Annexure- 5

TECHNICAL BID CRITERIA

Functional/ Technical Requirements Compliance Table

S.No	Functional/Technical Requirements	Compliance yes/No	Remarks
	A. General Features		
1	The solution should support Windows 7 and any future OS released by the OEMs		
2	Solution should work in multi vendor environment		
3	The solutions should support both Domain and non-Domain based User – User Group policies.		
4	The solution should support a client based (standalone) instance (without server).Agent policy should work even when the computer is not connected to the Corporate Network		
5	The solutions should protect itself against manipulation – attacks		
6	The ability to password protect the client to prevent uninstallation or change of settings.		
7	The solution should be designed to run specifically for self-service terminal		
	B. Central Management		
1	The solutions should be managed from a central point of management on real time basis		
2	The solution should support event logging .Ensure real-time monitoring of security relevant hardware- and software events. it is required to collect all the audit trails at a central location and review them on a daily basis.		

3	Solution should support multiple Physical/Logical Hard drives		
4	The solutions should support remote installation via software distribution tool		
5	The solutions should also support local installations		
C. Access Management			
1	The solution should allow for the remote user management		
2	The solution should support One Time expiring passwords (Dynamic Admin password)		
3	The solution should support online and offline password management		
4	The solution shall be managed from a central point of management and should work with any standard ATM agent monitoring solution.		
5	The Solution should support various map and dashboard views with filtering capabilities for instant access to security status of terminals/devices. Like OS hardening status, Dynamic admin password status, solution installation status etc.		
6	The solution should support - Deploy and update Security Policies and configurations as given by the OEM/MSP and other agencies from time to time.		
7	The solution should provide SMS and E-mail alerts for significant / critical events/changes.		
8	The solution shall not have performance impact of the existing ATM and the peripheral devices e.g. Switch, CD, Bunch Note Acceptor, Cash Recyclers.		

9	The solution shall allow remote management of user credentials according to strong password and industry requirements or Bank's IT security or audit dept.		
10	The solution shall allow an administrator to define different roles for various users & groups and assign each of them specific user rights.		
11	The solution should provide additional hardening capability to the operating system, irrespective of the OEM(which is based on ATM industry best practices). Basic Hardening + additional Hardening as per the security advisories received from time to time .		
12	The solution should support –Detailed Event and Log information available along with hardware information for a complete picture of a device's actual status.		
13	The solution shall be able to disable Auto-run facility of exe file from a network or a USB port.		
14	The solution shall be able to set Windows Admin/other User Password Centrally.		
15	The solution should support security at ATMs for required time interval or no. of reboots for maintenance work which require the field engineer to have administrator rights. But at no time should an admin password needs to be shared with engineer. The right should be granted based on token system(this should work when the ATM is not connected to the bank's ATM network)		
D. Disk Encryption		The solution should support Full hard disk encryption(FHDE)	

1	The solution should enable for an exact status of disk encryption to be retrieved and display centrally on a monitoring system		
2	The solution should be capable of changing the configuration of the hard disk encryption and the parameters used to encrypt		
3	The solutions should have the capability to decrypt an ATM hard drive outside of the ATM for recovery purpose only using the relevant encryption key.		
4	The ATMs should still cater to customers while the hard disk is being encrypted (during installation)		
5	The solution shall support Encryption of all data (user files as well as system files) from an ATM's and Cash Recyclers hard disk.		
6	The solution shall protect data confidentiality when a system is out of operation.		
E. Hardening		The solution should provide additional hardening capability to the operating system, irrespective of the OEM	
1	The solution should be able to dynamically change the hardening policy of the OS on the ATM from time to time		
2	The solution should be able to block USB ports on the ATM through centralized Control		
3	OS Hardening solutions should support user (role based) access to the terminals based on tokens (no need to distributed user credentials)		
4	The solution should have a user Interface to be able to customize and manage the hardening policies		
5	The Operating System Hardening should be managed and administered centrally		

6	During policy distribution to the ATM's, the hardening policies should be protected against manipulation		
7	The hardening solution should also be extended to browsers and other software components running on self-service terminals e.g. personal firewalls, ip-address / port management .		
8	The solutions should protect against malware/Viruses being injected on to the machine and any other unauthorized Software installations. Via local means e.g. USB drive, CDROM, network etc.		
9	The solution should protect against the manipulation of executables e.g. .exe, .dll, .class etc. and scripts e.g. .js, .bat etc.		
10	The solution should protect against the unauthorized updating / changing of configuration – property files		
11	The solution should have firewall functionality		
12	The solution should be capable of identifying behavior anomalies within the ATM software		
13	The solution should issue alert / warning/ prevent once a threat has been identified		
14	The solution should block the unauthorized installation of software		
F. Intrusion Detection And Protection (anti malware/anti-virus)		The solution should have provision to block USB ports on the ATM	
1	The solution should be protected against being manipulated		
2	The solutions should protect against malware/Virus which may be injected locally or remotely on to the machine.		

