**UCO BANK**

**Department of Information Technology**

**Request for Proposal (RFP) For RFP for Supply, Installation, Commissioning & Maintenance of HSM RFP REF NO: UCO/DIT/138/2016-17 Date: 30/04/2016 Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s), Amendments, Addendums and Corrigendum's**

| SL. No. | Page No / Clause No | Terms& Conditions as per RFP | Queries/Suggestions by the Bidder (s) | Bank's Response (s) |
|---|---|---|---|---|
| 1 | Page No-11, | The Bidder must submit Earnest Deposit Money in the form of Bank Guarantee valid for an period of 180 Days in favour of UCO Bank payable at Kolkata of Rs 2,00,000/- | We wish to inform that we are registered with NSIC. The certificate is attached. As per Govt. policy for procurement, firms registered with NSIC are exempted from payment of EMD and Tender Fee. Kindly confirm for the same. | Requirement Stands as per RFP |
| 2 | Page No-21, Point No-6 | The HSM should be delivered within 3 weeks from the date of placing the purchase order. | We request you to change delivery time of HSM from 3 weeks to 4- 5 weeks from date of placing the Purchase Order. | The subject clause stands modified as:<br><br>The HSM should be delivered within 4 weeks from the date of placing the purchase order. |

| | | | | |
|---|---|---|---|---|
| **3** | Page No-22, Point No-10 | In case of late delivery of equipment by the vendor, 1% per week of the value of undelivered portion of the purchase order after 3 week s from the date of order, subjected to maximum of 10% of the undelivered portion of the equipment. | We request you to change In case of late delivery of equipment by the vendor, 1 % per week minimum to 0.5 % per week of the value of undelivered portion as per the purchase order & , subject to maximum value of 10% , we request you to be change up to 5% maximum of the undelivered portion of the equipment. | Requirement Stands as per RFP |
| **4** | Page 38/ Annex C/ 5 | The proposed HSM must be PCI-HSM 2.0 Certified. | As per UPI Guidelines, FIPS 140-2 Level 2 HSM General Purpose HSM is required. PCI -HSM 2.0 is releated to Payment HSM.<br><br>Kindly modify it to "The proposed HSM must be FIPS 140-2 Level 2 Certified" | The subject clause stands modified as:<br><br>The proposed HSM must be FIPS 140-2 Level 2 Certified |
| **5** | Page 38/ Annex C/ 8 | Capable of translating up to 1600 PIN triple DES Pin block Per second and minimum of 140 PIN triple DES Pin block Per second | This is feature of payment HSM and not applicable to General Purpose HSM.<br>Kindly modify it to HSM should be capable to perform minimum 300 RSA signature of 2048 bit key | The subject clause stands modified as:<br><br>HSM should be capable to perform minimum 300 RSA signature of 2048 bit key |
| **6** | Page 38/ Annex C/ 10 | It should support following Crypto Graphic Standard: DES and Triple DES Algorithms - Provide PIN encryption, PIN Authorization and message authentication capabilities. | PIN encryption, PIN authorization etc are features of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |

| | | | | |
|---|---|---|---|---|
| **7** | Page 38/ Annex C/ 12 | The relevant security settings in the firmware should have PCI compliant values | PCI standards are related to Payment HSM.<br>This should be modified to "The relevant security settings in the firmware should have FIPS 140-2 compliant values" | The subject clause stands modified as:<br><br>The relevant security settings in the firmware should have FIPS 140-2 compliant values |
| **8** | Page 38/ Annex C/ 13 | Shipment of the HSM should be compliant as per PCI HSM requirement | PCI standards are related to Payment HSM.<br>This should be modified to "Shipment of the HSM should be compliant as per FIPS 140-2" | The subject clause stands modified as:<br><br>Shipment of the HSM should be compliant as per FIPS 140-2 |
| **9** | Page 38/ Annex C/ 16 | Should have GUI/CLI available with 2 factor Authentication using USB Tokens | This is feature of payment HSM and not applicable to General Purpose HSM.<br>Kindly modify it to "Should have GUI/CLI available with Authentication as per FIPS 140-2 Level 2 standards" | The subject clause stands modified as:<br><br>Should have GUI/CLI available with Authentication as per FIPS 140-2 Level 2 standards |
| **10** | Page 38/ Annex C/ 19 | All Features for the HSM should be enabled by default and should not require purchase of any additional license for PIN transaction Processing, EMV Processing etc. | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |
| **11** | Page 38/ Annex C/ 21 | Key Block support (superset of ANSI X9.24) , | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |
| **12** | Page 38/ Annex C/ 22 | DUKPT (DES and Triple-DES) | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |

| | | | | |
|---|---|---|---|---|
| **13** | Page 38/ Annex C/ 24 | Cryptographic module certified to FIPS: 140-2 Level 3, 46, 81, 180-3, 186-3, 198 | As per UPI requirement, Cryptographic module certified to FIPS: 140-2 Level 2 | The subject clause stands modified as:<br><br>Cryptographic module certified to FIPS: 140-2 Level 2 |
| **14** | Page 38/ Annex C/ 25 | PCI HSM 2.0 Standard | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |
| **15** | Page 38/ Annex C/ 30 | Tamper resistance meeting requirements of PCI HSM 2.0 & FIPS 140-2 Level 3 | As per UPI requirement, HSM should be Tamper resistance meeting requirements of FIPS 140-2 Level 2 | The subject clause stands modified as:<br><br>HSM should be Tamper resistance meeting requirements of FIPS 140-2 Level 2 |
| **16** | Page 38/ Annex C/ 33 | Device hardening - ability to disable functions not required by the host application | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |
| **17** | Page 38/ Annex C/ 34 | Audit trails and 2 Factor Authentication for Auditor using USB tokens | Audit trails should be as per FIPS 140-2 Level 2 | The subject clause stands modified as:<br><br>Audit trails should be as per FIPS 140-2 Level 2 |
| **18** | Page 38/ Annex C/ 36 | Reporting of Authorization State identifies whether commands are Host, Console, or All | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |
| **19** | Page 38/ Annex C/ 38 | Reduced Key check value: 6 HEX | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |

| | | | | |
|---|---|---|---|---|
| **20** | Page 38/ Annex C/ 39 | Encrypted decimalization table | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |
| **21** | Page 38/ Annex C/ 41 | PIN never appears in the clear outside of a tamper resistant security module as per PCI PIN security requirements | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |
| **22** | Page 38/ Annex C/ 42 | Key Entry Mechanism are protected as per PCI HSM 2.0 requirements | This is feature of payment HSM and not applicable to General Purpose HSM. Kindly delete this clause | Please refer to Annexure C, Technical Specification |
| **23** | Page 19 / 1.1 | As per PCI DSS Standards, HSM is required for managing hardware devices at Bank's UPI Server Locations to enable UPI Transactions. Bank shall provide access to their HSM for Key Management. | As per UPI Guidelines, FIPS 140-2 Level 2 HSM General Purpose HSM is required. PCI DSS Standards is related to Payment HSM.<br>Kindly modify it to "As per UPI requirement, PKI HSM is required for storing decryption keys at Bank's UPI Server Locations to enable UPI Transactions. Bank shall provide access to their HSM for Key Management." | The subject clause stands modified as:<br><br>As per UPI requirement, PKI HSM is required for storing decryption keys at Bank's UPI Server Locations to enable UPI Transactions. Bank shall provide access to their HSM for Key Management. |

| | | | | |
|---|---|---|---|---|
| **24** | Page 27 | Annual Maintenance Contract- The vendor should also quote separately for AMC at site for the 4th & 5th years for HSMs from the date of expiry of warranty. The AMC rate should not be more than 8%. For Hardware Security Module, Vendor should undertake to provide maintenance support at agreed rates and arrange for spare parts for a minimum period of 5 years (3 Years Warranty + 2 Years AMC). | Bidder need to keep sufficient resource and infrastructure in place to provide continues support for bank, 8% AMC is very less. Industry standard AMC rate is between 15-20% we request you to keep AMC @ 15% | Requirement Stands as per RFP |
| **25** | Page 22/7/C | Payment of AMC - The payment towards the AMC charges for the maintenance of the HSM Devices will be paid on quarterly basis in arrears. | We request you to modify as follows - The payment towards the AMC charges for the maintenance of the HSM Devices will be paid on yearly basis in advance. | Requirement Stands as per RFP |
| **26** | | Additional Technical Query | We would also like to understand your requirement of RSA 2048 signing speeds. Please clarify on this signing speed. | The subject clause stands modified as:<br><br>HSM should be capable to perform minimum 300 RSA signature of 2048 bit key |
| **27** | Page No- 11/4 | Amount of EMD Rs. 2,00,000/- | EMD amount is too high w.r.t bid value. Request to make EMD amount as Rs 50,000 /- max | Requirement Stands as per RFP |
| **28** | Page No- 21/7 | For Hardware (HSM)<br>a.70% of the Hardware Cost will be paid on the delivery of Hardware (HSM)<br>b.20% of the Hardware Cost will be paid after the successful installation of the HSM.<br>c.10% of the Hardware Cost will be paid after the 3 months of the Go-Live | Since only Cards are involved & proven & tested by selective OEMs, request not to block 10% for 3 months.<br>Please change payment terms as : 80% on Delivery & 20% on installation or within 1 month of delivery whichever is earlier. Already PBG @10% will be taken by Bank. | Requirement Stands as per RFP |

