[1][THE SECOND SCHEDULE

[*See* sub-section (*1*) of section 3A]

ELECTRONIC SIGNATURE OR ELECTRONIC AUTHENTICATION TECHNIQUE AND PROCEDURE

Sl. No.	Description	Procedure
(1)	(2)	(3)
[2][1.	e-authentication technique using Aadhaar [3][or other] e-KYC services	Authentication of an electronic record by e-authentication Technique which shall be done by— (*a*) the applicable use of e-authentication, hash, and asymmetric crypto system techniques, leading to issuance of Digital Signature Certificate by Certifying Authority (*b*) a trusted third party service by subscriber's key pair-generation, storing of key pairs [4][* * *] and creation of digital signature provided that the trusted third party shall be offered by the certifying authority. The trusted third party shall send application form and certificate signing request to the Certifying Authority for issuing a Digital Signature Certificate to the subscriber. (*c*) Issuance of Digital Signature Certificate by Certifying Authority shall be based on e-authentication, particulars specified in Form C of Schedule IV of the Information Technology (Certifying Authorities) Rules, 2000, digitally signed verified information from Aadhaar [5][or other] e-KYC services and electronic consent of Digital Signature Certificate applicant. (*d*) The manner and requirements for e-authentication shall be as issued by the Controller from time to time. (*e*) The security procedure for creating the subscriber's key pair [6][and other e-KYC services] shall be in accordance with the e-authentication guidelines issued by the Controller. (*f*) The standards referred to in Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 shall be

[1] Subs. by Act 10 of 2009, s. 49, (w.e.f. 27-10-2009).
[2] Ins. by G.S.R. 61(E), dated 27-1-2015 (w.e.f. 28-1-2015).
[3] Ins. by S.O. 1119(E), dated 1-3-2019.
[4] The words "on hardware security module" omitted by G.S.R. 539(E), dt. 30-6-2015 (w.e.f. 6-7-2015).
[5] Ins. by S.O. 1119(E), dated 1-3-2019.
[6] Ins. by S.O. 1119(E), dated 1-3-2019.

		complied with, in so far as they relate to the certification function of public key of Digital Signature Certificate applicant. [1][(*g*) The manner in which the information is authenticated by means of digital signature shall comply with the manner and standards specified in Rules 3 to 12 of the Digital Signature (End entity) Rules, 2015 in so far as they relate to the creation, storage, and verification of Digital Signature]
[2][2.	e-authentication technique and procedure for creating and accessing subscriber's signature key facilitated by trusted third party	Authentication of an electronic record by e-authentication technique which shall be done by— (*a*) the applicable use of e-authentication, hash and asymmetric crypto system techniques leading to issuance of Digital Signature Certificate by Certifying Authority, provided that Certifying Authority shall ensure the subscriber identity verification, secure storage of the keys by trusted third party and subscriber's sole authentication control to the signature key. (*b*) Identity verification of Digital Signature Certificate applicant shall be in accordance with the Identity Verification Guidelines issued by Controller from time-to-time. (*c*) The requirement to operate as trusted third party shall be specified under e-authentication guidelines issued by the Controller. (*d*) a trusted third party shall (*i*) facilitate Identity verification of Digital Signature Certificate applicant; (*ii*) establish secure storage for subscriber to have sole control for creation and subsequent usage of subscriber's signature key by sole authentication of subscriber; (*iii*) facilitate key pair-generation, secure storage of subscriber's signature key and facilitate signature creation functions; (*vi*) facilitate the submission of DSC application form and certificate signing request to the Certifying Authority for issuing a Digital Signature Certificate to the DSC applicant, and

[1] Subs. by G.S.R. 446(E), for "(g)" dated 27-4-2016 (w.e.f. 27-4-2016)."

[2] Ins. by S.O. 3472(E), dated 29-9-2020.

	(*v*) facilitate revocation of Digital Signature Certificate and destruction of subscriber’s signature key. (*e*) The manner and requirements for authentication and storage of keys shall be as issued by the Controller from time to time under e-authentication guidelines (*g*) The security procedure for creating the subscriber's key pair shall be in accordance with the e-authentication guidelines issued by the Controller. (*h*) The standards referred to in Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 shall be complied with, in so far as they relate to the certification function of public key of Digital Signature Certificate applicant. (*i*) The manner in which information is authenticated by means of digital signature shall comply with the manner and standards specified in Rule 3 to 12 of Digital Signature (End entity) Rules, 2015 in so far as they relate to the creation, storage and verification of Digital Signature.]