

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
1	NPCI/EOI/2024-25/IT/06	11	Chapter 2- 2.3	Preparation of System Requirement Specification Document:	What type of deployment we are expecting to have, SaaS-On-prem. If it is on-prem is it going to be on bare metal or one of the cloud service provider.		This is for bidder to respond based on their solution
2	NPCI/EOI/2024-25/IT/06	19	5.2 Return of EMD	EMDs (in the form of BGs) furnished by all unsuccessful Bidders will be returned on shortlisting of successful Bidders at the end of EOI process. Shortlisted successful Bidders will be eligible for subsequent RFP/RFQ process. EMDs of these shortlisted bidders will be carried forward to the RFP/ RFQ process. NPCI reserves the right to either proceed for RFP/RFQ process or cancel the requirement. In case of cancellation of the requirement, the EMDs of shortlisted bidders will be returned.	1) In the case of the bidder winning the RFP, is there any further security deposit/EMD to be submitted while receiving the Purchase Order? 2) Within how many days, will the EMD BG be returned to the unsuccessful bidder?		1) Currently we have floated EOI not RFP. Shortlisted successful Bidders will be eligible for subsequent RFP/RFQ process. Successful bidder in RFP/RFQ have to submit PBG agst purchase order. 2) We will immediately initiate return of EMD (in the form of BG) to unsuccessful bidder after completion of Eligibility & Technical evaluation process of EOI.
3	NPCI/EOI/2024-25/IT/06	39	ANNEXURE M - 1.3	API Monitoring: Continuously monitor API calls for abnormal behavior or potential security breaches	Do vendor to log all the api calls made over the NPCI app and then we do the profiling (i.e discovery) to all the request to understand the possible breaches?		This is for bidder to respond based on their solution
4	NPCI/EOI/2024-25/IT/06	39	ANNEXURE M - 1	Anomaly Detection: Recognize unusual patterns of behavior that may indicate a security threat.	Is this around the threat detection information data only or any other expectation.		This is to identify anomalous behaviour of user on application to identify rogue user
5	NPCI/EOI/2024-25/IT/06	39	ANNEXURE M - 1.6	User Behavior Analytics: Monitor and analyze user interactions to identify potential insider threats or compromised accounts	Is this some where close to repackageing of the app getting account information compromised		This understanding is correct
6	NPCI/EOI/2024-25/IT/06	39	ANNEXURE M - 1.7	Context aware protection: Leverage data to map user behaviour and trigger additional security measures if anomalies are detected	Leverage data is something being refer to the api/account/ip etc and then additional security measure is something should auto trigger based on past analysis.		This understanding is correct
7	NPCI/EOI/2024-25/IT/06	39	ANNEXURE M - 1.8	Adaptive response: Adjust security measures based on the threat level without disrupting the user.	Are we expecting user to get notified about the reason they are getting blocked for. Is this around the response user gets in the form of toast message post detection.		This is for bidder to respond based on the proposed solution capabilities
8	NPCI/EOI/2024-25/IT/06	40	ANNEXURE M - 4.7	Ability to define and enforce custom security policies.	Expectation here is to have configuration available over gui/console to enable security policies.		This understanding is correct
9	NPCI/EOI/2024-25/IT/06	39	ANNEXURE M - 3.5	Support for custom logging profile creation to include specific data points			Solution should allow NPCI to create customize logging profile to get granular information
10	NPCI/EOI/2024-25/IT/06	40	ANNEXURE M - 4.8	Dynamic adjustment of security policies based on real-time threat intelligence.	Do we need to support protection policy upgrade based on the response we are getting in realtime.		This understanding is correct
11	EOI	39-40	Annexure M		Considering the likely usage of the solution by banking institutions, it is recommended that the RASP solution should be SDK-based, without any dependency on the Bidder or OEM for app version updates.		This is for bidder to respond based on the proposed solution capabilities

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
12	EOI	39	Annexure M		<p>To further enhance the security of the mobile application(s) with which the RASP solution will be integrated, it is recommended to add the following features in the mandatory technical compliance:</p> <p>a) RASP solution to understand Device Kernel behavior and identify root detection at the OS Process level.</p> <p>b) RASP solution to perform runtime validation of Checksum to confirm the integrity of the mobile application</p> <p>c) RASP solution to detect Elevation of Privileges by the attacker</p> <p>d) RASP solution to detect if the mobile app is running on an outdated operating system</p> <p>e) RASP solution to enforce Device Policy as per business needs</p> <p>f) RASP solution to detect if the mobile app is running on an unsecure Wi-Fi network</p> <p>g) RASP solution to detect Proxy & VPN connections</p> <p>h) RASP solution to detect if any blacklisted / harmful application is present on the mobile device.</p> <p>i) RASP solution to prevent APK file Decompileation.</p>		This is for bidder to respond based on the proposed solution capabilities