| | | | | |
|---|---|---|---|---|
| **29** | Page No- 21/6 | The HSM should be delivered within 3 weeks from date of placing the Purchase Order | As these are not standard cards for SI , back end order formalities to be completed , so please change delivery as 5 weeks. | The subject clause stands modified as:<br><br>The HSM should be delivered within 4 weeks from date of placing the Purchase Order |
| **30** | Page No- 23/10 | 1% per weeek for delivery/warranty repair/AMC | Please change it to 0.5% per week for all categories. | Requirement Stands as per RFP |
| **31** | Corrige ndum | Last Date and Time for receipts of tender bids is 21.05.2016 at 03:00 pm | **Last Date and Time for receipts of tender bids is extended upto 24.05.2016 at 03:00 pm. The technical bid will be opened on the same day at 3:30 PM** | |

**Addendum:**

**Bidders are informed that Bank has changed the "<u>Commercial Format (Annexure- G)</u>" and "<u>Technical Specification (Annexure-C)</u>" Bidders are requested to use these modified formats only while submitting the bid.**

**Date:16/05/2016**

**Annexure-G**

## Revised Commercial Format

| SL | Item Description | Qty. | Make & Model | Unit Cost | Applicable Tax Type & % | Applicable Taxes (₹) | Total Cost including all applicable taxes (₹) |
|---|---|---|---|---|---|---|---|
| 1 | HSM card for UPI | 02 | <please specify> | | | | |
| 2 | Annual Maintenance Support | 1st Year AMC | | | | | |
| | | 2nd Year AMC | | | | | |
| 2 | HSM card for CTS Chennai | 02 | Safenet-LUNA PCIe 7000 v5.0 HSM | | | | |
| 3 | Annual Maintenance Support | 1st Year AMC | | | | | |
| | | 2nd Year AMC | | | | | |
| 4 | Backup HSM for CTS Chennai | 01 | Safenet-LUNA Back up remote HSM | | | | |
| 5 | Annual Maintenance Support | 1st Year AMC | | | | | |
| | | 2nd Year AMC | | | | | |
| 6 | Transactional HSM Card for Debit Card PIN Generation ( Bank Sponsored RRBs) (Performance Model- 50 TPS, 2 PSU, 2 Gig Ports) | 02 | <please specify> | | | | |
| 7 | Annual Maintenance Support | 1st Year AMC | | | | | |
| | | 2nd Year AMC | | | | | |
| 5 | Total Cost of Ownership (TCO) in figures | | | | | | |
| 6 | Total Cost of Ownership (TCO) in words | | | | | | |

**Note:**

1. **The AMC rate should not be more than 8% of final rates for HSMs and the bidder shall be required to quote the rate applicable for 2 years for HSMs after the expiry of warranty period.**
2. **VAT/CST and service Tax would be paid extra at actual on submission of relevant invoice and proof.**
3. **No increase in costs, duties, levies, taxes, charges, etc. irrespective of reasons (including exchange rate fluctuations, etc.) whatsoever, shall be admissible during the currency of the contract.**
4. **Bidders should strictly quote in the format and for periods as mentioned above.**
5. **No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid**
6. **The actual cost of Octroi will be reimbursed as applicable.**
7. **The quantity mentioned above is indicative only bank may increase or decrease the quantity as per the requirement.**

