Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

सत्यमेव जयते

National e-Governance Division

MOBILE AS INSTRUMENT OF DIGITAL IDENTITY & FINANCIAL INCLUSION

MOBILE.ID DEFINED

- "Mobile Identity"(or "mobile ID") –
  - "virtual", integrated identity based on identified physical identity, can be linked to either, few, or all biometrics, including and especially voice,
  - Not only linked to Mobile number but in some cases also brings mobility – means device agnostic/ independent and is easily and safely portable
  - Would also be verifiable anywhere and everywhere within the country, and would thereby be a tool for both authentication and authorization.
- Ideal mobile ID would also lend itself to being rolled out quickly with sufficient safeguards.
- Operationally, Mobile ID would be an additional channel for establishing personal identity

CONCEPT & TECHNOLOGIES

POSSIBLE SOLUTIONS

- Aadhaar-linked Mobile Number
- Mobile-based Public Key Infra (PKI) or Digital Signature Certificate (DSC)
- Mobile + Voice Biometrics

LINKING AADHAAR & MOBILE NUMBER

- Aadhaar and Mobile Number
  - Linking mobile number of an individual with her Aadhaar number, →transporting individual's physical identity into the Mobile world.
- How to link Aadhaar Number with Mobile Number:
  - **At UIDAI**
    - During Enrollment,
    - During existing Online/Manual process of UIDAI to update Mobile number
  - **At Service Provider(SP) – viz Gas agency/ ration card agency**
    - Through SMS by sending (SP unique No.+ Aadhaar No) and then performing Aadhaar Demographic Authentication(Mobile No. +Aadhaar No.)
    - Through Online Channel → By first logging into SP site and providing Aadhaar number and then performing Demographic Authentication and linking Mobile with Aadhaar in database.
  - **At Telecom Operator**
    - OTP/Biometric based e-KYC
    - By sending SMS to Telco and then performing Aadhaar Demographic Authentication
    - By using existing Online utility prepared by UIDAI to seed Aadhaar No. in Sp database - https://rasf.uidai.gov.in/seeding/User/ResidentSplash.aspx

AADHAAR + MOBILE NO. - BENEFITS & APPLICABILITY

- Aadhaar - Close to 70 crore strong resident database, who are uniquely identifiable.
- Linking will enable an eco-system for m-governance in the country.
- Govt. will be able to identify, authenticate, and provide services to residents via the mobile phone with no added cost.
- Applications can use mobile authentication in the following ways:
  - Perform a demographic auth. with Aadhaar number and Mobile Number after receiving the same over SMS/Web;
  - Request for an OTP to be sent to registered mobile and accept that for 2 factor authentication;
  - Biometric based authentication using advanced Mobile phones which have biometrics readers installed on the screen.
  - Even if Aadhaar not seeded in department, services can perform authentication by inserting Aadhaar number at Telco's message gateway before SMS reaches SP.
  - Set up 6-digit PIN at Aadhaar and use it for authentication along with Aadhaar and mobile no.

AADHAAR + MOBILE NO. – CHALLENGES & RECOMMENDATIONS

- Mobile numbers are re-issued to new subscribers after a certain period of expiry.
  - For a solution which envisages linking Aadhaar, which is permanent in nature, to a person's mobile number would require
    - that the person changes his mob. No. in data base as soon as he gets a new number, as mobile number can not be permanently allotted to a person.

    OR

    - One mobile number to be permanently allotted to just one person, and no transfer happens even after deactivation
- Aadhaar enrolment is voluntary and hence delivery of services by authenticating users on the basis of Mobile Number (which are linked to Aadhaar number) cannot be made the only channel for authenticating users over the Mobile networks.
  - Existing mode of authenticating users will continue to be used and Aadhaar based Mobile ID authentication shall be an alternate channel.
- SPs need to become AUA and tie up with ASAs so as to do Aadhaar based authentication.
  - SP should be given free of cost authentication services by ASAs.
- SPs and TSPs need to seed their databases with mobile nos. and Aadhaar nos.

