Government of India
Ministry of Communications & IT
Department of Telecommunications
Access Services Cell
Sanchar Bhawan, 20, Ashoka Road, New Delhi – 110 001

File No: 800-29/2010-VAS **Dated: 08.12.2014**

To

M/s Airtel for Lucknow
M/s Relaince for Bhopal
M/s Idea for Delhi
M/s Vodafone for Kolkata
M/s BSNL for Bangalore

Subject: Proof of Concept (POC) for use of 'Aadhaar' e-KYC service of Unique Identity Authority of India (UIDAI) for issuing mobile connections to subscribers.

It has been decided to carry out a POC for using e-KYC service of UIDAI for issuing mobile connections. In the e-KYC service, customer authorize UIDAI through Aadhaar authentication using biometric to provide his/her demographic data (name of the customer, name of father/ husband, address, date of birth, and gender) along with his/her photograph (digitally signed and encrypted format) to Telecom Service Providers (TSPs). As per UIDAI, digitally signed electronic KYC data provided by UIDAI is machine readable, making it possible for the TSPs to directly store it as the customer record in their database for purposes of mobile service.

2. For carrying out POC, following procedure is to be followed while issuing mobile connections using on line Aadhaar based biometric authentication:

i. The Telecom Service Providers shall maintain the details including complete address and code of its all points of sale along with names and Aadhaar number of corresponding agents.
ii. TSPs shall have capability of populating the details of Point of Sale (POS)/ agent in the Customer Application Form (CAF) format in respect to sl. no. 23, 24 & 25 along with POS name as required in the instructions issued vide letter no. 800-09/2012-VAS dated 09.08.2012, on the basis of demographic details of agent of POS received from UIDAI.
iii. Customer desirous to purchase mobile connection shall visit to an authorized POS of TSPs and may carry their original Aadhaar Card or hardcopy of e-Aadhaar letter downloaded from UIDAI website, which displays Aadhaar Number clearly
iv. On approaching of the customer desirous of seeking a mobile connection, authorized agent of point of sale shall online authorize UIDAI by way of biometric authentication using his/her finger(s) or iris to provide his/her demographic data (name, name of father/ husband, complete address, date of birth/ year of birth & gender, photograph) and UIDAI shall provide the same in a digitally signed and encrypted format along with Aadhaar Number to the TSP.
v. After verification of the agent of POS on basis of his/ her demographic details received by TSP from UIDAI, a CAF as prescribed under instructions dated

09.08.2012 shall get displayed by TSP on the terminal of POS and details of point of sale/agent as required in the prescribed CAF format shall get populated by TSP in read only and un-editable form. In addition, the Aadhaar number of agent of POS shall also be populated in CAF in read only and un-editable form.

vi. Until and unless the agent of POS is authenticated through UIDAI as above, no CAF shall get displayed on the screen of concerned POS.

vii. In the similar manner/ fashion, the customer shall also online authorize UIDAI to provide his/her demographic data (name, name of father/ husband, complete address, date of birth/ year of birth & gender, photograph) and UIDAI shall provide the same in a digitally signed and encrypted format along with Aadhaar Number to the TSP.

viii. The demographic details of customer received from UIDAI shall automatically get populated by the TSP in read only and un-editable format on the already displayed CAF format on POS terminal, as required in the CAF format in instructions dated 09-08-2012.

ix. Rest of the information needed for prescribed CAF should be entered by authorized agent at POS.

x. For every biometric/iris authentication (customer and POS's agent), UIDAI will give a unique response code with date & time stamp. All the response codes along with date & time stamp received during the process should also be automatically captured in the CAF and shall also be stored in database of TSP.

xi. After completion of all the entries in the CAF, a printout of the CAF shall be taken for signature and other formalities by the customer &POS agent as required under instructions dated 09-08-12. A unique serial number shall also be assigned automatically to each CAF by the TSP which will also be stored in database apart from reflecting on each printed CAF.

xii. Only after the completion of above steps, the CAF details so captured on terminal may be submitted online to TSP for updating the database of TSP.

xiii. The signed CAF shall be stored physically by TSP for any future requirements of DoT and LEAs.

xiv. The CAF for next connection shall be opened only after the process for one connection is completed and CAF displayed at the terminal of POS is closed by the agent. The agent should not be able to open the CAF once completed, closed and submitted.