**Annexure-C**

## Technical Specification- HSM Card for UPI- General Purpose

| S. No | Description of Requirement | Compliance (Yes/No) |
|---|---|---|
| 1. | **Make:** <please specify> | |
| 2. | **Model:** <please specify> | |
| 3. | **General Aspects:** | |
| 4. | The proposed HSM should have dual connectivity support. | |
| 5. | The proposed HSM must be FIPS 140-2 Level 2 Certified | |
| 6. | The proposed HSM must be FIPS140-2 Level 3 Certified. | |
| 7. | The proposed HSM should support SHA-256 RSA 2048 Format | |
| 8. | HSM should be capable to perform minimum 300 RSA signature of 2048 bit key | |
| 9. | It should support multi-threading so as maximum performance can be achieved. | |
| 10. | Capable to support DES and 3DES KEY lengths 112 bit,168 bit | |
| 11. | The relevant security settings in the firmware should have FIPS 140-2 compliant values | |
| 12. | Shipment of the HSM should be compliant as per FIPS 140-2 | |
| 13. | End to End Pin/Password Encryption | |
| 14. | Management facilities: | |
| 15. | Should have GUI/CLI available with Authentication as per FIPS 140-2 Level 2 standards | |
| 16. | Support SNMP | |
| 17. | Utilization statistics - Health check diagnostic and error logs | |
| 18. | Key Managements: | |
| 19. | Security Certification: | |
| 20. | Cryptographic module certified to FIPS: 140-2 Level 2 | |
| 21. | NIST SP800-20, SP800-90(A) | |
| 22. | FIPS approved Random number generator | |
| 23. | FIPS approved algorithms | |
| 24. | **Security features:** | |
| 25. | HSM should be Tamper resistance meeting requirements of FIPS 140-2 Level 2 | |
| 26. | Detection of cover removal in addition to Alarm triggers for motion, voltage and temperature | |
| 27. | Multiple alarm triggers for motion, voltage and temperature | |
| 28. | Audit trails should be as per FIPS 140-2 Level 2 | |
| 29. | **Key Features:** | |
| 30. | Secure Key Storage and Generation for all key types used | |
| 31. | Secure Host communication using TLS or SSL | |

## Technical Specification- HSM Card for CTS Chennai

| S. No | Description of Requirement | Compliance (Yes/No) |
|---|---|---|
| 1. | **Make: Safenet** | |
| 2. | **Model: LUNA PCIe 7000 v5.0 HSM** | |
| 3. | **Operating System Support** - Windows, Linux, Solaris | |
| 4. | **API Support**-- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL, Ruby, Python | |
| 5. | **Cryptography** | |
| 6. | PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, Open SSL | |
| 7. | Full Suite B support | |
| 8. | Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined and Brainpool curves | |
| 9. | Symmetric: AES, RC2, RC4, RC5, CAST, DES, Triple DES,ARIA, SEED | |
| 10. | Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512),SSL3-MD5-MAC, SSL3-SHA-1-MAC | |
| 11. | Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode) | |
| 12. | **Physical Characteristics** | |
| 13. | Power Consumption: 12W maximum, 8W typical | |
| 14. | Temperature: operating 0°C – 50°C | |
| 15. | **Security Certifications** | |
| 16. | FIPS 140-2 Level 2 and Level 3 | |
| 17. | Common Criteria EAL4+ (in process) | |
| 18. | BAC & EAC ePassport Support | |
| 19. | **Safety and Environmental Compliance** | |
| 20. | UL, CSA, CE | |
| 21. | FCC, KC Mark, VCCI, CE | |
| 22. | RoHS, WEEE | |
| 23. | **Host Interface-** PCI-Express X4, PCI CEM 1.0a | |
| 24. | **Reliability-** MTBF more than 2,10,000 hrs | |

## Technical Specification- Backup HSM Card for CTS Chennai

| S. No | Description of Requirement | Compliance (Yes/No) |
|---|---|---|
| 1. | **Make: Safenet** | |
| 2. | **Model: LUNA Backup Remote HSM** | |
| 3. | **Operating System Support** - Windows, Linux, Solaris | |
| 4. | **API Support**-- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL, Ruby, Python | |
| 5. | **Cryptography** | |
| 6. | PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, Open SSL | |
| 7. | Full Suite B support | |
| 8. | Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, KCDSA, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined and Brainpool curves | |
| 9. | Symmetric: AES, RC2, RC4, RC5, CAST, DES, Triple DES,ARIA, SEED | |
| 10. | Hash/Message Digest/HMAC: SHA-1, SHA-2 (224-512),SSL3-MD5-MAC, SSL3-SHA-1-MAC | |
| 11. | Random Number Generation: FIPS 140-2 approved DRBG (SP 800-90 CTR mode) | |
| 12. | **Physical Characteristics** | |
| 13. | Power Consumption: 12W maximum, 8W typical | |
| 14. | Temperature: operating 0°C – 50°C | |
| 15. | **Security Certifications** | |
| 16. | FIPS 140-2 Level 2 and Level 3 | |
| 17. | Common Criteria EAL4+ (in process) | |
| 18. | BAC & EAC ePassport Support | |
| 19. | **Safety and Environmental Compliance** | |
| 20. | UL, CSA, CE | |
| 21. | FCC, KC Mark, VCCI, CE | |
| 22. | RoHS, WEEE | |
| 23. | **Host Interface-** PCI-Express X4, PCI CEM 1.0a | |
| 24. | **Reliability-** MTBF more than 2,10,000 hrs | |

