

Corrigendum-3 to GeM Bid ref no. GEM/2023/B/3303425 dated 24/03/2023 for Supply, Installation, Maintenance of Tablet Computers for total period of 3 Years (1-year warranty and 2 years of AMC).

It is decided to amend the following in respect of the above GeM bid:

a. GeM bid document (Bid End date/ Bid Opening Date, Page no. 1):

Description	Existing details	Amended details
Bid End Date/Time	27-04-2023, 15:00:00	<u>02-05-2023</u> , 15:00:00
Bid opening Date/Time	27-04-2023, 15:30:00	<u>02-05-2023</u> , 15:30:00

Sl. No.	Section/ Annexure/ Appendix of the GeM bid	Clause No.	Existing	Amended
b.	GeM bid ref. No. GEM/2023/B/3303425 dated 24/03/2023  Buyer Added Bid Specific Terms and Conditions  Additional Terms and Conditions:	<u>Annexure-2 Technical Requirements for Tablet Computers in Canara Bank</u>	Clause:9  Operating System: Android 11 Only	Clause:9  Operating System: Android 12 or 13
c.	GeM bid ref. No. GEM/2023/B/3303425 dated 24/03/2023  Buyer Added Bid Specific Terms and Conditions  Additional Terms and Conditions:	<u>Annexure-2 Technical Requirements for Tablet Computers in Canara Bank</u>	Clause 15:  Bio-metric device with FRM/FIR complied RD Services with L0 & L1 Support, compatible with android.	Clause 15:  Bio-metric device with FRM/FIR complied RD Services with L1 Support device, compatible with android.
d.	GeM bid ref. No. GEM/2023/B/3303425 dated 24/03/2023  Buyer Added Bid Specific Terms and Conditions  Additional Terms and Conditions:	<u>Annexure-1 Scope of Work</u>	Clause 16:  Selected bidder/OEM must provide Two(2) version upgrades on operating system, without any cost to the Bank	Clause 16:  Selected bidder/OEM must provide Three(3) version upgrades on operating system, without any cost to the Bank



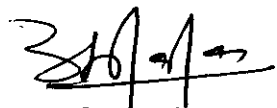
e.	<p>GeM bid ref. No. GEM/2023/B/3303425 dated 24/03/2023</p> <p>Buyer Added Bid Specific Terms and Conditions</p> <p>Additional Terms and Conditions:</p>	<p><u>Annexure-1</u> <u>Scope of</u> <u>Work</u></p>	<p>New Clause:</p>	<p><b>Clause 17:</b></p> <p>Comply with L1 Support Device:</p> <p>Security implementation has Level 1 compliance if the signing and encryption of biometric is implemented within the Trusted Execution Environment (TEE) where host OS processes or host OS users do not have any mechanism to obtain the private key or inject biometrics. In this case, management of private keys need to be fully within the TEE. Any storage outside the TEE will require the keys to be wrapped using the TEE instance specific AES 256 bit keys. The host OS should not have access to biometric capture except through the TEE. All of the processes related to create a biometric PID block must be executed within the TEE (at a level below the host OS):</p> <ol style="list-style-type: none"> <li>1. Biometric processing/extraction to create the bio element</li> <li>2. Signing the bio element.</li> <li>3. Encryption of the PID block</li> </ol> <p>The following processes must take place within a hardware key store</p>
----	--	--	--------------------	--

				<p>(secure crypto block).</p> <p>1. Identity of the chip Ci (look at section Pre-Certified Hardware Identity) should be stored in the secure crypto block or wrapped with the instance specific unique key (non extractable and stored within the secure crypto block) if stored outside. Chip identity should be non clonable.</p> <p>2. Key pair generation</p> <p>3. Signing the bio element</p> <p>It is required to minimize the attack surface at the system level by using methods such as but not limited to hidden traces, protective meshing, encrypted communication etc. Minimizing the attack surface is in line with the objective 1 of this document. In addition, it is recommended that temper responsiveness be implemented for the system.</p>
--	--	--	--	---

All the other instructions and terms & conditions of the above GeM bid shall remain unchanged.

Please take note of the above amendments while submitting your response to the subject GeM bid.

Date: 25/04/2023  
Place: Bengaluru

  
Deputy General Manager

