Response to Pre-bid Queries

Response to Pre-bid Queries

RFP for Selection of Agency for Supply, Installation, Commissioning & Maintenance of Hardware Security Module for Department of Science & Technology, Gandhinagar.
(Tender No. HWT181017472)

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Venders	Responses to Vendors
	Page No./Section No./ Clause No.	Tender Description		
1	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 2	Should comply to standards FIPS 140-2 Level 3, ROHS	Pls add :- EAL 4 EAL4+ :- It is a requirement of UIDAI of UIDAI also, because of Evaluation Assurance Level (EAL) – the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) .	Please refer revised RFP
2	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 2	Should comply to standards FIPS 140-2 Level 3, ROHS	Pls Add :- FCC part 15 Class B. FCC part 15 Class B :- The Federal Code Of Regulation (CFR) FCC Part 15 is a common testing standard for most electronic equipment. FCC Part 15 covers the regulations under which an intentional, unintentional, or incidental radiator that can be operated without an individual license. FCC Part 15 covers as well the technical specifications, administrative requirements and other conditions relating to the marketing of FCC Part 15 devices. Depending on the type of the equipment, verification, declaration of conformity, or certification is the process for FCC Part 15 compliance. FCC Part 15 Subpart B is for unintentional radiators. The category of unintentional radiators includes a wide variety of devices that contain clocks or oscillators and logic circuitry but that do not deliberately generate radio frequencies emissions. Among the common unintentional radiators are personal computers, peripherals, receivers, radios, TV sets, and cable TV home terminals. FCC Part 15 Section 15.101 has a very informative table for unintentional radiators. Two levels of radiation and conducted emissions limits for unintentional radiators are specified in FCC Part 15 Subpart B. Class B digital devices, the lower more strict limits. Manufacturers are encouraged to meet the Class B digital device limits. Manufacturers are encouraged to meet the Class B digital device limits.	Please refer revised RFP
3	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 8	Random Number Generation –FIPS 140-2 approved	NIST Recommended :- Random Number Generation –FIPS 140-2 approved DRBG (SP 800-90 CTR mode). - This has been recommended by NIST, for strenthen the security parametres through HSM.	Please refer revised RFP

Sr. No.	Tender Reference Page No./Section No./ Clause No.	Tender Description	Query / Clarification / Suggestions from the Venders	Responses to Vendors
4	Page No. 15 /SECTION – 4/ 4.1 Technical Specifications/s/n 10	All keys must be stored in FIPS certified hardware/device	As per the UIDAI Security parameter :- All Keys are always stored securely in FIPS certified Hardware and never stored "In Software" or "In File" in any form. Keeping high standard of security , UIDAI has already insisted on the best practices which say HSM should "GENERATE" , "STORE" , "USE" and "DESTROY" the Keys with in the HSM and the whole life cycle of keys should be managed within the FIPS certified tamper resistant Hardware, if any HSM allows Keys to travel outside the HSM and store the Keys in software in any of the form than it doesn't called HSM on the first place itself as it doesn't have capabilities of storing the Keys with the tamper resistant Hardware Security Module.	Please refer revised RFP
5	Page No.16 /SECTION – 4/ 4.1 Technical Specifications/s/n 18	HSM should have the capabilities of 20 partitions in single appliance	As per the CCA guidlines Guidelines:- The proposed HSM should have minimum 20 "Partitions" / "Virtual HSM" with each having its own serial number as per CCA/UIDAI guidelines so as it can allow to store different certificates in each partition. Each partition should be protected with unique set of user id and password to grant access. The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act. CCA is an apex body, has been formed to formulate the best policies & guidelines in the interest of the country.	Please refer revised RFP

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Venders	Responses to Vendors
	Page No./Section No./ Clause No.	Tender Description		
6	General Query/Suggestion		Pls Add:- Complete hardware based storage of key material for entire Life cycle. HSM is a FIPS certified Cryptographic Hardware appliance, which has its own secured FIPS certified boundaries , it can GENERATE and STORE 15K+ Keys inside its tamper resistant hardware memory only, for protection if Keys comes out of Hardware then "PROTECTION" words become meaningless for Hardware Security Module (since HARDWARE BASED KEYS STORAGE IS THE BACKBONE OF COMPLETE HSM CONCEPT for security measure only), if Keys travels outside and reside in software then the word "PROTECTION" becomes null and void and Keys outside the HSM are prone to cryptographic analysis and any vulnerability in the OS or software will allow to comprise the keys, since Hardware has its own capacity the Cryptographic FIPS certified HSM may store 25K+ RSA 2048 bits Keys , which is a very large number and in no condition any organisation would require more than 10K -20k.	Please refer revised RFP
7	General Query/Suggestion		Add:- HSM should be compliant to IPv4 & IPv6. As per DOT policy all the IP devices should be IPv4 + IPv6 Compliant	Please refer revised RFP
8	General Query/Suggestion		Add:- Support for complete use of ECC curves for commercial activities like issuance of Digital certificates generated using the same curves to external parties without need of any additional licenses. This has been recommended by CCA and in the near future ECC would replace RSA because of the performance and security, and once departmenet ask the same customer will ask for the future ready HSM at the same price now itself and if this caluse will be become very important	Please refer revised RFP

