No.C.VII.1/2015-ITW(QRs)-(4) 1619

भारत सरकार/Government of India

गृह मंत्रालय/Ministry of Home Affairs

पुलिस आधुनिकीकरण प्रभाग /Police Modernization Division

संभरण-I डेस्क /Prov.I Desk

Jaisalmer House, 26 Man Singh Road,
New Delhi, dated the 17th Aug, 2015

To,

DsG: AR, BSF, CISF, CRPF, ITBP, SSB, NSG & BPR&D.

Subject: QRs and Trial Directives of Multi-Level Security Authentication Device with Digital Signature for VPN on Internet.

Sir,

The undersigned is directed to refer to the subject mentioned above and to say that the QRs and Trial Directives in respect of QRs and Trial Directives of Multi-Level Security Authentication Device with Digital Signature for VPN on Internet as per Annex- "A" and Annex-'"B", respectively have been approved by the competent authority in MHA.

2. Henceforth, all the CAPFs should trial evaluate and procure the above item, required by them, strictly as per the laid down QRs.

3. Concerned CAPFs will be accountable for correctness of the QRs and Trial Directives of QRs and Trial Directives of Multi-Level Security Authentication Device with Digital Signature for VPN on Internet.

Yours faithfully,

(M. N. Sukole)
Under Secretary to the Govt. of India

Encl: As above.

Copy forwarded for necessary action to:

SO (IT), MHA - With the request to host the QRs and Trial Directives of QRs and Trial Directives of Multi-Level Security Authentication Device with Digital Signature for VPN on Internet on official website of MHA (under the page of Organizational Set up, Police Modernization Division-Communication Equipments).

Copy to: DDG (Procurement), MHA

(R.K. Soni)
Section Officer (Prov.I)

APPX-'A'

QRs/Technical Specification of Multilevel Security Authentication Device

Hard Token

S/No.	Specifications	Requirements
1	Hard Token	Two factor authentication Token should comply industry standard certification [e.g. PCI, FFIEC, HIPAA(optional)]. The hardware token should be tamper proof and not have any changeable parts.
2	Dynamically generate a new password within every 60 or less seconds	The Token should generate a new password at least within 60 seconds.
3	Support for Pass code with OTP (One Time Pass code)	Two Factor Authentication should support PASSCODE (combination digits numeric/alphanumeric PIN and a pseudorandom token no).
4	Time Sync with the Authentication Server	The password generated by the token should be in sync with the authentication server
5	Six Digit Numerical Password	The password generated by the token should be a six digit numerical password to ensure it cannot be guessed in a given time frame
6	Token Life Span	The token should have a 1 or 3 or 5 years battery life.
7	Unique Identity	Every token should have an unique identity and should be unique to the user
8	Multi Application Support	It should be possible to integrate the same token with other applications if required.
9	Small and convenient form factor	The token should have a small form factor which can ensure ease of carrying.
10	Token Activation	User should be able to activate the token on his own after mapping in authentication server
11	Token bound with user	The authentication server can map the two usernames to the UserIDs

** ***

Mobile Token

S/No.	Specifications	Requirements
1	Mobile Token	Two factor authentication Token should be comply industry standard certification [e.g. PCI, FFIEC, HIPAA(optional)]. The hardware token should be tamper proof and not have any changeable parts.
2	Dynamically generate a new password within every 60 or less seconds	The Token should generate a new password atleast within 60 seconds.
3	PIN Protected	Token on mobile can should be alphanumeric pin protected
4	Time Sync with the Authentication Server	The password generated by the token should be in sync with the authentication server
5	Six Digit Numerical Password	The password generated by the token should be a six digit numerical password to ensure it cannot be guessed in a given time frame
6	Multi OS Support	The Mobile token should be available as a software form factor that can be installed on a Windows Mobile, iOS, Android, Blackberry etc
7	Unique Idenitiy	Every token should have an unique identity and should be unique to the user
8	Multi Application Support	It should be possible to integrate the same token with other applications if required.
9	IMEI / UID Binding	The mobile token generator should be bound with the IMEI device. The application installed on one IMEI / UID should not be installed on another
10	Token bound with user	The authentication server can map the two usernames to the UserIDs

