Madam/ Dear Sir

Sub: Sealed quotation for conducting UIDAI's AUA / KUA Compliance Audit for Banks Aadhar Authentication Application

Nainital Bank Limited is hosting for UIDAI's AUA / KUA Compliance Audit for Banks Aadhar Authentication Application through CERT-IN empaneled auditors.

PURPOSE: To engage CERT-In empaneled Auditing firm, which has the capability and experience to conduct a comprehensive Application / functional /Information Systems Audit of UIDAI's AUA / KUA Compliance Audit for Banks Aadhar Authentication Application.

Process & Timeframe

The following is an indicative timeframe for the overall selection process. Bank reserves the right to vary this timeframe at its absolute and sole discretion should the need arise. Changes to the timeframe will be relayed to the affected Respondents during the process.

Description	Due Date
Issue quotation Notification	24.03.2021
Last date of receiving written request for clarifications	26.03.2021
Email ID for clarifications	ciad@nainitalbank.co.in
SPOC from Bank	**Manoj Dwivedi, Manager IS Audit,**
SPOC Mobile No	**7055101509**
SPOC for Audit Scope	**Rajendra Kumar, Sr. Manager, 9456780111**
SPOC Email ID	ciad@nainitalbank.co.in
Mode for submission of quotation	Sealed Quotation or password protected
Last date for submission	**06.04.2021**
Address	Central Internal Audit Division THE NAINITAL BANK LIMITED 4th Floor, UPRNN Building C-20 / 1A / 7 Sector 62, Noida Uttar Pradesh – 201309 Ph:-120-2401083
Duration of Audit	Within 10 Days from the date of PO
Submission of Draft report	Within 10 days from the date of PO
Submission of Final Report	Within 10 days from the date of Submission of Draft Report
Compliance Audit	Within 10 days from the intimation date for compliance audit
Physical Location of audit	Mumbai/Pune
Remote Access	Delhi/Noida

Location: Physical Audit will be conducted Mumbai or Pune In cash physical visit is not possible, then remote access will be over VPN/ Bank's network from bank Branch/ office at Delhi/noida location.

Date & Time for sharing Password- 07.04.2020 (Between 1PM to 2 PM) may extend time but note before 1 PM at nlp.delhi@nainitalbank.co.on only

A. ELIGIBILITY CRITERIA

Sr. No	Eligibility Criteria	Support Documents to be submitted
1	The vendor should be Company/Firm/ Organization registered in India	Certificate of Incorporation & Commencement of Business (whichever applicable) should be submitted
2	The vendor should have a valid CERT-In Empanelment.	Cert-in empanelment Document.
3	The SP should have a pool of resources who possess qualifications such as :CISA/ CISSP/ CCNA/ CISM/ GIAC(SANS)	Detail required to share
4	The vendor should have audited UIDAI's AUA /KUA Compliance Audit / Information Audit/Application Audit/ Functional Security audit at least any two Indian Bank Banks (one Schedule Commercial Bank)	Copy of relevant certificate/ purchase order and Client certificate.
5	The vendor should not be banned/blacklisted/ debarred by any Bank/PSU/GOI Department/ Indian Financial Institute	An undertaking letter to be enclosed by vendor
6	Vendor should have at least 3 to 4 year experience in offering Auditing services such as IS audit, Application audit ,Security assessment, defining security policies procedures & baselines, Risk Assessment, security Consulting assignments to clients in India.	Copy of relevant certificate/ purchase order and Client certificate.

B. AUDIT SCOPE: ANNEXURE I

C. COMMERCIAL FORMAT: Annexure II

D. RIGHT TO REJECT: Bank reserves the absolute and unconditional right to reject the response to this inquiry if it is not in accordance with its requirements and no further correspondence will be entertained by the Bank in the matter. The Bank may decide not to accept any quote or may accept a quote that is not a lowest quote. The bank reserves the right to cancel the tender process at any point in time

E. Last Date of Submission of Quotation:

The last date for submission the sealed quotation is of password protected is 06.04.2021 at mentioned.

