	4. System should be capable of signing multiple formats including PDF, Zip files etc.	All other formats apart from PDF will get signed as PKCS#7 attached signature. Please confirm if this is fine or something else is required.	understanding is correct
10	74	10.1 Appendix 1: Technical and Functional Specifications	11. System should have measures to control the documents which can be signed.	How will the solution know which documents are to be signed and which are not to be signed? What criteria are expected to be used? Please help to define the rules for identifying the documents which are okay for signing.	**Clarification :** As per current scenario every document passed on to signing solution will get signed. In case any rules/criteria were required in future , the selected bidder will draft the rules in coordination with existing application owner/OICL.
11	74	10.1 Appendix 1: Technical and Functional Specifications	14. No un-authenticated document should be allowed to be signed.	How will the solution know which documents are to be signed and which are not to be signed? What criteria are expected to be used? Please help to define the rules for identifying the documents which are okay for signing.	**Clarification :** As per current scenario every document passed on to signing solution will get signed. In case any rules/criteria were required in future , the selected bidder will draft the rules in coordination with existing application owner/OICL.
12	74	10.1 Appendix 1: Technical and Functional Specifications	15. Should be able to send the daily status report of success & failure.	Daily reports are generated as audit-trail logs in CSV format. Please confirm if the solution should also have the facility for sending the audit-trail logs as email.	**Clarification:** The solution should have capability to integrate with SMTP server/solution for sending automated reports.
13	74	10.1 Appendix 1: Technical and Functional Specifications	16. System should have Security level based access control.	The proposed solution supports role based access control. There are different roles like user, profile administrator, signer, company administrator etc. Please confirm if anything more is required to address the requirement of OICL.	understanding is correct
14	74	10.1 Appendix 1: Technical and Functional Specifications	19. The proposed solution should support instant real time signing and should integrate with OICL Application.	For integrating with OICL application, we can provide a web-service interface (SOAP or REST as per customer need) to do things like pushing documents in the system, triggering signing, pulling signed documents from the system, etc. Is anything else needed?	understanding is correct
15	74	10.1 Appendix 1: Technical and Functional Specifications	General query	Please confirm the number of "signers". How many DSCs would be on the HSM?	approx. 10-12 digital signatures
16	74	10.1 Appendix 1: Technical and Functional Specifications	General query	On how many servers would the solution be installed? Would OICL provide and configure load-balancer for achieving load distribution and high availability? How many machines in all, including DC / DR, production / UAT, etc. would be required?	**Clarification:** Currently solution is installed at 2 servers at DC and at 1 server at DR. In future if OICL intendes to use physical load balancer for load distribution among servers, the onus of integrating solution with Load balancer will be of bidder, necessary support will be provided from OICL.

RFP for Supply, Installation, Implementation, Integration and Maintenance of Hardware Security Module (HSM) Technology solution for Digital Signatures and Key Management solution for Encryption
Tender Reference No.: OICL/HO/ITD/HSM/2022/01 Dated 19/04/2022
Response to Pre-Bid Queries

Sl. No.	RFP Page No.	Point / Section #	Existing Clause	Query Sought	OICL Reply
17	76	58/Appendix 1: Technical and Functional Specifications	The solution shall discover, create, renew and manage all the keys across heterogeneous environments and different geographical locations.	The discovery is applicable for the crypto objects when offloaded via external mechanism. Since OICL is using KMS which would generate keys and distribute, we would request OICL to kindly change the clause as suggested herewith: "*The solution shall create, renew and manage all the keys across heterogeneous environments and different geographical locations.* "	**Revised clause:** The solution shall create, renew and manage all the keys across heterogeneous environments and different geographical locations.