AADHAAR + MOBILE NO. – RECOMMENDATIONS

- As the Mobile Phone is easily transferable and Aadhaar number is also publicly available,
  - Services which require Low Level of Assurance should use this digital identity(Aadhaar no.+ Mobile No.) to authenticate users.
- Big departments need to be identified & mandated which will be asked to seed mobile number with Aadhaar number.
- DoT need to be asked to mandate TELCOs to create database of mobile numbers linked with Aadhaar number in a time bound manner. TRAI need to be asked to come out with tariff for each authentication at TELCOs database.
- The user departments should take a call for the authentication mechanism of using mobile number linked to Aadhaar based mobile ID and map its assurance level to risk/sensitivity of the service/application.

MOBILE PKI

- Mobile Digital Signature
  - PKI credentials (private, public keys) using secure hardware crypto tokens(which can be used on Mobile phones) helps in achieving the requirements of legally accepted digital signatures as laid out by CCA.
  - Various methods of storing DSC on Mobile
    - Cryptographic SIM (PKI stored on Secure Element of the SIM) – most suitable
    - Micro Secure Digital (SD) Cards (PKI stored in the memory cards)
    - Slim SIM (PKI stored in wafer and attached to SIM)
    - Extension SIM (PKI storage in detachable jacket of the SIM)

MOBILE PKI – BENEFITS

- PKI is widely used technology for digital identity management.
- Institutional framework is already in place for PKI in India.
- RBI issued a recent guideline to enable PKI in all financial transactions as additional option to make financial transactions more secure.
- Mobile based PKI is a tried and tested technology in several countries.
- PoCs seem to have been completed by some Telecom Operators in India including BSNL and Vodafone on SIM based PKI.
- High Security Assurance Levels.

MOBILE PKI - CHALLENGES AND RISKS

- PoCs conducted in India for SIM based Mobile ID meet the requirement of Common Criteria of EAL(Evaluation Assurance Level) and not as recommended by CCA(FIPS 140-1/2 Level2).
- Tariff of Mobile DSC may be high as even tariff associated with token based DSC is in range of Rs. 1150- 1900 for 2 years
- Digital certificates are issued maximum for 2 years thus causing repeated expenditure
- No single body to issue the crypto SIM card - multiple touch points for issuing digital certificates on SIM may cause coordination problems
- Issues of coordination that may arise due to change in Mobile number or loss of SIM card.

MOBILE PKI – RECOMMENDATIONS

- Private Key should be securely stored in the secure element of SIM/Device
- Primary Use Cases are Signing and Authentication
- Interoperable platform to be maintained
- Initial Pilots may be funded by Government
- Cost of scaling up to be subsidized by ecosystem players, who would then find ways of monetizing the same through increased adoption
- To check viability of the solution Government may facilitate or can be a part of PoCs carried out by other entities.
- DOT/ TRAI may be mandated to ensure that TELCOs provide DSCs on SIMs and prescribe the tariff.

VOICE BIOMETRICS

- Uses features of a person's voice to ascertain his identity
- User's voice sample is verified against his reference voice-print stored with the identity provider
- 3 ways of using voice biometrics

Text-dependent

System: *Please say your pass-phrase*

Caller: *India is great*

System: *Thank You*

In public service delivery scenario, this authentication is most suited.

Text-prompted

System: *Please say 91-71*

Caller: *91-71*

System: *Please say 37-48*

Caller: *37-48*

System: *97-25*

Caller: *97-25*

System: *Thank You*

To mitigate any risk associated with user playing a recorded voice.

