MGOV SERVICES
Mobile is here to stay …

MOBILE IDENTITY & AUTHENTICATION FRAMEWORK
APRIL 2018

Michael Edwards
Director Solutions Marketing - Segment SecureID
Business Unit Security & Connectivity
Tel: +49 40 56132158
Mobil: +49 171 4101653
Email: michael.edwards@nxp.com
Operations in 33 countries
>$10B Revenue
9000+ Patents

More than 100 facilities
~31,000 employees
Headquarters: Eindhoven

NXP at a Glance

Market Leader in...

- SECURE IDENTIFICATION
- RF POWER TRANSISTORS
- AUTOMOTIVE
- SMALL SIGNAL DISCRETE’S
- COMMUNICATIONS PROCESSORS
- BROAD-BASED MCUs

Note:
1. All financial figures are based on trailing twelve month reported information; R&D expense are non-GAAP
NXP Secure ID – product and service offering

PERSONALIZATION SERVICES
- OS Initialization
- Applet- & data loading
- Applet CC & FIPS cert. support
- Middleware

INLAY
- eCover
- Datapage
- Prelaminate

APPLICATIONS
- ICAO
- ePKI
- eHealth
- eVehicle
- Payment
- MIFARE

SECURE IC OS
- Native OS
- JavaCard OS

SECURE ICS
- 8KB -144KB user memory
Electronic National ID Application Summary

#1 electronic IDs WW

**Drivers**
- Reduce fraud
- Eliminate identity theft
- Enable gov online services

**Key Trends**
- Convergence of applications
- Mobile IDs derived from eIDs

**Use Models**
- Visual inspect. by service provider
- 2 & 3 factor authentication for online services

**Standards**
- None world-wide
- ICAO 9303 often leveraged
- EIDAS in Europe

**Key References**
35+ out of 65+ countries trust NXP ICs

- Ecuador
- Germany
- Thailand
- Malaysia
- Nigeria
- Indonesia

**Standard Product Configuration**

- Java Card OS
- CC EAL 6+
- CC EAL 5+
- CC EAL 4+
- ICAO/eID
- PKI
- MoC
The world has, without question, entered the age of online government services. Within the past decade, government agencies worldwide, at the national, state, and even local levels, have been moving quickly to provide websites that provide information, give access to services, and let people update their information.

### eGOV IS NOW GLOBAL

Making online government services available to citizens has several benefits, in terms of cost and convenience:

- Online access helps improve workflows and lower administrative costs.
- Gov. agencies can service a broader population with fewer personnel, and extend their coverage, without having to establish new offices.
- From the citizen’s point of view, eGov makes it easier to interact with government and get things done.

#### Transactional online services offered by national websites worldwide (2014 and 2016)

<table>
<thead>
<tr>
<th>Service</th>
<th>No. of countries offering the service in 2014</th>
<th>No. of countries offering the service in 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a personal account</td>
<td>101</td>
<td>142</td>
</tr>
<tr>
<td>Submit income taxes</td>
<td>73</td>
<td>114</td>
</tr>
<tr>
<td>Pay for utilities</td>
<td>41</td>
<td>104</td>
</tr>
<tr>
<td>Register a business</td>
<td>60</td>
<td>97</td>
</tr>
<tr>
<td>Pay fines</td>
<td>42</td>
<td>76</td>
</tr>
<tr>
<td>Apply for social security benefits</td>
<td>46</td>
<td>63</td>
</tr>
<tr>
<td>Apply for a birth certificate</td>
<td>44</td>
<td>55</td>
</tr>
<tr>
<td>Apply for environmental permits</td>
<td>40</td>
<td>55</td>
</tr>
<tr>
<td>Apply for marriage certificate</td>
<td>39</td>
<td>53</td>
</tr>
<tr>
<td>Register a motor vehicle</td>
<td>33</td>
<td>47</td>
</tr>
<tr>
<td>Apply for a driver’s license</td>
<td>29</td>
<td>38</td>
</tr>
<tr>
<td>Apply for a personal identity card</td>
<td>27</td>
<td>31</td>
</tr>
</tbody>
</table>

THE ARRIVAL OF mGOV

A growing number of today’s transactional services are designed to be accessed by a mobile device, such as a smartphone or tablet. This subcategory of eGov, known as mobile government or mGov, lets citizens use mobile apps and mobile websites to interact with a range of services.

The table shows the categories that Statista is tracking in mobile – covering everything from education and health to finance, welfare, labor, and environment – and confirms that support for mobile increased across all categories.

