

सं.के-11020/204/2017- यूआईडीएआई (ऑथ-1)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथेंटिकेशन डिवीज़न

जीवन भारती भवन, टॉवर 1, नवां तल,
कनाट सर्कस, नई दिल्ली -110001

दिनांक: 22.06.2017

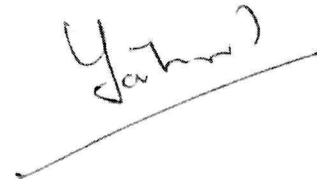
Circular

UIDAI offers two types of Authentication facilities viz. Yes/No authentication and e-KYC authentication. Authentication devices deployed by Authentication User Agency / e-KYC User Agency (AUA/KUA) initiate the authentication request and create encrypted PID block before forwarding it to authentication server of AUA/KUA for processing of domain specific transaction and creation of auth XML as per UIDAI authentication API. Further, upon receiving the auth XML from AUA, Authentication Service Agency (ASA) forwards it to CIDR. To ensure the integrity and non-repudiation, Authentication Server at CIDR, as a mandatory requirement, accepts only digitally signed auth XML through ASA. As mentioned in authentication API document and Regulation 9(2) of Aadhaar (Authentication) Regulations, 2016, *"Authentication request shall be digitally signed by the requesting entity (AUA/KUA) and/or by the Authentication Service Agency, as per the mutual agreement between them"*.


2. In e-KYC service, UIDAI encrypts the e-KYC response data using KUA public key and subsequently forwards the encrypted response to KUA. On receiving the encrypted response, the KUA decrypts the data using their own private key.

3. To further enhance the security of Aadhaar authentication eco-system, under Regulations 14(n) and 19(o) of Aadhaar (Authentication) Regulations, 2016, it is hereby decided to mandatorily use Hardware based Security Module (HSM) for digital signing of Auth XML and decryption of e-KYC data.

4. For digital signing of Auth XML, Authentication request shall be digitally signed by the requesting entity (AUA/KUA) and/or by the ASA using HSM, as per the mutual agreement between them. However, to decrypt the e-KYC response data received from UIDAI, the KUA shall necessarily use its own HSM. The HSM to be used for signing Auth XML as well as for e-KYC decryption should be FIPS 140-2 compliant.



5. Therefore, all AUA/KUA/ASA shall ensure the implementation of HSM in Aadhaar authentication services in aforesaid manner before 31st August, 2017 and submit the compliance report. Any non-compliance in this regard will amount to violation of Aadhaar Act, 2016, its Regulations and AUA / ASA Agreement (including schedule of financial disincentives) making the concerned liable for appropriate penal action as provided therein which shall be in addition to any other legal action as per relevant laws.


22/6/2017

(यशवंत कुमार)

सहायक महानिदेशक

दूरभाष : 011-23462606

To

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