

RD Services Integration Document

CURRENT VERSION DETAIL

Project Name	RD Services Solution for Android
Project Version	2.0.10

Prepared By	Date Prepared
Rajesh Goswami	25-June-2020
Approved By	Date Approved
Udita Singh	25-June-2020

References

RD Services Integration Document

DOCUMENT VERSION HISTORY

DOC Ver.	Description of Changes	Prepared By	Date Prepared	Reviewed By	Date Reviewed	Approved By	Date Approved
1.0	1 st production release	Rishi Dwivedi	26 Jul 2017	Udita Singh	26 Jul 2017	Udita Singh	26 Jul 2017
1.1	Added the new tag in the device info response, added the device compatibility check.	Rishi Dwivedi	28-Aug-2017	Udita Singh	28-Aug-2017	Udita Singh	28-Aug-2017
1.2	Added L0H checked and migration information from L0S to L0H, Backward compatibility issue E 3 as E2	Rishi Dwivedi	8-Sep-2017	Udita Singh	8-Sep-2017	Udita Singh	8-Sep-2017
1.3	Added face component for second factor authentication for xml pid block	Rishi Dwivedi	6-Jul-2018	Udita Singh	6-Jul-2018	Udita Singh	6-Jul-2018
1.4	Added face component for second factor authentication	Rishi Dwivedi	17-Aug-2018	Udita Singh	17-Aug-2018	Udita Singh	17-Aug-2018
1.5	Registration check before Capture	Rishi Dwivedi	20-Aug-2018	Udita Singh	20-Aug-2018	Udita Singh	20-Aug-2018
1.6	Bug fixing and UI change	Rishi Dwivedi	20-Aug-2018	Udita Singh	20-Aug-2018	Udita Singh	20-Aug-2018
1.7	Changes Suggest by UIDAI to enhance user experience.	Rishi Dwivedi	05-Sep-2018	Udita Singh	05-Sep-2018	Udita Singh	05-Sep-2018
1.8	Changes Suggest by UIDAI to enhance user experience and change rd service version for face delta	Rishi Dwivedi	19-Sep-2018	Udita Singh	19-Sep-2018	Udita Singh	19-Sep-2018
1.9	Update Google library along with safety net verify process in Kitkat OS	Rishi Dwivedi	05-Nov-2018	Udita Singh	05-Nov-2018	Udita Singh	05-Nov-2018
2.0	Remove face library and change the rdservice version according to UIDAI	Rishi Dwivedi	26-Dec-2018	Udita Singh	26-Dec-2018	Udita Singh	26-Dec-2018
2.1	Remove pgCount and pTimeout and add the certificate pinning.	Rishi Dwivedi	11-Feb-2019	Udita Singh	11-Feb-2019	Udita Singh	11-Feb-2019
2.2	New PID Encryption certificate for authentication services	Rajesh Goswami	20-Nov-2019	Udita Singh	20-Nov-2019	Udita Singh	20-Nov-2019
2.3	Support for Android 8 & Android 9 added.	Rajesh Goswami	20-Dec-2019	Udita Singh	20-Dec-2019	Udita Singh	20-Dec-2019
2.4	FIR ftype support	Rajesh Goswami	25-Jun-2020	Udita Singh	25-Jun-2020	Udita Singh	25-Jun-2020

Table of Contents

1. Introduction.....	4
2. Scope	4
3. Solution details	4
4. RD Service Installation Steps	6
5. Device registration Steps.....	6
6. Manual Check for RD updates	7
7. RD Service API Calling	7
7.1. Device Info Inputs.....	7
7.2 Device Info Outputs.....	7
7.3 Finger Capture API.....	9
7.4 Finger Capture Outputs:.....	12
8 Error Codes	14
9 Troubleshooting	15
10 Management Server Url Setting.....	16
10.2 To Enable Staging Url configuration Step.....	16
10.3 Preprod Url configuration Step	16
10.4 Production Url configuration Step	16
11 UIDAI Auth Server	16
12 S/W and H/W Requirements for new release.....	16
12.2 Prerequisites for S/W	16
12.3 Prerequisites for H/W.....	17
12.4 Any other tool.....	17
13 Error Code Troubleshooting	17
14 Package Name & References.....	22

1. Introduction

The RD service Solution is made as a compliance as per the UIDAI's latest specifications having version 2.5. This version is used by the Android Applications in which Aadhaar based services are being used by the help of biometric devices.