18	18	2.2 Scope for key Management Solution	The Key Management solution must have the capabilities to protect data against the physical theft of disk drives or Storage systems through it's support of standards-based (KMIP) encryption systems that are deployed with embedded encryption solutions ensuring that even if the disk drives (physical or virtual) are stolen, the data stored within them remains protected against unauthorized access.	Our understanding of this clause is that please correct "the KMS should work on KMIP and should support encryption solutions which supports KMIP protocol. Actual encryption of disk drives or Storage Systems, protecting data against physical theft is under encryption solution's scope"	Please be guided RFP.
19	22	Functional and Technical Requirement	The proposed box should be Common Criteria EAL 4+ certified.	FIPS and EAL4+ both works on different firmware's and digital signature CCA india has suggested FIPS 140-2 Level 3 compliant solution, so we request your kind authorities to kindly remove EAL4+ requirement as CCA do not allow to store Certificates in EAL4+ Device.	**Revised Clause :** The proposed HSM box/ cryptographic module used should have Common Criteria EAL 4+ certification in the name of the proposed OEM.
20	22	Functional and Technical Requirement	The proposed box should be Common Criteria EAL 4+ certified.	Also Non of the Box are EAL4+ certified, only Cryptographic module used inside Appliance is EAL4+ certified, so we would we request your kind authorities to modify "Box" to "Cryptographic Module".	**Revised Clause :** The proposed HSM box/ cryptographic module used should have Common Criteria EAL 4+ certification in the name of the proposed OEM.
21	18	2.2 Scope for key Management Solution	The Key Management solution must have the capabilities to protect data against the physical theft of disk drives or Storage systems through it's support of standards-based (KMIP) encryption systems that are deployed with embedded encryption solutions ensuring that even if the disk drives (physical or virtual) are stolen, the data stored within them remains protected against unauthorized access.	Our understanding of this clause is that please correct "the KMS should work on KMIP and should support encryption solutions which supports KMIP protocol. Actual encryption of disk drives or Storage Systems, protecting data against physical theft is under encryption solution's scope"	Please be guided by RFP.
22	19	22	Functional and Technical Requirement	FIPS and EAL4+ both works on different firmware's and digital signature CCA india has suggested FIPS 140-2 Level 3 compliant solution, so we request your kind authorities to kindly remove EAL4+ requirement as CCA do not allow to store Certificates in EAL4+ Device.	**Revised Clause :** The proposed HSM box/ cryptographic module used should have Common Criteria EAL 4+ certification in the name of the proposed OEM.
23	19	22	Functional and Technical Requirement	Also Non of the Box are EAL4+ certified, only Cryptographic module used inside Appliance is EAL4+ certified, so we would we request your kind authorities to modify "Box" to "Cryptographic Module".	**Revised Clause :** The proposed HSM box/ cryptographic module used should have Common Criteria EAL 4+ certification in the name of the proposed OEM.
24	18	2.2 Scope for key Management Solution	The Key Management solution must have the capabilities to protect data against the physical theft of disk drives or Storage systems through it's support of standards-based (KMIP) encryption systems that are deployed with embedded encryption solutions ensuring that even if the disk drives (physical or virtual) are stolen, the data stored within them remains protected against unauthorized access.	Our understanding of this clause is that please correct "the KMS should work on KMIP and should support encryption solutions which supports KMIP protocol. Actual encryption of disk drives or Storage Systems, protecting data against physical theft is under encryption solution's scope"	Please be guided by RFP.
25	22	Functional and Technical Requirement	The proposed box should be Common Criteria EAL 4+ certified.	FIPS and EAL4+ both works on different firmware's and digital signature CCA india has suggested FIPS 140-2 Level 3 compliant solution, so we request you to please remove EAL4+ requirement as CCA do not allow to store Certificates in EAL4+ Device.	**Revised Clause :** The proposed HSM box/ cryptographic module used should have Common Criteria EAL 4+ certification in the name of the proposed OEM.
