

सं.के-11020/205/2017- यूआईडीएआई (ऑथ-1)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथेंटिकेशन डिवीज़न

जीवन भारती भवन, टॉवर 1, 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.

Y. Jaiswal
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/update 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 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.


(Yashwant Kumar
Assistant Director General
दूरभाष : 011-23462606

To

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