Annexure I- Audit Scope

The scope of work for audit of UIDAI's AUA / KUA Compliance Audit for Banks Aadhar Authentication Application checklist v2.0.

Annexure II- Commercial

Sr. No	Description	Price (Exclusive Tax)
A	Physical (Mumbai,Pune) Audit of UIDAI's AUA / KUA Compliance Audit for Banks Aadhar Authentication Application(Draft report , Final Report and Compliance audit)	
Total Prices includes Travelling, Lodging and other expenses		
B	Remote access over VPN/ Bank's network from bank Branch/ office at Delhi/noida location. (Draft report , Final Report and Compliance audit)	
Total Prices includes Travelling,Lodging and other expenses		

F. No. K-11022/463/2016-UIDAI (Auth-II)

Government of India

Unique Identification Authority of India (UIDAI)

(AUTHENTICATION DIVISION)

UIDAI Hqrs,
3rd floor, Bangla Sahib Road,
Gole Market, New Delhi – 110 001.

Date: 29.01.2019
30

To,
All ASAs/AUAs/KUAs

Sub: Requesting Entity Compliance Checklist V2.0.

As you all are aware that UIDAI is constantly engaged in upgrading and streamlining its procedures and systems, in accordance with the provisions of Aadhaar Act 2016 and attached regulations, in order to provide hassle-free service par excellence to the resident as well as to ensure security and confidentiality of identity information and authentication records of individuals. Thus, it becomes imperative that all Aadhaar ecosystem partners are in perfect sync so as to create a synergy which will help immensely in realizing the aforementioned objectives.

It has however been pointed out in various audits that the ASAs/AUAs/KUAs are found lacking on many aspects as far as compliance of Aadhaar Act 2016, Regulations and other circulars issued by UIDAI is concerned, the reports of which have been shared with requesting entities from time - to - time.

In view of the above, the Competent Authority has approved implementation of 'Requesting Entity Checklist V 2.0' (copy enclosed). All requesting entities are hereby directed to ensure compliance to this checklist and to make sure that future audits are done in accordance with it in addition to compliance of provisions of Aadhaar Act 2016, its Regulations, AUA/KUA/ASA Agreement v4.0, various guidelines and circulars issued by UIDAI.

Encls: As above

अमित 30/01/19
(Amit Bhargav)
Dy. Director (Auth)

Requesting Entity Compliance Checklist_V2.0

Version History

Version number	Date	Review comments
V1.0		
V2.0		

237

Guidelines for the Auditor/Assessor:

1. All below points need to be checked for the entire ecosystem of requesting entity including all applications, sub-contract agencies (where there are many sub-contractors reasonable sample agencies to be checked), Sub-AUAs (where there are many Sub-AUAs reasonable sample Sub-AUAs to be checked), physical and logical infrastructure of the requesting entity.
2. The auditor/assessor is expected to mention details of the reason for compliance or non-compliance in the remarks section
3. The auditor/assessor is expected to provide reasonable evidences as part of the report to support the compliance status provided in the report
4. The auditor/assessor may add further points in this checklist to include details of the specifications/ requirements defined below. This is specifically for the points where the entire Regulation/ specification / notification / Circular / Policy etc. has been mentioned as a single checkpoint.

S No	Compliance Control	Yes/No	Remarks
1.	**Information to Aadhaar Number Holder**		
a.	The requesting entity should obtain consent of an individual before collecting their identity information for the purposes of authentication. The consent should be obtained in physical or preferably in electronic form.		
b.	The requesting entity should ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication.		
c.	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder of the nature of information that will be shared by the Authority (UIDAI) upon authentication.		
d.	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder of the uses to which the information received during authentication may be put by it.		
e.	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder of the alternatives to submission of identity information		
f.	The requesting entity should also ensure that the information listed in c, d, and e is also communicated in local language.		
g.	The requesting entity should maintain the logs for: a. Record of consent of the Aadhaar number holder for authentication. b. Record of disclosure of information (as mentioned in point (c), (d), (e) and (f) above) to the Aadhaar number holder at the time of authentication. For any given Aadhaar number holder, whose identity information was collected, the requesting entity should be able to demonstrate that consent was taken and disclosure of information was made.		
h.	The consent taken from the resident should in in accordance with the Aadhaar Act, 2016 and its regulations. No umbrella		