13	EOI	39	Annexure M		<p>It is also recommended to add the following malware control in the mandatory technical compliance:</p> <p>a) RASP solution to detect App Spoofing Attacks when the App is launched</p> <p>b) Malware protection should be based on behaviour methodology and not on signature methodology.</p> <p>c) RASP solution should work all the time as long as App is alive and active to protect from Malware threats, Not just on the launch of the App.</p> <p>d) RASP solution to identify Admin & Accessibility permission for Sideloaded Apps</p>		This is for bidder to respond based on the proposed solution capabilities
14	EOI	39-40	Annexure M		<p>Given the integration will be with banking and mission-critical mobile applications, it is imperative to include the following in the technical compliance section:</p> <p>Mobile App Security RASP solution must comply with the RBI's DPSC guidelines.</p>		This is for bidder to respond based on the proposed solution capabilities
15	EOI	31-34	Annexure H		<p>Since the OEM will be responsible for providing the solution, it is important to establish eligibility criteria for OEMs as well. Below are some key points to consider:</p> <p>1. OEM must have supplied, integrated, implemented, and supported the proposed solution in this EOI to at least 10 BFSI organizations in India in the last two financial years preceding the date of this RFP.</p> <p>• Out of the 10 BFSI organizations mentioned above, at least 5 should be Banking organizations and the OEM should have implemented the solution for their Mobile Banking Apps.</p> <p>• Out of the 5 Banking projects atleast 2 projects should have a minimum of 10,00,000 users.</p> <p>2. The OEM should have a permanent office in India and must be operating for at least 3 years as of the bid publishing date.</p> <p>3. The OEM should have minimum of 2 Implementation and Support Centre in India.</p> <p>4. The OEM should have at least 40 technically skilled employees in India.</p> <p>5. The OEM should have India Hosted Security Cloud for SaaS offering. The Cloud offering should be proven with at least 5 Banks utilising the India hosted security cloud.</p>		This is for bidder to respond based on the proposed solution capabilities
16	EOI				<p>It is recommended to include the requirement related to the Government of India's guidelines on public procurement, giving preference to 'Make in India' solutions.</p>		No change in EOI clause.

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
17	EOI				Kindly confirm the nature of hosting (On Prem / SaaS). In case of On Prem Hosting, please specify who will provide the necessary hardware and software for hosting the solution.		Hardware will be provided by NPCI in case of on prem deployment, any additional software licenses requirement should be included in the posposed solution BOM
18	EOI	39-40	Annexure M		Considering the likely usage of the solution by banking institutions, it is recommended that the RASP solution should be SDK-based, without any dependency on the Bidder or OEM for app version updates.		This is for bidder to respond based on the proposed solution capabilities
19	EOI	39	Annexure M		To further enhance the security of the mobile application(s) with which the RASP solution will be integrated, it is recommended to add the following features in the mandatory technical compliance: a) RASP solution to understand Device Kernel behavior and identify root detection at the F24+ level		This is for bidder to respond based on the proposed solution capabilities
20	EOI	39	Annexure M		It is also recommended to add the following malware control in the mandatory technical compliance: a) RASP solution to detect App Spoofing Attacks when the App is launched b) Malware protection should be based on behaviour methodology and not on signature methodology. c) RASP solution should work all the time as long as App is alive and active to protect from Malware threats, Not just on the launch of the App. d) RASP solution to identify Admin & Accessibility permission for Sideloaded Apps		This is for bidder to respond based on the proposed solution capabilities
21	EOI	39-40	Annexure M		Given the integration will be with banking and mission-critical mobile applications, it is imperative to include the following in the technical compliance section: Mobile App Security RASP solution must comply with the RBI's DPSC guidelines.		This is for bidder to respond based on the proposed solution capabilities
22	EOI	31-34	Annexure H		Since the OEM will be responsible for providing the solution, it is important to establish eligibility criteria for OEMs as well. Below are some key points to consider: 1. OEM must have supplied, integrated, implemented, and supported the proposed solution in this EOI to at least 10 BFSI organizations in India in the last two financial years preceding the date of this RFP. • Out of the 10 BFSI organizations mentioned above, at least 5 should be Banking organizations and the OEM should have implemented the solution for their Mobile Banking Apps. • Out of the 5 Banking projects atleast 2 projects should have a minimum of 10,00,000 users. 2. The OEM should have a permanent office in India and must be operating for at least 3 years as of the bid publishing date. 3. The OEM should have minimum of 2 Implementation and Support Centre in India. 4. The OEM should have at least 40 technically skilled employees in India. 5. The OEM should have India Hosted Security Cloud for SaaS offering. The Cloud offering should be proven with at least 5 Banks utilising the India hosted security cloud.		This is for bidder to respond based on the proposed solution capabilities
23	EOI				It is recommended to include the requirement related to the Government of India's guidelines on public procurement, giving preference to 'Make in India' solutions.		No change in EOI clause.
