THE FUTURE OF ePASSPORTS AND BORDER CROSSINGS

A look at where technology might take us

By Peter Schmallegger, NXP Semiconductors

NXP


PASSPORT

INTRODUCTION

The way international travel and border crossings take place is the subject of ever new challenges and continues change. The International Civil Aviation Organization (ICAO), the United Nations agency that oversees international air travel, formulates global policies and strategies to respond to these realities. Their main objective, as outlined in the ICAO TRIP (Traveler Identification Program) 2013 strategy, is to provide security and facilitation for international travel.

In particular, the ICAO defines the formats used in **electronic passports** (ePassports or biometric passports), which contain a type of secure integrated circuit (IC), called a secure microcontroller. ePassports now represent the majority of passports in circulation, and deliver major advancements in terms of security. There are several generations of ePassport technology currently in use, and new technologies and specifications are on the horizon. -

This white paper summarizes the capabilities of existing and upcoming ePassport formats, and considers how new technologies for secure credentialing could change how we think about privacy, security, and even identity itself.

CONTENTS

1. ePASSPORTS: TODAY AND TOMORROW

Having been used by hundreds of millions of people worldwide for over a decade, the **ePassport** is no longer a novelty.

The ICAO, which defines standards for international travel documents, including ePassports, reports that 120 of their approximately 200 member states now issue electronic travel documents, and finds that more than 80% of all passports are now ePassports. In all, that accounts for more than 730 million active travel documents that incorporate the electronic format.

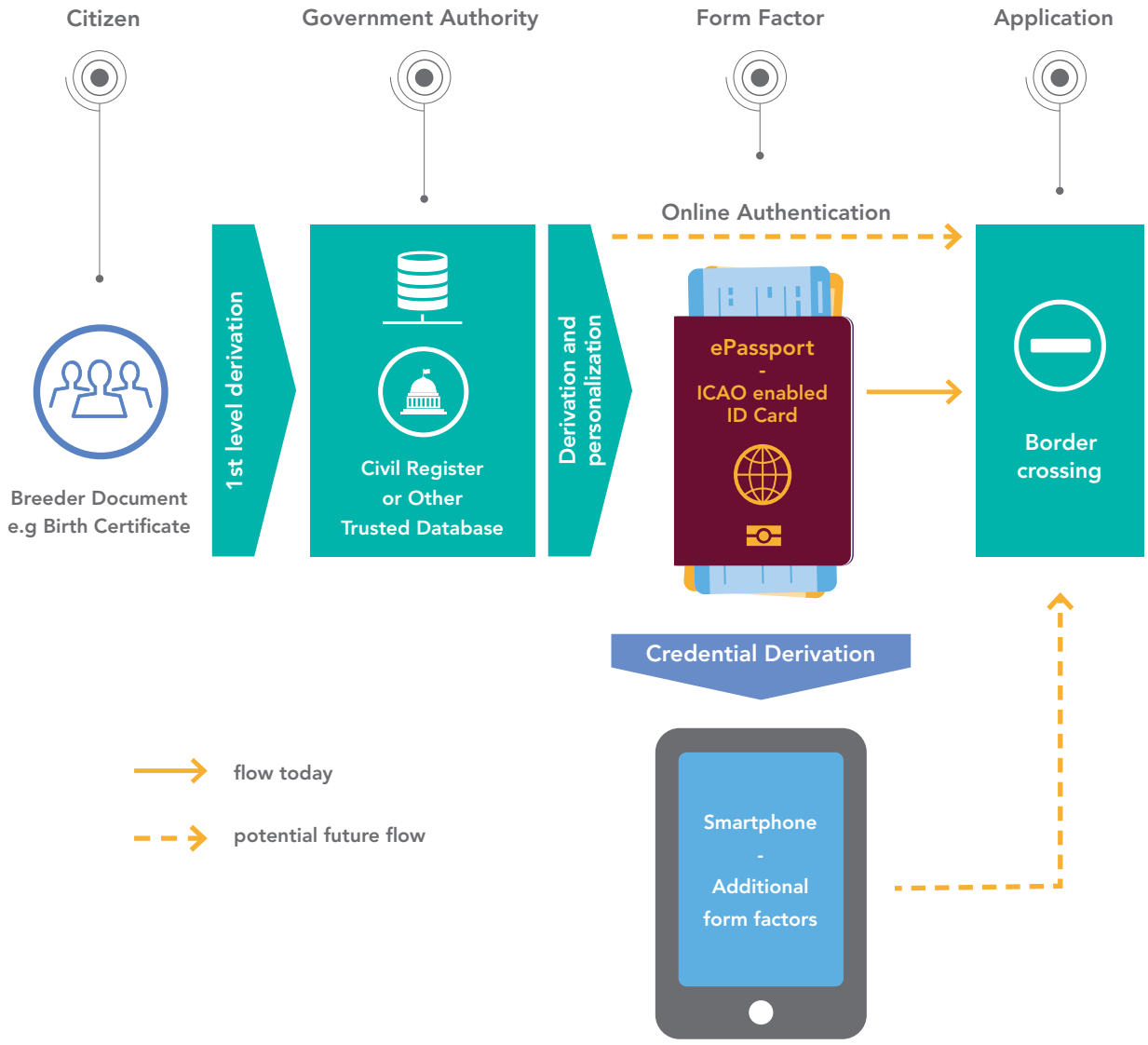
The arrival of ePassports has led to the development of other innovations, too. For example, when **ePassports** were first introduced, they were read by humans. Now, however, many border crossings use automated border control (ABC) gates, which offer a high degree of accuracy and speed, while enabling border control staff to focus on more security relevant tasks. Several thousand ABC gates are already in use worldwide, supporting many millions of ePassport transactions daily.