S No	Compliance Control	Yes/No	Remarks
	consent should be taken for sharing e-KYC or Aadhaar number of the residents with other entities.		
i.	If Applicable, the requesting entity should comply with the Notification No. 13012/79/2017/Legal-UIDAI (No. 6 of 2017) dated 19th December 2017 regarding "Process for placing and overriding bank accounts on Aadhaar Payment Bridge–National Payments Corporation of India (NPCI) Mapper". The requesting entity should comply with the following: a. Override request pertaining to an Aadhaar holder should be accompanied bythe name of his current bank on the APB mapper and confirmation from the requesting bank that it has obtained the requisite consent of the Aadhaar holder for switching to the requesting bank on the mapper. b. Send request for mapping of a new account or overriding an existing bank account to NPCI only after taking explicit informed consent of their customers. c. Inform each account holder through sms and email within 24 hours that a request has been sent to NPCI to put his bank account on the mapper or, as the case may be, to change his bank account on the NPCI mapper (providing the name of current bank on the mapper and the last four digits of the account number of the new bank alongwith the bank name) and in case he does not want to put his new bank account on the mapper, then the customer should be provided a methodology to reverse this mapping. d. If a customer does not have email or mobile number and communication cannot be sent, then his physical signature on a paper consent form should be obtained prior to sending the request to NPCI mapper. e. The records of consents obtained in (b) and the communications made in Para (a),(b), and(c) and scanned copy of the consent form in (d) shall be retained for 7 years by the banks as per the UIDAI Regulations. f. Make available the aforesaid records at the time of audit as per the provisions of Aadhaar (Authentication) Regulations, 2016.		
j.	The requesting entity should make provisions for sharing the consent related information with visually/audibly challenged divyangjan in an appropriate manner.		
2.	**Security of the Authentication Devices and Applications**		
a.	Requesting entity should capture the biometric information of the Aadhaar number holder using certified and registered biometric devices.		
b.	Requesting entity should necessarily encrypt and secure the biometric data at the time of capture.		
c.	The client applications and software used for authentication should conform to standard APIs (latest) and specifications laid down by the authority. Sub-AUAs should use client applications (SDK) developed/digitally signed by AUA.		
d.	After collecting necessary demographic and / or biometric		

235

S No	Compliance Control	Yes/No	Remarks
	information and/ or OTP from the Aadhaar number holder, the client application should immediately package and encrypt these input parameters into PID block before any transmission, and should send it to server of the requesting entity using secure protocols.		
e.	Requesting entity should ensure that encryption of PID Block takes place at the time of capture on the authentication device.		
f.	In the case of assisted devices and applications where operators need to mandatorily perform application functions, operators should be authenticated using some authentication scheme such as password, Aadhaar authentication, smart card based authentication, etc. Under no circumstances should the assisted devices and applications store the Aadhaar number, biometrics and/or e-KYC of the resident.		
g.	The encrypted PID block should not be stored unless it is for buffered authentication for a short period of time and after transmission, it should be deleted. Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database.		
h.	Requesting entity should whitelist all the applications (Web/ Android/ iOS or any other client applications) in public domain with requesting entity name, application name, logo and URL etc. The requesting entity should comply with all the requirements of UIDAI circular K-11022/667/2017-UIDAI (Auth-II) dated 27 September 2017 (Whitelisting of Aadhaar based applications developed by AUAs, KUAs and Sub-AUAs).		
i.	The requesting entity should comply with all the requirements of UIDAI Circular K-11022/460/2016-UIDAI (Auth-II) dated 28 February 2017. (Instruction for providing Authentication or eKYC Services by AUA KUA to Sub-AUA)		
3.	**Network, systems, key management and Data vault requirements**		
a.	Requesting entity should establish and maintain necessary authentication related operations, including own systems, processes, infrastructure, technology, security, etc., which may be necessary for performing authentication.		
b.	Requesting entity should establish network connectivity with the CIDR, through an ASA duly approved by the Authority, for sending authentication requests.		
c.	Requesting entity should ensure that the network connectivity between authentication devices and the CIDR, used for sending authentication requests is in compliance with the standards and specifications laid down by the Authority for this purpose.		
d.	Perform Source Code review of the modules and applications used for Authentication and e-KYC as well as vulnerability assessment and Configuration assessment of the infrastructure.		
e.	Requesting entity should employ only those devices, equipment, or software, which are duly registered with or		