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Venders	Responses to Vendors
	Page No./Section No./ Clause No.	Tender Description		
9	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 2	Should comply to standards FIPS 140-2 Level 3, ROHS	Pls add :- EAL 4 EAL4+ :- It is a requirement of UIDAI of UIDAI also, because of Evaluation Assurance Level (EAL) – the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) .	As per Serial no. 1
10	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 2	Should comply to standards FIPS 140-2 Level 3, ROHS	Pls Add :- FCC part 15 Class B. FCC part 15 Class B :- The Federal Code Of Regulation (CFR) FCC Part 15 is a common testing standard for most electronic equipment. FCC Part 15 covers the regulations under which an intentional, unintentional, or incidental radiator that can be operated without an individual license. FCC Part 15 covers as well the technical specifications, administrative requirements and other conditions relating to the marketing of FCC Part 15 devices. Depending on the type of the equipment, verification, declaration of conformity, or certification is the process for FCC Part 15 compliance. FCC Part 15 Subpart B is for unintentional radiators. The category of unintentional radiators includes a wide variety of devices that contain clocks or oscillators and logic circuitry but that do not deliberately generate radio frequencies emissions. Among the common unintentional radiators are personal computers, peripherals, receivers, radios, TV sets, and cable TV home terminals. FCC Part 15 Section 15.101 has a very informative table for unintentional radiators. Two levels of radiation and conducted emissions limits for unintentional radiators are specified in FCC Part 15 Subpart B. Class B digital devices, the lower more strict limits. Manufacturers are encouraged to meet the Class B digital device limits. Manufacturers are encouraged to meet the Class B digital device limits.	As per Serial no. 2

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Venders	Responses to Vendors
	Page No./Section No./ Clause No.	Tender Description		
11	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 8	Random Number Generation –FIPS 140-2 approved	NIST Recommended :- Random Number Generation –FIPS 140-2 approved DRBG (SP 800-90 CTR mode). - This has been recommended by NIST, for strenthen the security parametres through HSM.	As per Serial no. 3
12	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 10	All keys must be stored in FIPS certified hardware/device	As per the UIDAI Security parameter :- All Keys are always stored securely in FIPS certified Hardware and never stored "In Software" or "In File" in any form. Keeping high standard of security , UIDAI has already insisted on the best practices which say HSM should "GENERATE" , "STORE" , "USE" and "DESTROY" the Keys with in the HSM and the whole life cycle of keys should be managed within the FIPS certified tamper resistant Hardware, if any HSM allows Keys to travel outside the HSM and store the Keys in software in any of the form than it doesn't called HSM on the first place itself as it doesn't have capabilities of storing the Keys with the tamper resistant Hardware Security Module.	As per Serial no. 4
13	Page No.16 /SECTION – 4/ 4.1 Technical Specifications/s/n 18	HSM should have the capabilities of 20 partitions in single appliance	As per the CCA guidlines Guidelines:- The proposed HSM should have minimum 20 "Partitions" / "Virtual HSM" with each having its own serial number as per CCA/UIDAI guidelines so as it can allow to store different certificates in each partition. Each partition should be protected with unique set of user id and password to grant access. The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act. CCA is an apex body, has been formed to formulate the best policies & guidelines in the interest of the country.	As per Serial no. 5