Here's how the process works today. Citizens provide proof of citizenship to a government authority. The proof of citizenship usually comes from what's referred to as a source or "breeder" document. In this case, the breeder document is often a certificate of birth or marriage. The government authority stores information from the breeder document in a civil register or some other type of trusted database. The government authority then derives a secure, personalized credential, in the form of an ePassport (or ICAO-enabled ID card). At the border, ePassports are checked for authenticity before citizens can complete their crossing.

In the future, a "virtual mobile identity" could be derived from an already issued government credential, such as an ePassport, and securely loaded onto a mobile device, such as a phone, a wearable, or a token. The secure credential would be stored temporarily, according to adequate security assurance levels. The ICAO 9303 NTWG (New Technology Work Group) is defining policies and standards for this type of virtual mobile identity. Another approach would be to have border crossing use online authentication that accommodate the infrastructure and policy procedures for pre-qualified citizens. Feasibility studies for these approaches are already underway.

Figure 1 gives a high-level illustration of how government-issued travel documents like ePassports or ICAO-enabled ID cards are created, administered and used today. The diagram also shows that, in future, the credential-derivation process could enable the use of mobile phones and other form factors, including online authentication.

Figure 1 - Border Crossing Application Showing ePassport (today) and Mobile Credential (future)



- **Physical Identity:** Actual Citizen
- **Digital Identity:** Electronic counterpart of Physical Identity
- **Credential:** Technical implementation to proof your Digital Identity
- **Form Factor:** Device carrying the Credential

MULTIPLE BENEFITS

The adoption of **ePassports** has created a highly secure, truly interoperable global infrastructure for international travel. Today's ePassports work at any border crossing equipped with an ICAO-compliant infrastructure. This alone is a big benefit to border-control agencies as well as the average traveler, since it means people spend less time waiting in line, and it's more convenient to go from place to place.

ICAO's ePassport standards have strengthened international security, by making it harder to steal identities, and by helping to prevent illegal immigration and trans-border crime. Having electronic travel documents makes it easier for airlines and government officials to clear low-risk traffic, and lets them identify problem cases more readily. The setup makes the enforcement of travel regulations more effective and more efficient.

The security mechanisms used by the travel document's integrated circuit (IC) make it much more difficult to steal, copy, or fake an official travel document, so there's less fraud. The government body issuing the document loads information about the passport holder onto the chip in a high-security environment, so as to ensure authenticity. The stored data is readable at a border crossing, to confirm the passport's authenticity, but is protected from being changed or copied. The IC is designed to resist attempts to steal, modify, or misuse the data, and ceases to work properly if physically tampered with.

Demand for stolen and forged passports is, unfortunately, at an all-time high, thanks in part to factors like the refugee crisis, the rise in international terrorism, and the increase in organized criminal activity, including human trafficking. The use of ePassports makes it harder to present doctored or illegally issued travel documents as the real thing, and helps reduce black-market trade in travel documents.

2. THE ICAO 9303 PROTOCOLS AND LOGICAL DATA STRUCTURE (LDS)

The average lifespan for any passport, electronic or otherwise, is from five to ten years. A lot can happen in that time, especially since technologies continue to evolve and new security threats continue to present themselves.

The goal for ePassport technology is to keep current with the latest capabilities and requirements, so the latest travel documents offer the strongest security, but without losing support for the legacy standards that cover passports still in circulation. This need to maintain backward compatibility has created a mixed landscape of in-place technology.

Every ICAO-compatible ePassport that's been issued to date uses the same format for programming and storing data on the chip. Following the ICAO-defined Logical Data Structure (LDS), the chip stores information as read only, meaning the data can't be changed once the travel document has been issued. The chip also "seals" the data to protect it from tampering. What can differ, however, is how the chip shares its LDS data with an authorized reader terminal. There are currently three generations of protocols, all recognized by the ICAO and based on the ICAO document 9303. Known as BAC, EAC, and SAC (see sidebar), all three generations of protocols perform the same basic operation of authenticating the chip and accessing its data, but each successive generation adds new mechanisms that make the transaction more secure.

THE 3 GENERATIONS OF ePASSPORT SECURITY MECHANISMS

BASIC ACCESS CONTROL (BAC)

Introduced by the ICAO in 2005, BAC is still used by the majority of ePassports in circulation today. BAC can store a high-resolution facial image, but doesn't offer dedicated protection for additional types of biometric data.

01

EXTENDED ACCESS CONTROL (EAC)

Developed by Germany in 2006 and recognized (but not mandated) by the ICAO, EAC builds on BAC to add dedicated protection for biometric data. The European Union made EAC mandatory for all ePassports in June 2009.