26	22	Functional and Technical Requirement	The proposed box should be Common Criteria EAL 4+ certified.	Also Non of the Box are EAL4+ certified, only Cryptographic module used inside Appliance is EAL4+ certified, so we would request you to modify "Box" to "Cryptographic Module".	**Revised Clause :** The proposed HSM box/ cryptographic module used should have Common Criteria EAL 4+ certification in the name of the proposed OEM.
27			General Query	Will there be SSO between your INLIAS system and the signing solution?	**Clarification:** As of now there is no SSO between INLIAS system and signing application.
28	74	10.1 / 4 /Appendix 1: Technical and Functional Specifications	System should be capable of signing multiple formats including PDF, Zip files etc.	All other formats apart from PDF will get signed as PKCS#7 attached signature. Is this fine or is something else needed?	understanding is correct
29	74	10.1 / 11 / Appendix 1: Technical and Functional Specifications	System should have measures to control the documents which can be signed	How will the solution know which documents are ok to be signed and which are not? What criteria are expected to be used? How do you define which documents are ok to sign?	**Clarification :** As per current scenario every document passed on to signing solution will get signed. In case any rules/criteria were required in future , the selected bidder will draft the rules in coordination with existing application owner/OICL.
30	74	10.1 / 14 / Appendix 1: Technical and Functional Specifications	No un-authenticated document should be allowed to be signed	How will the solution know which documents are ok to be signed and which are not? What criteria are expected to be used? How do you define which documents are ok to sign?	**Clarification :** As per current scenario every document passed on to signing solution will get signed. In case any rules/criteria were required in future , the selected bidder will draft the rules in coordination with existing application owner/OICL.
31	74	10.1 / 15 / Appendix 1: Technical and Functional Specifications	Should be able to send the daily status report of success & failure	Daily reports are generated as audit-trail logs in CSV format. Are they also required to be sent as email?	**Clarification:** The solution should have capability to integrate with SMTP server/solution for sending automated reports.
32	74	10.1 / 16 / Appendix 1: Technical and Functional Specifications	System should have Security level based access control	Our system supports role based access control. There are different roles like user, profile administrator, signer, company administrator etc. Is anything else needed?	Understanding is correct
33	74	10.1 / 19 /Appendix 1: Technical and Functional	The proposed solution should support instant real time signing and should integrate with OICL Application	For integrating with OICL application, we can provide a web- service interface (SOAP or REST as per customer need) to do things like pushing documents in the system,system, etc. Is anything else needed? triggering signing, pulling signed documents from the	Understanding is correct
34			General Query	How many signers are going to be there? How many DSCs on the HSM?	approx. 10-12 digital signatures
35			General Query	On how many servers would the solution be installed? Would OICL provide and configure load- balancer for achieving load distribution and high availability? How many machines in all, including DC / DR, production / UAT, etc.?	**Clarification:** Currently solution is installed at 2 servers at DC and at 1 server at DR. In future if OICL intendes to use physical load balancer for load distribution among servers, the onus of integrating solution with Load balancer will be of bidder, necessary support will be provided from OICL.
36			General Query	As per the RFP, hope there is no EMD Amount in this RFP. Pls confirm.	Please be guided by RFP
37	16	Project Timelines:	Delivery Timelines	8 Weeks should be the delivery timelines for Hardware delivery and Implementation should be 10- 12 weeks.	**Revised Timelines :** 1. Supply and delivery of Appliance, Software and Hardware at DC and DR = Deliver at OICL respective locations within **10 weeks** from the date of issuance of Purchase Order, 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations= Within **12 Weeks** from the date of issuance of purchase order, 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) = Within **14 Weeks** from the date of issuance of purchase order , 4. Trainings = All the trainings to be completed within 1 week from the date of request for training from OICL , 4. Disaster Recovery Drill = Within 2 weeks from the date of request from OICL
38	14	2.6 Existing inventory and buyback of HSM Devices	Bidder shall offer OICL for buyback of HSM devices in working/non-working condition. The Quote for the same has to be provided in the Bill of Material.	This is totally depending on OEM whether he will buyback. We request you to remove this clause	Please be guided by RFP
39	28	Payment Terms	Buy Back clause.	This is totally depending on OEM whether he will buyback. We request you to remove this clause	Please be guided by RFP
40	28	Payment Terms	ATS/AMC Payment Terms	Payment terms shall be in annual advance. We have to pay 100% advance to OEM.	Please be guided by RFP