24	EOI				Kindly confirm the nature of hosting (On Prem / SaaS). In case of On Prem Hosting, please specify who will provide the necessary hardware and software for hosting the solution.		Hardware will be provided by NPCI in case of on prem deployment, any additional software licenses requirement should be included in the posposed solution BOM


Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
25	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	11	2.4	10. Training to nominated officials and making them capable of doing L1 & L2 support.	Please clarify training should be provided by the OEM or the Bidder.	-	OEM to provide the training
26	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	11	2.2.4	Bidder is liable to provide 24x7x365 days support for procured solution and related components.	Please request you confirm, if the 24x7x365 days support is required till the Post-implementation support for 3 years or even after that period. Else clarify.	-	This will be required for the term of the contract
27	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	12	2.7	3. Successful bidder should provide 90 Days of hand holding support post Go-Live or till solution stabilisation. 5. The successful bidder shall operate the deployed system for four to twelve weeks (after GO - Live) to fix all the implementation issues without any additional cost to NPCI.	Please confirm that the time period 4 to 12 weeks (after Go-live) is included in the 90 days duration of providing hand holding support post Go-Live or till solution stabilisation.	-	90 Days of hand holding support post Go-Live or till solution
28	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	19	5.3.4	Bidder violates any of the provisions of the EOI up to submission of Performance Bank Guarantee.	Kindly mention the PBG amount/% of total contract value whichever is applicable for submission of Performance Bank Guarantee.	-	PBG need to submit by successful bidder against purchase order. Details of PBG will be mentioned in RFP/RFQ document. Pls note that this is only EOI and not a RFP/ RFQ process.
29	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	39-40	Annexure M	Indicative functionalities are mentioned below: We hereby declare that all the above stated indicative functionalities and any other additional functionality that NPCI may require would be made available in the solution...	In light of the solution's probable use by financial institutions, it is advised that RASP be SDK-based and independent of the bidder or OEM in terms of app version updates. Please refer the additional remarks.	Considering the likely usage of the solution by banking institutions, it is recommended that the RASP solution should be SDK-based, without any dependency on the Bidder or OEM for app version updates.	This is for bidder to respond based on the proposed solution capabilities
30	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	39	Annexure M	Indicative functionalities are mentioned below: We hereby declare that all the above stated indicative functionalities and any other additional functionality that NPCI may require would be made available in the solution...	Please refer the additional remarks.	To further enhance the security of the mobile application(s) with which the RASP solution will be integrated, it is recommended to add the following features in the mandatory technical compliance: a) RASP solution to understand Device Kernel behavior and identify root detection at the OS Process level. b) RASP solution to perform runtime validation of Checksum to confirm the integrity of the mobile application c) RASP solution to detect Elevation of Privileges by the attacker d) RASP solution to detect if the mobile app is running on an outdated operating system e) RASP solution to enforce Device Policy as per business needs f) RASP solution to detect if the mobile app is running on an unsecure Wi-Fi network g) RASP solution to detect Proxy & VPN connections h) RASP solution to detect if any blacklisted / harmful application is present on the mobile device. i) RASP solution to prevent APK file Decompileation.	This is for bidder to respond based on the proposed solution capabilities

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
31	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	39	Annexure M	Indicative functionalities are mentioned below: We hereby declare that all the above stated indicative functionalities and any other additional functionality that NPCI may require would be made available in the solution...	Please refer the additional remarks.	It is also recommended to add the following malware control in the mandatory technical compliance: a) RASP solution to detect App Spoofing Attacks when the App is launched b) Malware protection should be based on behaviour methodology and not on signature methodology. c) RASP solution should work all the time as long as App is alive and active to protect from Malware threats, Not just on the launch of the App. d) RASP solution to identify Admin & Accessibility permission for Sideloaded Apps	This is for bidder to respond based on the proposed solution capabilities
32	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	39-40	Annexure M	Indicative functionalities are mentioned below: We hereby declare that all the above stated indicative functionalities and any other additional functionality that NPCI may require would be made available in the solution...	Please refer the additional remarks.	Given the integration will be with banking and mission-critical mobile applications, it is imperative to include the following in the technical compliance section: Mobile App Security RASP solution must comply with the RBI's DPSC guidelines.	This is for bidder to respond based on the proposed solution capabilities
33	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	31-34	Annexure H	Eligibility Criteria Response	Please refer the additional remarks for suggestions.	Since the OEM will be responsible for providing the solution, it is important to establish eligibility criteria for OEMs as well. Below are some key points to consider: 1. OEM must have supplied, integrated, implemented, and supported the proposed solution in this EOI to at least 10 BFSI organizations in India in the last two financial years preceding the date of this RFP. • Out of the 10 BFSI organizations mentioned above, at least 5 should be Banking organizations and the OEM should have implemented the solution for their Mobile Banking Apps. • Out of the 5 Banking projects atleast 2 projects should have a minimum of 10,00,000 users. 2. The OEM should have a permanent office in India and must be operating for at least 3 years as of the bid publishing date. 3. The OEM should have minimum of 2 Implementation and Support Centre in India. 4. The OEM should have at least 40 technically skilled employees in India. 5. The OEM should have India Hosted Security Cloud for SaaS offering. The Cloud offering should be proven with at least 5 Banks utilising the India hosted security cloud.	This is for bidder to respond based on the proposed solution capabilities
34	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	-	-	-	Request you to please add the suggested Make In India clause as per the additional remarks.	It is recommended to include the requirement related to the Government of India's guidelines on public procurement, giving preference to 'Make in India' solutions.	No change in EOI clause.
