



ICAO LITE :

**Addressing the huge e-ID
market with a product
combining ICAO
features, versatile
architecture and
low entry cost**

driving trust **inside**
SECURE

www.insidesecond.com

CONTENTS:

About the Authors:.....	3
Carloman Grelu, PHD.....	3
Bertrand Moussel, MBA.....	3
Executive Summary.....	3
Analysis of the Current ID Market.....	4
Mega-trends.....	4
Classes of applications.....	4
Early deployments.....	5
Identification ecosystem.....	6
Requirements for non-travel applications.....	7
Compliance with ICAO workflows.....	7
ICAO standard data group definitions.....	7
Chip lifecycle.....	7
Partitioning the memory between static, signed data and variable data.....	8
The ICAO-Lite document value proposition.....	9
Price positioning versus other solutions.....	10
Full standards compliance.....	10
Efficient photograph storage.....	11
Match-On-Chip option reduces risk of stolen checking stations.....	12
Adding value to documents and processes.....	13
Broader usage than travel.....	13
Universal reading of static and variable data.....	13
Reading and checking with NFC phones.....	13
Multi-step checking: visual, chip read, remote server access.....	13
Remote ID checking via Internet, NFC phones or USB keys.....	13
ROM-based applets for managing variable data.....	14
File manager and BAC and EAC mechanisms.....	14
E-Purse.....	14
Match on chip.....	14
Other applets.....	15
ISO 15693 compliance for convergence with access control and ticketing.....	15
Convergence with payment cards.....	15
Consequences for the document definition.....	15
Chip size.....	15
Example of an ICAO-Lite ROM and EEPROM structure.....	16
Future evolution.....	17
E-citizen documents and e-signing.....	17
Match on chip for Internet remote access, travel cards, etc.....	17
Extending use to semi-private and private entities.....	17

ABOUT THE AUTHORS

Carloman Grelu, PHD

Carloman Grelu is a regional sales engineer at INSIDE Secure focusing on secure identity and e-documents. He joined the company in 2006 as product engineer, and was involved with validating the company's first NFC silicon. Since then, he has taken on greater responsibility for developing INSIDE's secure documents and identification products, and has been active in creating a new ID business line. Prior to INSIDE, he was at STMicroelectronics' R&D center in Crolles, France. Mr. Grelu has a PhD in microelectronics from University of Lyon, France.

Bertrand Moussel, MBA

Bertrand Moussel is responsible for INSIDE Secure sales in Europe and Latin America, and leads the company's efforts in the global ID market, focusing on growing new opportunities in public-sector organizations for the company's ICAO-Lite solutions. With an extensive background in smartcard and IT technologies, Mr. Moussel has held a variety of executive positions prior to joining INSIDE. He served as a board member for RENAVE, Mexico's outsourced vehicle identification data repository. He led numerous smartcard initiatives in Argentina, Peru, El Salvador and Mexico, and served as managing director of SEDIR, a GEMPLUS subsidiary dedicated to building and integrating ID solutions for numerous Latin American countries. He also launched and built GEMPLUS' Latin American business. In 2005, he joined Oberthur Card Systems to lead the banking and transport business units, and was appointed South America Director.

EXECUTIVE SUMMARY

The electronic ID market started about ten years ago with the adoption of the ICAO standard for travel documents (e-Passports). Prior to that, field use of smart chips in plastic cards for electronic ID was based exclusively on proprietary implementations. The ICAO standard provided the first real structure for this market.

Although the ICAO standard's benefits are undeniable, the electronic passport itself cannot be extended to other electronic ID applications because the entire smart-chip memory is fixed and sealed at issuance. This is a shame because many governmental electronic ID applications could benefit from this standards approach. The calculating power and secure storage capabilities of smart chips could be used to simplify, automate and protect citizens in their daily lives, and reinforce the control government agencies wield in many crucial areas such as healthcare, social benefits, voting and others.

This white paper describes in detail the "ICAO-Lite" approach, which can be summarized as combining, in one low-cost ID document, the robustness and knowledge gained from ICAO workflows with the versatility of the smartcard industry and its ability to manage secure transactions and information.

We will first present the requirements of future ID documents, and then describe the benefits of dividing available smart-chip memory between fixed demographic data and securely managed, variable data. A description of the ICAO-Lite chip is then provided, with special attention given to security issues, different possible physical form factors and biometric elements. We will show how the concept of an "ID applet suite" can bring real value to government-related issuers by simplifying and streamlining their various application deployments. At the same time, the versatility of the platform will allow ID system integrators to focus on innovative solutions for the ID market.

We believe ICAO-Lite solutions will expand and diversify while maintaining a solid, standardized, common platform of interoperability, and will extend beyond the public arena to adoption by semi-public and even private bodies.

With its unique combination of standards-based approach and powerful tools for development, we believe the ICAO-Lite concept will prove the right solution for many of the identification issues facing a variety of organizations today.

ANALYSIS OF THE CURRENT ID MARKET

Mega-trends

Following the events of September 11 in the U.S. and the widespread focus on increased security, as well as increased cross-border travel by individuals, the need to develop more stringent and efficient methods of identification became obvious. This process started with the creation of more secure travel documents in the form of e-Passports, which resulted in the first international standard in that field, the ICAO (International Civil Aviation Organization).