Text-independent

System: *What can I do for you?*

Caller: *I want to fetch details of my passport application*

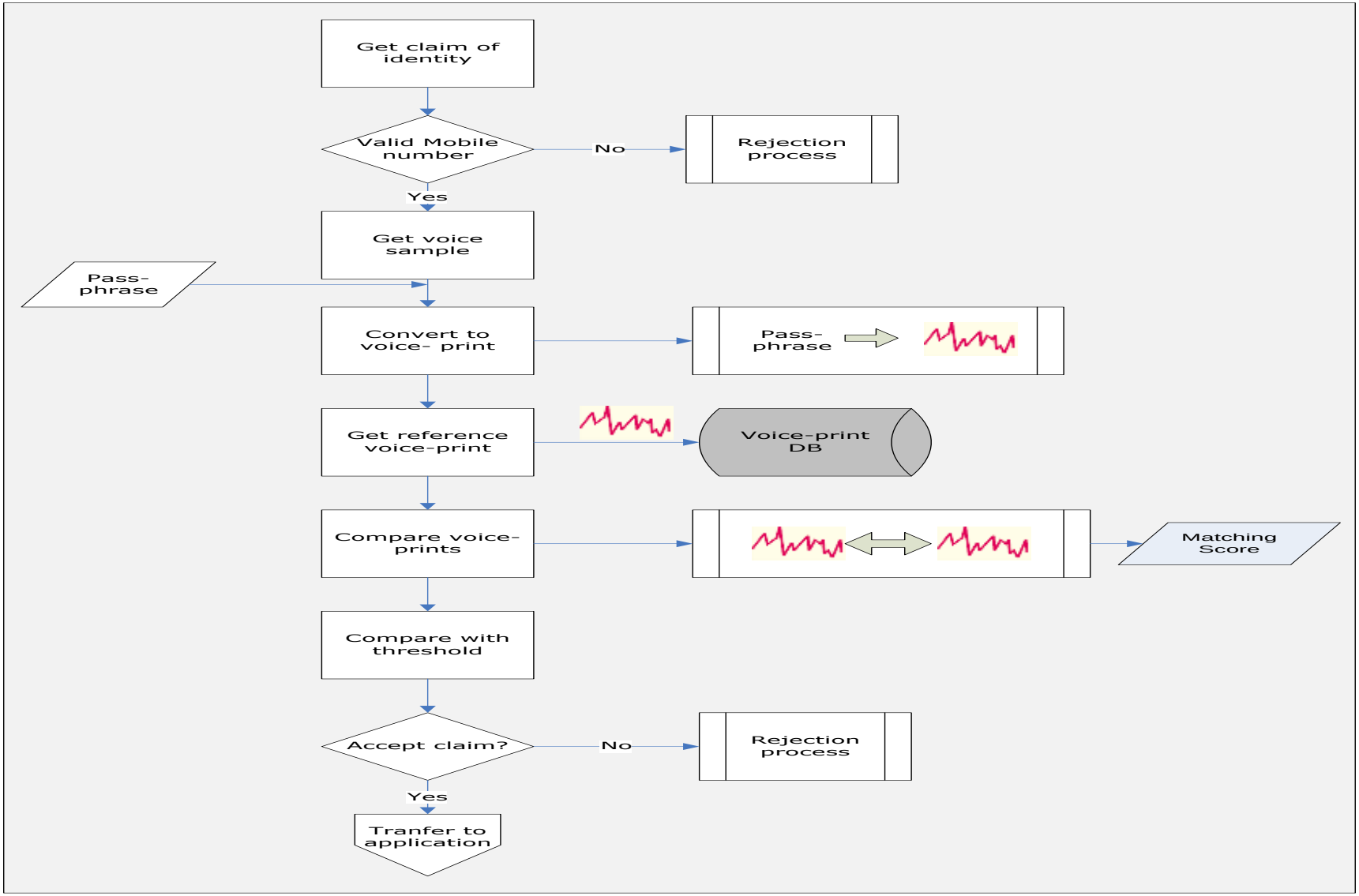
System: *Please wait till the information is fetched*

PAUSE while the system is verifying the identity of the caller.

System: *Thank you for waiting, your request will be processed now*

More suited for defense/intelligence purposes where voice to be identified from a large database of voice-prints & without letting that person know.