02

SUPPLEMENTAL ACCESS CONTROL (SAC)

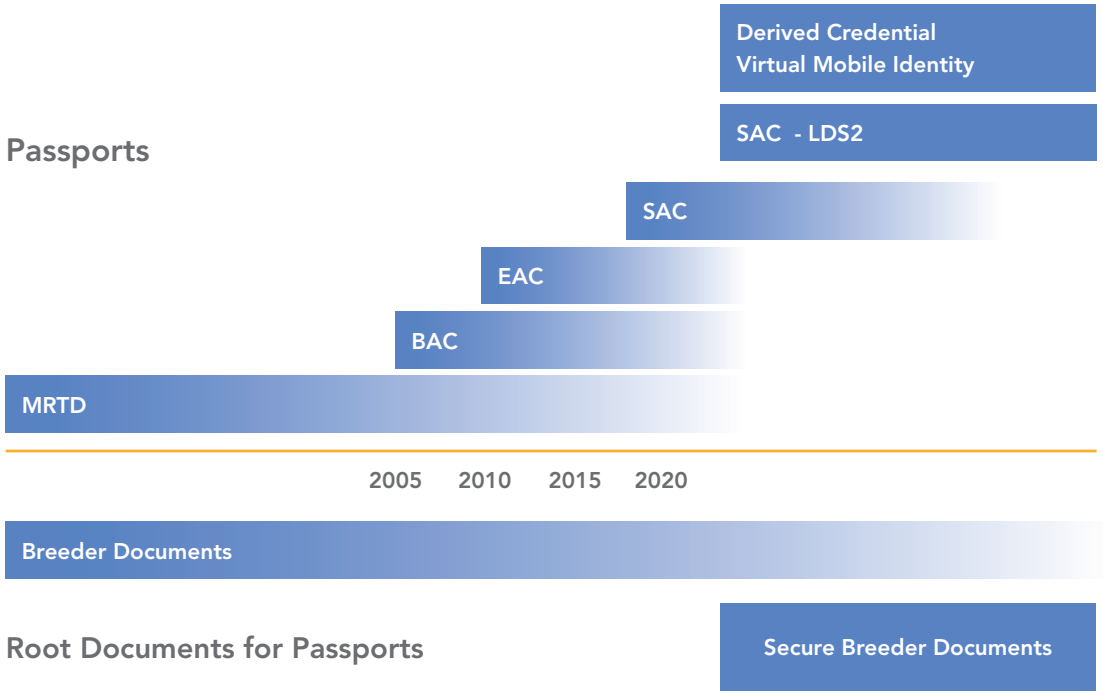
Introduced by the ICAO in 2010 as a supplement to BAC and EAC, SAC is upgrading both protocols. SAC supports biometric data, adds asymmetric cryptography for encryption, and simplifies key derivation with a six-digit Card Access Number (CAN).

03

The European Union has already transitioned to the latest SAC format, and many will follow their lead. But there are plenty of passports and locations that still use the earlier formats and will continue to do so for some time. For maximum interoperability, and to be sure automated border checkpoints can service the broadest user base, all three generations of protocols still need to be supported by border crossing infrastructures in the near term.

Figure 2 shows the evolution of passports and their associated breeder documents, starting with paper-based machine-readable travel document (MRTD) passport formats to the latest versions of ePassports and beyond. Within the next five years or so, new formats of ePassports are expected to come online, as are new types of breeder documents, issued according to a more secure and better-controlled process that includes security mechanisms that protect against tampering.

Figure 2 - The three generations of ePassport security mechansims currently in use



3. PASSPORT DATA BECOMES FULLY DIGITAL WITH LDS2

By introducing the **LDS format**, the ICAO created a platform for international interoperability and established a foundation for worldwide use of **ePassport technology**. The LDS format is a basic building block of ePassports, because it defines the fixed, read-only data structure on the chip.

At present, the LDS1 formats encompass an electronic version of what is commonly referred to as "page two" or the "data page" of the travel document. This covers the information that serves to identify who the traveler is and who issued the travel document. This information is, for the most part, static and remains true during the passport's lifetime. The rest of the passport information, relating to visas, travel stamps, and so on, is not covered by LDS1 formats. This kind of information is still physically entered after page two of the passport booklet.

Leaving the rest of the passport in a paper-only format has left a number of vulnerabilities in the document itself. The physical stamps used by each country can vary in their format, the ink they use, and the information they provide, and require time-consuming manual inspection. Perhaps more important, though, in terms of security and traffic management, the information provided by traditional stamps can be forged, stolen, or copied, and this adds risk to any border-control process. Also, paper-only information is not accessible to ABC inspection systems.

To eliminate these vulnerabilities and create a fully electronic passport, a new LDS is needed. A few years ago, the ICAO's NTWG commissioned a sub-group that has begun work on a new policy and technology framework. The new format is now known as LDS2. The target capabilities of LDS2 have been outlined in various ICAO documents and presentations.

LDS2 represents the next step for ePassports, because it will create an ePassport that can be updated with information as time goes by. LDS2 will be optional at the beginning, and will retain backward compatibility with the LDS1 formats, while adding a read-write function. It will extend the use of ePassports by adding applications that make it possible to store travel data (such as visas and travel stamps), along with other information, such as more advanced biometrics or special programs for frequent travelers.

Taken as a whole, these new features are expected to make the act of crossing a border easier, faster, and more convenient. At the same time, the enhancements offered by LDS2 will add further protections that strengthen the document's ability to deter counterfeiting, copying, and unauthorized reading or writing. The credentialing service supported by LDS2 reflects the latest advances in data protection, and as a result offers stronger, more resilient functionality, for smoother border-crossing operations.

With ePassports based on LDS2, the chip will be able to run several passport functions that increase efficiency, lower the administration effort, and add security. Here are some examples:

ELECTRONIC TRAVEL STAMPS

The stamps that show where a traveler has been, and when, will become digital. Electronic travel stamps will enable greater consistency, enhanced security, easier access to information, and faster viewing of key details. The electronic format will make it easier for countries to share information, for increased collaboration on cross-border issues, and will reduce the costs associated with designing, shipping, and storing physical stamps.