2. Scope

Scope of this document is limited to following.

Integrate RDService with any other Android application for using Aadhaar based services.

3. Solution details

Name: MorphoSCLRDService_V1.1.5.apk

Version : 1.1.5

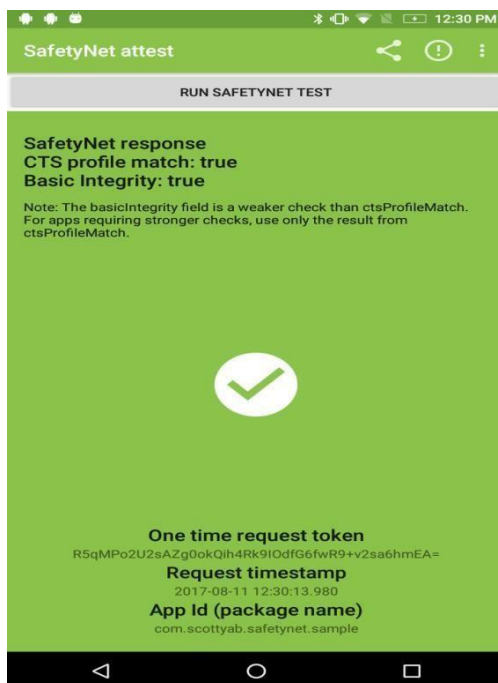
Prerequisites:

Before installing the RD first check the device compatibility using the below app, if the test is OK then only the RD service will run successfully.

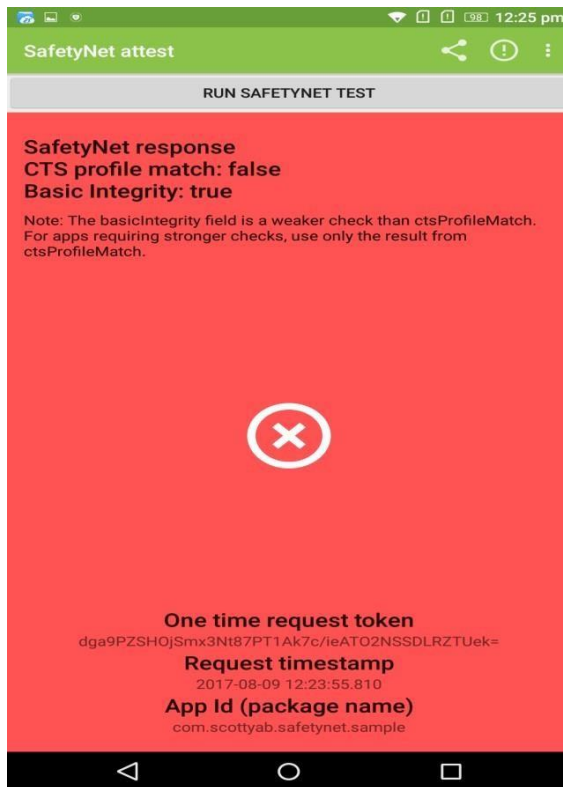
The link for the app is as below you need to down load the app and run the same for test.

Link : <https://play.google.com/store/apps/details?id=com.scottyab.safetynet.sample>

On success below screen will appear:



On Failure below screen will appear:



4. RD Service Installation Steps

- Copy the MorphoSCLRDService_V1.1.3_DT.apk in phone storage
- Go to phone **settings**→**Security**→**Unknown sources**→**check**.
- Click on apk on at defined path and install it.
- Please ensure the devices is not the **Rooted**.

5. Device registration Steps

There is a change in the registration flow from the previous versions, in this release the calling APP need to call the RD Service app for device registration. Now, it is automatic, earlier there was a need. Registration via intent has been deprecated in this version but will continue to work

- Connect the MSO1300_E / MSO1300_E2 / MSO1300_E3 device
- Client app(Any app that intends to use RD Service for Capture/DeviceInfo calls.) need to call registration intent with OTP

```
Intent intent = new Intent("android.intent.action.SCL_RDSERVICE_OTP_RECIEVER");  
intent.putExtra("OTP", currentOtp);  
intent.setPackage("com.scl.rdservice");  
sendBroadcast(intent);
```

2.1 With OTP Window :

Client app must forward OTP either by asking it from user or fetching one from its application server.