** ***

Authentication Manager

S.No	Specifications	Requirement
1	Same Authentication Server for All type of Tokens & Deployment Option	The same authentication manager should be used to authenticate both the Hard Token user as well as SMS token user. The authentication manager should provide both the software based solution and hardware appliance based solution. It is upto CUSTOMER to choose the deployment option Hardware/Software(Virtual) depending on the requirements.
2	Emergency access to user	The authentication manager should provide alternate method of authentication in case of token failure to validate user
3	Support for custom API based Plug Ins	Should provide APIs to enable building of agents for home grown applications.
4	Sync users and user details	Authentication manager should be provide facility of sync of all the users from the Internal database, current LDAP or other authentication agent. The server should regularly sync with LDAP/Other auth agent and make auto modifications where necessary if allowed
5	Lock / Unlock a user	The authentication manager should have provision to lock a particular user on numerous wrong attempts or unlock a particular user .
6	Associate users to Token	The authentication manager should have provision to assign a Token to a user.
7	Portable Architecture	Authentication manager should have inbuilt RADIUS Server.The authentication manager should have provision to create separate logical groups and if required create separate administrator(s) for these groups.
8	Role & Policy set for different tokens and users	The authentication server should allow the administrator freedom to create his own policies and assign them to different set of users. Should have inbuilt admin roles like: Security Domain Administrator, User Administrator, Token Administrator, Privileged Help Desk Administrator, Help Desk Administrator, Agent Administrator
9	Authenticate different applications with the same auth manager	It should be possible to integrate multiple applications. It should be possible to assign different set of policies for each
10	Manage Tokens	Should support emergency access for in case of lost, misplace, or damaging of tokens for both online and offline users.
11	GUI	The software should have an easy to use GUI for authentication manager administration. Should have a web based management console and should allow N level delegation of administrators.
12	Back Up / Restore	Authentication manager should allow backup/restoration of server configuration and user database.
13	High Availability	The solution should be provided with High Availability and automatic failover between each system. Should provide agent based load balancing and high availability capabilities using multiple primary and replica servers. database replication communication between replica server should be encrypted. Should allow setting up of minimum 4 replicas for failover and load balancing & high availability. Should have inbuilt support for clustering to improve throughput performance and achieve scalability.
14	Logs Management	The access and other system logs generated by the system / OTP engine should provide for audit trials. All activities at admin console should have an audit trail of all logon attempts and operations. Logs and should be tamper proof. Option to export logs to other log server for analytiv view should be available.
15	Multi-OS Support	Authentication manager should be all leading operating system viz. work on Linux / Solaris / Windows / Vmware environments.
16	Support a wide variety of VPN's	The solution should support integration with most popular firewalls, SSL IPSEC VPNs, routers,

		RADIUS servers, NAC clients, VPN clients, Citrix servers window servers(2003008 32 and 64 bit) local and RDP logon, wireless access points etc.
17	Token Assignment	Should provide inbuilt database for user record creation and token assignment that could be automatically synced with external LDAP if allowed
18	Reports	Should have inbuilt reports like: Administrators with a Specified Role Users with Disabled Accounts Users and User Groups Missing From User database(internal/external) User and User Group Life Cycle Activity Users with Days Since Last Login Using Specific Token Expired User Accounts Principals Never Logged In with Token Distributed Token Requests and Token Expiration Authentication Activity Should provide extensive customized reporting for administrator
19	Inbuilt RADIUS	Authentication server should have inbuilt RADIUS Server for ease of integration with end systems that support RADIUS based authentication.

Pavitra Chakravarty,
DC (IT), CRPF

Col. S. Balakrishanan,
GC, ESG, NSG

K. Ramasubramanian,
Sr. T.D., NIC

Pardeep Yadav,
AC, ITBP

Shailendra Kumar
20/4/15
IG (Comn), CRPF

Mayank Kumar Dansena,
AC (IT), CRPF

Lt. Col. P. S. Manhas,
SC, ESG, NSG

Alok Roy Choudhary,
SSA, NIC

Sonu Sikarwar,
AC, CISF

A. P. S. Virk,
DC (IT), BSF

Sanjeev Kumar,
AC, SSB

Amarjeet Singh,
E. ASSTT. DIR., DCPW

S. M. Hasnain,
DIG (IT), CRPF

[Approved / ~~Not Approved~~]

