सूचना प्रौद्योगिकी और संचार विभाग

GOVERNMENT OF RAJASTHAN
Department of Information Technology & Communication

F No: F11(172)/DoIT/Project/13/Vol-3/ UDB-105 Date : 16/02/2021

Order

Subject: Regarding implementation of Aadhaar Data Vault to store Aadhaar numbers by Sub-AUA applications.

Ref:

- **UIDAI Circular no. 11020/205/2017-UIDAI(Auth-1) dated 25.07.2017,**
- **DoIT&C Letter no. F11(172)/DoIT/Project/13/vol-3/00060/2020 dated 06.01.2020**
- **reminder letter F11(172)/DoIT/Project/13/Vol-3/00582 – 00595 dated 27-01-2020**

Aadhaar number is being used as primary ID of the residents by various user organizations like Government departments, Banks, Income Tax Department, Private Sectors etc. To avail the different benefits/services, Aadhaar number holder has to share the Aadhaar number to various entities and entities store the Aadhaar number as reference key to deliver their services/benefits.

In order to enhance the security level for storing the Aadhaar numbers, it has been mandated that all Sub-AUAs (Departments/Organizations registered with DoIT&C to use Aadhaar Authentication services) that are collecting and storing Aadhaar number for specific purposes under the Aadhaar Act 2016, shall start using Reference keys mapped to Aadhaar numbers through tokenization in all systems. Aadhaar number and any information connected to Aadhaar number shall only be stored in Aadhaar Data Vault. Storing of Aadhaar number and any information connected to Aadhaar number in plain text is strictly prohibited by UIDAI.

The course of action to implement the process by all Sub-AUAs is hereby outlined as below:

1. All Sub-AUAs are directed to mandatorily store Aadhaar numbers and any connected Aadhaar data (eg. eKYC XML containing Aadhaar number and data) on a separate secure database/vault/system. This system will be termed as "Aadhaar Data Vault" and will be the only place where the Aadhaar number and only connected Aadhaar data will be stored.
2. Sub-AUAs are allowed to store any relevant demographic data and/or photo of the Aadhaar number holder in other systems (Such as customer database) as long as Aadhaar number is not stored in those systems.
3. Each Aadhaar number is to be referred by an additional key called Reference key. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault.

4. All business use-cases of Sub-AUAs shall use this Reference key instead of Aadhaar number in all systems where such reference key need to be stored/mapped, i.e. all tables/systems requiring storage of Aadhaar numbers for their business transactions should from now onwards maintain only the reference key. Actual Aadhaar number should not be stored in any business databases other than Aadhaar Data Vault.

5. Access to Aadhaar Data Vault shall be made secure and accessed through internal systems only.

6. The Aadhaar number and any connected data maintained on the Aadhaar Data Vault shall always be kept encrypted and access to it strictly controlled only for authorized systems. Keys for encryptions are to be stored in HSM devices only.

7. Aadhaar numbers along with connected data if any (such as eKYC XML containing Aadhaar numbers and demographic data) shall only be stored in a single logical instance of Aadhaar Data Vault with corresponding reference key. Appropriate HA/DR provisions may be made for the vault with same level of security.

8. The Aadhaar Data Vault containing Aadhaar number/data and the referencing system must be kept in a highly restricted network zone that is isolated from any untrusted zone and other internal network zones.

9. Only trusted communications must be permitted in and out of the vault. This should ideally be done via API/Micro-service dedicated to get the mapping and controlling access to the API/Micro-service at application level. Any unauthorized users needing to access this mapping must go via applications allowing them to view/access this data with appropriate user authentication and logging.

10. The Aadhaar Data Vault must implement strong access controls, authentication measures, monitoring and logging of access and raising necessary alerts for unusual and/or unauthorized attempts to access.

11. The Aadhaar Data vault should support mechanisms for secure deletion/updation of Aadhaar number and corresponding data if any as required by the data retention policy of the Sub-AUAs.

12. The chosen reference key generation method is to ensure that recovery of the original Aadhaar number must not be computationally feasible knowing only the reference key or number of reference keys. It is suggested that a UUID (Universally Unique Identifier represented via hex string) scheme be used to create such reference key so that from such reference key, Aadhaar number can either be guessed or reverse engineered.

Further, to support the Sub-AUAs, DoIT&C has created central Aadhaar Data Vault and web services which can be used by Sub-AUAs to implement Aadhaar Data Vault in their premises.

For encryption/decryption of the Aadhaar number Sub-AUAs may use the web service "HSM as a service" and for generation of reference key for stored Aadhaar number Sub-AUAs may use the web service "DSM as a service". Sub-AUAs may refer to the integration document to use these web services for implementing Aadhaar Data Vault.