41		FM Manpower	General Query	Is there any specific skill set required for L1/L2 resources?	please be guided by RFP.
42		FM Manpower	General Query	Do you need L1 & L2 resources in both locations DC & DR or any one of the locations. Pls clarify. How many L1 & L2 resources is required	Please be guided by RFP.
43		Commercial Format, Optional items	General Query	Optional Items are mandatory or optional to quote?	**Clarification :** Bidder has to quote all optional items.

RFP for Supply, Installation, Implementation, Integration and Maintenance of Hardware Security Module (HSM) Technology solution for Digital Signatures and Key Management solution for Encryption
Tender Reference No.: OICL/HO/ITD/HSM/2022/01 Dated 19/04/2022
Response to Pre-Bid Queries

Sl. No.	RFP Page No.	Point / Section #	Existing Clause	Query Sought	OICL Reply
44	18	7/2.2 Scope for key Management Solution	To ensure optimal data protection, solution provided must support the ‘Bring Your Own Key (BYOK)’ model or “Host your own Key (HYOK)” and take end- to-end responsibility of securely storing and managing the encryption keys used by its “Cloud Service Providers(CSPs)” during the encryption process on-premise on a FIPS 140-3 or above certified Key Management appliance.	Since the Key Management appliance is backed up with HSM which FIPS 140-2 level 3 , request you to change the clause to reflect the same "during the encryption process on-premise on a FIPS 140- 2 Level 3 or above certified Key Management appliance."	**Revised Clause:** To ensure optimal data protection, solution provided must support the ‘Bring Your Own Key (BYOK)’ model or “Host your own Key (HYOK)” and take end-to-end responsibility of securely storing and managing the encryption keys used by its “Cloud Service Providers(CSPs)” during the encryption process on-premise on a FIPS 140-2 Level 3 or above certified Key Management appliance.
45	76	58/Appendix 1: Technical and Functional Specifications	The solution shall discover, create, renew and manage all the keys across heterogeneous environments and different geographical locations	The discovery is applicable for the crypto objects when offloaded via external mechanism. Since OICL is using KMS which would generate keys and distribute, request you to change the clause to "The solution shall create, renew and manage all the keys across heterogeneous environments and different geographical locations."	**Revised clause:** The solution shall create, renew and manage all the keys across heterogeneous environments and different geographical locations.
