e-KYC Service in Customized Mobile Devices

[1]A.Sree Vyjayanthi, [2] Y. Dinesh Kumar
[1,2]Asst.Professor [1] 1.akellasreevyjayanthi@gmail.com [2] ydinesh@diet.edu.in

[1,2]Department of Computer Science and Engineering

[1,2]Dadi Institute of Engineering and technology, Visakhapatnam.

Abstract

Unique Identification Authority of India (UIDAI) offers e-KYC service that enables KYC (Know your Customer) process to be performed electronically with explicit authorization by Customer. As a part of the e-KYC process, the Customers authorize UIDAI to provide their demographic data along with their photograph to service requestors. Knox is an enterprise mobile security solution. It addresses most of the security issues in Android and one can have the benefits of using a personal device without the need to carry and secure a separate device. Amalgamating the above features helps minimizing the document work while providing security to the data and device.

Key Words : Unique Identification Authority of India (UIDAI); e-KYC (electronic Know Your Customer); authorization; Demographic; Android;

1. Introduction

Know Your Customer (KYC) is a mandatory process that most organizations require their customers to complete. An Aadhaar card can be used as a KYC document, but the manual KYC process takes a long period of time.

e-KYC (electronic Know your Customer) is a service offered by UIDAI (Unique Identification Authority of India) with the objective to generate the KYC of any customer digitally using the information provided for Aadhaar Registration that includes the customer's Photograph, Biometrics (Finger print and IRIS) and Demographic data. Using this information, stored in the UIDAI servers a customer can be authenticated anytime and anywhere which eliminates the necessity of traditional paper work of preparing, collating and authenticating the documents manually which saves time, effort and cost of clients and customers.

The recent evolution of smart phones encouraged Employees of organizations to get their personal phones to work. It is because of the applications available in smart phones that provide access to corporate email which makes employees easy to respond to work. BYOD "Bring Your Own Device" increases the security risks in managing corporate data while accessing confidential data of a company. IT administrators are unable to handle the problem of protecting confidential corporate data from the unprotected personal devices. For example, when corporate data resides on a personal phone all this data will be managed individually. Misusage of corporate devices is also a happening situation where Employees login with their corporate devices and may switch to other applications, and start using corporate device for personal works.

Customized mobile devices restricts the usage of the handsets and improves security levels. The Knox security application provides customizations and creates a new layer on the devices that helps in separating personal and professional data. This new layer appears to provide a new version of the device and restricts the usage of the handset.

2. Literature Survey

To promote the employees work from any location using any suitable mobile device an End User Devices Strategy is introduced by The Cabinet Office of UK. To adopt this strategy the organizations have to meet certain standards, and deploy cost effective commercial devices. The End User Devices security framework provided by

(CESG) Communications Electronics Security Group, also defines certain controls and provide guidance to organizations for configuring the device at its best to meet the requirements, highlighting the areas which meet the security framework requirements.

Android is the most used operating system and is of great interest in the Mobile market for its diverse features. It is provided with a security architecture having several mechanisms to protect information stored in a Device. The data confidentiality is not guaranteed in this architecture. File system encryption is only provided which protects the information in the device when the device is turned off and locked by password.

Samsung Knox is a technology provided by Samsung for mobile devices which easily separates and protects personal and corporate data maintaining a partition between them. The corporate data is protected by a container which can be accessed by the applications of corporate use, and cannot be accessed from applications that are personal. It allows the centralized management at the corporate level, and guarantees a homogenous configuration on the devices of a company. Detailed understanding of the features, functionality and implementation of Knox is a scope of this project.

The further study also revealed that there are other products Android for Work and Blackberry UEM that have similar features to Samsung Knox. The Industry Analyst Gartner Group compared 12 different platforms - Android 4, 5, and 6; BlackBerry 10; BlackBerry android; iOS 8 and 9; Samsung Knox; Windows Phone 8.1 and 10 (Lumia and Desktop) and rated Knox as the best for **corporate managed security** to mobile devices.

3. e-KYC Service in Customized Mobile Devices

Whenever a person wants to enter into a relationship with an entity (any organization) to initiate any transactions, he/she has to submit multiple documents such as address proof, ID proof and others, to prove his/her authentication. These documents have to be verified by a third person (gazetted officer). Only after the successful verification of the third party personnel the documents gain their validity and can be submitted to any organization. The Disadvantages include-

- This is a time taking process as it involves preparing, collating and authenticating the documents manually.
- Possibilities of forged documents.
- No authorization of the customers.

To eliminate carrying hardcopies of multiple documents all time, Customers who have a valid Aadhaar number can access their data from UIDAI Central Data Repository any time by providing their consent. Operating model briefs the actions involved in the Aadhaar Authentication / e-KYC . The Key Actors and the data flow of Aadhaar authentication is specified in the figure below.