ELECTRONIC VISAS

The authorizations that let people enter and stay in a country will become digital, too. An embassy will be able to generate an electronic visa and add it to the chip, making it easier for people to get their authorizations in order. Adding the visa directly to the document reduces the need to rely on the databases that currently maintain this information, with the result that visa systems are less subject to network outages and connection errors, and can support third-party validation more readily.

ADDED BIOMETRICS

It will be possible to add a new biometric (such as a fingerprint or an iris scan) after the passport is issued. Support for post-issuance updates gives countries more choices in national policy, and lets them expand their approach to secondary biometric storage and trusted traveler programs. People who opt to participate in a fast-track program, for example, can add a biometric as part of their enrollment in the program. Also, updates don't have to be limited to biometrics. If a photo n eeds to change, a revised image can be added to the chip, with the result that fewer new passports need to be issued. There are fewer delays associated with changes, and facial recognition can be more dependable because it's more up to date. Storing the biometric data on the chip itself, and not in a backend database, gives the citizen a greater sense of control over personal information, and lets the passport act as a more complete token for identification.

Table 1 - LDS1 versus initial version of LDS2

	LDS1 formats	LDS2 formats
Read Only	X	X
Read/Write Capable		X
eTravel Stamp		X
eVisa		X
Updatable Biometrics		X

Table 1 shows the ways LDS2 will extend the capabilities for ePassports compared to LDS.

The LDS2 specification is nearing finalization and may be published as early as 2017. The ICAO is working with standards organizations, such as ISO, and ICAO member states to refine the processes that will enable global implementation for LDS2. The technical specification is being aligned with international policy, and technology companies are evaluating the requirements for new LDS2 chips.

For the LDS2 process to work, each issuing country will need to have bilateral country contracts in place, and will need to be prepared for the increased complexity associated with certification handling. At the same time, chip makers will need to produce ICs that have higher processing rates, larger memories, and faster cryptography speeds. This work is already underway, as semiconductor manufacturers move to smaller geometries and next-generation nodes for the Central Processing Unit (CPU), transition to non-volatile memories, which can access data faster, and implement improved crypto engines. Developers are also evaluating the use of Very High Baud Rate (VHBR) technology, to improve transaction speed in the application. However, since using VHBR also increases complexity and cost, the gains in transaction speed may not, ultimately, be worth the extra effort and expense.

4. PHYSICAL AND ELECTRONIC FORENSIC SECURITY ASSURANCE

Information in an **ePassport** is protected two ways: by the large number of physical security features present in the passport booklet, and by the electronic security features present in the passport IC. The physical security features of the booklet can be assessed according to different assurance levels and forensic procedures. The passport IC is validated according to ICAO 9303 protocols that support international compliance and document authenticity.

By and large, today's passport ICs offer more capacity and functional flexibility than the ICAO 9303 protocols call for. These extra capabilities represent a thus-far untapped potential to implement more advanced security features. This functionality could be used on a national or international level, depending on the implementation approach and the extent of international cooperation.

For example, passport ICs could support customer-specific commands that enable new forensic processes and security relevant assessments specific to the individual requirements one or more nations. The implementation of customer-specific functionality in the chip could introduce additional security and efficiency to the process of border management, and could deliver unprecedented document security and fraud prevention.

5. SECURE BREEDER DOCUMENTS

As described above, **breeder documents** are the physical evidence accepted by national authorities to establish a claim of identity. Traditional breeder documents are paper documents with limited or no security features. They are rather easy to temper or forge and represent a weakness in the whole life cycle of secure passports. This means it's possible for a person to use a counterfeit breeder document to apply for and receive a genuine, secure passport.