Prakash Mishra, IPS
DG, CRPF

Trial Directives for Multilevel Security Authentication Device

Hard Token

S/No.	Specifications	Trial Directive
1	Hard Token	Documents submitted by the company and with the physical verification of token
2	Dynamically generate a new password within every 60 or less seconds	Check for two consecutive passwords generated by the token. The gap between the two passwords generated should not be more than 60 seconds
3	Support for Pass code with OTP (One Time Pass code)	Verify with documents and verification on device
4	Time Sync with the Authentication Server	Verified with the documents specification
5	Six Digit Numerical Password	Verified same on the token
6	Token Life Span	Verify with the document and same will show in authentication manager
7	Unique Identity	The user should generate passwords on two different tokens. The tokens should show a difference sequence of password generated
8	Multi Application Support	The same token should be used on two different applications
9	Small and convenient form factor	Verify from the data sheet and physical appearance
10	Token Activation	The authentication manager should provide a URL wherein which the user should be able to activate the token on its own after allotement of id from administrator
11	Token bound with user	The administrator should assign the same token to two different usernames belonging to the authentication manager

Mobile Token

S/No.	Specifications	Trial Directive
1	Mobile Token	Documents submitted by the company and with the physical verification of token
2	Dynamically generate a new password within every 60 or less seconds	Check for two consecutive passwords generated by the token. The gap between the two passwords generated should not be more than 60seconds
3	PIN Protected	The user should able to loging with the combination of user PIN & passcode before he would be allowed to authenticate
4	Time Sync with the Authentication Server	Verified with the documents specification
5	Six Digit Numerical Password	Verified same on the token
6	Multi OS Support	Mobile tokens should be demonstrated on Android, iOS and windows platform
7	Unique Identity	The user should generate passwords on two different tokens. The tokens should show a difference sequence of password generated
8	Multi Application Support	The same token should be used on two different applications
9	IMEI / UID Binding	The user should attempt to install a mobile token on two different handsets. He should not be able to install the same token on more than one handset
10	Token bound with user	The user should assign the same token to two different usernames belonging to the same user

Authentication Manager

S.No	Specifications	Trial Directive
1	Same Authentication Server for All type of Tokens & Deployment Option	Verify from the datasheet and by Using the same authentication maanager user should be able to assign different types of tokens
2	Emergency access to user	Verify from the datasheet and verifying the featuer on authentication manager in administrative mode.
3	Support for custom API based Plug Ins	Data Sheet and technical specifications. A proof of concept with any customized solution
4	Sync users and user details	Data Sheet. A proof of concept
5	Lock / Unlock a user	Datasheet and verify same in authentication manager in

94

		administrative mode
6	Associate users to Token	An management interface where the administrator can assign tokens in the authentication manager
7	Portable Architecture	The administrator should be able to create different admins role for management
8	Role & Policy set for different tokens and users	The administrator should be able to create different set of policies for different users on authentication manager
9	Authenticate different applications with the same auth manager	The administrator should be able to create different authentication identity(Local / LDAP / RADISU) in the same authenitcation manager
10	Manage Tokens	The administrator should be able to assign, unassign, disable, lock / unlock a token from the server
11	GUI	All functionality of authentication manager and self service portal for remote user should be cheked by POC.
12	Back Up / Restore	The administrator should be able to schedule / take a backup and restoration of same in the other server
13	High Availability	Data Sheet and technical specifications, or with proof of concept
14	Logs Management	Data Sheet and technical specifications, or with proof of concept
15	Multi-OS Support	Data Sheet and technical specifications, or with proof of concept by installing on differnet OS / in virtual environment
16	Support a wide variety of VPN's	Data Sheet and technical specifications, or with proof of concept
17	Token Assignment	Data Sheet and technical specifications, or with proof of concept
18	Reports	Data Sheet and technical specifications. Same can be verified with proof of concept
19	Inbuilt RADIUS	Data Sheet and technical specifications. Same can be verified with proof of concept

Pavitra Chakravarty,
DC (IT), CRPF

Mayank Kumar Dansena,
AC (IT), CRPF

A. P. S. Virk,
DC (IT), BSF

Col. S. Balakrishanan,
GC, ESG, NSG

Lt. Col. P. S. Manhas,
SC, ESG, NSG

Sanjeev Kumar,
AC, SSB

K. Ramasubramanian,
Sr. T.D., NIC

Alok Roy Choudhary,
SSA, NIC

Amarjeet Singh,
E. ASSTT. DIR., DCPW

Pardeep Yadav,
AC, ITBP

Sonu Sikarwar,
AC, CISF

S. M. Hasnain,
DIG (IT), CRPF

Shailendra Kumar
IG (Comn), CRPF
20/4/11

[Approved / Not Approved]

Prakash Mishra, IPS
DG, CRPF