VOICE BIOMETRICS – AUTHENTICATION PROCESS FLOW



VOICE BIOMETRICS - BENEFITS

- No requirement of dedicated PoS device
  - Works with any standard equipment – like mobile phone/ landline, normal voice or speaker
  - No need of dedicated interface devices like finger-print/iris scanners
- Provides strong authentication when combined with phone
  - Multi-factor authentication – what you are (voice), what you possess (mobile phone), what you know (text pass-phrase)
- Can be used remotely - from any where in world
  - User need not be present at the PoS

Gartner study:

"Voice biometrics has been proven effective as an authentication method that works. It does not generate a false-positive or true-negative between 87% and 97% of the time, depending on the quality and consistency of the voiceprints"

VOICE BIOMETRICS - CHALLENGES AND RISKS

- Vulnerable to environmental conditions
  - Background and channel noise
  - Variable and inferior micro-phones
  - Extreme hoarseness, fatigue and vocal stress
- Requires enrolment
  - To link mobile number, voice print and Aadhaar
  - Vocal changes with age would require fresh enrolment/update of voice print at given ages of a person
- Recorded Voice
  - Strong liveness test can be employed to eliminate the risk of a recorded voice being played in a text-dependent verification
  - Text-prompted method can be used
- Localization requirements
  - A text-dependent voice based verification would require to address needs of recording the voice sample in different languages and identifying them during verification process.
  - Addressed by strong localization solutions attached to the voice biometric systems.

VOICE BIOMETRICS - BEST PRACTICES

- Voice biometrics + Mobile number together should form Mobile ID
  - Will enable one-to-one mapping
  - Will provide stronger authentication
- Voice prints should be updated regularly – say 10 years interval or at specified age
  - To mitigate voice changes accompanying age
- Use text-dependent voice prints for stronger authentication
- Implementation should be staggered to minimize disruption to service delivery using existing mechanisms

VOICE BIOMETRICS - RECOMMENDATIONS

- As any other Mobile ID, the voice biometrics should also be an additional option to already existing factors of authentication
- Each user departments should take a call for the authentication mechanism using voice biometric based mobile ID and map its assurance level to risk/sensitivity of the service/application
- The voice print of the user and her mobile number should be linked to her Aadhaar
- Voice print enrollment can be done using Aadhaar KYC
- Enrollment can be done by
  - established government institutions like UIDAI, CCA OR
  - a new government entity

VOICE BIOMETRICS - INTERNATIONAL/DOMESTIC IMPLEMENTATIONS

- Australian Taxation Office
- Centrelink
- 'Proof-of-life' for Pensioners in Mexico City
- Proof of Life Philippines
- National Australia Bank (NAB)
- U.S. Bank Expands Voice Biometric Solution
- Abu Dhabi Commercial Bank
- Banco Santandar Mexico
- ING BANK

- BARCLAYS BANK UK
- Vanguard
- Turckcell Voice Biometrics
- TD Water House
- Tatra Banka
- Vodacom
- Deployments in INDIA
  - Large private sector bank in India is understood to be deploying.
  - Micro Finance institution Basix use Voice Biometric based authentication to deliver delivery services to 300000 users.

INSTITUTIONAL MECHANISMS AND FRAMEWORK

CHALLENGES FOR POLICY MAKERS

Challenges	Mobile + Aadhaar	Mobile + Digital Signature	Mobile + Voice Biometric
Building trust in the mobile environment.	Yes	Yes	Yes
Identify trusted agencies for mobile id .	Exist	Exist	Yes
Define a general framework for the use of mobile id	Yes	Yes	Yes
Standards in areas such as application programming interfaces and data interchange in mobile environment	Yes	Yes	Yes
Evolve detailed procedures for authentication	Yes	Yes	Yes
Define duties of certificate issuing authorities like CCA/UIDAI /new authority for authentication mechanisms	Exist	Exist	Yes
Regulations on dispute resolution with roles and responsibilities	Yes	Yes	Yes
Define mechanism for usage for each deptt.	Yes	Yes	Yes
Large field trials with a heterogeneous sample population before deployments	Yes	Yes	Yes