**Technical Specification- Transactional HSM Card for Debit Card PIN Generation (Bank Sponsored RRBs)-Payment HSM**

| S. No | Description of Requirement | Compliance (Yes/No) |
|---|---|---|
| 1. | **Make:** <please specify> | |
| 2. | **Model:** <please specify> | |
| 3. | **Key management standards supported** | |
| 4. | •compliant with ANSI X9.24; superset of X9 TR-31<br>•X9 TR-31 Key Block support<br>•RSA Remote Key Transport<br>•DUKPT<br>•Master/Session Key Scheme<br>•Racal Transaction Key Scheme<br>•AS2805 support | |
| 5. | **Cryptographic algorithms supported** | |
| 6. | • DES and Triple-DES key lengths 112 bit, 168 bit<br>• AES key lengths 128 bit, 192 bit, 256 bit<br>• RSA (up to 2048 bits)<br>• FIPS 198-1, MD5, SHA-1, SHA-2 | |
| 7. | **Performance options** | |
| 8. | •Range of performance options up to 1500 Triple-DES PIN block translates / second using key blocks<br>• Multi-threading to optimize performance | |
| 9. | **Host connectivity** | |
| 10. | •Asynchronous (v.24, RS-232)<br>•TCP/IP & UDP (10/100/1000 Base-T) – dual ports for resilience<br>• FICON | |
| 11. | **Certifications / validations** | |
| 12. | •Cryptographic module certified to FIPS: 140-2 Level 3, 46, 81, 180-3, 186-3, 198<br>• PCI HSM<br>• APCA<br>• GBIC<br>• MEPS<br>• NIST SP800-20, SP800-90(A) | |
| 13. | **Security features** | |
| 14. | •Multiple master keys option enabling cryptographic isolation<br>•Two-Factor Authentication of security officers using smart cards<br>•Dual physical locks and/or smart cards control authorization levels<br>•Tamper-resistance exceeding requirements of PCI HSM and FIPS 140-2 Level 3<br>•Detection of cover removal in addition to alarm triggers for motion, voltage and temperature<br>•Device 'hardening' - ability to disable functions not required by the host application | |

| | | |
|---|---|---|
| | •Audit trails | |
| 15. | **Physical characteristics** | |
| 16. | •Form Factor: 2U 19" rack mount • Height: 85mm (3.35")<br>•Width: 478mm (18.82")<br>•Depth: 417mm (16.42")<br>•Weight: 7.3kg (16lb) with single PSU, 7.5kg (16.5lb) with dual PSU<br>•Electrical Supply: 100 to 240V AC Universal input, 47 to 63 Hz. Dual power supply option on all models for resilience<br>•Power Consumption: 100W (maximum)<br>•Operating Temperature: 0 deg C to 40 deg<br>• Humidity: 10% to 90% (non-condensing) | |
| 17. | **Card payments support** | |
| 18. | •American Express/MasterCard/VISA PIN and Card Verification functions<br>•EMV 3.X and 4.X transactions and messaging (inc. PIN Change)<br>•Remote Key Loading to NCR, Diebold and Wincor-Nixdorf ATMs<br>•MasterCard On-behalf Key Management (OBKM)<br>•Integration with all major payment authorization and switching applications | |
| 19. | **Financial services standards supported** | |
| 20. | •ISO: 9564, 10118, 11568, 13491, 16609<br>•ANSI: X3.92, X9.8, X9.9, X9.17, X9.19, X9.24, X9.31, X9.52, X9.97<br>• X9 TR-31, X9 TG-3/TR-39, APACS 40 & 70, AS2805 Pt 14 | |