2.2 Without OTP Window :

Client app can delegate OTP entry to RD Service. When RD Service receives this fixed OTP i.e. SCL-9999-8888-777, it tried to register the device believing that device is already white listed and in case registration fails from server it simply opens a dialogue asking user to enter OTP. This method is useful when client app provider decides to 1- Deliver OTP via out of band channels e.g SMS, Email etc. Please note that OTP and Activation Code are used synonymously in this document.

OR

- white list the devices upfront. (White listed devices do not require OTP for registration)

6. Manual Check for RD updates

- Launch RD Service
- Click Right top most rotation icon

7. RD Service API Calling

Mechanisms to discover the RD Service and invoke these methods are described in later sections of this document.

7.1. Device Info Inputs

Below code used to call DEVICE INFO mechanism of RD Services for getting DEVICE INFO data.

```
Intent intent = new Intent("in.gov.uidai.rdservice.fp.INFO");
intent.setPackage("com.scl.rdservice");
startActivityForResult(intent, DEVICE_INFO);
```

Description:

Set int DEVICE_INFO = any integer value

7.2 Device Info Outputs

Just override **onActivityResult** method in your Application.

```
@Override
protected void onActivityResult(int requestCode, int resultCode, Intent data) {
super.onActivityResult(requestCode, resultCode, data);
    if (resultCode == RESULT_OK) {
        Bundle b = data.getExtras();
        if (b != null) {
            String deviceInfo = b.getString("DEVICE_INFO", "");
            String rdServiceInfo = b.getString("RD_SERVICE_INFO", "");
            String dnc = b.getString("DNC", "");
            String dnr = b.getString("DNR", "");
            if (!dnc.isEmpty() || !dnr.isEmpty()) {
                showLogInfoDialog("Device Info", dnc + dnr + " " + deviceInfo + rdServiceInfo);
            } else {
                showLogInfoDialog("Device Info", deviceInfo + rdServiceInfo);
            }
        }
    }
}
```

DEVICE_INFO Data Format & Description

```
<DeviceInfo dpId="" rdsId="" rdsVer="" dc="" mi="" mc="" >  
<additional_info> <Param name="serial_number" value=""/>  
</additional_info></DeviceInfo>
```

Description :

/*
dpId – (mandatory) Unique code assigned to registered device provider.
rdsId – (mandatory) Unique ID of the certified registered device
service. rdsVer – (mandatory) Registered devices service version. dc
– (mandatory) Unique Registered device code. mi – (mandatory)
Registered device model ID.
mc – (mandatory) This attribute holds registered device public
key certificate. This is signed with device provider key. serial_number
– (Optional) Serial number of MSO fingerprint device. */

RD_SERVICE_INFO Data Format & Description

```
<RDService status="READY|USED|NOTREADY|..." info="provider info for display  
purposes">  
<Interface id="CAPTURE" path="/rd/capture" />  
<Interface id="DEVICEINFO" path="/rd/info" />  
  
</RDService>
```


7.3 Finger Capture API

Use below intent code to Capture Finger print and getting PID data.

Finger Capture Input:

```
Intent intent = new  
Intent("in.gov.uidai.rdservice.fp.CAPTURE");  
intent.setPackage("com.scl.rdservice"); intent.putExtra("PID_OPTIONS",  
responseXml);  
startActivityForResult(intent,  
AUTHENTICATION_REQUEST);
```

Description:

Set int **AUTHENTICATION_REQUEST** =

any integer value Set **String**

responseXml = "<PidOptions ver="">

<Opts env="P" **fCount="1" fType="0" | ftype= "1"** iCount="" iType=""

pCount="" pType="" pgCount="" pTimeout="" **format="0"**

pidVer="2.0" timeout="" otp="" wadh="" posh=""/>

<Demo></Demo>

<CustOpts>

<!-- no application should hard code these and should be configured on app or AUA servers. These parameters can be used for any custom application authentication or for other configuration parameters. Device providers can differentiate their service in the market by enabling advanced algorithms that applications can take advantage of. -->

<Param name="" value="" />

</CustOpts>

</PidOptions>"

Above XML data content's description:

Where:

PidOptions:

ver: Version of the PidOptions spec. Currently it is "1.0". This is necessary to allow applications to gracefully upgrade even when RD service may be upgraded. **RD Service must support current version and one previous version** to allow apps to upgrade at different points in time.