INTERNATIONAL BEST PRACTICES

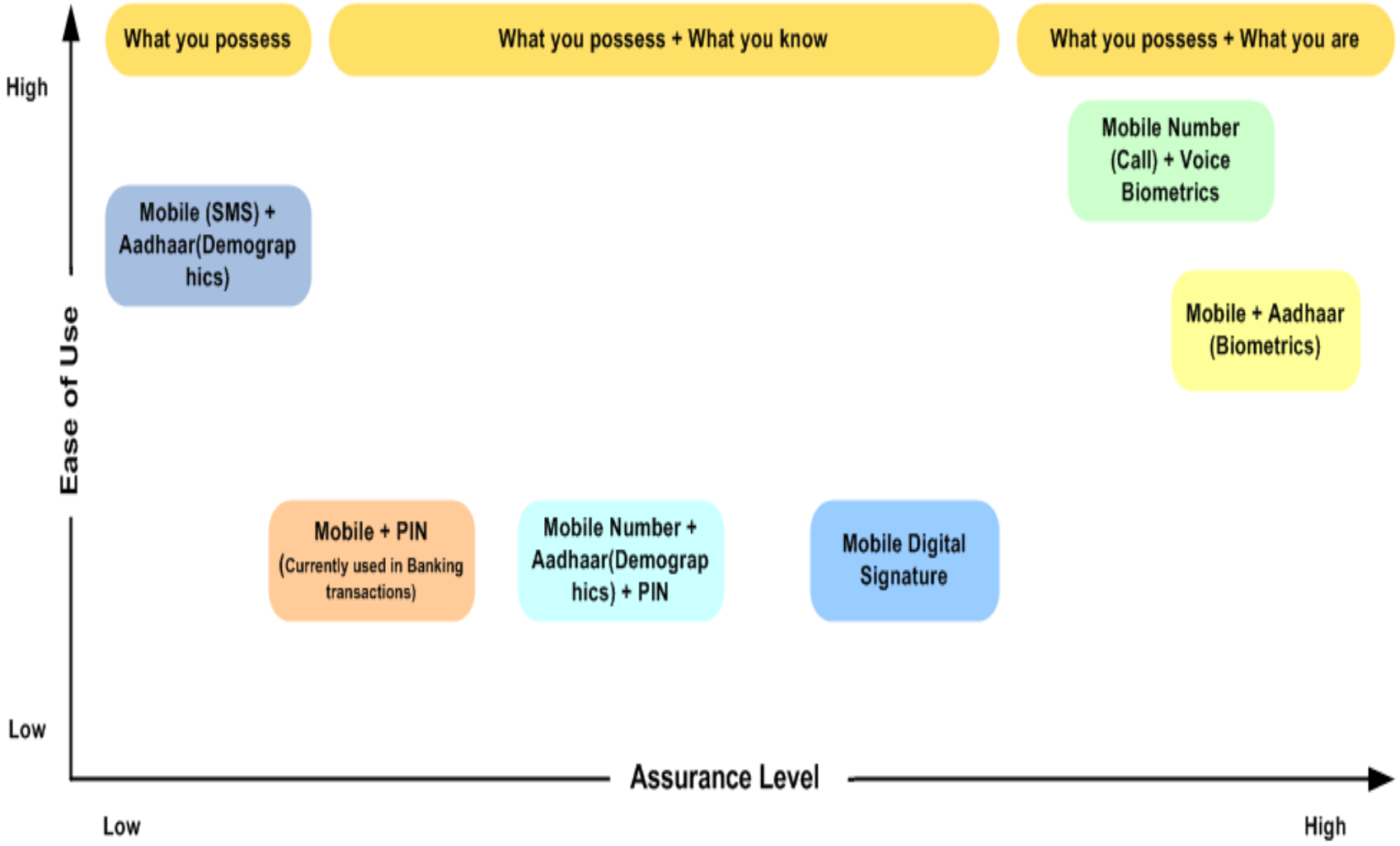
- Process based approach
  - European Commission takes a ‘process based’ perspective.
  - directives and regulations around:
    - Electronic identification, signature and trusted services for electronic transactions
    - Data protection and privacy regulations
    - Technical standards
    - Sectoral regulations such as e-commerce regulation
- Many international standards
  - International Organisation for Standardisation
    - 'ISO/IEC 24745:2011 -Biometric Information Protection standard
  - International Telecommunications Union
    - Publishes standards on the use of Information and Communication Technologies (ICTs)
  - BSI Committee IST/44 - Biometrics
  - BS ISO/IEC 14888-3:2006+A2:2012- Security techniques including digital signatures
  - Electronic Signatures and Infrastructures Technical Committee (TC ESI)
    - Electronic Signatures and Infrastructures standardization
  - European Directive
    - Directives on e-commerce including mobile payment
    - Technology neutral authorization directive 2002/20/EC
    - E-money Directive (Directive (2009/110/EC)
    - Directive on Privacy and Electronic Communications 2002/58/EC