46	28	3.1.9 Table Payments Terms	SN 1 Hardware Delivery70%, Hardware Installation 30% SN 2 Software Delivery 70%, Successful completion 30% SN 4 AMC/ATS Quarterly in arrears SN5 FM MANPOWER Quarterly in arrears	**Kindly request you to amend clause as per below** Hardware Delivery 90%, Hardware Installation 10% Software Delivery 90%, Successful completion 10% AMC/ATS Yearly Advance FM MANPOWER Monthly in arrears	Please be guided by RFP
47	16-17	1.6 Project Timeline	SN1- Supply and delivery of Appliance, Software and Hardware at DC and DR - **Deliver at OICL respective locations within 6 weeks from the date of issuance of Purchase Order** SN2- Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations- Within 8 Weeks from the date of issuance of purchase order SN3-Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR)-Within 10 Weeks from the date of issuance of purchase order Trainings - All the trainings to be completed within 1 week from the date of request for training from OICL Disaster Recovery Drill- Within 2 weeks from the date of request from OICL	Kindly request you to amend clause as per below SN1- Supply and delivery of Appliance, Software and Hardware at DC and DR - Deliver at OICL respective locations within 20 to 22 weeks from the date of issuance of Purchase Order SN2- Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations- Within 22 to 26 Weeks from the date of issuance of purchase order SN3-Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR)-Within 26 Weeks from the date of issuance of purchase order Trainings - All the trainings to be completed within 2 week from the date of request for training from OICL Disaster Recovery Drill- Within 4 weeks from the date of request from OICL	**Revised Timelines :** 1. Supply and delivery of Appliance, Software and Hardware at DC and DR = Deliver at OICL respective locations within **10 weeks** from the date of issuance of Purchase Order, 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations= Within **12 Weeks** from the date of issuance of purchase order, 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) = Within **14 Weeks** from the date of issuance of purchase order , 4. Trainings = All the trainings to be completed within 1 week from the date of request for training from OICL , 4. Disaster Recovery Drill = Within 2 weeks from the date of request from OICL
48	74	10.1 Functional and Technical Requirement Point no 4	System should be capable of signing multiple formats including PDF, Zip files etc.	All other formats apart from PDF will get signed as PKCS#7 attached signature. Is this fine or is something else needed?	understanding is correct
49	74	10.1 Functional and Technical Requirement Point no 11	How will the solution know which documents are ok to be signed and which are not? What criteria are expected to be used? How do you define which documents are ok to sign?	How will the solution know which documents are ok to be signed and which are not? What criteria are expected to be used? How do you define which documents are ok to sign?	**Clarification :** As per current scenario every document passed on to signing solution will get signed. In case any rules/criteria were required in future , the selected bidder will draft the rules in coordination with existing application owner/OICL.
50	74	10.1 Functional and Technical Requirement Point no 14:	No un-authenticated document should be allowed to be signed	· How will the solution know which documents are ok to be signed and which are not? What criteria are expected to be used? How do you define which documents are ok to sign?	**Clarification :** As per current scenario every document passed on to signing solution will get signed. In case any rules/criteria were required in future , the selected bidder will draft the rules in coordination with existing application owner/OICL.
51	74	10.1 Functional and Technical Requirement Point no 15:	Should be able to send the daily status report of success & failure	· : Daily reports are generated as audit-trail logs in CSV format. Are they also required to be sent as email?	**Clarification:** The solution should have capability to integrate with SMTP server/solution for sending automated reports.
52	74	10.1 Functional and Technical Requirement Point no 16:	System should have Security level based access control	Our system supports role based access control. There are different roles like user, profile administrator, signer, company administrator etc. Is anything else needed?	Understanding is correct
53	74	10.1 Functional and Technical Requirement Point no 19:	The proposed solution should support instant real time signing and should integrate with OICL Application	For integrating with OICL application, we can provide a web-service interface (SOAP or REST as per customer need) to do things like pushing documents in the system, triggering signing, pulling signed documents from the system, etc. Is anything else needed?	Understanding is correct
54	74	General Query	•How many signers are going to be there? How many DSCs on the HSM? •On how many servers would the solution be installed? Would OICL provide and configure load-balancer for achieving load distribution and high availability? How many machines in all, including DC / DR, production / UAT, etc.?	Kincly clarifyi	**1.** approx. 10-12 digital signatures , **2.** Currently solution is installed at 2 servers at DC and at 1 server at DR. In future if OICL intendes to use physical load balancer for load distribution among servers, the onus of integrating solution with Load balancer will be of bidder, necessary support will be provided from OICL
55	18	7/2.2 Scope for key Management Solution	To ensure optimal data protection, solution provided must support the ‘Bring Your Own Key (BYOK)’ model or “Host your own Key (HYOK)” and take end-to-end responsibility of securely storing and managing the encryption keys used by its “Cloud Service Providers(CSPs)” during the encryption process on-premise on a FIPS 140-3 or above certified Key Management appliance.	Since the Key Management appliance is backed up with HSM which FIPS 140-2 level 3 , request you to change the clause to reflect the same "during the encryption process on-premise on a FIPS 140-2 Level 3 or above certified Key Management appliance."	**Revised Clause:** To ensure optimal data protection, solution provided must support the ‘Bring Your Own Key (BYOK)’ model or “Host your own Key (HYOK)” and take end-to-end responsibility of securely storing and managing the encryption keys used by its “Cloud Service Providers(CSPs)” during the encryption process on-premise on a FIPS 140-2 Level 3 or above certified Key Management appliance.