3	The solution should protect against the manipulation of executables e.g. .exe, .dll, .class etc. and scripts e.g. .js, bat, .bat etc.		
4	The solution should protect against the unauthorized updating / changing of configuration – property files		
5	The solution should issue alert / warning once a threat has been identified		
6	The solution should block the unauthorized installed software		
7	The solution should have capability to allocate only required ATM resources to the White listed application. And during the running of the Whitelisted application should monitor if only those resources are being accessed. In case of any deviation, alert should be raised and resources should be blocked. Further, any outdated malware definitions on a terminal should be highlighted in a centralized dashboard.		
G. Other Requirements		Only permitted applications to be run in the Machines using Sandboxing concept **or equivalent,** thus effectively nullifying the need of any anti-virus solution.	
1.	To whitelist only the required applications to be Run in the ATMs.		
2.	Access to external devices should be centrally controlled		
3.	All files to be protected from damages		
4.	Doesn’t allow any registry level changes		
5.	Detect and Block Unused Services and Applications		
6.	Disabling Auto play Options which allows software to run from removable media		
7.	NPCI/RBI and Industry regulation and audit compliance to be followed from time to time.		

8.	Investigate and report suspicious activities like deviating or non-consistent transaction or event patterns which are caused by unauthorized system usage.		
9.	Terminal Security Delivers end-to-end protection from all side network and local attacks		
10.	Protection/detection policies to monitor files, settings, events and logs, and report anomalous behaviour through Centralized Dashboard.		
11.	Mechanism to validate and allow ATM Engineers to perform Maintenance Activities.		
12.	All the updates/ releases in the solution during the contract period to be provided to the bank without any additional cost.		
13.	24 x 7 support to be made available from the Technical Assistance Center (TAC)		
14.	Auto Run facility should be disabled.		
15.	Access should be time based admin access and dynamic password.		
16.	Presentation on product		
17.	Any other USP & enhanced security of the product		

(Non compliances of any of the line items will summarily disqualifying the bidder)

Yours faithfully,

SIGNATURE
(Name & Designation, seal of the firm)

(Any bid not fulfilling any of the eligibility cum technical criteria under **MANDATORY REQUIREMENTS** or even having said “**Yes**” in the bid document but found “**No**” on the ground during actual evaluation would be summarily rejected).

Technical Evaluation

S.No	Functional/Technical Requirements	Compliance yes/No	Remarks
	A. General Features		
1	The solution should support Windows 7 and any future OS released by the OEMs	2	
2	Solution should work in multi vendor environment	1	
3	The solutions should support both Domain and non-Domain based User - User Group policies.	1	
4	The solution should support a client based (standalone) instance (without server).Agent policy should work even when the computer is not connected to the Corporate Network	2	
5	The solutions should protect itself against manipulation - attacks	2	
6	The ability to password protect the client to prevent uninstallation or change of settings.	2	
7	The solution should be designed to run specifically for self-service terminal	1	
	B. Central Management		
1	The solutions should be managed from a central point of management on real time basis	1	
2	The solution should support event logging .Ensure real-time monitoring of security relevant hardware- and software events. it is required to collect all the audit trails at a central location and review them on a daily basis.	1	
3	Solution should support multiple Physical/Logical Hard drives	1	
4	The solutions should support remote installation via software distribution tool	1	

5	The solutions should also support local installations	1	
C. Access Management			
1	The solution should allow for the remote user management	1	
2	The solution should support One Time expiring passwords (Dynamic Admin password)	2	
3	The solution should support online and offline password management	2	
4	The solution shall be managed from a central point of management and should work with any standard ATM agent monitoring solution.	1	
5	The Solution should support various map and dashboard views with filtering capabilities for instant access to security status of terminals/devices. Like OS hardening status, Dynamic admin password status, solution installation status etc.	2	
6	The solution should support - Deploy and update Security Policies and configurations as given by the OEM/MSP and other agencies from time to time.	1	
7	The solution should provide SMS and E-mail alerts for significant / critical events/changes.	1	
8	The solution shall not have performance impact of the existing ATM and the peripheral devices e.g. Switch, CD, Bunch Note Acceptor, Cash Recyclers.	1	
9	The solution shall allow remote management of user credentials according to strong password and industry requirements or Bank's IT security or audit dept.	1	