RECOMMENDATIONS

Recommendations	Mobile + Aadhaar	Mobile + Digital Signature	Mobile + Voice Biometric
Strengthen existing organizations like CCA, RBI, DoT, UIDAI etc to administer mobile identity	Yes	Yes	Yes
Finalize technical standards for mobile identity based on international standard	Yes	Yes	Yes
Life time of Digital Signature to be at least 5 years	NA	Yes	NA
Sectoral guidelines to enable mobile id as valid identity	Yes	Yes	Yes
CCA to be empowered to issue mobile id	Yes	Yes	Yes
IT Act 2000, Amended 2008, to be modified to treat all frauds in mobile identity at par with frauds in Digital Signature	Yes	Yes	Yes
Need for a robust grievance handling mechanism	Yes	Yes	Yes
Clearly defines the liability in case of data breach/ unauthorized transactions between the citizen, the service provider and trusted agency.	Yes	Yes	Yes
Capacity building in government to detect and investigate fraud using mobile id	Yes	Yes	Yes
E-authentication framework , e-Pramaan, to include authentication based on voice biometrics	NA	NA	Yes

RELEVANCE VIS-À-VIS DELIVERY OF PUBLIC SERVICES

EASE OF USE *VS.* ASSURANCE LEVEL



INDICATIVE BEST FIT-MOBILE ID FOR PUBLIC SERVICE DELIVERY

Type of Service	Minimal sensitivity; Public & Semi-public data		Moderate Sensitivity; Private Data; Moderate impact in case of breach.		High sensitivity; Transactional Data; High impact in case of breach		Very High sensitivity; Very private/financial information; very high impact in case of breach
Assurance level Required	Low	Low	Medium	Medium	Strong	Strong	Very Strong
AS-IS Authentication Mechanism	Username + Password in most of the cases; Few applications use DSC but more for signing than authentication; Mobile used for second factor – for OTP based verification.						
Proposed Mobile ID Types	SMS with Aadhaar - Demographic authentication	Call from mobile - Demographic authentication	Mobile No. + Aadhaar + PIN	Aadhaar + OTP	Mobile + Voice Biometric	Mobile no. + DSC	Mobile no. + Voice + Aadhaar
Best-fit ePramaan Level	Level 1		Level 2		Level 3		Level 4
Current Mobile Usage for Authentication	Mobile Number verification for information services		Mobile + PIN and Mobile + OTP – Mobile Banking		Not Used		
Example	Exam results, Duplicate bills - water, electricity, etc Telebanking - initial verification;		Financial transactions, Land records, Birth/Death Certificates etc.		Student scholarships; disbursal of public benefits; Pension; PDS, MNREGA;	Income Tax filing; Property Registration; Financial transactions	Financial transactions, eVoting, eKYC, Passport, Visa

CHALLENGES AND RISKS

- In case of single mobile no. used for a family group:
  - Separate authentication procedures have to be registered for a member of family.
  - SIM PKI feature will be for a single individual
- Establishing the accountability for upkeep of the services till last mile.
- Change Management/Awareness to establish use of Mobile as an Identity
- Threshold in user acceptance. Solution should be easy to procure/deploy and adopt.
- Common specifications and open standards will be vital to ensure identity solutions are interoperable and can thus be used across different services.