56	76	58/Appendix 1: Technical and Functional Specifications	The solution shall discover, create, renew and manage all the keys across heterogeneous environments and different geographical locations.	The discovery is applicable for the crypto objects when offloaded via external mechanism. Since OICL is using KMS which would generate keys and distribute, request you to change the clause to "The solution shall create, renew and manage all the keys across heterogeneous environments and different geographical locations."	**Revised clause:** The solution shall create, renew and manage all the keys across heterogeneous environments and different geographical locations.
57	32	4.16	If the Bidder fails to meet the Project Timelines as per Section 1.6, OICL shall without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to 0.5% of the contract price for every week (seven days) or part thereof of delay, up to maximum deduction of 10% of the total contract price. Once the maximum is reached, OICL may consider termination of the contract.	**Kindly request you to amend clause as per below** If the Bidder fails to meet the Project Timelines as per Section 1.6, OICL shall without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to 0.5% of theundelivered item price for **every two week** or part thereof of delay, up to maximum deduction of **5%** of the total contract price. Once the maximum is reached, OICL may consider termination of the contract.	Please be guided by RFP
58	28	3.1.9 Payment Terms - 4. AMC/ATS	Quarterly in arrears	We Request OICL to Kindly amend this to Yearly in advance because we will be paying the same to OEM on same terms. More-over this will reduce the cost to OICL beacuse every provider will add on this finance cost in their commercials.So we request OICL to kindly change the Payment terms to Yearly or Half Yearly in Advance.	Please be guided by RFP
59	28	3.1.9 Payment Terms - 5. FM Manpower	Quarterly in arrears	We Request OICL to kindly amend this to Quartely in advance or monthly in advance bacause this will reduce the cost to OICL beacuse every provider will add on this finance cost in their commercials.So we request OICL to kindly change this to Quartely in advance or monthly in advance.	Please be guided by RFP
60	17	1.6 Project Timelines - S.No.2	Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations - within 8 Weeks from the date of issuance of purchase order	We Request OICL to kindly amend delivery timeline from 8 weeks to 12 weeks for the delivery as same has been confirmed by the OEM for the delivery. Further confirmation can be taken from OEM's for the same.	**Revised Timelines :** 1. Supply and delivery of Appliance, Software and Hardware at DC and DR = Deliver at OICL respective locations within **10 weeks** from the date of issuance of Purchase Order, 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations= Within **12 Weeks** from the date of issuance of purchase order, 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) = Within **14 Weeks** from the date of issuance of purchase order , 4. Trainings = All the trainings to be completed within 1 week from the date of request for training from OICL , 4. Disaster Recovery Drill = Within 2 weeks from the date of request from OICL

RFP for Supply, Installation, Implementation, Integration and Maintenance of Hardware Security Module (HSM) Technology solution for Digital Signatures and Key Management solution for Encryption

Tender Reference No.: OICL/HO/ITD/HSM/2022/01 Dated 19/04/2022

Response to Pre-Bid Queries

Sl. No.	RFP Page No.	Point / Section #	Existing Clause	Query Sought	OICL Reply
61	17	1.6 Project Timelines - S.No.3	Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) - within 10 Weeks from the date of issuance of purchase order.	We request OICL to kindly amend this to 14 weeks after PO basis our extension request for deliver of Hardware.	**Revised Timelines :** 1. Supply and delivery of Appliance, Software and Hardware at DC and DR = Deliver at OICL respective locations within **10 weeks** from the date of issuance of Purchase Order, 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations= Within **12 Weeks** from the date of issuance of purchase order, 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) = Within **14 Weeks** from the date of issuance of purchase order , 4. Trainings = All the trainings to be completed within 1 week from the date of request for training from OICL , 4. Disaster Recovery Drill = Within 2 weeks from the date of request from OICL
62			General Query	Will there be SSO between your INLIAS system and the signing solution?	**Clarification:** As of now there is no SSO between INLIAS system and signing application.
