Solution Architecture

Document History

<Provide information on how the development and distribution of the Solution Architecture is controlled and tracked. Use the table below to provide the version number, date, author, and a brief description of the reason for creating the revised version>

Version No.	Date	Author	Revision Description

Table of Contents

1. Device Provider Information

<Provide information related to Device Model, Sensor Model, Operating System, Modality for which RD service is required>

S. No	Basic Information	Device Vendor Comments
1	Entity applying for RD service certification	
2	Device Model applying for RD service certification	
3	Sensor Models for RD service certification is requested (RD service may support multiple sensors)	
4	Name of entity which applied for original sensor certification	
5	Operating System(s) with version(s) for which RD service is supported (There will be separate installable for each OS)	
6	Modality (Fingerprint / Iris)	
7	Level of compliance claimed (L0/L1)	
8	Discrete / Integrated / POS	

2. Solution Architecture

<System architecture describes the architecture of the proposed registered device solution including all hardware and software components. Providing detailed solution architecture is mandatory during applying for certification (Add diagrams wherever is applicable) >

2.1 Diagram showing the solution architecture and all its components

<Describe solution architecture and explain why it is compliant with the L0/L1 registered device specifications>

2.2 Biometric into the RD service

<Show that is not possible to insert a (stored) biometric into the RD service and get it signed and encrypted>

2.3 Extract the private key

<Show that it is not possible to extract the private key of the registered device>

3. For L1 Compliance

< Applicable only for L1 >

3.1 Provide Hardware Block Diagram with component list

<Please share the hardware block diagram with component list >

3.2 Provide Datasheets for IC's used in the design

<Please share the Datasheets for IC's used in the design>

3.3 Provide internationally relevant certifications for Trusted Execution Environment if available

<If available, please share the internationally relevant certifications for TEE >

3.4 Describe secure boot sequence

<Please share the secure boot sequence in detail>

3.5 Describe secure storage of keys (Valid for L0 compliance devices with hardware keystore)

<Explain secure storage of keys (Valid for L0 compliance devices with hardware keystore >

3.6 Sequence diagram to show biometrics are signed and encrypted within the trusted execution environment.

<Please share the sequence diagram to show biometrics are signed & encrypted within TEE>

3.7 Sequence diagram for key rotation

<Please share the sequence diagram for key rotation >

3.8 Sequence diagram for secure software upgrade

<Please share the sequence diagram for secure software upgrade >

3.9 Sequence diagram for UIDAI public key update

<Please share the sequence diagram for UIDAI public key update >

3.10 Provide methodology and tools to allow certifying agency to verify the L1 compliance for final certification

<Please share the methodology and tools to allow certifying agency to verify the L1 compliance for final certification>

4. For L0 Compliance

4.1 Describe the software keystore implementation

<Approach used for software keystore implementation in detail>

4.2 Standard Keystore Implementation

<Describe the approach used for Android, CSP, Java keystore, P12, etc.>

4.2.1 Describe standard keystore used with links to description

<Please share the standard keystore used with links >

4.2.2 Confirm that capture, sign and encrypt service is written in natively compiled code

<Also confirm that capture, sign and encrypt service is written in natively compiled code with approach>

4.3 Custom Keystore Implementation

<Describe the custom keystore implementation with approach >

4.3.1 Location of Keystore File

<Describe the approach in details>

4.3.2 File permission details

<Describe the approach in details>

4.3.3 Keystore access rights

<Describe the approach in details>

4.3.4 Password generation logic

<Describe the logic used for Password generation >

4.3.5 Password strength

<Describe the complexity of password >

4.3.6 Dynamic ability in password

<Describe the approach in detail>

4.3.7 Confirm that capture, sign and encrypt service is written in natively compiled code

<Also, confirm that capture, sign and encrypt service is written in natively compiled code with approach>

5. Sequence Diagram for "init" Function

<Describe the sequence diagram for the "init" function implementation. The details should contain all the hop points (function names and the assessors and the file names of the binary should be used as the module name) till it reaches the sensor, for all below points>

5.1 Sequence Diagram for device registration

<Share the sequence diagram showing the device registration process>

5.2 Sequence diagram for key rotation

<Share the sequence diagram showing the Key rotation process>

5.3 Sequence diagram for RD service update

<Share the sequence diagram for RD service update process>

5.4 Sequence diagram for UIDAI Public Key update

<Share the sequence diagram for UIDAI Public Key update process>

6. Sequence Diagram for "capture" Function

<Submit code for RD service and capture, sign and encrypt service.