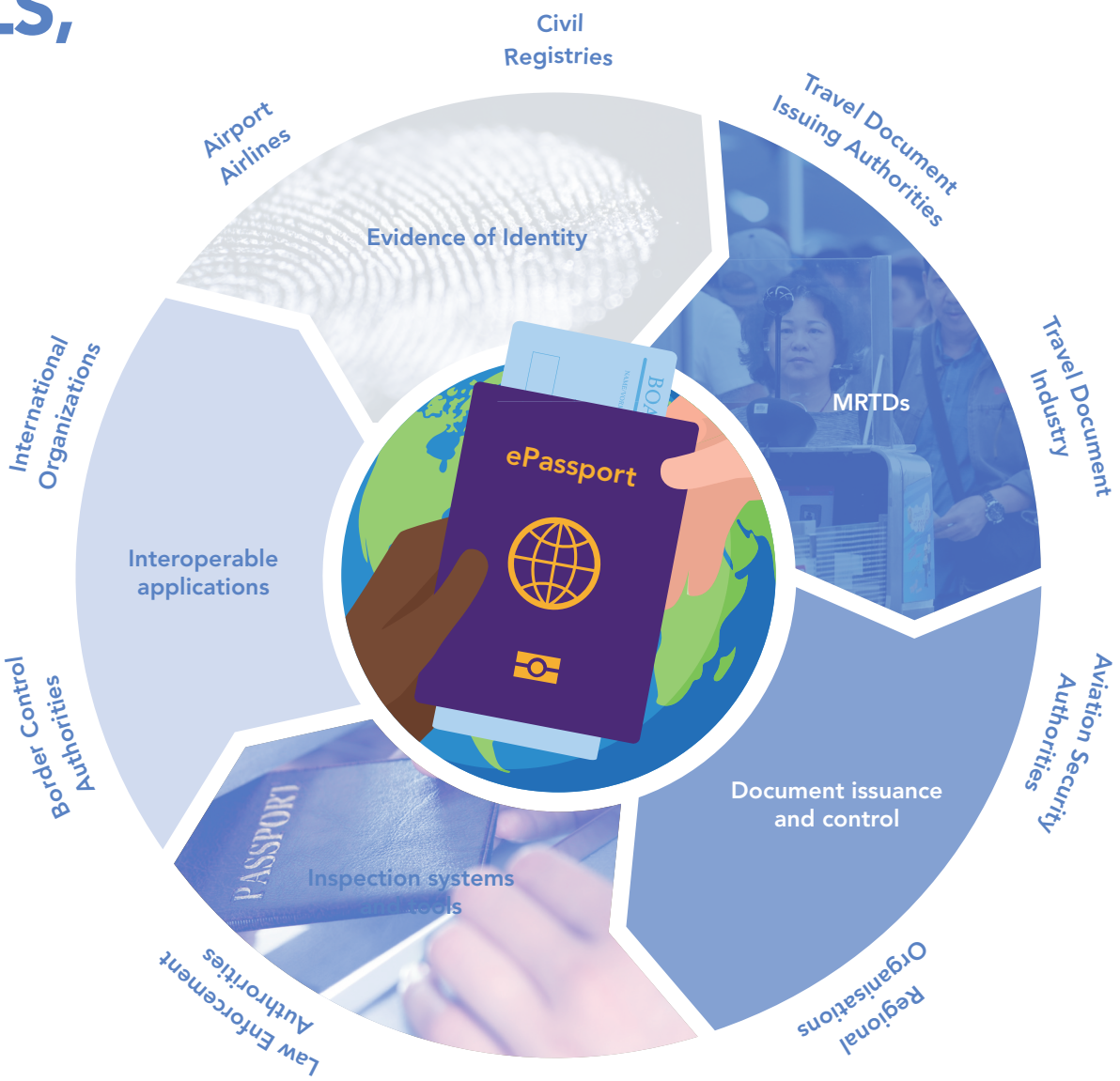
The underlying idea of secure breeder documents is to improve the document security and therefore to reinforce the confidence in the application process and issuance of passports. While some assurance approaches have been implemented in a few countries, they remain insufficient to provide breeder documents in complete security and trustworthiness at a time when this is increasingly necessary.

6. THE FUTURE OF SECURE CREDENTIALS, AND THEIR IMPLICATIONS

The ICAO vision for the "TRIP" Strategy makes border-control systems more secure, more intelligent, and more interoperable, and opens up the potential to do things like securely migrate credentials to other electronic devices beyond passports, including mobile phones.

As shown in Figure 3, the TRIP Strategy uses automated issuance, control, and inspection, along with electronic passports and interoperable applications, to create synergies within the travel universe. The concept connects everything from civil registers and state authorities with international organizations and private enterprises, including airlines.

Figure 3 - The ICAO "TRIP" Strategy -



Source: ICAO MRTD Report (Issue 3, 2013)

From there, it creates possibilities for even more options, including mobile and wearable formats that can record comings and goings, support special services for frequent travelers, integrate with commercial loyalty programs, and more. Here are some of the ways the TRIP Strategy could benefit travelers and border officials:

FASTER PROCESSING

Using multiple, advanced biometrics with reduced transaction times could enable walk-through border control that scans and authenticates a person in seconds, for faster processing and greater convenience.

SMARTER SERVICES

Having larger onboard memories could make it possible to store more than just basic data and travel visas. For example, passports could also log regional exits and entrances, for a better understanding of patterns and trends, and greater insight into individual threats.

BEYOND BOOKLETS

Moving to a secure yet all-electronic format makes it possible to translate functionality into just about any form factor. Government-issued credentials could be used as the accredited basic building block to facilitate credential derivation into a mobile phone, a bracelet, a piece of jewelry, or a "virtual" ID, for online use.

