



## VIDs - Introducing a Two Layer Security for Aadhar

### What is the issue?

\n\n

\n

- The Unique Identification Authority of India (UIDAI) has been facing a lot of criticism over privacy violations.
- Hence, to reinforce privacy protection, UIDAI has proposed the Virtual Ids, which would be a two-layer security system.

\n

\n\n

### Why Virtual IDs?

\n\n

\n

- Allegations of access to personal information by random entities, without the consent of individual Aadhaar holders were rampant.
- The widespread fear of misuse of demographic data is also heightened by the fact that India still does not have a data-protection law.
- To address this, UIDAI unveiled the concept of Virtual Ids, which is one of the most significant changes since its inception eight years ago.
- This is a concept of two-layer security system that prevents the possibility of the numbers being stored in many databases.
- Notably, “Virtual Id Numbers” are envisioned to be substituted in all places that require one to give out their unique ID (Aadhaar number).

\n

\n\n

### How does Virtual Ids (VID) work?

\n\n

\n

- The VID will be a 16-digit random number, which an Aadhaar-holder can generate and use in place of his UID (Aadhar Number).
- This will ensure that the Aadhaar number is no longer shared, thus obviating any chance of it being leaked.
- What makes the VID user-friendly is that it is linked to the Aadhaar number and there can only be one VID at any point in time for a particular number.
- Moreover, only the Aadhaar-holder will be able to generate the VID and it will be a temporary number, unlike Aadhaar, which stays the same forever.
- Hence, it is pointless to hold on to someone's VID as it is merely a temporary number like banking "One Time Passwords" (OTPs).

\n

\n\n

### **What are the other supporting Changes brought in?**

\n\n

\n

- UIDAI has also changed the Aadhar based e-KYC norms, which is the norm for service providers for identifying their customer and maintaining uniqueness.
- Just like how UID was replaced by VID on the Aadhar holder's side, UID has been replaced by a UID token on the service provider's side.
- UID token is a 72-character alphanumeric string that is meant only for system use and acts as a unique-identification serial for a particular customer.
- This prevents the service provider from knowing their consumer's Aadhar Number either directly from them or through the verification data base.
- Most Authentication User Agencies (AUAs) are expected to only use the UID token, instead of the Aadhaar number.
- Such AUAs will be called local AUAs, while the few that continue to use the Aadhaar number will be called global AUAs.

\n

- This structure will ensure that even if a local AUAs database is hacked, the Aadhaar number of customers will not be threatened.

\n

\n\n

### What is the way forward?

\n\n

\n

- Both the VID and new e-KYC norms significantly address privacy concerns by protect the Aadhaar number from being exposed in day-to-day transactions.
- But privacy experts and activists say that there is a lot more to be done to ensure foolproof security for critical personal information.
- Notably, Aadhaar seeding with all existing databases should be revoked.
- Also, the new VID system should ensure that it doesn't become too difficult for the poor and illiterate masses will to engage with.

\n

\n\n

\n\n

**Source: Business Standard**

\n



**IAS PARLIAMENT**  
*Information is Empowering*  
A Shankar IAS Academy Initiative