35	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	-	-	-	Kindly confirm the nature of hosting (On Prem / SaaS). In case of On Prem Hosting, please specify who will provide the necessary hardware and software for hosting the solution.	-	Hardware will be provided by NPCI in case of on prem deployment, any additional software licenses requirement should be included in the proposed solution BOM

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
36	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	3	Importan Note	2. Bank Guarantee of Rs. 5,00,000/- (Rupees Five lakhs only) towards Bid Security in Folder 'A'- Earnest Money Deposit (EMD) in the form of Bank Guarantee ONLY. The Bidder shall strictly not remit any amount on account of EMD.	Please confirm that if the Bidder is an MSME can they be exempted from submitting the EMD.	-	Exemption for EMD is not applicable as NPCI is not a Government organization. All bidders who are participating need to submit EMD amount in the form of Bank Guarantee, before last date of Bid submission (BG should be valid for 6 months with 12 months claim period). Hard copy of BG needs to be submitted.
37	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	10	2.1	The selected bidder is required to supply, and appropriately install, deploy, integrate the Mobile Application Security Solution as defined above for NPCI as per the timelines and SLA levels prescribed in the EOI. The bidder should have a 24x7x365 days support contact center in order to log the calls. Contact center numbers should be provided to the NPCI along with the escalation matrix mentioning the contact person's name, number, and designation in the company.	It's understood that the OEM will be responsible to install and implement the tool in NPCI environment, the bidder will play the role of liaisoner, rest activities of support will be in the bucket of OEM. Please clarify.	-	This is for bidder to have agreement with proposed solution OEM
38	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	10	2.2	The successful bidder shall provide all necessary back-to-back support from OEM(s) for delivery, installation, configuration, testing, operationalisation and support of the respective network components (appliances, softwares etc.).	It's understood that the OEM will be responsible to install and implement the tool in NPCI environment, the bidder will play the role of liaisoner, rest activities of support will be in the bucket of OEM. Please clarify.	-	This is for bidder to have agreement with proposed solution OEM
39	NPCI/EOI/2024-25/IT/06 dated 11th October 2024	11	2.3 Preparation of System Requirement Specification Document:	2.3 Preparation of System Requirement Specification Document:	It's understood that the OEM will be responsible to install and implement the tool in NPCI environment, the bidder will play the role of liaisoner, rest activities of support will be in the bucket of OEM. Please clarify.	-	This is for bidder to have agreement with proposed solution OEM
40	NPCI/EOI/2024-25/IT/06 dated 11th October 2024		2.4 Implementation	2.4 Implementation	Please confirm our understanding, that the OEM will be responsible to install and implement the tool in NPCI environment, the bidder will play the role of liaisoner, rest activities of support will be in the bucket of OEM	-	This is for bidder to have agreement with proposed solution OEM
41	NPCI/EOI/2024-25/IT/06 dated 11th October 2024		2.5. Cyber Security Requirements	2.5. Cyber Security Requirements	Please confirm our understanding, that the OEM will be responsible to install and implement the tool in NPCI environment, the bidder will play the role of liaisoner, rest activities of support will be in the bucket of OEM	-	This is for bidder to have agreement with proposed solution OEM
42	NPCI/EOI/2024-25/IT/06 dated 11th October 2024		2.6. Knowledge Transfer (KT)	2.6. Knowledge Transfer (KT)	Please confirm our understanding, that the OEM will be responsible to install and implement the tool in NPCI environment, the bidder will play the role of liaisoner, rest activities of support will be in the bucket of OEM	-	This is for bidder to have agreement with proposed solution OEM
43	NPCI/EOI/2024-25/IT/06 dated 11th October 2024		2.7. Go-Live	2.7. Go-Live	Please confirm our understanding, that the OEM will be responsible to install and implement the tool in NPCI environment, the bidder will play the role of liaisoner, rest activities of support will be in the bucket of OEM	-	This is for bidder to have agreement with proposed solution OEM
44	(EOI) for Procurement of Mobile Application Security Solution	8	5.3 , 5.4	Return of EMD	What should be the EMD validity and the claim period? If we get eligible in EOI_RFP then when we will get the BG return and when we will be eligible to claim it as we have to again submit PBG		1) EMD in the form of BG should be valid for 6 months with 12 months claim period. 2) We will immediately initiate to return of EMD (in the form of BG) to unsuccessful bidder after completion of Eligibility & Technical evaluation process of EOI.