Percentage of countries offering mobile government services (2014 and 2016)

The table shows the categories that Statista is tracking in mobile – covering everything from education and health to finance, welfare, labor, and environment – and confirms that support for mobile increased across all categories.
The increased support for mobile access is directly tied to the near universal adoption of mobile devices. Since 2015, the number of mobile-phone subscriptions worldwide has approximately equaled the number of people on the planet – about 7 billion.

THINKING MOBILE FIRST

In light of the trend that many citizens now use mobile devices to access information, make purchases, and conduct other forms of business, governments at the national, state, and local levels have started adopting the philosophy of “think mobile first.” They’re making mobile technology a priority in their online strategies and, in many cases, designing sites and services with mobile in mind.

• Them mobile-centric approach also requires balancing security requirements with the need for ease of use.
• It’s essential for government agencies to consider the security mechanisms for mobile access at the earliest phases of mGov design and development.
Mobile is here to stay …

Design considerations

best practices for delivering the right combination of security and convenience
What is it about

Provide secure, privacy-enhancing services that conveniently connect users to critical online services, ideally using digital credentials they already have and trust on devices they already use.
Vision and Value of a federal identity management

Using a single or federated ID to access multiple services is something private organizations are pursuing, as well, since the approach enables secure use of private digital information while extending the service offering.

Carrying one or more credentials

- Border Crossing
- Government Services
- Healthcare
- Online Transaction
- Social Media
- Payment

Form Factor

Derivation

- DIGITAL ID
- SHARED DIGITAL ID
- NETWORKS
- LINKING PEOPLE & DEVICES
- SIMPLIFIED ACCESS
- PROVIDES CHOICE
- PROTECTS PRIVACY
LEVERAGE CONTEXT-AWARE AUTHENTICATION

In many of today’s online applications, developers are forced to make a tradeoff between security and convenience. As the level of needed protection increases, ease of use tends to go down, since the authentication process becomes more complex.

The added level of flexibility afforded context-aware authentication means it’s easier to choose the right level of security for each situation.

Support of context aware authentication methods to optimize security, convenience, and costs

Identification method depends on device type and features
- Biometric sensor (e.g. fingerprint, face, voice)
- Non-biometric (e.g. PIN, TAN, password)

Identification method is economical
- Most economical ID solution is chosen for particular situation and application

Identification method depends on security requirements of use cases
- Simple authentication for low-stake applications (e.g. small payments)
- Multifactor authentication for high stake applications (e.g. access health records)
In the world of identity and access management, the level of assurance refers to the degree of confidence that a credential is neither fraudulent nor stolen, and that the person using the credential is the person to whom the credential was issued.

- When granting access to any government service, the level of assurance needs to meet the requirements of a given use case. A low-risk transaction, for example, is likely to require a lower level of assurance than a high-risk one.
- The security mechanisms supported by an authentication platform typically dictate the level of assurance, and provide a starting point for balancing the tradeoffs involved with risk, complexity, and cost.

**Described by NIST, eIDAS**
*Strong push to support Mobile Identities in multiple environments*

**Risk Mitigation for the citizen and Relying Party**
*Relying Party (RP) makes the authorization decisions based on what was provided.*

**Enables IDPs to reach into the public space**
*Standards (OIDC, FIDO, VoT) bridge identity gaps and reduce the Identity Zoo*
Derived Identities

The use of standardized, time-tested eID formats helps lower development costs, makes the deployment easier to scale, and increases stakeholder confidence. Building on the foundation of eIDs, derived credentials make it easier, safer, and more convenient to deploy and maintain mGov services.

Physical documents used to generate eIDs and derived credentials remain the foundation of all government services – online or offline – and remain the root credentials in case there are any problems with the network infrastructure associated with eGov or mGov services.

- **LOA/VoT is wired into the platform**
  Each assertion provides context to the RP about the device/app/user.

- **Service Workflow Engines**
  Customizable with influence from IDP, RP, Device & User

- **Crypto-signature is not static on the device**
  DI signature are rotated & protected.

- **Device & App Context**
  Centralized “meta” knowledge about the nature of the device, user, and mode of authentication.
THE MOBILE ID ARCHITECTURE

The derived credential is just one part of the overall architecture used to store, process, and communicate the data necessary for secure authentication.

A typical Mobile ID architecture makes use of the following items:

**MOBILE ID** – This is the derived credential and the Mobile application that hosts it. The Mobile ID resides in its own “vault”, ideally an eSE. The vault is a secure container that stores and processes data, and communicates with entities external to the mobile device, in a way that keeps the data private and safe.