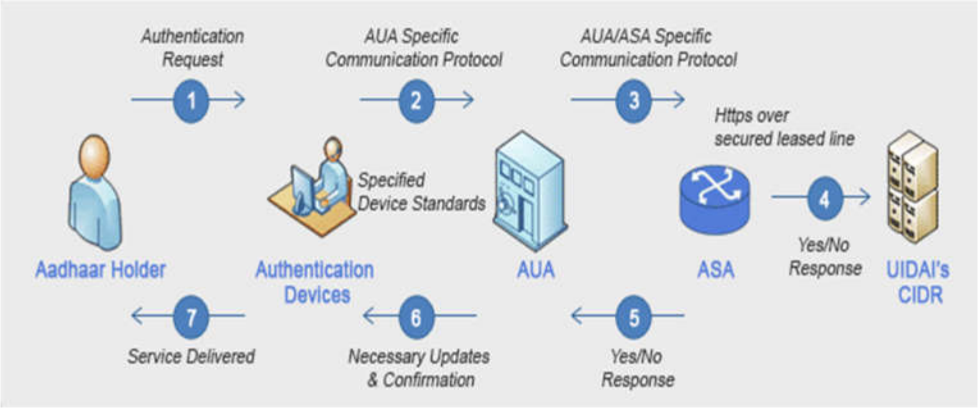
Authentication Request
1
AUA Specific Communication Protocol
2
AUA/ASA Specific Communication Protocol
3
Https over secured leased line
4
Specified Device Standards
Aadhaar Holder
Authentication Devices
AUA
ASA
Yes/No Response
UIDAI's CIDR
7
Service Delivered
6
Necessary Updates & Confirmation
5
Yes/No Response

Figure 1 : Operating Model of Authentication /e-KYC

Customer is an individual who have a valid Aadhaar Number and is willing for a transaction.

Authentication Devices are electronic devices that are used to perform Aadhaar Authentication. These devices collect, prepare, and transmit the personal identity data (PID) from customers, and transmit the collected information in forms of authentication packets for authentication and are also responsible for receiving the authentication results. Examples of authentication devices include desktop PCs, laptops, Point-of-Sale (PoS), handheld mobile devices and tablets.

Authentication User Agency (AUA) may be government / public / private legal agency registered in India, that uses Aadhaar Authentication services of UIDAI.

Authentication Service Agency (ASA) is an entity that provides necessary infrastructure for ensuring secure network connectivity and related services for enabling AUA to perform Authentication .

Central Identities Data Repository (CIDR) is the centralized database situated in one or more locations that contains the details of the customers with their corresponding demographic and biometric information.

After collecting the Aadhaar number and biometrics (fingerprint/iris) or OTP from the customer, the client application packages and encrypts these input parameters into PID(Personal Identity Data) block before any transmission, and sends to server of AUA.After validating the Aadhaar number, AUA server passes the authentication request to the CIDR, using the ASA's gateway . As per the mutual Agreement between the ASA and AUA, the authentication request are digitally signed.Based on the mode of authentication request (OTP/biometrics), the CIDR validates the input parameters against the data stored therein and returns a Boolean Yes or No authentication response, or an e-KYC report with demographic data.In all modes of authentication (OTP/biometrics), the Aadhaar number is mandatory and is submitted along with the input parameters such that authentication is always reduced to a 1:1 match.

Hence Instant KYC can be delivered anywhere and anytime.

To start using the application, any organization requires a valid license key and certificates issued by UIDAI. Using these certificates and license keys the application can perform its functions. Customizations are also equally important as they eliminate the issues relating to the device and application security.

The Authentication Service Agency (ASA) provides Aadhaar services in the form of an application to the user agencies(AUA's). The Application development will be done in ASA and are deployed to the devices in a secured way by using an interface. The AUA will be provided with the credentials to access the interface and deploy the application into their devices .

1. Knox Workspace : Knox Workspace ensures government grade security to the applications and the device. For deploying the application in the Knox Container certain permissions are to be provided at the admin level. After granting the required permissions to the device and application, the application in the particular device will be ready for performing the required transactions.

If at all the Application needs to be modified further the workspace mode of deployment supports for change. Here the responsibility of the ASA is to develop the application and upload the application in the interface. Using the Login credentials provided to access the interface AUA deploys the application into their devices and starts using. It is clear that both the AUA and ASA are involved for deploying the application. The same procedure is to be followed whenever changes to application are required.

2. Knox Customizations : Knox Customization offers certain tools and services for the personal devices to work as service oriented devices and meet their unique needs. This particular solution is suited for one time deployment of the application in a device. Once the device is loaded with the application , no changes are allowed for the application. Wiping the entire device also does not work once the application is deployed and starts using. Here the same procedure is followed where both the AUA and ASA are involved for deployment.

3. Knox Premium : Knox Premium provides cloud based mobility management with an on device container that promotes remote management and helps in improving the existing infrastructure. This Solution is totally managed by the ASA and there is no necessity for the AUA to interact with. The entire Application Deployment into a single device or a bulk of devices is centrally done by the admin from ASA. For this process to be done the IMEI Number of the device to which the application is to be deployed should be known to the administrator of ASA.

4. Conclusion

This e-KYC application is more beneficial to use as it is cost effective, easy to implement and meets the stringent security requirements of various Governments.

Extending the Security framework of Knox to non- Samsung mobile devices and providing a generalized application that meets the similar features of Knox can be the future work for this project.

5. References

1. Samsung Document : no author ," Samsung Knox - UK Government EUD Guidance " August 2016 Online [Available] https://kp-cdn.samsungknox.com/8157966746bd3be1ce8cd951bbd4745f.pdf

2. "The Technology Overview of Samsung Knox" Online [Available] https://ww8w.samsungknox.com/en/knox-technology

3. UIDAI Document : no author ,"Aadhaar e-KYC API 2.0" Online [Available] https://uidai.gov.in/images/aadhaar_ekyc_api_2_0.pdf

4. Alexander Oprisnik, Daniel Hein and Peter Teufl , "Identifying cryptographic functionality in android applications"Security and Cryptography (SECRYPT), 2014 11th International Conference