With nearly everyone having a smartphone, with its functionality as an extremely versatile, networked mini-computer, it’s time to recognize this technology as an extremely convenient but also secure carrier for governmentally issued identities, equal to electronic national ID cards and passports. With NFC as a low-friction, radio-based communication link that is fully available now, the smartphone is expected to become a much more convenient complement to governmental documents. This paper looks at the motivation for using smartphones as IDs and gives an overview of the technology required to make this application a reality.

**A MOBILE REVOLUTION**

The first mobile phones were commercially launched in the early 1980s, but the last five years in particular have brought significant breakthroughs in mobile communications. Gartner reports global smartphone sales at 169 million units in Q3, 2012, a 46.9% jump over Q3, 2011. This represents nearly 40% of the 427.8 million phones forecasted to ship in Q3, 2012. This is remarkable considering what the smartphone has become: a powerful, mobile computer used to not only make calls, but also to send instant messages, emails, and media, capture video, play music, search the Internet, access mobile banking services, book travel, tweet, provide Facebook updates to friends, and more.

Much of this has been attributed to the significant leap forward caused by Apple’s iPhone 3G, introduced in 2008, which redefined the term “smartphone”. There are many contributing factors to recent mobile trends, starting with the smartphones themselves, but also including applications, cloud-based services and app stores, as well as more advanced wireless networks. Today, a very broad variety of smartphone models is now offered, and the market is able to serve nearly everyone’s demand for functionality, performance, and design.

**APPS, STORES, AND CLOUDS**

The dramatic changes in mobile that have happened since the introduction of the iPhone are in part due to the parallel developments in applications (“apps”), online app marketplaces (such as Apple’s iPhone App Store and Android Marketplace Play Store), and cloud-based services for laptops, tablets, and mobile phones. The merging of mobile music players and smartphones, together with the easy-to-use music online stores (including Apple’s iTunes), happened in parallel and helped push smartphones into becoming mobile computing platforms.

App innovation was enabled by the easy distribution and promotion of smartphone applications on online application stores. Apple introduced the iPhone App Store in 2008, and started with 552 apps available at launch.

---

2 PC Magazine Encyclopedia, “Definition of a Smartphone”, October 2011
3 TechCrunch, “iPhone App Store Has Launched (Updated)” citing Pinch Media, Michael Arrington, July 10th, 2008
The success of the popular smartphones and the accessibility of app stores is evidenced by their dramatic growth. As of September 2012, there were 700,000 apps published on the iPhone App Store and 675,000 on Google’s Play Store.

Many of these apps were cloud-based services adapted to support these more capable mobile devices. In this context “the cloud” refers to applications and web-based services made available, in real time, over the Internet or through other wireless networks. Examples include with Google Maps, ADP payroll processing, the U.S. Postal Service, Bloomberg, and even conventional credit card processing services. Such cloud-based services have had their own rapid innovations, driven by companies such as Salesforce.com, Dropbox, Evernote, and Google, among others. And, for nearly all applications available as cloud-based services, mobile platforms such as smartphones and tablets are increasingly used for access.

**NEXT-GENERATION NETWORKS**

None of the smartphones, applications or app market/cloud connectivity innovations would have been possible without higher-bandwidth mobile and wireless networks to access these features while on the go. The migration of mobile networks from older network technologies to 3G and now 4G has enabled data services with increasingly greater upload and download speeds. With this, higher-quality applications, gaming, and communication experiences have been enabled on mobile platforms. This is similar to the broadband Internet explosion that enabled better online experiences by delivering faster connection from PCs to websites a decade earlier.

**THE REAL MOBILE TREND: UX**

Today, the mobile industry uses one term to describe what has become the driving factor in mobile: the user experience (UX). The user experience builds on advances in smartphones, mobile networks, and applications/services to create a seamless and increasingly engaging way to use mobile phones. With Facebook’s social-networking experience, users can share an image of an event and connect in real time with friends. With Rovio’s Angry Birds, users can engage in online experiences, like introducing new characters into the game by tapping a plush toy, or unlocking new shared gaming sessions and levels by tapping two phones together.

