Required Minimum Specifications
Make , Model & General Aspects
The proposed HSM should have dual connectivity support-TCP/IP & UDP
The proposed HSM should have ability to store one LMK (TDES or AES) and upgradable upto 20 on extra cost basis if required.
HSM should be able to process upto 20 functions per second (CPS) which include PIN translation and other payment functions from day 1 for DC & DR & 20 functions per second which include PIN translation for UAT / Test
HSM should support field upgradability upto 7000 functions (CPS) on extra cost basis if required.
The porposed HSM should offer seamless migration of keys from existing HSMs, with or without any additional support from the OEM's professional services team.
It should support multi-threading so as maximum performance can be achieved.
Support of all major card schemes (American Express, Discover, JCB, Mastercard, UnionPay and Visa)
Mastercard On-behalf key management (OBKM) support
Support both Magnetic stripe and EMV-based data preparation and personalization including mobile provisioning
Support Payment credential issuing – cards, mobile secure elements, wearables, connected devices and host card emulation (HCE) applications
HSM should support all the EFT standard cryptographic functions for debit and credit card management.
HSM should support TR-34 and TR-31 keyblocks to comply with PCI-DSS requirement.
HSM should support ECC keys as defined in FIPS 186-3 (P-256, P-384 & P-521).
HSM should support RSA keys (up to 4096 bit),DES, 3DES KEY lengths 112 bit,168 bit and AES algorithm.
The relevant security settings in the firmware should have PCI compliant values.
Shipment of the HSM should be compliant as per PCI HSM requirement.
Support SNMP

OEM should have a support center in India and should have their own warehouse in India so that any Hardware support (RMA) can be provided easily & without any delay
OEM should be able to provide references from atleast 5 Indian Banking customers who are using Same OEM HSM in Production environment for more than 5 Years In India
The proposed HSM must be running in production at minimum 10 banks/fintech for more than one year
Management Facilities
Should have GUI and CLI available with 2 factor Authentication using smart cards.
Remote Management capability through a Remote Administration Platform (RAP) certified by PCI
HSM should have dedicated management ethernet port.
HSM should support M of N capability.
Utilization statistics - Health check diagnostic and error logs
Remote Key loading facility manufactured by same OEM that is PCI approved
Key Managements
Should support ISO 9564, ISO 10118, ISO 11568, ISO 13491 and ISO 16609 financial service standards.
ANSI: X9.97,X3.92, X9.8, X9.9, X9.17, X9.19, X9.31, X9.52 and X9.24.
ASC X9 TR-31, X9 TR-34, X9 TG-3/TR-39
Should support Thales Key Block format
APACS 40 & 70
HSM should support Format preserving encryption (FPE).
DUKPT (DES, Triple-DES and AES), PIN printing and Generation via a dedicated printer port
Cryptographic Algorithm support

Asymmetric public key algorithms: RSA (upto 4096 bit), ECDSA and ECDH, ECC as defined in FIPS 186-3 (P-256, P-384 & P-521)
Symmetric algorithms: AES (key lengths upto 256 bit) , DES and Triple DES (key lengths upto 168 bit or higher) DUKPT,HMAC, MD5, SHA1, SH2, SHA3
Hash/message digest: SHA-1, SHA-2 (224,256,384,512 bit)
Security Certification
Latest PCI-HSM 3.0 certification in the OEM's name [certification is must]
HSM remote management solution must have PCI HSM v3 Remote Access Platform (RAP) certification in the OEM's name
FIPS 140-2 Level 3 certification in the OEM's name [certification is must]
AusPayNet
Security Features
Tamper resistance meeting requirements of PCI HSM 3.0.
Sensitive data erased immediately in the event of any tamper attack
Strongest security settings implemented by default
Detection of cover removal with addition to Tamper-evident seals, intrusion detection switches and alarm triggers for motion, voltage and temperature
Device hardening - ability to disable functions not required by the host application
Payment HSM should have Dual Physical lock along with console cables
Two-factor authentication for the operator is must
Secure Host communication using TLS or SSL
Audit logs with user control over the scope of events recorded
PIN never appears in the clear outside of a tamper resistant security module as per PCI PIN security requirements

Key Entry Mechanism are protected as per PCI requirements
Remote key loading facilities to NCR , Diebold and POS devices.
Physical Characterstics.
Form Factor - 1U 19” rack mount
Voltage - 90 to 264 VAC
Power Consumption- 80W (maximum)
Temperature Range- -25 deg C to 70 deg C
Dual hot swappable power supply and fans for redundancy
Safety and Environmental compliance
RoHS2, WEEE, UL, UL/CA, UL-AR, CE, BIS, FCC, Canada ICES, RCM, KC, VCCI and REACH
Warranty
3 Years