For any kind of support, details of Technical support team are as follows:-

1. Sh. Ranveer Singh, Dy. Director (Mob. – 9784436635, ranveersingh.doit@rajasthan.gov.in)
2. Sh. Pankaj Jaldeep, Programmer (Mob. – 8058185187, pankajjaldeep.doit@rajasthan.gov.in)
3. Sh. Subhash Pannu, Project Manager (Mob. – 9602663260, pm.uid@rajasthan.gov.in)
4. Sh. Aryan Jain, Developer (Mob. 96366311031)

Therefore, all the Sub-AUAs registered with DoIT&C are requested to ensure implementation of Aadhaar Data Vault and send compliance report about the same within 1 month of issuance of this letter so that same may be apprised to UIDAI. You are requested to treat this on priority.

In case of non-receipt of compliance report, in exercise of the provisions of Regulation 14(n) of the Aadhaar (Authentication) Regulations, 2016 and Regulations 5 and 6 of Aadhaar (Sharing of Information) Regulations, 2016, any non-compliance shall be dealt under section 42 of the Aadhaar Act, 2016 and shall also attract financial disincentives as per the schedule of the Sub-AUA agreement by UIDAI.

Enclosed:

1. HSM and DSM service Integration Document.
2. UIDAI circular dated 25.07.2017

(Virendra Singh)
Commissioner & Special Secretary
DoIT&C, Jaipur

F No: F11(172)/DoIT/Project/13/Vol-3/UDB-105 **Date :** 16/02/2021

Copy to following for information and necessary action:

1. P.S. to Commissioner and Special Secretary, DoIT&C.
2. Director cum Joint Secretary, Directorate of Economic and Statistics, Planning Department, Yojna Bhawan, Jaipur (Rajasthan)
3. Additional Mission Director (NHM) & Joint Secretary, Department of Medical Health and Family Welfare, Swasthya Bhawan, Tilak Marg, C-scheme, Jaipur (Rajasthan) 302005
4. Drug Controller, Drug Control Organization, Directorate of Medical & Health services, Swasthya Bhawan, Tilak Marg, C-Scheme, Jaipur (Rajasthan)-302005

5. Senior Electrical Inspectorate, Electrical Inspectorate Department,F-55, Krishna Marg, Nandpuri, 22 Godam, Jaipur
6. Project Director, Rajasthan Grameen Ajeevika Vikas Parishad (Rajeevika), 3rd Floor, RFC-Block , Udyog Bhawan, Tilak Marg, C-Scheme, Jaipur (Rajasthan)
7. Managing Director, Rajasthan Knowledge Corporation Limited,7A, Jhalana Institutional Area, Behind R.T.O, Jaipur – 302004
8. Deputy General Manager, Rajasthan Skill & Livelihoods Development Corporation, J-8-A, EMI CAMPUS, Jhalana Institutional Area, Jhalana Doongari, Jaipur(302004)
9. Additional Inspector General (Admin.),Registration & Stamps department, Panjiyan Bhawan, Lohagal-Janana Hospital Road (Sikar Road),Ajmer-305001
10. Additional Food Commissioner cum Director (Consumer Affairs), Food and Civil Supplies Department, Food Building, Govt. Secretariat, Jaipur (Rajasthan)
11. Settlement Commissioner cum CEO, Settlement Department, Rajasthan Bhu Abhilekh Adhunikikaran Society, Viman Bhawan, Gopalbari, Jaipur – 302001
12. Additional Director (Vigi. & Admin) and Joint Secretary, Social Justice and Empowerment Department, Ambedkar Bhawan G-3/1, Rajmahal Residency Area, Jaipur, Rajasthan 302005
13. Secretary, Jaipur Development Authority, Ram Kishor Vyas Bhawan, Indra Circle, Jawaharlal Nehru Marg, Jaipur-302004
14. Superintendent of Police, State Crime Records Bureau, Rajasthan Police Academy, Panipech, Nehru Nagar, Jaipur – 302016
15. Director, Directorate of Secondary Education, Samta Nagar, Bikaner, Rajasthan 334001
16. Registrar, Co-operative Societies, Rajasthan Co-operative Department, Nehru Sahkar Bhawan, Bhawani Singh Road, Jaipur
17. Managing Director, Rajasthan state co-operative bank Ltd.,DC-1, LalKothi Shopping Center, Opposite Nehru Balodyan, Tonk Road, Jaipur-15
18. Commissioner, Agriculture Department, Pant Krishi Bhawan, Jaipur, Rajasthan
19. Officer-In-Charge, Emitra Project, DoIT&C HQ, Jaipur
20. Officer-In-Charge, Raj-SSO, DoIT&C HQ, Jaipur
21. Officer-In-Charge, Raj e-Vault, DoIT&C HQ, Jaipur
22. Officer-In-Charge, Recruitment Portal ,DoIT&C HQ, Jaipur
23. Officer-In-Charge, e-PDS Project ,DoIT&C HQ, Jaipur
24. Guard file.