Sr. No.	Tender Reference Page No./Section No./ Clause No.	Tender Description	Query / Clarification / Suggestions from the Venders	Responses to Vendors
14	General Query/Suggestion		Pls Add:- Complete hardware based storage of key material for entire Life cycle. HSM is a FIPS certified Cryptographic Hardware appliance, which has its own secured FIPS certified boundaries , it can GENERATE and STORE 15K+ Keys inside its tamper resistant hardware memory only, for protection if Keys comes out of Hardware then "PROTECTION" words become meaningless for Hardware Security Module (since HARDWARE BASED KEYS STORAGE IS THE BACKBONE OF COMPLETE HSM CONCEPT for security measure only), if Keys travels outside and reside in software then the word "PROTECTION" becomes null and void and Keys outside the HSM are prone to cryptographic analysis and any vulnerability in the OS or software will allow to comprise the keys, since Hardware has its own capacity the Cryptographic FIPS certified HSM may store 25K+ RSA 2048 bits Keys , which is a very large number and in no condition any organisation would require more than 10K -20k.	As per Serial no. 6
15	General Query/Suggestion		Add:- HSM should be compliant to IPv4 & IPv6. As per DOT policy all the IP devices should be IPv4 + IPv6 Compliant	As per Serial No. 7
16	General Query/Suggestion		Add:- Support for complete use of ECC curves for commercial activities like issuance of Digital certificates generated using the same curves to external parties without need of any additional licenses. This has been recommended by CCA and in the near future ECC would replace RSA because of the performance and security, and once departmenet ask the same customer will ask for the future ready HSM at the same price now itself and if this caluse will be become very important	As per Serial no. 8

Sr. No.	Tender Reference Page No./Section No./ Clause No.	Tender Description	Query / Clarification / Suggestions from the Venders	Responses to Vendors
17	Page No.13 /SECTION – 3/ ELIGIBILTY CRITERIA	Proposed solution should be deployed at minimum 02 projects in last 2 years. Work Orders / Client Certificates confirming year and area of activity	Work Orders / Client Certificates please grant submission of OEM Work Orders / Client Certificates confirming experience in such project for the last 2 year.	Please refer revised RFP
18	General Query/Suggestion		Further to given Eligibility criteria, we suggest to add below parameter: OEM should have direct presence in india last 5 years and should have 50 R&d engineers on OEM's payroll only. Justification: As the UIDAI is frequently changing/updating specifications, it is required to have OEM presence in india since last 5 years so that they have knowledge of all the updates. Also they should have atleast 50 R&D engineers so that they can provide fast service as and when required.	No change
19	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 2	Should comply to standards FIPS 140-2 Level 3, ROHS	Pls add :- CC EAL 4+, FCC part 15 Class B Justification: EAL4+ :- It is a requirement of UIDAI of UIDAI also, because of Evaluation Assurance Level (EAL) – the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) . FCC part 15 Class B:- Class B Digital Device." A digital device that is marketed for use in a residential environment notwithstanding use in commercial, business and industrial environments. Examples of such devices included, but are not limited to, personal computers, calculators, and similar electronics devices that are marketed for use by the general public.	As per Serial no. 1, 2

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Venders	Responses to Vendors
	Page No./Section No./ Clause No.	Tender Description		
20	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 5	Key Exchange Symmetric Algorithm: AES, DES, Triple DES	we suggest addition of RC2, RC4, RC5, SEED Justification: RC2, RC4, RC5, SEED :- These are stream cyphers which are normally utilised in multiple implementation across board and generally requested crytographic operations. They will also be required to implement refrence number/tokenization scheme as per UIDAI circular no: 11020/205/2017 - UIDAI (Auth-I) Dt.25/7/2017.	Please refer revised RFP
21	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 8	Random Number Generation –FIPS 140-2 approved	we suggest addition of DRBG (SP 800-90 CTR mode) Justification: This has been recommended by NIST, for strengthen the security parameters throuh HSM.	As per Serial no. 3
22	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 10	All keys must be stored in FIPS certified hardware/device	WE Suggest: Keys must be hardware stored and proteted complete hasrware based storage of key material for entire Life cycle keys are always in hardware and never stored in software or file format in any form. Justification to our suggestion: Keeping high standard of security, UIDAI has already insisted on the best practices which say HSM should " GENERATE", " STORE","USE" and " DESTROY" the key with in the HSM and the whole life cycle of keys should be managed within the FIPS certified tamper resistant hardware, if any HSM allows keys to travel outside the HSM on the first place itself as it doesn't have capabilities of storing the keys with the tamper resistant hardware security module. Please refer to the UIDAI circular no: 11020/205/2017 - UIDAI (Auth-I) Dt.25/7/2017.	As per Serial no. 4

