GOVNEXT

Secure Mobile Governance and Technology

GovNext India Foundation

Secure Mobile Governance and Technology

GOVNEXT

VISION

- Empower governments with digital governance leading to visibility & control on people, financial assets and economy.
- Inclusive for all strata of society & empower every citizen through digital banking revolution.

MISSION

- Provide Digital Banking & Financial Services On A Trusted PlaKorm among government, businesses & citizens converging all G2C services with traceability, actionable data analytics and regulatory compliance leading to accelerated commerce and economic growth

Our Approach

GOVNEXT

Objective

- Promote less-cash more electronic payments
- Reduce overall cost of handling cash and physical currency stock in circulation
- Enable convenient payment methods such as Bio-metric payments
- Integrated mCommerce and electronic payments

Detractor

- Cash withdrawal at ATMs and Bank counters
- Lack of Infrastructure and Incentive to accept non cash and electronic payments.
- Preference for ecommerce payment on delivery
- Payment terminal cost is a deterrent for banks and passed on to Merchants

Enablers

1. **Government**: Provide incentives to consumers to pay through debit/credit card (12.3m in UAE). For ex: 1% cash back much like in other countries
2. **Central Bank, Banking Division**: Ability to Cash-in (deposit in account) at Merchant POS terminal to reduce cash in circulation
3. **Central Bank, Customer**: Wide availability of affordable-and-yet-secure self service 'payment terminals' at all homes, pilgrimage locations, hotel rooms, stations, offices and public places. Customer pays for the terminal at easy EMI to earn the cash back incentive.
4. **Central Bank**:
    1. Ability to pay securely & conveniently by card to regular billers and home delivery e-commerce companies.
    2. Ability to electronically transfer money locally or overseas with ease from home.
5. Ability to pay swi‘ly by one's fingerprint or voice.

Our Vision for Mobile Governance

GOVNEXT

“To partner with government, healthcare sector and banks in order to perpetuate an ecosystem that would provide ubiquitous healthcare benefit management system, electronic payment and auditable services to citizens in a frictionless manner”.

1. Citizens

Leverage existing smart ID card infrastructure, bank cards, Identity Management and Location based infrastructure and deliver government benefits through an integrated benefit management system driven by NFC ID cards, NFC mobile phones, NFC tablets, cost-effective mobile Point Of Service (POS) devices, thus ensuring universal acceptance.

2. Government Officials, Hospitals, Pharmacies and Banks

Empower officials to positively identify the beneficiary, create authenticated audit trails, preventing fraud, corruption and any possible pilferage. Support Smart cards, NFC tags, magnetic swipe cards, and biometric (photo, face, voice, fingerprint) identification as well as location-based and Device-based identification solutions. Convert Hospitals and pharmacies into authentic Government Business Correspondents.

3. Integrated Payment and Identity Platform

Build a secure, fast and flexible payment network enabling seamless connections between citizens, doctors, government officials, police and merchants to provide secure, irrefutable identity-based transactions, and superior analytics, clean audit rails over any available network.

Trusted Execution Environment on Smart Phone - Features

GOVNEXT

Trusted ExecuQon Environment (TEE)

- Is a hardware secure environment relying on hardware-based Roots of Trust
- Has Zero extra hardware cost as it is part of the main device application processor
- Protects in particular from so‘ware threats including malware and rooted devices

TEE delivers hardware-security for applications by

- Is a hardware secure environment relying on hardware-based Roots of Trust
- Has Zero extra hardware cost as it is part of the main device application processor
- Protects in particular from so‘ware threats including malware and rooted devices

Trusted Execution Environment (TEE)

TEE delivers hardware-security for applications by

- A secure area of the main processor of a smart phone (or any connected device including tablets, settop boxes and televisions).
- Guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. The TEE as an isolated execution environment is providing security features such as isolated execution, integrity of Trusted Applications along with confidentiality of their assets.
- Offers an execution space that provides a higher level of security than a rich mobile operating system (mobile OS) and more functionality than a 'secure element' (SE) on SIM.

TEE Enables applications to leverage hardware-based:

- EMV credentials, fingerprint, photograph stored in TEE
- Protection for sensitive application logic and data
- Trusted GUI

TEE provides strong, hardware-based security to connected devices:

- Hardware protection of secure content
- Isolation from software threats
- Application asset protection
- User authentication
- Device binding and attestation

TEE Use Case – Mobile Financial Services

GOVNEXT

TEE delivers hardware-security for applications by

- Open loop transactions based on EMV, HCE tokens for credit and debit card payments.
- Visa Paywave, MC Paypass, AMEX Expresspay supported on TEE
- Remote open loop card provisioning through OTA services
- Tap & Pay with TEE EMV credentials without user interaction with trusted GUI for real =me feedback.
- Personalize user experience, improved services through TEE.
- Mobile security to mitigate risks of provisioning new IoT services with or without customer interaction.
- Token Storage – Protecting limited use keys for HCE and in-app channels
- Offline User verification – Biometrics, PINs and caches for enhanced User Experience
- Non-repudiation – Trusted display and transaction confirmation
- Mobile Wallets – Protec=ng private crypto keys

The TEE can protect assets and cryptographic operations of a given service provider. Banks can use this environment to distribute their services in a trusted manner. The TEE can be used to securely authenticate the platform hosting the service, protect cryptographic keys with Root of Trust. It is also possible to deploy applications on the TEE without requiring user interaction with the device, preserving the user experience.

TEE Use Case – Internet of Things (IoT)

GOVNEXT

- Secure connectivity to enterprise through data privacy leveraging TEE.
- Prevention of unauthorized use of emergency services which in some situations matters of life and death.
- The TEE provides IoT developers an integral platform to manage identities, authentication, authorization and permissions associated with devices and users.
- Strong security protects private keys, certificates and policies that enable multi tenant services and user controlled access that will accelerate the next wave of IoT devices.
- With TEE based advanced controls and the real power of preserving privacy in the hands of users, can create new economies scale as a leader in IoT services.

Technical Use cases:

- Secure boot to prevent firmware modification by users
- FOTA & secured application update protection
- Digital Rights Management (DRM) key protection
- Hardware unique key anti-cloning – data binding and strong authentication
- Run time integrity checking
- Device attestation
- Biometric template matching
- Protection of sensitive peripherals

TEE based Trusted IoT ApplicaQons:

1. Mobile Governance Apps
2. Healthcare Services – Monitoring and control
3. Home/Industrial Automation
4. Automotive in-vehicle infotainment (IVI) system
5. TEE-EMV based In app purchasing
6. TEE based offline Parking & Toll payments
7. Automated Attendance Recording