234

S No	Compliance Control	Yes/No	Remarks
	approved or certified by the Authority or agency specified by the Authority for this purpose as necessary, and are in accordance with the standards and specifications laid down by the Authority for this purpose.		
f.	Requesting entity should comply with all the requirements of UIDAI circular K-11020/204/2017-UIDAI (Auth-I) dated 22 June 2017 (Implementation of HSM by AUA/KUA/ASA) .		
g.	Requesting entity(which is allowed to store Aadhaar number) and other entities are mandatorily required to collect and store Aadhaar number and any connected data on a separate secure database/vault/system termed as "Aadhaar Data Vault". This will be the only place where Aadhaar number and any connected data should be stored. Each Aadhaar number is to be referred by an additional key called as Reference key. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault. The requesting entity should comply with all the requirements of the UIDAI circular K-11020/205/2017-UIDAI (Auth-I) dated 25 July 2017 (Circular for Aadhaar Data Vault).		
4.	**Security Framework Policies for requesting entity**		
a.	For better decoupling and independent evolution of various systems, it is necessary that Aadhaar number/ Virtual ID be never used as a domain specific identifier. In addition, domain specific identifiers need to be revoked and/or re-issued and hence usage of Aadhaar number as the identifier does not work since Aadhaar number is permanent lifetime number. **Example:** Instead of using Aadhaar number as bank customer id or license number or student id, etc., always have a local, domain specific identifier and have the mapping in the backend database.		
b.	A requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:— a. specified parameters of authentication request submitted; b. specified parameters received as authentication response; c. the record of disclosure of information to the Aadhaar number holder at the time of authentication; and d. record of consent of the Aadhaar number holder for authentication, but shall not, in any event, retain the PID information, Aadhaar Number/Virtual ID		
c.	The logs of authentication transactions should be stored for audit purposes for 2 years online and then archived for 5 years.		
d.	Software to prevent malware/virus attacks should be put in place and anti-virus software installed to protect against viruses. Additional networks security controls and end point authentication schemes may be put in place.		
e.	Periodic standard certification and audit process should be established for applications, devices, and overall networks		

S No	Compliance Control	Yes/No	Remarks
	across the ecosystem and also to ensure the compliance to standard security policy and procedure.		
f.	Wherever possible, only the domain specific identifier should be captured at the device end and not the Aadhaar number/ Virtual ID. For e.g. — Wherever possible, requesting entities should only capture their domain specific identifier (bank a/c no, ration card no along with family member id, LPG customer account no, etc.) — On the requesting entity server, when forming the authentication input XML, retrieve the Aadhaar number from requesting entity database using domain specific identifier.		
g.	Requesting entity should ensure the license keys are kept secure and access controlled.		
h.	Requesting entity should establish a Data privacy policy addressing the privacy aspects of Aadhaar as defined under the Aadhaar Act, Regulations and specifications. Such policy shall also be compliant to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Such policy shall be published on the website of requesting entity.		
i.	The requesting entity shall ensure that it has provisions for periodic reviews and assessments of its systems, infrastructure, etc., by a UIDAI empanelled or CERT-In empaneled agency to ensure compliance with Aadhaar Act, Regulations and specifications on an annual basis or as defined by UIDAI.		
j.	Requesting entity should establish an Information Security Policy and Procedures addressing the security aspects of Aadhaar as defined under the Aadhaar Act, Regulations and specifications.		
5.	**Compliance Requirements**		
a.	The requesting entity has to set up an effective grievance handling mechanism and provide the same via multiple channels.		
b.	The requesting entity should be in compliance with the Intellectual Property provisions as defined in the agreement with UIDAI.		
c.	The requesting entity should comply with the Aadhaar Act, 2016.		
d.	The requesting entity should comply with Aadhaar (Authentication) Regulations, 2016.		
e.	The requesting entity should comply with Aadhaar (Data Security) Regulations, 2016.		
f.	The requesting entity should comply with Aadhaar (Sharing of Information) Regulations, 2016.		
g.	The requesting entity should comply with UIDAI Information Security policy in respect to AUA/KUA available in the compendium on UIDAI official website.		
h.	The requesting entity should comply with Aadhaar Do's and Don'ts available in the compendium on UIDAI official website.		