45	ANNEXURE M - Technical Compliance	39	1.3	API Monitoring: Continuously monitor API calls for abnormal behavior or potential security breaches	This is not related to RASP and API monitoring should be considered as separate solution and should not be part of RASP RFP. Request you to consider removing this point from this RASP Rfp.	If this point is required to be part of this RFP than kindly elaborate on the requirements for API monitoring in detail.	This is for bidder to respond based on the proposed solution capabilities
46	ANNEXURE M - Technical Compliance	39	1.5	Anamoly Detection: Recognize unusual patterns of behavior that may indicate a security threat	Realtime behaviour pattern is not Related to RASP and behaviour monitoring and analytics should be considered as separate solution and should not be part of RASP Rfp. Reuest you to consider removing this point from this RASP Rfp.	If this point is required to be part of this RFP than kindly elaborate on which behaviour patterns are being expected for realtime monitoring.	This is for bidder to respond based on the proposed solution capabilities

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
47	ANNEXURE M - Technical Compliance	39	1.6	User Behavior Analytics: Monitor and analyze user interactions to identify potential insider threats or compromised accounts	Realtime behaviour monitoring is not Related to RASP and behaviour monitoring and analytics should be considered as separate solution and should not be part of RASP Rfp. Reuest you to consider removing this point from this RASP Rfp.		This is for bidder to respond based on the proposed solution capabilities
48	ANNEXURE M - Technical Compliance	39	1.7	Context aware protection: Leverage data to map user behaviour and trigger additional security measures if anomalies are detected	Realtime behaviour monitoring is not Related to RASP and behaviour monitoring and analytics should be considered as separate solution and should not be part of RASP Rfp. Reuest you to consider removing this point from this RASP Rfp.		This is for bidder to respond based on the proposed solution capabilities
49	ANNEXURE M - Technical Compliance	39	1.1	Detect time manipulation check on the device	RASP should be ale to protect attacks irrespective device time is manipulated or not. What is expected in time manipulation detection.		Solution should detect and take action on time manipulation activity
50	ANNEXURE M - Technical Compliance	40	4.4	Support for different integration methods (e.g., SDK, API).	Request to also include No Code, Low Code wrapping/integration method.	No Code, Low Code integration method has many advantages. It helps prevent any human errors while integrating, faster rollout, very low integration efforts etc.	This is for bidder to respond based on the proposed solution capabilities
51	ANNEXURE M - Technical Compliance			Virtual Space Detection		Check if the application is launched as via a virtual space app such as Parallel Space, Dual Space or similar.	This is for bidder to respond based on the proposed solution capabilities
52	ANNEXURE M - Technical Compliance			Tap Jacking		Checks if another application has hijacked the app and recording user's taps/clicks.	This is for bidder to respond based on the proposed solution capabilities
53	ANNEXURE M - Technical Compliance			Screen Shot and Screen recording in iOS		Checks if a screen shot or screen recording is preformed on iOS	This is for bidder to respond based on the proposed solution capabilities
54	ANNEXURE M - Technical Compliance			JS obfuscation		RASP solution should also be able to obfuscate Javascript files used within the application	This is for bidder to respond based on the proposed solution capabilities
55	ANNEXURE M - Technical Compliance			Dynamic Configuration Change		RASP solution should also be able to dynamically update securcity polices without re-publishing the App.	This is for bidder to respond based on the proposed solution capabilities
56	ANNEXURE M - Technical Compliance			No Server dependency		The RASP solution should be capable of self-protecting the application without relying on server-based signatures. Therefore, it must operate independently of a client-server architecture, ensuring effective protection even in offline or hostile environments. This is also important for NPCI from peer to Peer offline payment perspective	This is for bidder to respond based on the proposed solution capabilities
57	ANNEXURE M - Technical Compliance	39		Dynamic Code Analysis: Detect and block malicious code execution at runtime	Request for removal as it isn't available in an MDM solution	Request NPCI to consider Government experience for evaluation	This is for bidder to respond based on the proposed solution capabilities
58	ANNEXURE M - Technical Compliance	39		Memory Protection: Safeguard against buffer overflows, memory corruption, and other memory-based attacks	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
59	ANNEXURE M - Technical Compliance	39		API Monitoring: Continuously monitor API calls for abnormal behavior or potential security breaches	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
60	ANNEXURE M - Technical Compliance	39		Tamper Protection: : Identify and prevent unauthorized modifications to the app's code or configuration	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
61	ANNEXURE M - Technical Compliance	39		Anamoly Detection: Recognize unusual patterns of behavior that may indicate a security threat.	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
62	ANNEXURE M - Technical Compliance	39		User Behavior Analytics: Monitor and analyze user interactions to identify potential insider threats or compromised accounts	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
63	ANNEXURE M - Technical Compliance	39		Context aware protection: Leverage data to map user behaviour and trigger additional security measures if anomalies are detected	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
64	ANNEXURE M - Technical Compliance	39		Adaptive response: Adjust security measures based on the threat level without disrupting the user	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
65	ANNEXURE M - Technical Compliance	39		Detect for mod android deployments, blacklisted application, keyloggers and Sandbox environment	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
66	ANNEXURE M - Technical Compliance	39		Detect time manipulation check on the device	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
67	ANNEXURE M - Technical Compliance	39		Detect application installation source for sideloaded application	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