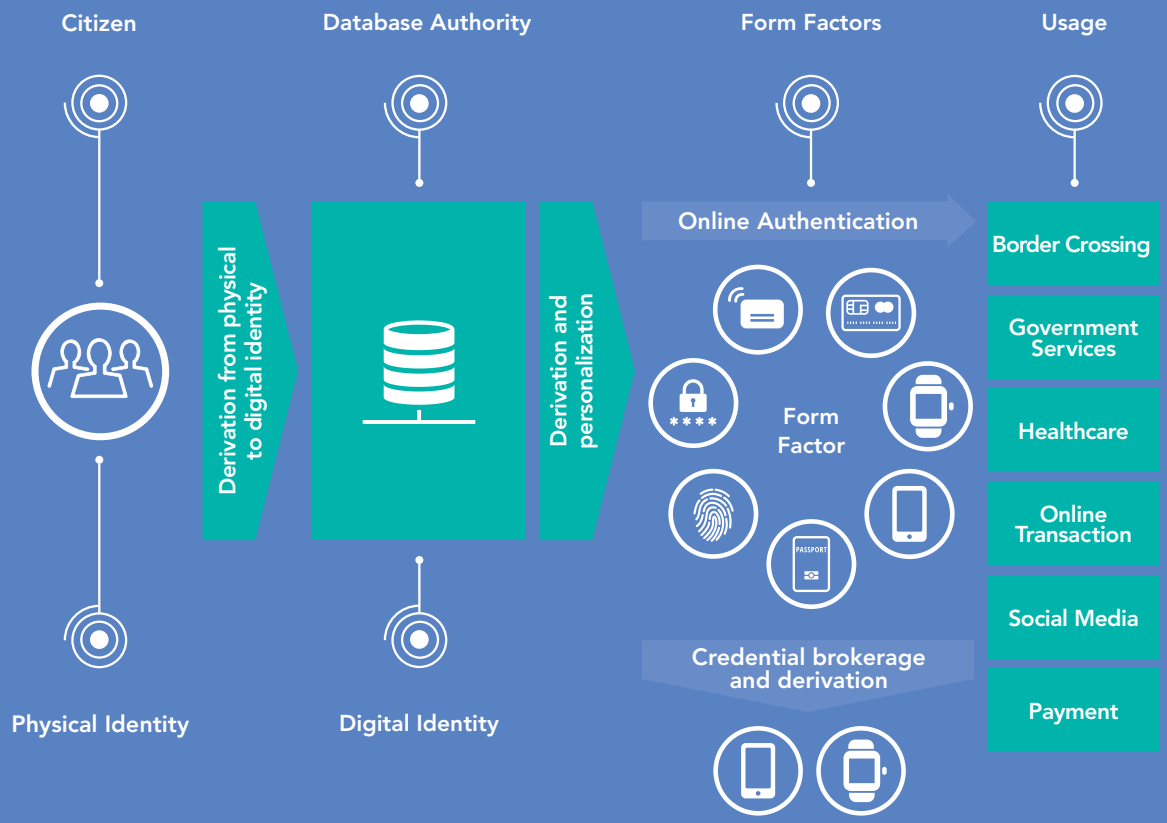
CROSSOVER APPLICATIONS

Advanced security mechanisms make the credential safer than ever, and let the credentials be used in other applications, beyond border control. For example, government-issued credentials could be used with other public-sector services, such as healthcare or tax payments, and could be used with private-sector products and services, such as travel apps from airlines and car-rental agencies.

Daily reports on stolen citizen data and hacked firewalls remind policy makers about their responsibility to ensure uncompromised citizen identity. The ICAO's work on future generations of passports and virtual credentials has broader potential beyond the passport itself. By placing the necessary credentials in an electronic format, identity documents like passports will be able to take on new functions, new form factors, and new applications, all while maintaining the necessary levels of security.

To understand how government-issued credentials might influence trends in electronic credentialing, it's useful to look at how security credentials are already being used **Figure 4** outlines today's most common applications for electronic security credentials, in border crossings and beyond. The basic process for credentialing is essentially the same for each application: a verified citizen provides data to an issuing authority (a government agency, a bank, a healthcare provider, etc.), and is issued a secure, electronic credential that can then be used to access various services, such as crossing a border, making a purchase, or getting medical treatment. Today's credentials come in many forms, ranging from tangible items, such as smartcards and ePassports, to more virtual formats, such as credentials used with mobile phones, wearables, or via online authentication.

Figure 4 - Sample Use Cases for Electronic Security Credentials



- **Physical Identity:** Actual Citizen
- **Digital Identity:** Electronic counterpart of Physical Identity
- **Credential:** Technical implementation to proof your Digital Identity
- **Form Factor:** Device carrying the Credential

The increased use of mobile derived credentials is likely to change the credentialing landscape. The next generation of credentialing applications offer the potential for crossover compatibility, with credentials issued by one organization being recognized by another. An **ePassport** could, for example, be used to authenticate identity for an online purchase. Some of these use cases are already in place and support (or will soon support) mobile formats, and others are still under discussion. The role that social media will play in the evolving ecosystem for credentials is still open.

The **ICAO TRIP Strategy**, and the rest of the ICAO's roadmap for ePassports, reflects this trend toward crossover use of security credentials. This ongoing evolution will introduce new considerations, especially in terms of how citizen information will be collected and used. There are important implications to consider when examining these new concepts, and several international groups have started looking at these issues. We summarize their concerns here, by presenting some of the questions being raised about how future ePassport applications will be implemented, managed, and regulated.

We don't offer definitive answers to these questions, or recommend particular approaches for addressing the concerns, but instead summarize the issues as a way to contribute to the dialog. We think that, by raising the somewhat philosophical questions about the future of identity, we can help meet everyone's goal of developing technology in a way that delivers the greatest benefit and transparency.

ARE GOVERNMENT-ISSUED CREDENTIALS THE ONLY OPTION?

Up to now, government agencies have typically been the ones to issue internationally-standardized and recognized credentials. But are government-issued credentials the only valid format? What about the other credentials people use in their day-to-day lives? Could an ePassport work beyond border control? The ability to create strong, protected credentials won't be limited to border crossing. Is there a way to consolidate the many credentials we use – to access government services, manage our bank account, or log into social media sites – so there are fewer credentials to issue and maintain? Can government-issued credentials represent the secure root credentials for private businesses across many applications? And can it be the trusted platform to authenticate people, without having yet the industry to invest into the same capability again?

DOES IT MAKE SENSE TO INVOLVE THIRD PARTIES?

With the trend toward outsourcing, is there a way to give private organizations the ability to issue credentials? How would these third-party credentialing organizations be regulated, to ensure compliance and uncompromised data protection? What would the requirements be for gaining authorization to issue credentials?

WHAT'S THE BEST WAY TO UPDATE CREDENTIALS?

What about adding new information as time goes on? The LDS2 format can accept new data, and is designed to keep documents up to date, but where should those updates come from? Social media collect a lot of data. Should social media be a contributor to citizen information, and used to create a credential?

HOW DO WE MOVE THIS BEYOND AIRPORTS?

Given the flexibility in form factors and the choices available for biometrics and security, how can we make sure that every border crossing – not just airports – supports the necessary technologies? Up to now, the ICAO has provided specifications and regulatory requirements, but their focus has traditionally been air travel. What about people traveling on foot, by car, or by boat? Can the ICAO charter be extended to cover all types of border crossings?