With the combined innovations of smartphone technology, including NFC, apps, and networks, the UX is an evolving, increasingly enhanced target. NFC short-range radio technology looks especially promising to create a low-friction bridge between the physical and virtual worlds, since it makes it easy to connect to online services in the vicinity of the smartphone and gives the user zero administration effort with its tap-and-go interface. Most recently, the promise of the smartphone as wallet, holding an ID card, building access card, transit card, loyalty cards, and payment cards, has received attention from companies like Google and major mobile network carriers, and that attention has generated news headlines and media buzz.

**Trends in Electronic Government ("eGov")**

The first eGovernment applications based on smartcards were deployed in the 1990s, but mass adoption only started in 2004, when ICAO selected secure microcontrollers to make passport cloning much more difficult, if not impossible.

Secure ID microcontrollers are now at the heart of many eGovernment applications, making it more convenient for citizens to use internet-based government services, and increasing the security and efficiency of government.

In 2001, the 9/11 tragedy triggered broad adoption of secure smart-card solutions in passports and identity cards to prevent identity theft, illegal immigration, and terrorism.

After the first wave of electronic passport implementations, which took place between 2005 and 2008 and were driven by a U.S. mandate for non-visa-waiver countries to integrate secure microcontrollers into the machine-readable passports, the advantages of integrating a secure microcontroller in government documents became apparent to many.

---

4 CNET, “Can Apple’s App Store maintain its lead over Google Play Store?”, Sep. 27th 2012
5 InfoWorld, “What cloud computing really means”, Eric Knorr and Galen Gruman
6 TheNextWeb, “Rovio To Launch Angry Birds Free with Magic, Requires NFC To Unlock Levels”, Matt Brian. April 19, 2011
With more than 100 countries now having migrated to electronic passports (ePP), the third generation of ePP specification is in rollout. More than 55 countries have already introduced electronic national ID cards, and secure ID microcontrollers are now a proven technology, in terms of security features, in government documents.

In all kinds of government-issued ID documents, eGovernment technology delivers the following benefits:
- Better, faster, and more efficient access to public services, such as medical treatment, social security, and financial administration
- Improved safeguarding of privacy and fraud prevention by using secure technologies to protect personal data and preventing identity theft
- Safer international travel and communications, and improved cooperation between countries

At present, it is common for individuals to carry multiple government-issued cards, such as a national identity card, driver’s license, health card, and/or student card. The construction and design of such identity-related cards varies from plain plastic cards to microcontroller-based smartcards.

Through the availability of high-performing secure radio technology, modern microcontroller-based smartcards are becoming rapidly contactless. Contactless technology offers a longer lifetime and higher tolerance to harsh environmental conditions like humidity and aggressive chemicals. But even more, contactless connectivity creates the simple and easy-to-understand method of just presenting a card to an identification or interaction point.

A clear trend in the government market for identity-related solutions is a move toward more secure microcontroller-based card solutions. With proper implementation, a secure microcontroller-based “Identity Card” solution will be:
- User-friendly, which will encourage stakeholders to increase usage
- Interoperable, adding value through cross-functional use in different areas
- More secure, increasing the trust of citizens in their government

**The Intersection of Mobile and e-Gov**

**SMARTPHONES AS EGOV CREDENTIALS**

Digital identity became a reality with the deployment of several electronic IDs, including electronic passports based on the international ICAO standard, electronic national ID cards, electronic driving licences, electronic health cards, and e-Government service cards.

Until now, the identity document has been owned by the government, and even often by one government agency. It is already difficult, when generating the specification of a national eID, to align several agencies from one government. Agreeing on a specification for a government-wide credential which can be supported by a third-party token, such as a mobile phone, can seem like an impossible feat.

However, looking at this from the citizen’s perspective, it is less convenient to have several smartcards in one wallet. People may leave home without their wallet, but they rarely forget their mobile phone. Having a copy of the identity card or driver’s license in the phone would allow more flexibility in the identification process.