68	ANNEXURE M - Technical Compliance	39		Integrity Checks: Ensure that the application's code and data have not been altered	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
69	ANNEXURE M - Technical Compliance	39		Anti Debugging: Detect and block attempts to debug the application in real time	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
70	ANNEXURE M - Technical Compliance	39		Jailbreak/Root Detection: Identify and block to applications running on compromised (jailbroken/rooted) devices	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
71	ANNEXURE M - Technical Compliance	39		Code Obfuscation: Protect the app's code and sensitive data from reverse engineering	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
72	ANNEXURE M - Technical Compliance	39		Encryption: Support SSL Pinning and protect against tampering hooking etc and encrypting critical resources	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
73	ANNEXURE M - Technical Compliance	39		Implement and manage custom encryption routines with in app to ensure data protection	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
74	ANNEXURE M - Technical Compliance	39		Selective Security enforcement : Allowing developer to chose security measures on most critical part of application	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
75	ANNEXURE M - Technical Compliance	39		Prevent decompilation of application and make code unreadable through multiple layer of obfuscation	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
76	ANNEXURE M - Technical Compliance	39		Prevent application to load if changes detected in system libraries or presence of modding applications	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
77	ANNEXURE M - Technical Compliance	39		Run time code verifications to ensure app code is not altered or new code segments added	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
78	ANNEXURE M - Technical Compliance	39		Detailed logging capability to record security events and activities for forensic analysis and compliance reporting.	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities

NPCI/EOI/2024-25/IT/06 dated 11th October 2024							
INVITATION FOR EXPRESSION OF INTEREST (EOI) FOR PROCUREMENT OF MOBILE APPLICATION SECURITY SOLUTION							
Responses to Pre-Bid Queries							
							
Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
79	ANNEXURE M - Technical Compliance	40		Real time alerts to generate immediate notifications for critical security incidents	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
80	ANNEXURE M - Technical Compliance	40		Compliance Reporting : Generate reports that help in meeting regulatory requirements (e.g., GDPR, etc)	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
81	ANNEXURE M - Technical Compliance	40		Audit logs : Maintain a clear audit trail of all security-related activities for compliance audits.	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
82	ANNEXURE M - Technical Compliance	40		Support for custom logging profile creation to include specific data points	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
83	ANNEXURE M - Technical Compliance	40		Minimum Performance Overhead: Ensure the RASP solution doesn't significantly impact app performance	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
84	ANNEXURE M - Technical Compliance	40		Dynamic adjustment of security policies based on real-time threat intelligence.	Request for removal as it isn't available in an MDM solution		This is for bidder to respond based on the proposed solution capabilities
85	EOI schedule	Page 7	Point 6	Last date and time for Bid Submission	We kindly request NPCI to extend the bid submission deadline to 15th November 2024, as we need time to incorporate the changes suggested in the pre-bid response. Additionally, there are dependencies on certain documents from the statutory auditor, and the upcoming Diwali festival week includes several holidays.		No change in terms
86	2.1 General terms of the scope of work:	page 10	2.1 General terms of the scope of work:	Scope includes providing complete solution including software licenses and other required components, supply, implementation, integration, support services and customization of Mobile Application Security Solution.	Does solution to provide the SDK or complete mobile application that will embbed in NPCI (client) applications ? Please clarify		This is for bidder to respond based on the proposed solution capabilities
87	2.1 General terms of the scope of work:	page 10	2.1 General terms of the scope of work:	Scope includes providing complete solution including software licenses and other required components, supply, implementation, integration, support services and customization of Mobile Application Security Solution.	Q, Can you pelase specify the custimization requirement in detail for Mobile Application secuity solution ?		This will depend on proposed solution capabiliti
88	2.1 General terms of the scope of work:	page 10	2.1 General terms of the scope of work:	The bidder should have a 24x7x365 days support contact center in order to log the calls.	Q, What is the volume of existing application (user base) using the application ? Does the scope of contact center is limited to logging the compliant ? Does Client (NPCI) provide the lease line or/ common contact support number ?		This is for Bidder to provide support to NPCI to address product specific issues and not for end customer
89	2.1 General terms of the scope of work:	page 10	2.1 General terms of the scope of work:	The successful bidder shall provide all necessary back-to-back support from OEM(s) for delivery, installation, configuration, testing, operationalisation and support of the respective network components (appliances, softwares etc.).	Does third party software such as database or servers provide by the client (NPCI) ? Kindly confirm		Hardware will be provided by NPCI in case of on prem deployment, any additional software licenses requirement should be included in the posposed solution BOM
90	3.2 Eligibility Criteria for Bidders	page 13	3.2 Eligibility Criteria for Bidders	The bidder should have successfully implemented a minimum of one (1) innovative idea and should provide client reference for the same	We have implemented an innovative offline token solution at two different banks and other security and compliance solutions. Can this be considered for the bid? Additionally, the solution was deployed under our parent company's name, and we are a 100% subsidiary of the parent company. Could you please confirm if the parent company's experience is eligible for consideration in this bid?		1) This Eligibility Criteria is applicable for only for startups. 2) Solution was deploy by parent company will not be consider.