Opts:

Int *fCount* (optional) number of finger records to be captured (0 to 10)

Int *fType* (optional) ISO format (0 for FMR or 1 for FIR), 0 (FMR) is default Int

iCount (optional) number of iris records to be captured (0 to 2)

Int *pCount* (optional) number of face photo records to be captured (0 to 1)

Int *format* (mandatory) 0 for XML, 1 for Protobuf

String *pidVer* (mandatory) PID version

Int *timeout* capture timeout in seconds

Int *pgCount* (optional) number of face gesture records to be captured (1 to 2)

Int *pTimeout* (optional) face capture timeout in milliseconds (10000 to

40000) String *otp* (optional) OTP value captured from user in case of 2factor

auth String *wadh* (optional) If passed, RD Service should use this within PID block root element "as-is".

String *posh* (optional) if specific positions need to be captured, applications can pass a comma delimited position attributes. See "posh" attribute definition in Authentication Specification for valid values. RD Service (if showing preview) can indicate the finger using this. If passed, this should be passed back within PID block. Default is "UNKNOWN", meaning "any" finger/iris can be captured.

env: (optional) UIDAI Authentication environment for which capture is called.

Valid values are "P" (Production), "PP" (Pre-Production), and "S" (Staging).

If blank or if the attribute is not passed, RD service should default this to "P". This is provided to allow same RD service to use different UIDAI public key based on the environment.

Demo: Element allows demographic data to be passed to form PID block as per authentication specification.

https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf

CustOpts: Allows vendor specific options to be passed. Param element may repeat.

Note : `<Param name="" value="" />` (Applicable only when MSO 1300 Device firmware upgraded. Then set name = "KEY" and value = "hex encode key which you got at device's firmware upgrade time".

7.4 Finger Capture Outputs:

Just override onActivityResult method in your Application.

```
@Override
protected void onActivityResult(int requestCode, int resultCode, Intent data) {
    super.onActivityResult(requestCode, resultCode, data);
    if (requestCode == AUTHENTICATION_REQUEST) {
        if (resultCode == RESULT_OK) {
            Bundle b = data.getExtras();
            if (b != null) {
                String pidData = b.getString("PID_DATA"); // in this variable you will get Pid data
                String dnc = b.getString("DNC", ""); // you will get value in this variable when your finger
                // print device not connected
                String dnr = b.getString("DNR", ""); // you will get value in this variable when
                // your finger print device not registered.
            }
        }
    }
}
```

PID Data format:

```
<PidData>
  <Resp errCode="" errInfo="" fCount="" fType="" iCount="" iType="" pCount="" pType=""
  pgCount="" pTimeout="" nmPoints="" qScore="" />
  <DeviceInfo />
  <Skey ci="">encrypted and encoded session key</Skey>
  <Hmac>SHA-256 Hash of Pid block, encrypted and then encoded</Hmac>
  <Data type="X|P"> base-64 encoded encrypted pid block </pid> </PidData>
```

Where:

PID_DATA:

Int **errCode** (mandatory) 0 if no error, else standard error codes

String **errInfo** (optional) additional info message in case of error/warning

Int **fCount** (mandatory for FP) number of finger records actually captured

Int **fType** (mandatory for FP) actual format type – 0 (FMR) or 1 (FIR)

Int **iCount** (mandatory for Iris) number of iris records actually captured

Int **iType** (mandatory for Iris) actual Iris format (0 for IIR)

Int **pCount** (mandatory for Photo) number of face photo records actually captured. Face is supported with Finger or OTP.

Int **pType** (mandatory for Photo) face format. Face is supported with Finger or OTP.

Int **pgCount** (optional) number of face gesture records actually captured.

Int **pTimeout** (optional) face capture timeout.

Int **nmPoints** (mandatory for FMR capture) Number of minutiae points when FMR is captured. Applications may use this for accepting or retrying the capture. If multiple fingers are captured, send comma delimited numbers.

Int **qScore** (optional) If quality check is done, send a normalized score that is between 0 and 100. Device providers may allow configuration within RD service to use specific quality check algorithms to be enabled. Either it can be configured within RD service or applications can pass those under PidOptions² CustOpts Param³.

Skey:

String **skey** (mandatory) encrypted session key as per auth spec

String **ci** (mandatory) UIDAI public key identifier as per auth spec

Hmac:

String **hmac** (mandatory) hmac value as per auth spec.