63	74	10.1 / 4 /Appendix 1: Technical and Functional Specifications	System should be capable of signing multiple formats including PDF, Zip files etc.	All other formats apart from PDF will get signed as PKCS#7 attached signature. Is this fine or is something else needed?	Understanding is correct
64	74	10.1 / 11 / Appendix 1: Technical and Functional Specifications	System should have measures to control the documents which can be signed	How will the solution know which documents are ok to be signed and which are not? What criteria are expected to be used? How do you define which documents are ok to sign?	**Clarification :** As per current scenario every document passed on to signing solution will get signed. In case any rules/criteria were required in future , the selected bidder will draft the rules in coordination with existing application owner.
65	74	10.1 / 14 / Appendix 1: Technical and Functional Specifications	No un-authenticated document should be allowed to be signed	How will the solution know which documents are ok to be signed and which are not? What criteria are expected to be used? How do you define which documents are ok to sign?	**Clarification :** As per current scenario every document passed on to signing solution will get signed. In case any rules/criteria were required in future , the selected bidder will draft the rules in coordination with existing application owner.
66	74	10.1 / 15 / Appendix 1: Technical and Functional Specifications	Should be able to send the daily status report of success & failure	Daily reports are generated as audit-trail logs in CSV format. Are they also required to be sent as email?	**Clarification:** The solution should have capability to integrate with SMTP server/solution for sending automated reports.
67	74	10.1 / 16 / Appendix 1: Technical and Functional Specifications	System should have Security level based access control	Our system supports role based access control. There are different roles like user, profile administrator, signer, company administrator etc. Is anything else needed?	Understanding is correct
68	74	10.1 / 19 /Appendix 1: Technical and Functional	The proposed solution should support instant real time signing and should integrate with OICL Application	For integrating with OICL application, we can provide a web- service interface (SOAP or REST as per customer need) to do things like pushing documents in the system,system, etc. Is anything else needed? triggering signing, pulling signed documents from the	Understanding is correct
69			General Query	How many signers are going to be there? How many DSCs on the HSM?	approx. 10-12 digital signatures
70			General Query	On how many servers would the solution be installed? Would OICL provide and configure load- balancer for achieving load distribution and high availability? How many machines in all, including DC / DR, production / UAT, etc.?	**Clarification:** Currently solution is installed at 2 servers at DC and at 1 server at DR. In future if OICL intendes to use physical load balancer for load distribution among servers, the onus of integrating solution with Load balancer will be of bidder, necessary support will be provided from OICL.