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
91	3.2 Eligibility Criteria for Bidders	Page 14	3.2 Eligibility Criteria for Bidders	2. Turnover & profitability Other than MSME The bidder should have reported minimum annual turnover of Rs.15 crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in each of the last 3 financial years(2020-21, 2021-22 and 2022-23).	We request NPCI to change this clause to - "The bidder should have reported minimum annual turnover of Rs.6 crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in at least 2 out of last 3 financial years (2020-21, 2021-22 and 2022-23)."		No Change in EOI
92	Chapter 6 Evaluation Process	Page 22	1. Technical Scoring Matrix	EOI Presentation Part – B (Bidder Evaluation Matrix) - Customer BFSI reference in India- Minimum 2 (15)	As per our understanding, these experience letters need to be submitted by the OEM or the Principal Bidder. Kindly confirm if this is correct. Additionally, we request the bank to confirm if customer references from outside India are also acceptable.		This is customer reference required from both OEM and bidder. Only Indian references are acceptable
93	Chapter 6 Evaluation Process	Page 22	1. Technical Scoring Matrix	EOI Presentation Part – B (Bidder Evaluation Matrix) - Customer BFSI reference in India- Minimum 2 (15)	Bidder can provide the confirmation to customer reference on the letter head only.		Yes
94	Chapter 6 Evaluation Process	Page 22	1. Technical Scoring Matrix	Size of the deployment in terms of number of Users and Servers (5)	Could NPCI please confirm the minimum deployment size, in terms of the number of users and servers, required to achieve the full score of 5 out of 5?		Deployment similar to NPCI size and capacity will be the requirement.
95	EOI-for-Procurement-of-Mobile-application-security-solution	Page 10	2.1	Solution should protect apps against a wide range of threats and attacks as they occur, protect sensitive data, detect anomalies and perform adequate encryption and obfuscation functions on the application without impacting app performance.	Is there an existing list of threats, attacks, sensitive data, required encryption and application performance indicators to which we could refer to?		This is for bidder to respond based on the proposed solution capabilities
96	EOI-for-Procurement-of-Mobile-application-security-solution	Page 10	2.1	Scope includes providing complete solution including software licenses and other required components, supply, implementation, integration, support services and customization of Mobile Application Security Solution.	We assume here that source code of security mechanisms, and the solution components are not required as apart of the deliverable. A support in the form of software licensing is enough. Are we correct?		This understanding is correct
97	EOI-for-Procurement-of-Mobile-application-security-solution	Page 10	2.1	Scope includes providing complete solution including software licenses and other required components, supply, implementation, integration, support services and customization of Mobile Application Security Solution.	What sort of customization are expected here? Are further customization required as well during the support period?		Any additional feature requirement from existing solution will be taken up seperately with successful bidder
98	EOI-for-Procurement-of-Mobile-application-security-solution	Page 10	2.1	The selected bidder is required to supply, and appropriately install, deploy, integrate the Mobile Application Security Solution as defined above for NPCI as per the timelines and SLA levels prescribed in the EOI. The bidder should have a 24x7x365 days support contact center in order to log the calls. Contact center numbers should be provided to the NPCI along with the escalation matrix mentioning the contact person's name, number, and designation in the company.	Can the SLAs be shared with the bidders already, to help defining the project scope and necessary resources.		This will be shared with successful bidders
99	EOI-for-Procurement-of-Mobile-application-security-solution	Page 11	2.2.6	Bidder to ensure validation of architecture, configuration, policies etc by OEM before go- live	Where the bidder assume the responsibility to validate such materials, can we assume it is NPCI who will create the materials, such as the solution architecture and configuration requirements?		This will be bidders responsibility
100	EOI-for-Procurement-of-Mobile-application-security-solution	Page 12	2.4.14	Meet compliance requirements.	Can we have access to the list of compliance requirements? And if certification are also to be completed as part of delivery?		This will be shared with successful bidders
101	EOI-for-Procurement-of-Mobile-application-security-solution	Page 12	2.5.1	The successful bidder to Provide cyber security in compliance with NPCI security requirements to protect the confidentiality, integrity, and availability of the information systems.	Can NPCI share the security requirements mentioned in this clause?		This will be shared with successful bidders as part of TPRM process