xv. Whenever the biometrics of customer is captured at POS, an acknowledgement should be generated automatically by the TSP having uniquely numbered acknowledgement receipt and provided to the customer as under:

a. In successful cases (wherein connection is finally provided to the customer), acknowledgment receipt shall contain the name of customer, date of birth, father's/husband's name, address of customer, gender, mobile number allotted, unique CAF number, UID number & name of POS's agent, address of POS, date & time stamp of capturing of customer' biometrics, acknowledgment receipt number, authentication status as success and Response Code received from UIDAI.

b. In failure cases (where connection could not be provided due to any reason), acknowledgement receipt shall contain only date & time stamp of capturing biometric of customer, UID number & name of POS's agent, address of POS acknowledgement receipt number and authentication status as fail and response code received from UIDAI.

c. Acknowledgement receipt number shall be updated in the CAF and database in successful cases.
d. The TSP shall preserve the logs of authentication activity containing date & time stamp of capturing biometric of customer, POS details, and authentication status (fail/success) for audit trail.

3. The finger print/iris data of customer/subscriber and POS's agent will nowhere be stored and displayed on the PoS device terminal in any format by TSP or its authorized POS.

4. The demographic data received from UIDAI should be stored directly by the TSP in its database as per the format defined in prevailing guidelines. The digitally signed e-KYC response received from UIDAI must be stored as-is for audit purposes as per existing guidelines for CAF storage and should not be edited/ altered/changed/modified/overridden by the TSP under any circumstances.

5. TSP should ensure that the POS application shall not have capability to access local file system of the device for either read or write with exception to only read access to device drivers and all process data should be accessed from TSP's Server only. TSP should ensure that the POS software application integrates with suitable STQC certified biometric devices (as suggested by UIDAI), safeguards security of process data and is accessible only to authorized users. The application should nowhere store any data including biometric information and should be compliant with Aadhaar e-KYC and Authentication service and Application Program Interface (API) specifications.

6. Only one mobile connection should be provided against one set of authentications of customer & POS agent from UIDAI. For another mobile connection, subject to ceiling regarding bulk connections provided in instructions dated 09.08.2012, the entire process as above shall be repeated.

7. In practice, One POS may cater to multiple TSPs. This aspect should be suitably kept in view.

8. The TSP shall use appropriate encryption regime to ensure security of data-in-transit (from UIDAI server to TSP data base), besides security of data-at-rest (at POS & TSP nodes).

9. For ensuring privacy/ data security requirement, TSP shall use suitable mechanism/ IT infrastructure at POS &TSP nodes which need to be regular vetted by TSP.

10. The application across all TSPs has to be same and hence POC should focus on this aspect also.

11. During POC, the volume of simultaneous session for biometric authentications from UIDAI server will be bare minimum. Hence, UIDAI has to ensure that in live system there is no delay in fetching demographic data based only on biometric authentication. However, there shall be an authentication time out of 30 seconds for every biometric authentication transaction. If no response is received within the timeout period, active transaction may be closed and the data captured in that transaction should be purged permanently.

12. During POC process, logs /access to all transactions done with UIDAI server and respective server /system shall be provided by TSPs. If DoT or LEAs require further visibility

into Central Identity Repository (CIDR) data then necessary cooperation shall be ensured by UIDAI.

13. This proof of concept shall not be applicable for bulk, outstation and foreign customers.

14. These instructions are being issued for the purpose of carrying out proof of concept only. The verification process for issuance of mobile connection shall continue as per instructions dated 09.08.2012. The proof of concept shall have no impact whatsoever on any process including CAF verification, CAF audit or imposition of penalty. For the same set of customers, both the processes (one normal process which is in force at present and second proof of concept as above) shall take place in parallel. The purpose of proof of concept is to only understand the e-KYC process of UIDAI.

15. The proof of concept shall take place for a period of six weeks under the over all supervision of TERM Wing DoT HQ.

Prashant Verma 08/12/2014

(Prashant Verma)
ADET(AS-II)

Copy to:

(i) Secretary, Deptt of Electronics & IT, New Delhi
(ii) DG & Mission Director, UIDAI, New Delhi with a request to depute a representative for validation.
(iii) Secretary, TRAI, New Delhi
(iv) Sr. DDG(TERM), DoT HQ, New Delhi
(v) JS(IS-I), MHA, New Delhi with a request to depute a representative for validation.
(vi) All Directors of AS Cell, DoT HQ.
(vii) COAI/AUSPI.