RD Services Integration Document

```
<DeviceInfo dpId="" rdsId="" rdsVer="" dc="" mi="" mc="" />
```

dpId – (mandatory) Unique code assigned to registered device provider.

rdsId – (mandatory) Unique ID of the certified registered device service.

rdsVer – (mandatory) Registered devices service version.

dc – (mandatory) Unique Registered device code.

mi – (mandatory) Registered device model ID.

mc – (mandatory) This attribute holds registered device public key certificate. This is signed with device provider key.

8 Error Codes

There are defined error codes defined by UIDAI that RD Services respond whether it has been success or failed because of some reasons.

Error Codes for RD Service

100 "Invalid PidOptions input. XML should strictly adhere to spec."

110 "Invalid value for fType"

120 "Invalid value for fCount"

130 "Invalid value for iType"

140 "Invalid value for iCount" 150

"Invalid value for pidVer"

160 "Invalid value for timeout"

170 "Invalid value for posh"

180 "Face matching is not supported"

190 "Invalid value for format"

200 "Invalid Demo structure"

210 "Protobuf format not supported"

700 "Capture timed out"

710 "Being used by another application"

720 "Device not ready"

730 "Capture Failed"

740 "Device needs to be re-initialized"

750 "RD Service does not support fingerprints"
760 "RD Service does not support Iris"
770 "Invalid URL"
999 "Internal error"
240 "UDIAI certificate from management server is invalid"

Error Codes for Register API

100 "Invalid XML format"
110 "Invalid XML Version"
120 "Invalid timestamp"
130 "Timestamp should not be older than <10 minutes>"
140 "Invalid DpId"
150 "Invalid mi"
160 "Digital Signature Validation Failed"
170 "Device Already Registered"
999 "Unknown Error"

9 Troubleshooting

NA

10 Management Server Url Setting

10.2 To Enable Staging Url configuration Step

- Launch RD Service
- Tap on Application logo which denotes value "1"
- Tap on Finger logo which denotes value "0"
- And match following patterns "0"+"0"+"1"+"0"+"1"+"0"+"0"+"1"+"1"+"0"+"1"

10.3 Preprod Url configuration Step

- Launch RD Service
- Tap on Application logo which denotes value "1"
- Tap on Finger logo which denotes value "0"
- And match following patterns "1"+"1"+"0"+"1"+"0"+"1"+"1"+"0"+"0"+"1"+"0"

10.4 Production Url configuration Step

- Launch RD Service
- Tap on Application logo which denotes value "1"
- Tap on Finger logo which denotes value "0"
- And match following patterns "1"+"1"+"1"+"1"+"1"+"1"+"1"+"1"+"1"+"1"+"1"

11 UIDAI Auth Server

This RD Service is tested with the below UIDAI Auth staging server, if there is any change the same will be updated.

Service: <http://developer.uidai.gov.in/auth>

AUA Key - MEaMX8fkRa6PqsqK6wGMrEXcXFI_oXHA-YuknI2uf0gKgZ80HaZgG3A

ASA Key - MG41Klrkk5moCkcO8w-2fc01-P7I5S-6X2-X7luVcDgZyOa2LXs3ELI

12 S/W and H/W Requirements for new release

12.2 Prerequisites for S/W

Android 4.4.4 and above versions

12.3 Prerequisites for H/W

MSO1300_E, MSO1300_E2, MSO1300_E3Sensor, Camera enabled smartphone
OTG enable mobile, Smartphone should have camera for Face auth

12.4 Any other tool

NA

13 Error Code Troubleshooting

S.No.	Error Code	Error Info	Occurrence	Solution
1.	100	Invalid PidOptions input. XML should strictly adhere to spec.	When RD Service calling application sends corrupt pidoption xml or may be incomplete pid option xml.	Before calling capture intent check pidoption xml format properly.
2.	110	Invalid value for fType	When RD Service calling application sends wrong value for finger type according to UIDAI registered device document.	Before calling capture intent check fType attribute value properly. It should be according to UIDAI registered device document.
3.	120	Invalid value for fCount	When RD Service calling application sends wrong value for finger count according to UIDAI registered device	Before calling capture intent check fCount attribute value properly. It should be according to UIDAI registered device document.
4.	130	Invalid value for iType	When RD Service calling application sends wrong value for iris type according to UIDAI registered device document.	Before calling capture intent check iType attribute value properly. It should be according to UIDAI registered device document.
5.	140	Invalid value for iCount	When RD Service calling application sends wrong value for iris count according to UIDAI registered device document.	Before calling capture intent check iCount attribute value properly. It should be according to UIDAI registered device document.
6.	150	Invalid value for pidVer	When RD Service calling application sends wrong value for pidblock version according to UIDAI registered device document.	Before calling capture intent check pidVer attribute value properly. It should be according to UIDAI registered device document.
7.	160	Invalid value for timeout	When RD Service calling application sends wrong value for timeout according to UIDAI registered device document.	Before calling capture intent check timeout attribute value properly. It should be according to UIDAI registered device document.