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
102	EOI-for-Procurement-of-Mobile-application-security-solution	Page 12	2.6.1	The successful bidder is expected to define the approach to have knowledge transfer to NPCI resources on the technical aspects of the solution.	What is NPCI team structure and size, for the team to be trained?		This will be shared with successful bidders
103	EOI	39-40	Annexure M		Considering the likely usage of the solution by banking institutions, it is recommended that the RASP solution should be SDK-based, without any dependency on the Bidder or OEM for app version updates.		This is for bidder to respond based on the proposed solution capabilities
104	EOI	39	Annexure M		To further enhance the security of the mobile application(s) with which the RASP solution will be integrated, it is recommended to add the following features in the mandatory technical compliance: a) RASP solution to understand Device Kernel behavior and identify root detection at the OS Process level. b) RASP solution to perform runtime validation of Checksum to confirm the integrity of the mobile application c) RASP solution to detect Elevation of Privileges by the attacker d) RASP solution to detect if the mobile app is running on an outdated operating system e) RASP solution to enforce Device Policy as per business needs f) RASP solution to detect if the mobile app is running on an unsecure Wi-Fi network g) RASP solution to detect Proxy & VPN connections h) RASP solution to detect if any blacklisted / harmful application is present on the mobile device. i) RASP solution to prevent APK file Decompilation.		This is for bidder to respond based on the proposed solution capabilities
105	EOI	39	Annexure M		It is also recommended to add the following malware control in the mandatory technical compliance: a) RASP solution to detect App Spoofing Attacks when the App is launched b) Malware protection should be based on behaviour methodology and not on signature methodology. c) RASP solution should work all the time as long as App is alive and active to protect from Malware threats, Not just on the launch of the App. d) RASP solution to identify Admin & Accessibility permission for Sideloaded Apps		This is for bidder to respond based on the proposed solution capabilities
106	EOI	39-40	Annexure M		Given the integration will be with banking and mission-critical mobile applications, it is imperative to include the following in the technical compliance section: Mobile App Security RASP solution must comply with the RBI's DPSC guidelines.		This is for bidder to respond based on the proposed solution capabilities
107	EOI	31-34	Annexure H		Since the OEM will be responsible for providing the solution, it is important to establish eligibility criteria for OEMs as well. Below are some key points to consider: 1. OEM must have supplied, integrated, implemented, and supported the proposed solution in this EOI to at least 10 BFSI organizations in India in the last two financial years preceding the date of this RFP. • Out of the 10 BFSI organizations mentioned above, at least 5 should be Banking organizations and the OEM should have implemented the solution for their Mobile Banking Apps. • Out of the 5 Banking projects atleast 2 projects should have a minimum of 10,00,000 users. 2. The OEM should have a permanent office in India and must be operating for at least 3 years as of the bid publishing date. 3. The OEM should have minimum of 2 Implementation and Support Centre in India. 4. The OEM should have at least 40 technically skilled employees in India. 5. The OEM should have India Hosted Security Cloud for SaaS offering. The Cloud offering should be proven with at least 5 Banks utilising the India hosted security cloud.		This is for bidder to respond based on the proposed solution capabilities

Sr. no.	Document Reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	NPCI Response
108	EOI				It is recommended to include the requirement related to the Government of India's guidelines on public procurement, giving preference to 'Make in India' solutions.		This is for bidder to respond based on the proposed solution capabilities
109	EOI				Kindly confirm the nature of hosting (On Prem / SaaS). In case of On Prem Hosting, please specify who will provide the necessary hardware and software for hosting the solution.		This is for bidder to respond based on the proposed solution capabilities
110	EOI	22	Part – B (Bidder Evaluation Matrix)	Customer BFSI reference in India- Minimum 2 (15)	We hereby request NPCI to consider Proposed Solution References of the OEM		Bidder for the proposed OEM
111	EOI	22	Part – B (Bidder Evaluation Matrix)	Size of the deployment in terms of number of Users and Servers (5)	We hereby request NPCI to consider Proposed Solution References of the OEM		Bidder for the proposed OEM