TAMIL NADU GRAMA BANK

RFP: TMD/16/2023-24 dated 29/12/2023

Clarifications-2

Sl No.	RFP Clause	Query received	Clarification from Bank
1	**SECTION 4 - SPECIFICATIONS AND ALLIED TECHNICAL DETAILS** TECHNICAL AND FUNCTIONAL SPECIFICATIONS 32. Ability to generate and store at least 5000 RSA keys (2048 and 10240) on board on demand and shall be secured inside HSM in accordance with FIPS 140-2 LEVEL 3 recommendations or equivalent.	This is vendor specific process. Please note that storing keys inside the HSM "Keys in box" limits storage capacity. Also it requires manual backups and additional backup HSMs to do that which increases the total cost substantially. Moreover, in the case the HSM fails, the entire infrastructure goes for a toss. This technology is specific to a particular OEM and not generic. The FIPS 140-2 Level 3 certification evaluates on the FIPS boundary and not on the key storage basis. The recommendation is to store the keys as encrypted application tokens and not keys which gives virtually unlimited capacity. Hence we request to kindly modify it to store within the FIPS 140-2 boundary, rather than inside the HSM.	Please adhere to the terms of RFP.
2	**SECTION 4 - SPECIFICATIONS AND ALLIED TECHNICAL DETAILS** TECHNICAL AND FUNCTIONAL SPECIFICATIONS 33.Should support for up to 5000 Transaction (Signing) per Second @ RSA 2048 bits	Since the requirement of HSM is for an ADV solution, hence RSA 2048 algorithm isn't used. The HSM will be used for encryption and decryption using an AES key. Hence 5000 AES-128 encryption/decryption should be fine. TPS of HSM should be either 3000 RSA 2048 signings/second or 5000 AES encryptions/decryption/second, NOT more than that.	Please adhere to the terms of RFP.

3	**SECTION 4 - SPECIFICATIONS AND ALLIED TECHNICAL DETAILS** TECHNICAL AND FUNCTIONAL SPECIFICATIONS 32. Ability to generate and store at least 5000 RSA keys (2048 and 10240) on board on demand and shall be secured inside HSM in accordance with FIPS 140-2 LEVEL 3 recommendations or equivalent.	Please note that storing keys inside the HSM "Keys in box" limits storage capacity. Also it requires manual backups and additional backup HSMs to do that which increases the total cost substantially. Moreover, in the case the HSM fails, the entire infrastructure goes for a toss. This technology is specific to a particular OEM and not generic. The FIPS 140-2 Level 3 certification evaluates on the FIPS boundary and not on the key storage basis. The recommendation is to store the keys as encrypted application tokens and not keys which gives virtually unlimited capacity. Hence we request to kindly modify it to store within the FIPS 140-2 boundary, rather than inside the HSM.	Please adhere to the terms of RFP.
4	**SECTION 4 - SPECIFICATIONS AND ALLIED TECHNICAL DETAILS** TECHNICAL AND FUNCTIONAL SPECIFICATIONS 33.Should support for up to 5000 Transaction (Signing) per Second @ RSA 2048 bits	Since the requirement of HSM is for an ADV solution, hence RSA 2048 algorithm isn't used. The HSM will be used for encryption and decryption using an AES key. Hence 5000 AES-128 encryption/decryption should be fine. TPS of HSM should be either 3000 RSA 2048 signings/second or 5000 AES encryptions/decryption/second, NOT more than that. ** With 3000 TSP Speed – Monthly transaction can be approx. 25 Crore – Which is far far more than requirement	Please adhere to the terms of RFP.

s