RD Services Integration Document

8.	170	Invalid value for posh	When RD Service calling application sends wrong value for posh according to UIDAI registered device document.	Before calling capture intent check posh attribute value properly. It should be according to UIDAI registered device document.
9.	180	Face matching is not supported	When RD Service calling application sends value for pCount and pType.	Morpho RD Service not supported face matching. So ignore/remove pCount and pType attributes.
10.	190	Invalid value for format	When RD Service calling application sends wrong value for format according to UIDAI registered device document.	Before calling capture intent check format attribute value properly. It should be according to UIDAI registered device document.
11.	700	Capture timed out.	If Customer not putting finger on sensor within giving timeout.	Make sure customer put their finger on sensor within giving timeout.
12.	710	Being used by another application.	If Fingerprint sensor busy by another application	Make sure fingerprint sensor should be in ready state. So call device info and check rd service status before calling capture. If RD Service status is ready than capture should be perform.
13.	710	Being used by another application.	If Fingerprint sensor busy by another application	Make sure fingerprint sensor should be in ready state. So call device info and check rd service status before calling capture. If RD Service status is ready than capture should be perform.
14.	720	Device not ready.	<p>If Fingerprint device haven't permission.</p> <p>During capture usb connection loose.</p> <p>Backward compatible issue</p>	Make sure fingerprint sensor has permission and USB cable connection should be perfect.
15.	730	Capture Failed	Some unknown issue	Retry process

RD Services Integration Document

16.	740	Device needs to be reinitialized	When RD Service environment changed	Do Registration
17.	760	RD Service does not support Iris	When RD Service calling application sends value for iCount and iType.	Morpho RD Service not supported eye matching. So ignore/remove iCount and iType attributes.
18.	999	Internal error	<ul style="list-style-type: none"> • Problem Occur during PID generation • During Finger Capture • Safety Net Integrity not passed so please refresh RD Service manually. 	<ul style="list-style-type: none"> • Retry Capture • Retry Capture • Launch RD Service and click refresh button at right top corner. • Please ensure that value of env attribute in PID
			<ul style="list-style-type: none"> • RD Service in different Environment • Device date time is not set to automatic. • Internal error 	<ul style="list-style-type: none"> • Option xml is correct(according to RD Service environment). • Phone date & time should be auto sync. • Please ensure that value of env attribute in PID Option xml is correct(according to RD Service environment).
19.	DNR	Device Not Registered	When Fingerprint device not registered	Do Registration
20.	DNC	Device Not Connected	When Fingerprint device not connected to phone	Please attached fingerprint device.

RD Services Integration Document

21.	NA	<ul style="list-style-type: none"> • Device Certificate Error • Device integrity could not be verified. Please check your connectivity. □ Connection Timeout. Please check your connectivity • Internal Error Occur. Please check your connectivity • Server not connected. • Network Error. Please check your connectivity 	When SafetyNet response could not be verified	<ul style="list-style-type: none"> • Retry twice • If issue persist after multiple retry then download Link and verify SafetyNet compliance.
22	<ul style="list-style-type: none"> • 991 • 992 	RD Service's security compromised, No longer service available.	When user try to recompile application and trying to fraud with application signature	Uninstall current application and download with playstore
23	<ul style="list-style-type: none"> • 240 	UDIAI certificate from management server is invalid	If PID encryption certificate at Management server and pinned PID encryption certificate same	Update the RD service to latest version

14 Package Name & References

Package Name: “com.scl.rdservice”

References

1. Registered Devices Technical Specification – Version 2.0 (Revision 1) – February 2017.
http://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_1.pdf
2. Aadhaar Authentication API Specification – Version 2.0 (Revision 1) – February 2017.
http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0_1.pdf