QR's/SPECIFICATIONS OF MOBILE SECURITY MANAGEMENT SYSTEM

OEM/ Vendors are required to respond/ comment on the following details and indicate which may/ may not be essential requirements of secure mobile communication system (as per questionnaire below).

Introduction. NSG intends to procure Mobile Security Management System to provide a secure mobile communication and key management along with server housed in NSG premises. The System will have a central server for key management and authentication of the user. The application will be loaded on each smartphone of user and through this app the voice & SMS will be secured. The system administrator will manage the mobile of users and will resist the unnecessary installation of other apps *and also resist the usage of camera, mic and location update required by some app* without permission of administrator. The specifications worked out are as mentioned below:-

S/NO	PARAMETERS	SPECIFICATIONS
SYSTEM.		
1	Design	Indigenous
2	Feature	Encrypted Voice & SMS Communication
3	Architecture	Support Client-Server
4	Subscriber	Support upto 500 & scalable upto 10,000
5	Modules	(a) Server module
		(b) Hardware based True Random Generator module
		(c) Application (App) for Smart Phones
		(d) Rugged Smart Phone
SERVER.		
6	Feature	(a) Secure application registration
		(b) Secure Subscriber management (Monitor and control Secure App remotely)
		(c) Facility of loading encryption algorithm in App by *user using external device*
		(d) Push desired Algorithm into secure phone App
		(e) Push key generated by Hardware based True Random generator module into secure phone App
		(f) *Create a group of users to share the address* book with in secure phone App users

23/08/16 23/8/16

NSG NSG BSF CRPF SSB ITBP DCPW

		(g) Monitor and record the log (Voice & SMS)
		(h) Remotely erase the memory and app if required
		(j) Remotely restrict the access to secure phone App
7	License for client	500 subscribers & extendable to 10,000
8	Processor	Quad core or higher
9	RAM	32 GB or higher
10	HDD	1 TB or higher
11	Interface	Gigabit Ethernet Interface
12	OS	Linux or Windows
13	*Hosting /Housing*	*In the premises of consignee*
RANDOM NUMBER GENERATOR.		
14	Features	(a) Should have no operating system
		(b) Micro controller based I/O interface
		(c) Flexibility to port new sampling procedure
		(d) User configurable Random number bit width
		(e) Maintain log of all changes
		(f) Multi level tamper detection system
		(g) In case of temper attempt, all data to be erased
15	*I/O Interface*	*(a) LCD /LED/any display interface for status & alert* messages
		(b) Keypad for configuring device
		(c) Port to communicate with PC
16	PC Interface	GUI based, for generating, testing & storing random numbers
17	Mounting	Table top/ Rack mountable
18	Power	240V/ 50-60 Hz
SMART PHONE.		
19	Screen Size	4" or higher
20	OS	Android (V 4.0 & above)
21	*CPU*	*Dual core or better*
22	Memory	RAM 2GB or higher, Internal storage 32 GB or higher
23	WLAN	Wifi 802 -11 b/g/n, hotspot
24	Bluetooth	V 4.0, A 2DP, EDR, LI or better
25	USB	Micro USB V 2.0
26	Encryption	FPGA/ Controller based or better for Voice & SMS communication
27	Control	Over all data, OS, App and feature to erase data through app or Server
28	Power	Li-Ion 3100 mAh Battery or better

23/08/16 23/8

NSG NSG BSF CRPF SSB ITBP DCPW

29	Rugged design	Water & Dust resistant (IP65)
30	Anti tamper	Multi level tamper detection mechanism
MOBILE APPLICATION (App).		
31	Design	Indigenous
32	Graphical user Interface	Icon based, simple in design, feature to have voice call or SMS on selected number from secured contact list
33	Support OS	Android 4.0 onwards
34	GUI Authentication	Using PIN or Biometric
35	Encryption	AES 256 Algorithm or higher
36	SAG Grading	Grade 2 or better
37	Key generation	Through Random Number Generator
38	Session Key	Separate key for each session
39	Connectivity	End to end secure communication over 2G/ EDGE, 3G, 4G/LTE, WiFi
40	Feature	Erases the secured memory and inactivate the app in case of emergency
41	Server Interface for voice	App communicate to server for signalling only and the voice is encrypted by mob app only
42	Server Interface for Data	App forward the encrypted message via Server, However server should not be able to decrypt the message
KEY MANAGEMENT SYSTEM.		
43	Fill Guns	Mother Fill Gun & Child Fill Gun
44	Feature	(a) Mother fill gun collect key from True Random Generator
		(b) Key data fill to be loaded into child fill gun from mother fill gun
		(c) Child fill gun is used to load key data file into secure handset.

23/08/16.
Sh Ish Atil, GC(Comn), HQ NSG

23/8/16
Col Naveen Sehrawat
GC, ESG, NSG

HQ BSF

DC BK Pandey
HQ CRPF

AC NA Yadav
HQ SSB

DCT Amit Gupta
HQ ITBP

Dy Dir Rajesh EKKa,
DCPW

(Approved/Not Approved)

DG, NSG

24/8/16.

TRIAL DIRECTIVES FOR MOBILE SECURITY MANAGEMENT SYSTEM

All parameters/specifications mentioned in QRs will be checked by the Board of Officers by ascertaining/verifying following checks in the presence of Vendor/Supplier/Manufacturer. In case of any discrepancies/problem, the vendor/rep of firm will demonstrate the features to the Board of officer of the force concerned. Further, if proper testing instrument for testing these parameters is not available with customer, same will be arranged by the vendor.