WHAT'S THE BEST WAY TO INTEGRATE NEW APPLICATIONS?

The trend toward integration and mobility opens up possibilities, including those described by the ICAO TRIP Strategy, to use ePassport credentials for other purposes. Is the ICAO the best choice to oversee the integration of other features, beyond travel documents? Would it be beneficial to have a central, international agency overseeing how ePassport credentials can be integrated with other services?

SHOULD THERE BE A SYSTEM FOR UNIQUE PERSONAL NUMBERS (UPNS)?

The United Nations is working with governments to create consistency with national registries. Does it make sense to elevate this above the national level, with the creation of an international registry that assigns a UPN to every person on the planet? Is it even possible to get widespread support for such an idea? If the UPN became a part of an ePassport credential, then who would be responsible for assigning UPNs and ensuring the UPN data is always current? How might national registries align with an international one?

HOW MUCH INFORMATION IS ENOUGH?

Future versions of ePassports will be equipped with larger memories, capable of storing more than they do now. What data might we gather, who might use it, and for what purpose? Are there applications, beyond security, that border-control services could support with this data? Could it be useful in studying trends in migration or medical conditions? Or might it be used to help find people in emergencies? How can we ensure that the information we gather is only used for beneficial purposes?

WHAT ABOUT CONVENIENCE FOR CITIZENS?

Much of the discussion about ePassports, identification, and credentialing, centers on the ways that border-control systems can be made more intelligent and more secure. But what about the citizen's point of view? Can ePassports follow the same path as other eGovernment programs, which aim to make it easier for people to interact with government services? Is there a way to integrate travel documents with other citizenship documents, such as drivers' licenses, healthcare cards, and so on? Can we realize the vision of having one base identity credential to access all these services?

DERIVED SECURE CREDENTIALS ON MOBILE PHONES?

Will derived secure credentials and associated life cycle management be supported by NFC and the secure element of a mobile phone? Will there be international standards to define and regulate how the mobile phone secure element can be used for secure credential management according to highest assurance levels?

7.THE VIEW OF A TECHNOLOGY PROVIDER

The ICAO policy for international border crossing can be seen as a major advancement in the way we create and use credentials on a global scale. At the center of the ICAO approach is the idea of integrating a chip into the passport, thereby making it both a paper-based and digital document, with physical and electronic security features.

For more than 20 years, chip-based electronic credentials have proven their worth when it comes to storing and managing private information. We admit to having a bias. NXP is the number-one supplier of chip-based solutions to eGovernment, and we lead the ePassport segment. Of the 120 ICAO member states that issue ePassports, 95 of them have qualified our technology. It should come as no surprise, then, that we support the continued use of chip-based security.

IN SUPPORT OF SILICON

Perhaps more important than our financial stake in silicon, though, is the fact that, from a security perspective, chip-based security solutions are working, and working exceptionally well. NXP's SmartMXTM with IntegralSecurity architecture, used in all our ePassport solutions, is a chip-based approach that is certified to the highest security rating (CC EAL 6+). It has been deployed in eGovernment in more than 1.5 billion secure IC solutions since 2005, and is used in some of the most sensitive security applications in existence, yet has never been, in its many years of widespread use, successfully hacked.