A phone-based solution would, of course, need to be deployed securely from the government server to the phone, and would require the phone’s secure element to be certified to the same level of security defined for the respective eGov smart card solution. In addition, secure handling of private data would need to be ensured by a Trusted Execution Environment (TEE) on the mobile phone.

Another possible application involves storing the certificate on the phone in order to authenticate access to e-services over the web. This application would not offer identification in the physical world, just in the virtual one. But it could make life easier, since the phone is often more convenient to use than a physical wallet.
TECHNOLOGY REQUIREMENTS
For mobile eGov applications to become a reality, the market requires mobile phones with adequate security and the ability to communicate with contactless ID cards and passport readers. This is the realm of NFC-enabled phones that support contactless communication protocols to emulate transit cards, payment cards, and even government ID cards. While not yet commonplace (see “Barriers to Adoption” below), the technology is now available, in advanced NFC smartphones, to deliver a mobile eGov application.

Part of this is due to the advanced security subsystem in these NFC phones. This includes a Secure Element, such as an NXP SmartMX secure microcontroller like those used in eGovernment applications worldwide for electronic passports and ID cards. These advanced security systems are suitable for secure data, advanced cryptography, firewalls, and hardware-based tamper resistance with advanced counter-measures against attacks, and meet the high-security standards dictated applications like credit cards, government ID cards, and so on.

Suitable security for such implementations has been defined under the framework set by Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria). The Common Criteria framework is based upon an international standard (ISO/IEC 15408) for computer security that is supported by predetermined security levels and third-party testing laboratories that validate such security. Such certifications, when granted, are set to varying depths of rigor in the certification process, called Evaluation Assurance Levels or EALs. The levels range from 1, for minimal assurance levels of basic functional testing against the intended use, to 7, for full verification of design and function. For eGovernment applications, controlling access to sensitive personal information is a fundamental requirement. As a result, a relatively high EAL of 4+ is required for electronic passport microcontroller solutions. In reality, most solutions are already at a 5+ level.

Smartphones are not likely to behave as single-purpose smart cards (imagine carrying a smartphone that functions only as a government ID token). Even with the same basic security system as found in passports, phones are unlikely to be used only as a government ID. The ability to load multiple applications, such as building access, transit access, and payment cards, gives the smartphone huge potential. To enable these secure, multi-application functions to share the same secure element, the Global Platform has created the concept of supplementary security domains (SSD). These domains define how the secure element can be allocated to several secure applications, including eGov applications, with separate keys to manage this domain. Since smartphones are “online” devices and secure applications are not always static (they can be upgraded or revoked), the ability to manage them over the air (or “OTA”) is also required and defined under Global Platform.

As noted throughout this white paper, there are several applicable standards that are relevant for mobile eGov applications. These include:
- Global Platform – an international, not-for-profit association, dedicated to smart card-related standards for interoperability and sustainability, whose most recent standards, as of December 2012, are defined in version 2.2.1 with several version 2.2 amendments A – E
- Common Criteria - international standard ISO/IEC 15408
- NFC Forum – an international, not-for-profit association dedicated to defining standards for interoperability between devices and services for Near Field Communication and existing contactless protocols. The relevant standard is ISO 14443

BARRIERS TO ADOPTION
One of the most visible challenges for mobile eGovernment applications has been the lack of NFC phones capable of supporting secure eGov applications. A key requirement for government adoption is to have capable phones broadly deployed. It may be possible for an agency to mandate that citizens pay for a government-owned ID card, but they cannot easily mandate purchase of a smartphone.

The lack of NFC phones is a barrier that is diminishing. While NFC has been commercially available for years, 2011 was the year when several providers of mobile operating systems (Google's Android Gingerbread+, RIM's Blackberry OS 7, and later, in 2012, Microsoft Windows Phone 8) released or announced support for NFC, and nearly all major mobile phone manufacturers integrated and featured NFC in the product line. As an illustration of the growing success of NFC, ABI Research estimated in November 2012, that the shipment of NFC handsets in 2012 would reach 102M units, and forecasted 285M units to be shipped in 2013.

