Annexure -D

Specification of Aadhar enabled bio metric Device /Machine

1. STQC Certified Device
2. UIDAI Approved authentication device for Aadhar
3. Compact and elegant
4. USB 2.0 Interface (High Speed)/ Standard USB compliant cable .
5. Fast Scanning & Matching speed
6. Choice to set different security levels for different FRR/FAR demand
7. Non - distorted image quality
8. Ergonomic design to guide finger position for effective scanning
9. High resolution >600 dpi(optional)
10. Successfully deployed in very harsh condition in remotest corners and dusty and tribal locations.
11. Suitably protected against dust and water ingress.
12. live Scan capability with ultra red below skin scanning .
13. Small template size, ISO approved
14. Real -life application- no problem in verifying smeared, scarred, strained and smudged fingers
15. Support verification on various server platforms
16. PIV capabilities ported to a verification scanner - absolutely low FTE
17. The reader is totally shock proof for accidental falls from table.
18. Software platforms :- windows 2000/2003/XP/Vista/7(32 bits and 64 bit) Linux with Kernel 2.6 (x86); win CE5.0 (x86 and Arm9), Android.
19. All device provider certificates should be procured from a certification authority
20. Fingerprint devices should register "in.gov.uidai.rdservice.fp.INFO" and “in.gov.uidai.rdservice.fp.CAPTURE”
21. Device provider can provide updated SDK/Driver. if UIDIA change any guide line then Device provider will make sure to provide updated SDK/driver.
22. biometric devices used for authentication shall be certified as required and as per the specifications issued, by the Authority from time to time for this purpose.

Note :- Registered devices MUST ensure the following;

1. There should be no mechanism for any external program to provide stored biometrics and get it signed and encrypted.

2. There should be no mechanism for external program/probe to obtain device private key used for signing the biometrics.

It is important to note that it is in device provider’s interest to ensure the above two items are implemented securely since any compromise on these will result in fraudulent activities signed using the device provider key. As per IT Act it is essential for the key owners (device provider) to protect the signature key and take responsibility for any compromise

* MPSSDM has reserv all the right's to update anu changes required any specification