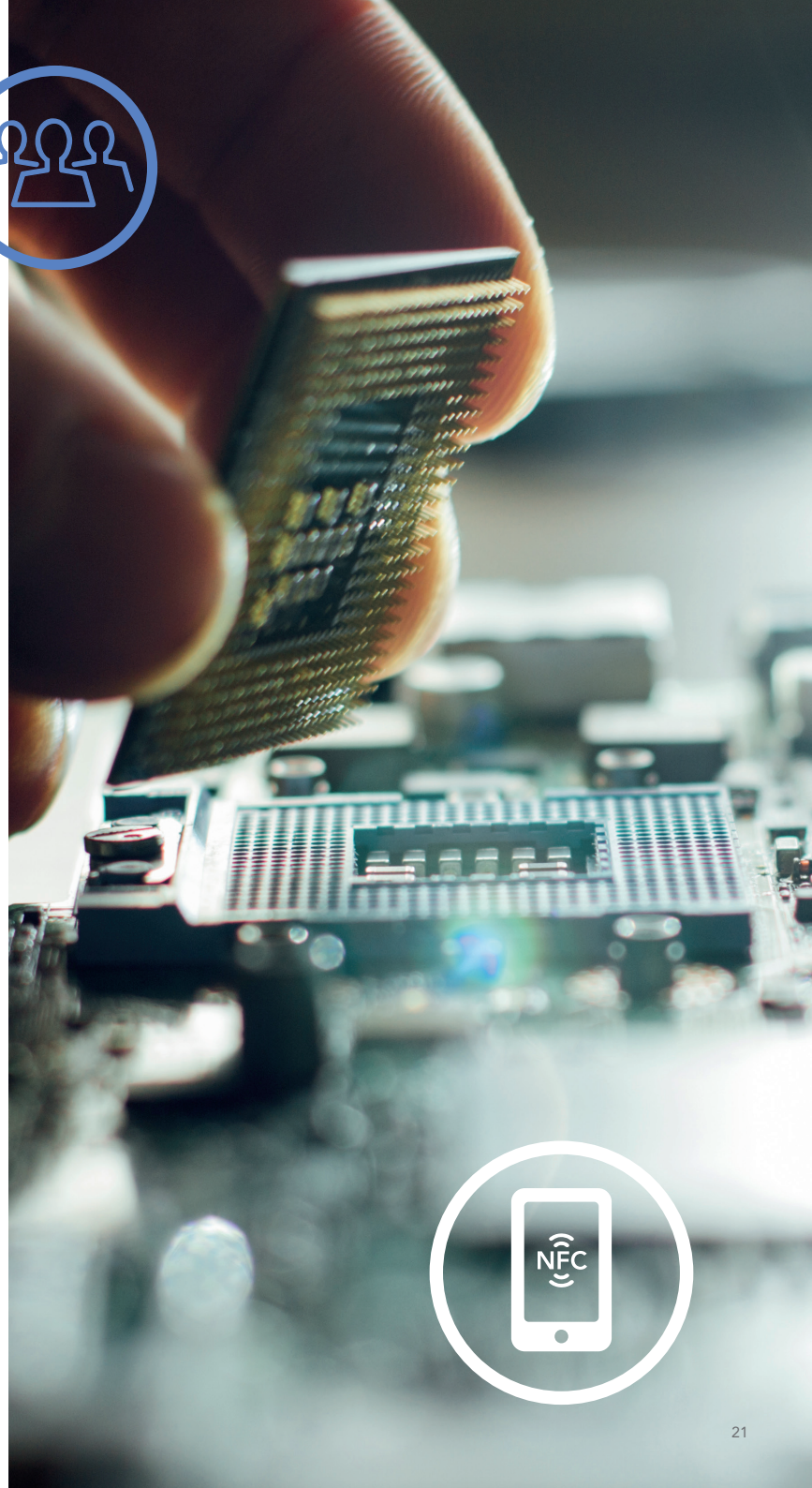
Our commitment to secure microcontrollers has yielded other innovations that reinforce the security architecture, creating an even stronger set of features relevant to ePassport and other applications. For example, our Physical Unclonable Function (PUF) is a patent-pending feature for electronic forensics that essentially gives each IC its own unique digital fingerprint. Our unique FlexMem format for nonvolatile memory provides faster access to securely stored data, while facilitating a high degree of flexibility. We pioneered the use of MOB contactless modules, which enable high-volume production of ePassport chips while protecting them from mechanical stress, environmental conditions, and security attacks, and recently introduced the MOB10, which makes it possible to add more security layers while producing a thinner, more robust polycarbonate inlay that enables use in the passport's data pages.

Contactless ISO 14443-compliant smartcard technology is one of the world's most widely used technologies, powering today's ePassports, eIDs, bank cards, and high-security access cards. It's fast, remarkably energy efficient, and proven secure. Contactless smartcard technology also provides seamless interactions with other electronic devices and form factors, as well as the electronic inspection infrastructure. Building on the experience gained from global deployment of contactless secure microcontroller technology in many mainstream applications, developers can be assured of a smooth implementation, and have a full ecosystem of suppliers to choose from.

NXP LEADERSHIP IN ID

As the number-one supplier of silicon solutions for eGovernment, with a track record of substantial contributions to the secure identification business in general, we have a unique perspective on security credentials and where they're headed.

- More than two decades spent collaborating with governments, authorities, and standards bodies to help guide the future of identification, interoperability, and security.
- Leading contributions to international standards, including ISO/IEC 14443, NFC, ICAO 9303 plus LDS2, EMVCO payment, and Common Criteria Security Certification.
- Commitment to secure microcontroller platforms, with ongoing evolution of the SmartMX family, which has been recognized for its benchmark approach to security, performance, and flexibility.
- Commitment to secure operating platforms, with the industry-leading JAVA OS, a global identity and mobile transaction solution.
- Consistent introduction technology breakthroughs, including secure, robust MOB modules, which are now the de-facto standard for smartcards, ePassports, and other electronic documents.
- Inventor of NFC (Near Field Communication) technology and leading supplier of secure element solutions into mobile phones.
- Deep expertise in secure credentialing, with Trusted Identity Management Solutions (TIMS) for flexible government credentialing services, including virtual mobile ID and online biometric authentication.



8. SUMMARY

The technologies used to enable safe border crossings continue to prompt discussion and raise questions about what, exactly, we mean by privacy, security, and even identity itself. The decisions we make, as we move ahead with border-crossing technologies, have far-reaching implications.

The potential benefits of future ePassport technologies come with challenges that will take time to address. Developing, testing, and refining the technology itself is just one aspect of the process – there is also work to do in terms of politics, breaking down barriers, sharing information, reigning in costs, and adding ease of use. From our perspective as a technology company, however, one thing is certain: chip-based identification will continue to be a fundamental building block of modern, future-proof security solutions.

NXP's prominence in the ePassport sector, along with our leadership positions in NFC, mobile transactions, payments, and the Internet of Things (IoT), make us a key stakeholder in the future of identification technology in general. We are working with other industry stakeholders to evaluate the technologies and policies required for the deployment of future border-crossing and identity solutions.

We understand that developing ePassport technology (or any technology for secure credentialing, for that matter), requires us to view the task not just as technologists, but as citizens, too. We firmly believe that the digital era rests on how we evolve secure electronic credentials. To ensure that evolution meets everyone's needs, we're encouraging all stakeholders to consider where ePassport technology and secure credential services might take us, so we can successfully design for whatever we want to come next.

To learn more about NXP's approach to silicon-based credentials and credentialing services, and the future of ePassports, visit: www.nxp.com/smartgovernance.

We welcome your opinion and invite you to contact us at peter.schmallegger@nxp.com.