**MOBILE ID MIDDLEWARE** – This is software that translates high-level API functions into commands that can be used by an eSE, TEE’s and other containers and interprets responses to provide feedback to calling applications. The Middleware is as well used to access issued eID cards enabling credential derivation.

**MOBILE APPLICATIONS** – These are services or applications that run on the mobile device and make use of the Mobile ID credentials.

**THE MOBILE ID ARCHITECTURE**

- **MOBILE ID**
- **MOBILE ID MIDDLEWARE**
- **MOBILE APPLICATIONS**
- **NFC & SE MW**
- **Trust ID SDK**
- **TRANSIT SDK**
- **NFC & SE**
- **Wallet**
- **Wallet Server**
- **Tokenization platforms (e.g. MDES)**
- **PTOs**
- **Issuers (Banks)**
- **Certificate Authority**
- **IdP’s & SP’s**
- **Payment**
- **Transit**
- **MGov**

- **HTTP**
- **JSON**
The overall Eco-System Landscape

Credential Holders

- Credential Users, Cards & Devices

(m)Gov. Applications Interfacing & Development

- eGov & private sector portals for services

Central Authentication Hub

- Core Infrastructure
- Central Authentication & Credentialing Services Provider

Solution Architect & System & Services Integration

- Government Central Authentication Hub
- Operator and Server hosting Service

- OIDC/SDK

- Core Infrastructure

RP’s/ & IDP’s

- Credential Providers & Subscribers

Application/Service providers

- Application Disability Parking
- Disability Bus Pass Application
- Freedom of Information Requests
- Change of Residence
- mDL
- mID
- Bank services
- Insurances
- Mobile SIM Providers
- Peer-to-Peer payment
- Etc.

- mApps
- (m)Websites
- vDocs
So the world is turning

MOBILE is here to stay...

MOBILE ID CARDS & DRIVER LICENSE

AUSTRIA
SWITZERLAND
GERMANY
UK (POC)

US Pilots:
- ALABAMA
- DELAWARE
- ILLINOIS
- IOWA
- TEXAS
- VIRGINIA
Regional overview

➤ North America: eGov solutions rely on private sector identities
  ▪ Some initiatives:
    ▪ UPS eGov services
    ▪ Canadian Gov. using bank identities for mobile services
    ▪ AAMVA started bi-literal mDL pilot, testing decentralized storage of credentials and attributes
  ▪ 12 NIST pilots financed by the federal government.

➤ Asia: Dominated by low value digital identities
  ▪ Leading countries: South Korea, Singapore, Malaysia

➤ Europe: Heterogeneous solutions
  ▪ **User/Pwd credentials**: in some leading countries: France, UK
  ▪ **eID based digital identities**: Belgium, Portugal, Spain, Germany, Estonia, Spain, Sweden, Finland, …
  ▪ **Banks and mobile ID**: Nordics, Moldova, Azerbaijan, Turkey, Canada

➤ Middle East/Africa: Mobile and eID solutions in ME
  ▪ **Middle East**: Oman, Qatar, Bahrain, UAE
  ▪ **Africa**: Nigeria, Kenya and SA starting to deploy mobile identity services.
Summery

• «Mobile Identity is here to stay…. »
  - Many initiatives for the development of (mobile) digital identity standards: eIDAS, NIST, ISO and as well ICAO started working groups on virtual documents
  - World bank ID4D (ID 4 Development) initiative to push & enable online services delivery, focus on education, healthcare, agriculture and others in general and as well via deployment of secure affordable mobile devices

• Cost saving remains a strong driver for the adoption of trust services
  - Developed countries massively shifting services to online channel.
  - Cost of digital transaction can be up to 50 times lower than face to face transaction (UK study).
  - Studies made in Norway, Australia, Denmark provide similar findings.

• The market is still fragmented
  - Different approaches: Government services centric or Private sector lead for specific purposes
  - Two main trends: Identity frameworks with standard interfaces/technologies or All-in-One proprietary approaches
Come and see our Mobile Driver License App - Booth C03

a platform for secure mobile credentialing & authentication of any virtual Gov document


2. Select a Mobile Identity to authenticate.

3. Enter PIN to unlock the selected Mobile credentials and attributes

4. virtual DL History overview
SECURE CONNECTIONS
FOR A SMARTER WORLD

Michael Edwards
Director Solutions Marketing - Segment SecureID
Business Unit Security & Connectivity
Tel: +49 40 56132158
Mobil: +49 171 4101653
Email: michael.edwards@nxp.com