(a) **Physical Checks.** In this category, specifications of the equipment will be checked physically as per QRs.

(b) **Functional Checks.** The vendors will show all the features/configuration of the equipment functioning on ground to the board of officers during trials.

(c) **Submission of Certificates.** Specification which cannot be checked due to lack of testing facilities/expertise, self certificate of OEM has to be provided by the vendor/bidder during trial.

S/NO	Parameters	Specifications	Trial Directives
SYSTEM.			
1	Design	Indigenous	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
2	Feature	Encrypted Voice & SMS Communication	
3	Architecture	Support Client-Server	
4	Subscriber	Support upto 500 & scalable upto 10,000	
5	Modules	(a) Server module	
		(b) Hardware based True Random Generator module.	
		(c) Application (App) for Smart Phones	
SERVER.			
6	Feature	(a) Secure application registration	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
		(b) Secure Subscriber management (Monitor and control Secure App remotely)	
		(c) Facility of loading encryption algorithm in App by user using external device	
		(d) Push desired Algorithm into secure phone App	
		(e) Push key generated by Hardware based True Random generator module into secure phone App	

23/8/16. 22/8

NSG NSG BSF CRPF SSB ITBP DCPW

		(f) Create a group of users to share the address book with in secure phone App users	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
		(g) Monitor and record the log (Voice & SMS)	
		(h) Remotely erase the memory and app if required	
		(j) Remotely restrict the access to secure phone App	
7	License for client	500 subscribers & extendable to 10,000	
8	Processor	Quad core or higher	
9	RAM	32 GB or higher	
10	HDD	1 TB or higher	
11	Interface	Gigabit Ethernet Interface	
12	OS	Linux or Windows	
13	Hosting /Housing	In the premises of consignee	
RANDOM NUMBER GENERATOR.			
14	Features	(a) Should have no operating system	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
		(b) Micro controller based I/O interface	
		(c) Flexibility to port new sampling procedure	
		(d) User configurable Random number bit width	
		(e) Maintain log of all changes	
		(f) Multi level tamper detection system	
		(g) In case of temper attempt, all data to be erased	
15	I/O Interface	(a) LCD /LED/any display interface for status & alert messages	
		(b) Keypad for configuring device	
		(c) Port to communicate with PC	
16	PC Interface	GUI based, for generating, testing & storing random numbers	
17	Mounting	Table top/ Rack mountable	
18	Power	240V/ 50-60 Hz	

23/08/16. 23/8

NSG NSG BSF CRPF SSB ITBP DCPW

SMART PHONE.			
19	Screen Size	4" or higher	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
20	OS	Android (V 4.0 & above)	
21	CPU	Dual core or better	
22	Memory	RAM 2GB or higher, Internal storage 32 GB or higher	
23	WLAN	Wifi 802 -11 b/g/n, hotspot	
24	Bluetooth	V 4.0, A 2DP, EDR, LI or better	
25	USB	Micro USB V 2.0	
26	Encryption	FPGA/ Controller based or better for Voice & SMS communication.	
27	Control	Over all data, OS, App and feature to erase data through app or Server.	
28	Power	Li-Ion 3100 mAh Battery or better	
29	Rugged design	Water & Dust resistant (IP65)	
30	Anti tamper	Multi level tamper detection mechanism	
MOBILE APPLICATION (App).			
31	Design	Indigenous	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
32	Graphical user Interface	Icon based, simple in design, feature to have voice call or SMS on selected number from secured contact list.	
33	Support OS	Android 4.0 onwards	
34	GUI Authentication	Using PIN or Biometric	
35	Encryption	AES 256 Algorithm or higher	
36	SAG grading	Grade 2 or better	
37	Key generation	Through Random Number Generator	
38	Session Key	Separate key for each session	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
39	Connectivity	End to end secure communication over 2G/ EDGE, 3G, 4G/LTE, WiFi	
40	Feature	Erases the secured memory and inactivate the app in case of emergency	

23/08/16. 23/8

NSG NSG BSF CRPF SSB ITBP DCPW

41	Server Interface for voice	App communicate to server for signalling only and the voice is encrypted by mob app only	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
42	Server Interface for Data	App forward the encrypted message via Server, However server should not be able to decrypt the message	
KEY MANAGEMENT SYSTEM.			
43	Fill Guns	Mother Fill Gun & Child Fill Gun	The Board will carry out physical and functional test of the mentioned parameter. In case of any discrepancies/ problem, the vendor/rep of firm will demonstrate the features to the Board of officer and will also submit the OEM compliance certificate.
44	Feature	(a) Mother fill gun collect key from True Random Generator	
		(b) Key data fill to be loaded into child fill gun from mother fill gun	
		(c) Child fill gun is used to load key data file into secure handset.	

23/08/16.
Sh Ish Aul, GC(Comn)
HQ NSG

23/8/16
Col Navin Sahrawat
GC, ESG, NSG

DC BK Pandey
HQ CRPF

HQ BSF

DCT Amit Gupta
HQ ITBP

AC NA Yadav
HQ SSB

(Approved/Not Approved)

Sh Rajesh EKKa, Dy Dir
DCPW

DG NSG