10	The solution shall allow an administrator to define different roles for various users & groups and assign each of them specific user rights.	1	
11	The solution should provide additional hardening capability to the operating system, irrespective of the OEM(which is based on ATM industry best practices). Basic Hardening + additional Hardening as per the security advisories received from time to time .	1	
12	The solution should support -Detailed Event and Log information available along with hardware information for a complete picture of a device's actual status.	1	
13	The solution shall be able to disable Auto-run facility of exe file from a network or a USB port.	1	
14	The solution shall be able to set Windows Admin/other User Password Centrally.	1	
15	The solution should support security at ATMs for required time interval or no. of reboots for maintenance work which require the field engineer to have administrator rights. But at no time should an admin password needs to be shared with engineer. The right should be granted based on token system(this should work when the ATM is not connected to the bank's ATM network)	1	
D. Disk Encryption		The solution should support Full hard disk encryption(FHDE)	
1	The solution should enable for an exact status of disk encryption to be retrieved and display centrally on a monitoring system	1	

2	The solution should be capable of changing the configuration of the hard disk encryption and the parameters used to encrypt	1	
3	The solutions should have the capability to decrypt an ATM hard drive outside of the ATM for recovery purpose only using the relevant encryption key.	1	
4	The ATMs should still cater to customers while the hard disk is being encrypted (during installation)	1	
5	The solution shall support Encryption of all data (user files as well as system files) from an ATM's and Cash Recyclers hard disk.	1	
6	The solution shall protect data confidentiality when a system is out of operation.	1	
E. Hardening		The solution should provide additional hardening capability to the operating system, irrespective of the OEM	
1	The solution should be able to dynamically change the hardening policy of the OS on the ATM from time to time	1	
2	The solution should be able to block USB ports on the ATM through centralized Control	1	
3	OS Hardening solutions should support user (role based) access to the terminals based on tokens (no need to distributed user credentials)	2	
4	The solution should have a user Interface to be able to customize and manage the hardening policies	1	
5	The Operating System Hardening should be managed and administered centrally	2	
6	During policy distribution to the ATM's, the hardening policies should be protected against manipulation	1	

7	The hardening solution should also be extended to browsers and other software components running on self-service terminals e.g. personal firewalls, ip-address / port management .	1	
8	The solutions should protect against malware/Viruses being injected on to the machine and any other unauthorised Software installations. Via local means e.g. USB drive, CDROM, network etc.	2	
9	The solution should protect against the manipulation of executables e.g. .exe, .dll, .class etc. and scripts e.g. .js, .bat etc.	2	
10	The solution should protect against the unauthorized updating / changing of configuration – property files	1	
11	The solution should have firewall functionality	1	
12	The solution should be capable of identifying behavior anomalies within the ATM software	2	
13	The solution should issue alert / warning/ prevent once a threat has been identified	1	
14	The solution should block the unauthorized installation of software	1	
F. Intrusion Detection And Protection (anti malware/anti-virus)		The solution should have provision to block USB ports on the ATM	
1	The solution should be protected against being manipulated	2	
2	The solutions should protect against malware/Virus which may be injected locally or remotely on to the machine.	2	
3	The solution should protect against the manipulation of executables e.g. .exe, .dll, .class etc. and scripts e.g. .js, bat, .bat etc.	2	

4	The solution should protect against the unauthorized updating / changing of configuration – property files	2	
5	The solution should issue alert / warning once a threat has been identified	1	
6	The solution should block the unauthorized installed software	1	
7	The solution should have capability to allocate only required ATM resources to the White listed application. And during the running of the Whitelisted application should monitor if only those resources are being accessed. In case of any deviation, alert should be raised and resources should be blocked. Further, any outdated malware definitions on a terminal should be highlighted in a centralized dashboard.	2	
G. Other Requirements		Only permitted applications to be run in the Machines using Sandboxing concept **or equivalent,** thus effectively nullifying the need of any anti-virus solution.	
1.	To whitelist only the required applications to be Run in the ATMs.	1	
2.	Access to external devices should be centrally controlled	1	
3.	All files to be protected from damages	1	
4.	Doesn’t allow any registry level changes	2	
5.	Detect and Block Unused Services and Applications	1	
6.	Disabling Auto play Options which allows software to run from removable media	1	
7.	NPCI/RBI and Industry regulation and audit compliance to be followed from time to time.	4	
8.	Investigate and report suspicious activities like deviating or non-consistent transaction or event patterns which are caused by unauthorized system usage.	1	

9.	Terminal Security Delivers end-to-end protection from all side network and local attacks	1	
10.	Protection/detection policies to monitor files, settings, events and logs, and report anomalous behaviour through Centralized Dashboard.	1	
11.	Mechanism to validate and allow ATM Engineers to perform Maintenance Activities.	1	
12.	All the updates/ releases in the solution during the contract period to be provided to the bank without any additional cost.	1	
13.	24 x 7 support to be made available from the Technical Assistance Center (TAC)	1	
14.	Auto Run facility should be disabled.	1	
15.	Access should be time based admin access and dynamic password.	1	
16.	Presentation on product	5	
17.	Any other USP & enhanced security of the product	5	
	Total	100	