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Venders	Responses to Vendors
	Page No./Section No./ Clause No.	Tender Description		
23	Page No.16 /SECTION – 4/ 4.1 Technical Specifications/s/n 18	HSM should have the capabilities of 20 partitions in single appliance	We suggest: As per the CCA guidlines Guidelines:- The proposed HSM should have minimum 20 "Partitions" / 'Virtual HSM" with each having its own serial number as per CCA/UIDAI guidelines so as it can allow to store different certificates in each partition. Each partition should have unique identification number to grant access. Justification to our suggestion: The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act. CCA is an apex body, has been formed to formulate the best policies & guidelines in the interest of the county. Please refer the page no. 18, point no. e of 2.5 of link: http://cca.gov.in/cca/sites/default/files/files/Guidelines/CCA-IVG.pdf.	As per Serial no. 5
24	Page No.16 /SECTION – 4/ 4.1 Technical Specifications/s/n 25	The key generation speed of HSM's should be minimum 10 (Ten) key pair per second (RSA 2048 bits)	We suggest: This have no relevance with AUA / ASA / KUA project since key generation process is a very rare occurrence and usually it's a one time process and hence, request you to remove the clause which is refractive in nature.	Please refer revised RFP

Sr. No.	Tender Reference Page No./Section No./ Clause No.	Tender Description	Query / Clarification / Suggestions from the Venders	Responses to Vendors
25	Page No.16 /SECTION – 4/ 4.1 Technical Specifications/s/n 32	At least 100 licenses with 200 Keys (100 pairs)	We suggest: Please add it should support complete use of ECC curves for commercial activities like issuance of Digital certificates generated using the same curves to external parties without need of any additional licenses. Justification to our suggestion: This will benefit department and need not to pay the extra amt. against the licenses. Both Central Certificate Authority of India and UIDAI are planning to adopt ECC usage instead of RSA (http://cca.gov.in/cca/sites/all/ECC-DRAFT SIGNATURE GUIDELINES for Public review-2013.pdf). In all such cases these algorithms would be used to extend servTces to multiple entities. Any licencing restricting the use of the same would cause a hindrance to these operations.	As per Serial no. 8
26	General Query/Suggestion		Please add: Complete hardware based storage of key material for entire Life cycle. Justification to our suggestion: Keys are always in Hardware and never stored in Software or file format in any form :- The primary reason for mandating HSM's by UIDAI is that the private keys be used for the operations involved should be highly secured and never extractable in any form from the HSM memory. Any HSM that does not follow the security architecture of ensuring Keys always remain within the HSM memory and never be exposed in any form to the application layer is under noncompliance of this objective. Please refer point (f) in the UIDAI circular no: 11020/205/2017 - UIDAI (Auth-I) Dt.25/7/2017.	As per Serial no. 6
27	General Query/Suggestion		Please add: HSM should be compliant to IPv4 & IPv6 Justification to our suggestion: As per DOT policy all the IP devices should be IPv4 + IPv6 Compliant	As per Serial No. 7

Sr. No.	Tender Reference Page No./Section No./ Clause No.	Tender Description	Query / Clarification / Suggestions from the Venders	Responses to Vendors
28	General Query/Suggestion		Please add: Support for complete use of ECC curves for commercial activities like issuance of Digital certificales generated using the same curves to external parties without need of any additional licenses. Justification to our suggestion: This has been recommended by CCA and in the near future ECC would replace RSA because of the performance and security, and once departmenet ask the same customer will ask for the future ready HSM at the same price now itself and if this clause will be become very important.	As per Serial no. 8
29	Page No.13 /SECTION – 3/ ELIGIBILTY CRITERIA	Proposed solution should be deployed at minimum 02 projects in last 2 years. Work Orders / Client Certificates confirming year and area of activity	Request to allow submission of OEM Work Orders / Client Certificates confirming year and area of activity for the mimimum 02 projects in the last 2 year.	As per Serial no. 17
30	General Query/Suggestion		We recommend Indian company as OEM having presence since last 4-5 years so that they have knowledge of all the updates of UIDAI. Also they should have atleast 40-50 technical engineers to provide support all the time whenever required.	No change
31	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 2	Should comply to standards FIPS 140-2 Level 3, ROHS	Pls add :- CC EAL 4+, FCC part 15 Class B EAL covers the complete development of a product. EAL 1 is most basic and cheapest to implement and evaluate and hence , we recommend EAL4+ version addition. FCC part 15 Class B is a Digital instrument, used in residential environment, yet used in commercial business.	As per Serial no. 1, 2