71			General Query	As per the RFP, hope there is no EMD Amount in this RFP. Pls confirm.	Please be guided by RFP
72	16	Project Timelines:	Delivery Timelines	8 Weeks should be the delivery timelines for Hardware delivery and Implementation should be 10- 12 weeks.	**Revised Timelines :** 1. Supply and delivery of Appliance, Software and Hardware at DC and DR = Deliver at OICL respective locations within **10 weeks** from the date of issuance of Purchase Order, 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations= Within **12 Weeks** from the date of issuance of purchase order, 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) = Within **14 Weeks** from the date of issuance of purchase order , 4. Trainings = All the trainings to be completed within 1 week from the date of request for training from OICL , 4. Disaster Recovery Drill = Within 2 weeks from the date of request from OICL
73	14	2.6 Existing inventory and buyback of HSM Devices	Bidder shall offer OICL for buyback of HSM devices in working/non-working condition. The Quote for the same has to be provided in the Bill of Material.	This is totally depending on OEM whether he will buyback. We request you to remove this clause	Please be guided by RFP
74	28	Payment Terms	Buy Back clause.	This is totally depending on OEM whether he will buyback. We request you to remove this clause	Please be guided by RFP
75	28	Payment Terms	ATS/AMC Payment Terms	Payment terms shall be in annual advance. We have to pay 100% advance to OEM.	Please be guided by RFP
76		FM Manpower	General Query	Is there any specific skill set required for L1/L2 resources?	Please be guided by RFP
77		FM Manpower	General Query	Do you need L1 & L2 resources in both locations DC & DR or any one of the locations. Pls clarify. How many L1 & L2 resources is required	please be guided by RFP.
78		Commercial Format, Optional items	General Query	Optional Items are mandatory or optional to quote?	Please be guided by RFP.
79	18	7/2.2 Scope for key Management Solution	To ensure optimal data protection, solution provided must support the 'Bring Your Own Key (BYOK)' model or "Host your own Key (HYOK)" and take end- to-end responsibility of securely storing and managing the encryption keys used by its "Cloud Service Providers(CSPs)" during the encryption process on-premise on a FIPS 140-3 or above certified Key Management appliance.	Since the Key Management appliance is backed up with HSM which FIPS 140-2 level 3 , request you to change the clause to reflect the same "during the encryption process on-premise on a FIPS 140- 2 Level 3 or above certified Key Management appliance."	**Revised Clause:** To ensure optimal data protection, solution provided must support the 'Bring Your Own Key (BYOK)' model or "Host your own Key (HYOK)" and take end-to-end responsibility of securely storing and managing the encryption keys used by its "Cloud Service Providers(CSPs)" during the encryption process on-premise on a FIPS 140-2 Level 3 or above certified Key Management appliance.
80	76	58/Appendix 1: Technical and Functional Specifications	The solution shall discover, create, renew and manage all the keys across heterogeneous environments and different geographical locations	The discovery is applicable for the crypto objects when offloaded via external mechanism. Since OICL is using KMS which would generate keys and distribute, request you to change the clause to "The solution shall create, renew and manage all the keys across heterogeneous environments and different geographical locations."	**Revised clause:** The solution shall create, renew and manage all the keys across heterogeneous environments and different geographical locations.
81	15	1.5 Eligibility Criteria	Bidder or OEM should have implemented similar solution in at least three BFSI companies with atleast 200 branches/offices in India during the past five years	We have asked to remove specification of bank with 200 branches and number of implementations" and suggesting below term in modified format - 'Bidder or OEM should have implemented similar HSM solution in at least ONE BFSI /PSU / Govt / Private Enterprise companies in India during the past five years'	Please be guided by RFP
82	16	1.6 Project Timelines	Supply and delivery of Appliance, Software and Hardware at DC and DR- Deliver at OICL respective locations within 6 weeks from the date of issuance of Purchase Order	We would like to request 10 weeks time for hardware delivery. Rest timelines will get changed accordingly.	**Revised Timelines :** 1. Supply and delivery of Appliance, Software and Hardware at DC and DR = Deliver at OICL respective locations within **10 weeks** from the date of issuance of Purchase Order, 2. Installation, configuration and commissioning of the solution and hardware at DC and DR specified locations= Within **12 Weeks** from the date of issuance of purchase order, 3. Creation and installation of Class 3 Company type Digital Signature in the Company prescribed locations (DC & DR) = Within **14 Weeks** from the date of issuance of purchase order , 4. Trainings = All the trainings to be completed within 1 week from the date of request for training from OICL , 4. Disaster Recovery Drill = Within 2 weeks from the date of request from OICL