The ownership of embedded Secure Elements (eSE) and its Issuer Security Domain (ISD) keys might be perceived as a hurdle for secure NFC application deployment. For secure NFC applications like mobile eGov, there is a need to establish a business (and "trusted") relationship with the eSE owner/issuer. This raises the question of whether a government will share keys with a commercial entity such as Google, RIM, Orange, or Verizon. Also, the co-existence of the eGov ID, along with commercial applets on a secure element, carries initial certification challenges. This will be solved over time, as clear demarcations are established for multiple SSDs in the Global Platform framework and are implemented in secure elements.

This framework also allows for a hierarchy of multiple Trusted Service Managers (TSMs) to manage a secure element that, in turn, allows a government agency to work with their traditional personalization service provider or TSM. At present, technical barriers include the amount of secure element memory and the implementation of Global Platform features around SSD, provisioning/ personalization, and OTA by both secure element providers and TSMs.

As with many mobile NFC applications, there are infrastructure-related barriers as well. In many regions of the world, eGov (whether card- or mobile-based), requires significant infrastructure upgrades (readers, networking, back-end databases and applications). There is a need to teach Government agencies about the economic and national security benefits of more advanced, fraud-resistant technology in today's security-conscious world. Such business cases tend to center on fraud reduction, improved security, and reduced cost of verification. Still, the cost of infrastructure upgrades may limit initial adoption in countries with significant benefits to gain or niche implementations like the “Clear” program for frequent/known travelers.

The last barriers are not technical in nature but rather have to do with user acceptance. The lack of acceptance can be present with government agencies for mobile applications as well as with end customers whose ID credentials would be stored on the mobile phone. End-user acceptance may face significant challenges as consumers believe that having all their ID and payment credentials stored on one mobile device creates concerns regarding ID theft and security. These are much like early concerns with the Internet, and may be exacerbated by the fact that mobile phones are always connected, of high value, and easy to lose or have stolen.

In some early project discussions, government and end user groups were merged by having employees of government agencies be, with their employee ID and access credentials provisioned into their mobile devices.
MOBILE E-ID EXPECTATIONS: 2012-2015
NFC Phones Arrive
In March 2013, during the Mobile World Congress, NXP announced that it has supplied NFC microcontrollers for 180 commercially available smartphone models that are enabled with NFC radio technology. This covers nearly all major OEMs, including Samsung, HTC, Motorola, LG, and Nokia.

Market research firms continue to update their market projections with ABI Research recently publishing their updated NFC device shipment projections as shown below.

Because of the advances in mobile and security technology, and the potential benefits in the area of eGov, we can expect to see early projects and activity in mobile eGov. As with other secure NFC applications, great attention will be given to early mobile eGov deployments, so as to gauge benefits, security considerations, and user experience.

CONCLUSION
Despite the exciting innovations and diminishing technical barriers in mobile, the phone is not expected to replace governmental documents on a broad scale in the foreseeable future. The mobile phone may start as a backup for many ID documents, but is not likely to be a replacement until capable secure NFC phone penetration is higher. Also, the differences in interest and agenda between government and private companies, the need to have physical evidence when electronic formats are lost or not functional, and other user-acceptance barriers will keep ID projects reliant upon existing eGov document technology. However, the mobile phone will emerge as an easy-to-carry complement to the eGov document or card, containing a copy of an identification certified by the government, allowing more flexibility in the identification process and thus making Mobile ID a core part of any smart-life solution.

About NXP
Based on trusted security, a complete product portfolio, and the best contactless performance, NXP is the leader in the overall ID market as well as in key market segments such as transport ticketing, eGovernment, access, infrastructure, RFID/Authentication, payments, and NFC. NXP provides the entire ID market with end-to-end solutions, enabling customers to create trusted solutions for a smarter life.

Figure 1: ABI Research projections for NFC device shipments by year (As of March 2013)

Smaller, More, and Better
As mobile phones continue to visibly improve in their capabilities, embedded NFC and the secure-element technology required for eGov and other applications will continue to evolve as well. Smaller and lower-cost NFC microcontrollers, equipped with increased secure memory storage and secure, multi-application elements (payment, transit, access, and authentication) will be designed into more handsets, tablets, PCs, and related accessories and NFC tags.