Sr. No.	Tender Reference Page No./Section No./ Clause No.	Tender Description	Query / Clarification / Suggestions from the Venders	Responses to Vendors
32	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 5	Key Exchange Symmetric Algorithm: AES, DES, Triple DES	we suggest addition of RC2, RC4, RC5, SEED These are stream cyphers and widely utilized in multiple implementations.	As per Serial no. 20
33	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 8	Random Number Generation –FIPS 140-2 approved	Please add DRBG (SP 800-90 CTR mode) The same is recommended by NIST.	As per Serial no. 3
34	Page No.16 /SECTION – 4/ 4.1 Technical Specifications/s/n 18	HSM should have the capabilities of 20 partitions in single appliance	Each partition should have its own unique serial number as per CCA/UIDAI guidelines issued in the month of july 2017. Please refer to the UIDAI circular and CCA web link: http://cca.gov.in/cca/sites/default/files/files/Guidelines/CCA-IVG.pdf.(Page 18/40 at Clause no.2.5.e)	As per Serial no. 5
35	Page No.16 /SECTION – 4/ 4.1 Technical Specifications/s/n 25	The key generation speed of HSM's should be minimum 10 (Ten) key pair per second (RSA 2048 bits)	Our recommendation: Please remove said clause. This have no relevance with AUA / ASA / KUA project.	As per Serial no. 28
36	General Query/Suggestion		We recommend to add "Complete hardware based storage of key material for entire Life cycle" - The basic reason of HSM implementation by UIDAI is that the private keys be used for the operations involved should be highly secure and not extractable in any form from the HSM memory. HSM that do not comply the security architecture of keys will remain inside the HSM memory and never visible to the application layer.	As per Serial no. 6
37	General Query/Suggestion		We recommend to add "HSM should be compatible to IPv4 & IPv6 as per the DOT policy".	As per Serial No. 7
38	General Query/Suggestion		We recommend to add "HSM should support complete use of ECC curves for commercial activities without need of any additional licenses" - It will beneficial for Department and not required any extra payment against the licenses.	As per Serial no. 8

Sr. No.	Tender Reference Page No./Section No./ Clause No.	Tender Description	Query / Clarification / Suggestions from the Venders	Responses to Vendors
39	Page No.15 /SECTION – 4/ 4.1 Technical Specifications/s/n 13	Provision of delivery of new device on its failure without returning the failed one.	This requirement is not clearly understood. As FIPS compliant, the HSMs have to provision to remove all the keys when sent for repairs. Therefore, this clause may please be modified to "Provision of delivery of temparary unit on its failure and replacing with repaired unit.	Please refer revised RFP
40	Page No.16 /SECTION – 4/ 4.1 Technical Specifications/s/n 16	Support for minimum 1000 signatures per second at 2048 bits minimum, scalable up to 3000 signatures per second.	HSMs are field upgradable upto 5,000 TPS. Normal UID operations, 500 SPS (signatures per second) very optimum as it can process 2.5 crore signatures per day. Additionally the algorithm is not mentioned. As per CCA 2048-bit RSA algorithm is legally valid in India. Therefore request you modify this clauses as " Support for minimum 500 signatures per second at 2048 bit RSA scalable upto 5,000 signatures per second on the same device.	Please refer revised RFP
41	Page No.13 /SECTION – 3/ ELIGIBILTY CRITERIA 3	Proposed solution should be deployed at minimum 02 projects in last 2 years. Work Orders / Client Certificates confirming year and area of activity	Request you to modify to:The bidder should have supplied HSM during the last 2 years to Public/Private sector Banks/BFSI/Government Organization.	As per Serial no. 17
42	Page No.19 /Service Level Agreement, Penalties & Payment Terms/5.2. Payments Terms	1. Supply, Installation, Integration, Testing and Commissioning of Network based Hardware Security Module (HSM) Appliance at GSDC site. A. Supply of Equipment and peripherals: Payment @50%, B. Installation, Integration Testing & Commissioning at site: Payment @20%, C. 03 Months after successful FAT: Payment @ 20%	Requesting to keep the payment terms as 70:10:10 as you are already asking PBG @ 10%. Liquidation of money at earlier stage will help to avoid loading unnecessary cost to the final price.	Please refer revised RFP

Sr. No.	Tender Reference		Query / Clarification / Suggestions from the Venders	Responses to Vendors
	Page No./Section No./ Clause No.	Tender Description		
43	Page No.19 /Service Level Agreement, Penalties & Payment Terms/5.2. Payments Terms	1. Supply, Installation, Integration, Testing and Commissioning of Network based Hardware Security Module (HSM) Appliance at GSDC site. Time Line: T1 = T0+30 Days	Requesting you to allow delivery upto 50 days as HSM are not commonly used products and takes time to import.	No change