(Ranveer Singh)
ACP (Dy. Director)
UID Project, DoIT&C

सं.के-11020/205/2017- यूआईडीएआई (ऑथ-I)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथंटीकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,
कनॉट सर्कस, नई दिल्ली -110001
दिनांक: 25.07.2017

Circular

Aadhaar Number is being used as primary ID of the residents by various user organizations like Banks, Telecoms, Government departments, Income Tax department, Private Sectors, etc. To avail the different benefits/services, Aadhaar Number Holder has to share the Aadhaar Number to various entities and the entities store the Aadhaar Numbers as reference key to deliver their services/benefits.

In order to enhance the security level for storing the Aadhaar numbers, it has been mandated that all AUAs/KUAs/Sub-AUAs and other entities that are collecting and storing the Aadhaar number for specific purposes under the Aadhaar Act 2016, shall start using Reference Keys mapped to Aadhaar numbers through tokenization in all systems.

The course of action to implement the process by all AUAs/KUAs/Sub-AUAs and other entities is hereby outlined as below:

(a) All entities are directed to mandatorily store Aadhaar Numbers and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and data) on a separate secure database/vault/system. This system will be termed as "Aadhaar Data Vault" and will be the only place where the Aadhaar Number and any connected Aadhaar data will be stored.

(b) Entities are allowed to store any relevant demographic data and/or photo of the Aadhaar Number Holder in other systems (such as customer database) as long as Aadhaar Number is not stored in those systems.

(c) 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.

(d) All business use-cases of entities shall use this Reference Key instead of Aadhaar number in all systems where such reference key need to be stored/mapped, i.e. all tables/systems requiring storage of Aadhaar numbers for their business transactions should from now onwards maintain only the reference key. Actual Aadhaar number should not be stored in any business databases other than Aadhaar Data Vault.

(e) Access to Aadhaar Data Vault shall be made secure and accessed through internal systems only.

25/7/17

(f) The Aadhaar number and any connected data maintained on the Aadhaar Data Vault shall always be kept encrypted and access to it strictly controlled only for authorized systems. Keys for encryption are to be stored in HSM devices only.

(g) Aadhaar numbers along with connected data if any (such as eKYC XML containing Aadhaar numbers and demographic data) shall only be stored in a single logical instance of Aadhaar Data Vault with corresponding reference key. Appropriate HA/DR provisions may be made for the vault with same level of security.

(h) The Aadhaar Data Vault containing Aadhaar number/data and the referencing system must be kept in a highly restricted network zone that is isolated from any untrusted zone and other internal network zones.

(i) Only trusted communications must be permitted in and out of the vault. This should ideally be done via API/Micro-service dedicated to get the mapping and controlling access to the API/Micro-service at application level. Any authorized users needing to access this mapping must go via applications allowing them to view/access this data with appropriate user authentication and logging.

(j) The Aadhaar Data Vault must implement strong access controls, authentication measures, monitoring and logging of access and raising necessary alerts for unusual and/or unauthorized attempts to access.

(k) The Aadhaar Data Vault should support mechanisms for secure deletion/updation of Aadhaar number and corresponding data if any as required by the data retention policy of the entities.

(l) The chosen Reference Key generation method is to ensure that the recovery of the original Aadhaar number must not be computationally feasible knowing only the reference key or number of reference keys. It is suggested that a UUID (Universally Unique Identifier represented via hex string) scheme be used to create such reference key so that from such reference key, Aadhaar number can neither can be guessed nor reverse engineered.

Therefore in exercise of the provisions of Regulation 14(n) of the Aadhaar (Authentication) Regulations, 2016 and Regulations 5 and 6 of Aadhaar (Sharing of Information) Regulations, 2016, any non-compliance shall be dealt under Section 42 of the Aadhaar Act, 2016 and shall also attract financial disincentives as per the schedule of the AUA/KUA agreement.

25/7/17

(Yashwant Kumar
Assistant Director General
दूरभाष : 011-23462606

To

1. All AUAs/KUAs and ASAs.
2. UIDAI Tech Center, Bengaluru