The details should contain all the hop points (function names and the accessors and the file names of the binary should be used as the module name) till it reaches the sensor>

6.1 Sequence diagram for Preview if available

<Share the sequence diagram for UIDAI Public Key update process>

6.2 Sequence diagram for Quality check if available

<If available, please share the sequence diagram for quality check process>

6.3 Sequence diagram for capture, sign and encrypt

<Share the sequence diagram for capture, sign & encrypt process>

6.4 Confirm that capture, sign and encrypt service and key management is implemented as native compiled code

<Also, confirm that capture, sign and encrypt service is written in natively compiled code with approach>

7. Registered Device (RD) Service Discovery

<Explain in detail>

7.1 Discovery of the RD Service

<Share the approach for discover of RD service>

7.2 Multiple RD Service on same host

<Explain the approach of handling the multiple RD service on same host >

7.3 Multiple applications talking to same RD service

<Explain the approach of handling the multiple applications talking to same RD service>

8. Management Server

<Include the complete information on the management server under this section with sufficient diagrams and supporting links. Please include the answers to following specific queries as well.

- *How do you recognize a device which is getting connected with Management Server is indeed your device when a new device is connected*
- *For a Registered Device, mention how the future identification of device is made for key rotation*
- *Explain how management client make sure that they are connecting to the correct Management Sever*
- *What are the ports which are open on the firewall>*

8.1 Management Server Architecture

<Share the Management Server Architecture Diagram with details>

8.2 Deployment and Security Architecture

<Share the deployment and security architecture in detail>

8.3 HSM security in the Management Server

<Explain in detail HSM security in the Management Server. Please

- *Screen shot (Single or multiple) showing all the available partitions and the fips level*
- *Keys should be not extractable inside the HSM. A screen shot to show that keys are enabled as not exportable setting>*

Appendix A – References

<Insert the name, version number, description, and location of any documents referenced in this document. Add rows to the table as necessary>

Table A.1 below summarizes the documents referenced in this document.

<Document Name and Version Number>	*<Document description>*	*<URL to where document is located>*

Table A.1: References

Appendix B – Key Terms

Table B.1 below provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Term	Definition
[Insert Term]	*<Provide definition of term and acronyms used in this document>*

Table B.1 - Appendix B: Key Terms

S.No	Overall	Device Vendor Comments	UIDAI - Approved (Yes / No)	UIDAI Comments (If Any)
1	Entity applying for RD service certification			
2	Sensor Models for RD service certification is requested (RD service may support multiple sensors)			
3	Name of entity which applied for original sensor certification			
4	Operating System(s) with version(s) for which RD service certification is required (There will be separate installable for each OS)			
5	Operating System(s) with version(s) for which RD service is tested			
6	Modality (Fingerprint / Iris)			
7	Level of compliance claimed (L0/L1)			
8	Diagram showing the solution architecture and all its components			
9	Show that is not possible to insert a (stored) biometric into the RD service and get it signed and encrypted			
10	Show that it is not possible to extract the private key of the registered device			
11	Submit source code for RD service and capture, sign and encrypt service			
	For L1 Compliance			
12	Provide Hardware Block Diagram with component list			
13	Provide Datasheets for IC's used in the design			
14	Provide internationally relevant certifications for Trusted Execution Environment if available			
15	Describe secure boot sequence			
16	Describe secure storage of keys (Valid for L0 compliance devices with hardware keystore)			
17	Sequence diagram to show biometrics are signed and encrypted within the trusted execution environment.			
18	Sequence diagram for key rotation			
19	Sequence diagram for secure software upgrade			
20	Sequence diagram for UIDAI public key update			
21	Provide methodology and tools to allow certifying agency to verify the L1 compliance for final certification			
	For L0 Standard Keystore			
22	Describe standard keystore used with links to description			
23	Confirm that capture, sign and encrypt service is written in natively compiled code			
	For L0 Custom Keystore Implementation			
24	Location of Keystore File			
25	File permission details			
26	Keystore access rights			
27	Password generation logic			
28	Password strength			
29	Dynamic ability in password			
	General RD Service Checks			
30	Capture, sign and encrypt service is written in natively compiled code (symbols are stripped)			
31	Mobile OS: RD Service does not start if device is rooted (SafetyNet API or equivalent)			
32	Adequate code obsfuscation in RD service			
33	USB/Bluetooth: RD Service checks the VID, PID of the device before startup			
	Sequence Diagram for "init" Function			
34	Sequence Diagram for device registration			
35	Sequence diagram for key rotation			
36	Sequence diagram for RD service update			
37	Sequence diagram for UIDAI Public Key update			
	Sequence Diagram for "capture" Function			
38	Sequence diagram for Preview if available			
39	Sequence diagram for Quality check if available			
40	Sequence diagram for capture, sign and encrypt			
	RD Service Discovery			
41	Discovery of the RD Service			
42	Multiple RD Service on same host			
43	Multiple applications talking to same RD service			
	Management Server			
44	Management Server Architecture			
45	High Availability for Management Server			
46	Secure connection from RD Service and Management Server			
47	Deployment and Security Architecture			
48	HSM security in the Management Server			
49	Device serial numbers pre-loaded into the Management Server			
50	Time sync between management Server and RD service every 24 hours			
51	HostID/DeviceID pair @ Management Server (Max Limit on Hosts per Device)			