INTERNATIONAL/DOMESTIC IMPLEMENTATIONS

- **Estonia**: Uses Mobile-ID (with the legal binding PKI-based signature) for offering public services and including e-voting.
- **Finland:** All e-government services are accessible through the integration of Finnish bank credential (bank ID) with the eGov portal.
- **Barcelona:** Through Mobile-ID, many Municipal services are being provided viz, towing information, duplicate copy of vehicle tax payment form, mobile payment of taxes and fines, check residents' register and electoral census details, residence certificate.
- **Oman:** Complements the national eID card, the mobile PKI SIM card adds true mobility for eGov services.
- **Iceland:** Many of Iceland's services are accessible with Mobile ID.
- **Norway:** Mobile ID enables three million users of Norway's BankID system to access e-banking services securely. Through Mobile-ID, user access their company's intranet, e-mail, and databases; and sign legally binding agreements.
- **Turkey:** Consumers access their accounts online through mobile ID.
- **Swedbank:** Uses PKI Mobile-ID to provide faster and more convenient customer service.
- **Omnitel:** Uses PKI based Mobile-ID to access a variety of e-services and digital signing.
- **Lithuania:** Mobile-ID is the most widely used mobile identity solution in Lithuania.

COMMERCIALS AND MARKET ECOSYSTEM

ECOSYSTEM – POSSIBLE ACTORS/ PLAYERS

1. Aadhaar-linked Mobile Number

- Unique Identification Authority of India (UIDAI)*

2. Mobile-based PKI / DSC

- Controller of Certifying Authorities (CCA)
- SIM manufacturers*
- SIM-PKI based solution providers*

3. Mobile + Voice Biometrics

- New or subsisting certifying/ licensing authority (such as UIDAI)
- UIDAI * (for seeding)
- Voice-biometric based solution providers

*May not apply in all cases

Common to all 3 implementations:

- Telecom Service Providers (TSPs)*
- Telecom Regulatory Authority of India (TRAI)
- Department of Telecommunications (DoT)
- Reserve Bank of India (RBI) and Banks
- Government departments/ public agencies for public services as well as for ID management (where applicable)
- Handset manufacturers*
- Value Added Services (VAS) players
- App providers
- Citizen users

ECOSYSTEM – SOME EMERGENT COST ASPECTS (BROAD LEVEL)

1) **Aadhaar-linked Mobile Number**
   - Integration effort will have cost implications

2) **Mobile-based PKI/ DSC**
   - PKI-SIM cards ~5 times costlier
   - Indicative cost of DSC (when procured individually):
     - Token cost (approx Rs. 500/-) which may partly/ wholly be taken up in the SIM component
     - Signature: In the range Rs. 1000 – Rs. 5000 across classes

3) **Mobile + Voice Biometrics**
   - 50c to US$1 per user (CAPEX)+ 20% AMC
   - 5-10 cents per transaction
     - *Expected to go down with volumes*

ECOSYSTEM – SOME EXISTING SOLUTION PROVIDERS

1) **Aadhaar-linked Mobile Number**
   - UIDAI and TSPs

2) **Mobile-based PKI/ DSC**
   - PKI-enabled SIM Cards: Gemalto, SmartTrust, Valimo Wireless

3) **Mobile + Voice Biometrics**
   - Voice Biometrics: Nuance, Agnito, Nice Systems, Pindrop security, TrustID, Victrio, CSID

ECOSYSTEM – READINESS & SUSTAINABILITY

- Sense of readiness amongst actors/ players is tempered with sense of additional investments
- Long-term sustainability requires:
  - Telco reach of/ to remote areas
  - Backing from top to implement the delivery
  - Enough volumes of Mobile-ID related benefits (to allow the market to breathe and grow)
  - Digital literacy across user-citizens and intuitive experience for user-citizens (being able to lend itself to "identification" without too much manual intervention)
  - Seamless experience across geographies (including domestic & international)

Thank You

Based on

DIGITAL INDIA WORKSHOP (17-Oct-2014) And Further Deliberations

सत्यमेव जयते

Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

National e-Governance Division