

Some prospective Bidders have asked for some clarification on some minor points, which have been clarified below:

RFP Volume	Page No.	Section No.	Excerpt from the RFP	Clarification
RFP volume I	50	2.2.1.2 Solution Analysis & Design (Point No g)	The SI must ensure that the OEM vetted sizing is proposed and must attach those vetted documents in technical solution.	For the sizing document based on the proposed architecture of the SI: <ol style="list-style-type: none"> 1. The H/W OEM has to certify their H/W in compliance with the H/W specifications and the proposed architecture 2. The Bidder/System Software OEM shall certify that the proposed licenses are compliant to the licensing matrix/policy of the OEM
RFP volume I	67	2.2.3.4	IFMS shall use Biometric Devices and Digital Signature Certificate along with password for user identity management. The SI shall be responsible for maintaining Biometric Devices and DSC for the IFMS users. The SI shall also maintain a link with the Digital certificate authority, the SIs of the DSC for authenticating the DSCs of the users of the IFMS.	Associated token and related software for Digital Signature Certificate (DSC) shall be procured by the Department and the SI must ensure that the DSC certificates are integrated with the offered solution for the required authentication and authorisation, transactional services, as per departmental rules / IT ACT and associated verification with the respective CA of the Subject, and associated technical guidance, troubleshooting, fixing of its CSR generation, regeneration and usage for the end users. Maintenance of the DSC repository is outside the scope of the SI
RFP volume I	85	3.5 PAYMENT TERMS & CONDITIONS	100% of total Managed IT Services Cost will be paid through QGR for the maintenance period of 7 years	Maintenance Period will be for 5 years after the go-live of all rollout locations.
RFP volume III	564	Form 10: Safe to host certificate for security audit	Sir, This is to inform you that the application/ website/ web portal namely “_____” which is going to be hosted at West Bengal State Data Center is safe to host at WBSDC and the security audit report(s) is/are attached herewith proving the same. I would like to request you for hosting the application at SDC environment. I also undertake that if there will be any change in the application, we will again undergo security testing of the application and once we will get security audit clearance, we will again provide this form to you for your record.	SI is required to conduct security audit during Pilot and final Rollout phases and this should be factored in for the financial bid. Moreover, the “security audit” certification and “safe to host” certification of the IFMS application during the entire period of contract covering O&M phase, is also entirely the responsibility of System Integrator, who will be selected through this tender. The security audit certification will be needed to be conducted prior to hosting the application in production environment at SDC whenever there will be any major code change/ process change in the application during O&M phase. However, the cost for security audit during the O&M phase (except for necessary support activities) need not be factored in for the financial bid

The above points have already covered under the existing RFP. So **there will be no extension of the last date of submission of Bid.**