S No	Compliance Control	Yes/No	Remarks
i.	The requesting entity should comply with all the requirements of UIDAI circular K-11020/198/2017-UIDAI (Auth-II) dated 22 May 2017. (Registered Device Certification of Biometric Devices whose STQC certificate is already expired)		
j.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/630/2017-UIDAI (Auth-II) dated 31 May 2017. (Circular for AUA/KUA and ASA Agreements V 4.0.)		
k.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/460/2016-UIDAI (Auth-II) dated 6 July 2017 (Appointment of Sub-AUA – Application & Undertaking)		
l.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/631/2017-UIDAI (Auth-II) dated 27 November 2017 (Sharing of e-KYC data with their Sub-AUAs).		
m.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/631/2017-UIDAI (Auth-II) dated 1 December 2017 (Discontinuation of partial match).		
n.	The requesting entity should comply with all the requirements of UIDAI circular K-11020/217/2018-UIDAI (Auth-I) dated 10 January 2018 (Implementation of Virtual ID, UID Token and Limited KYC).		
o.	The requesting entity should comply with all the requirements of UIDAI circular K-11022/219/2017-UIDAI (Auth-II) dated 15 January 2018 (Implementation of Face Authentication).		
p.	The requesting entity should comply with all the requirements of UIDAI Circular No. 04 of 2018, K-11020/217/2018-UIDAI (Auth-I), dated 1st May 2018 (Implementation of Virtual ID, UID Token and Limited KYC).		
q.	The requesting entity should comply with all the requirements of UIDAI Circular No. 05 of 2018, K-11020/217/2018-UIDAI (Auth-I), dated 16th May 2018 (Classification of Global AUAs and Local AUAs).		
r.	The requesting entity should comply with all the requirements of UIDAI Circular No. 06 of 2018, K-11020/217/2018-UIDAI (Auth-I), dated 04th June 2018 (Implementation of Virtual ID, UID Token and Limited KYC).		
s.	The AUAs should comply with Regulation number 15, Chapter-III, Aadhaar (Authentication) Regulations, 2016		
t.	The KUAs should comply with Regulation number 16, Chapter-III, Aadhaar (Authentication) Regulations, 2016		
u.	The Requesting Entity should comply with all relevant laws, rules and regulations, including, but not limited to, Aadhaar Act, 2016 and its Regulations, the Information Technology Act, 2000 and the Evidence Act, 1872, for the storage of logs.		
v.	The Requesting Entity should comply with Regulation number 22, Chapter-III,Aadhaar (Authentication) Regulations, 2016		

S No	Compliance Control	Yes/No	Remarks
w.	The Requesting Entity should comply with Regulation number 23, Chapter-III, Aadhaar (Authentication) Regulations, 2016		
x.	The Requesting Entity should comply with all the circulars, notices, mandates issued by UIDAI from time to time		

Note: In case of any interpretation issues between this checklist and Aadhaar Act or Regulations, the requesting entity should rely on the Aadhaar Act, its Regulations and other specifications issued by UIDAI.

Declaration by Audit Organization

I hereby declare that the above requirements have been audited and meet the UIDAI standards & Specifications.

Auditor Name:

Auditor Signature:

Date:

Seal/Digital Sign/Company Seal