| | |
|---|---|
| 1 | **Title** |
| | Development of secure, customized 3G/LTE end-points (Handsets/Dongles) for a captive mobile network |
| 2. | The user operates a captive pan-India 3G mobile communications network. Security-customized handsets are required for usage on the network to ensure end-point security. |
| 3. | **Objective** |
| | To develop security-customised, ruggedised, 3G/LTE communications end-points, both as handsets and dongles (for data access), for deployment on the user captive mobile network. |
| 4. | **Description** |
| | (a) Android OS based COTS handsets are presently being used on the network.<br><br>(b) Import route is not feasible due to sustained service and support issues. Existing 3G handsets are manufactured/assembled in India and customization to cater to specific security requirements needs design and development changes at assembly line.<br><br>(d) Vulnerabilities from information security aspects have been blocked at application level.<br><br>(e) The proposed customized-handsets would enhance end-point security on the communications network, for enhancing last-mile connectivity and consolidate Network-Centric warfare capabilities.<br><br>(f) Availability of the proposed security customized handsets will strengthen the enterprise network security of Services. |
| 5. | **Functional and Operational requirements in qualitative terms** |

| | |
|---|---|
| | (a) The device must support and implement containerization of official and personal data. Official data must be stored on cloud/ limited on-board memory in encrypted form.<br><br>(b) The device must have dual SIM slots with No.1 SIM for official communication only and No.2 SIM for personal communication.<br><br>(c) The SDK with premium and granular access to device architecture must be made available along with on-premise keys and licenses.<br><br>(d) The device must implement encrypted mode of communication using at least AES 256 algo with a provision to port buyer-specific Algo.<br><br>(e) The device must support 4G technologies including VoLTE along with backward compatibility to 3G.<br><br>(f) The device must have bio-metric access control features.<br><br>(g) The device OS and firmware must be updated on-premise with NO obligation to be connected to the Internet.<br><br>(h) The device must have a sturdy built with shatter-proof screen, water-resistant body.<br><br>(j) Device should have a feature for remote – location finding of the device in the event of loss. |
| 6. | **Functional and Operational requirements in quantitative terms** |
| | (a) Device should be powered by a processor with at least quad-core dimension, 2 GHz with a RAM of 4 GB.<br><br>(b) The device battery must provide at least 12 H of charged life while data usage is ON.<br><br>(c) Device battery temperature must not exceed 60 C at any |

| | |
|---|---|
| | time.<br><br>(d) Technology and parts should be available at least 3 years to maintain the system. |
| 7. | **<u>SAG Certification required</u>** |
| | (a) Crypto Acquisition policy (2006), SAG, DRDO.<br><br>(b) Framework for Certification of IT products , SAG, DRDO. |