Travel documents, including not only e-Passports but also some general-purpose identification cards used as travel documents, need an international standard as a core feature to enable citizens of one country to travel to another with seamless identification flows. The ICAO standard has been gaining acceptance over the past five years, and has helped build significant confidence in the electronic identification market. By mid-2009, more than one hundred countries have committed to issuing e-Passports by 2011, which could create some hurdles when travelling for citizens of countries not issuing these electronic documents.

Beyond travel documents, which focus on the single, primary task of crossing an international border, governments are looking to adopt more efficient, accurate identification methods as they try to cope with some general mega-trends. All countries, both developed and emerging, have an urgent need to control their healthcare expenses, especially in economies with aging populations. Profiling the population and distributing social care equitably is required everywhere, and typically includes sending acknowledgment receipts and statistics back to the agencies in charge. Voting is another cumbersome process for countries that want fast, accurate reporting of results, as well as for countries voting for the first time and deploying polling places in remote areas. Governments also need better identity methods for driving licenses, residence permits and some new initiatives in "e-citizenship."

The latest mega-trend in the shift to electronic ID documents is the emergence of the multi-application approach, in which a single document serves multiple purposes. This approach holds much promise, and some European countries have already starting using it, but it still has a long way to go.

Demand is growing for ways to ensure citizens and individuals are identified accurately in order to better manage their rights and obligations for voting cards, social benefit cards, healthcare cards and more. At the same time, there is an increasing demand for greater efficiency in managing and processing the identity interactions. Because of these trends, the use of electronic-based documents has become more accepted, and represents one step toward an answer to this global quest for more security, more throughput and more accuracy.

Classes of applications

2008 global smart card shipments million units	Memory	Microprocessor
Telecoms	380	3200
Financial services-Retail-Loyalty	30	650
Government-Healthcare	250	140
Transport	160	30
Pay TV	-	100
Others (including Corporate ID)	80	65
Total	900	4185
TOTAL	5085	

Source Eurosmart, données d'Avril 2009

Because of their standardization and popularity, ICAO e-Passports have been the main driver of integrated circuit or "chip" use in the identification market in 2009.

The table below, published by the analyst firm Eurosmart, shows chip use by government-run identity applications, split between memory and microprocessors, reached a total of 390 million units in 2008. This level is approximately two thirds the size of chip use in the payments market, and is already the third largest market for chips in the smartcard industry.

What is more remarkable is that government-run identity applications are already the number one market for contactless chips, at 260 million units, more than twice as large as the second place payments market (see next table below). The primary driver of this has been the e-Passport, which accounted for nearly 60 million microprocessor units in 2008 and is accelerating in use. This high-value market is shaping the identification industry, not only in component use, but also in terms of service, issuing and reading infrastructures.

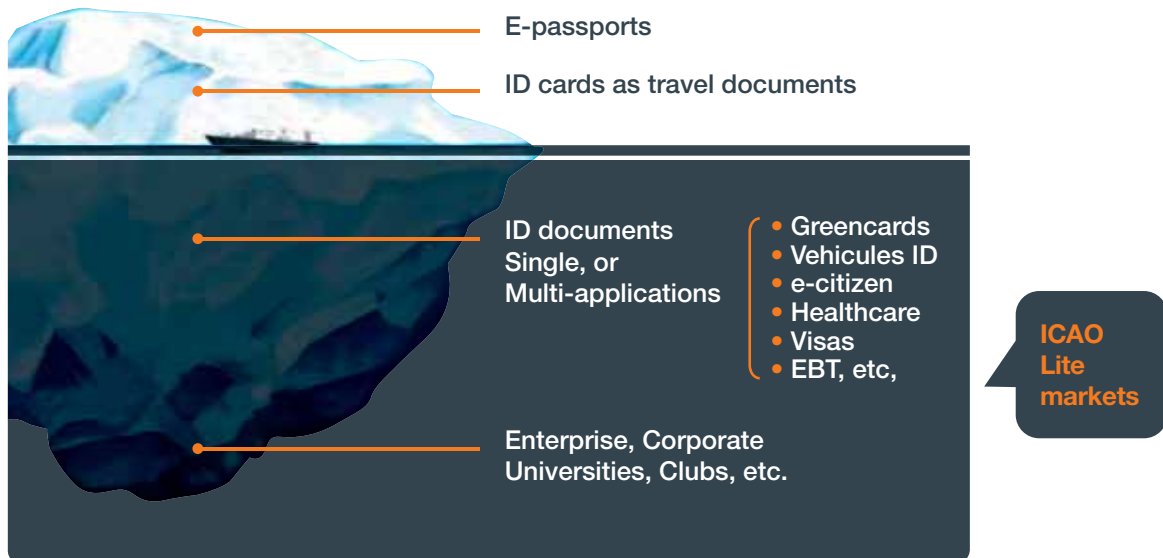
In addition to the contactless microprocessors used in e-Passports, we see 80 million contact-type microprocessor chips shipped, signaling important new applications of these devices in driving licenses, healthcare IDs and some multi-application documents. These have been issued initially using contact technology for compatibility with existing infrastructures (PC readers, kiosks, etc.), and, in the medium term, may migrate to contactless technology for reliability and cost reasons.

Finally, 250 million memory chips have been issued (including 200 million contactless), which is testimony to the numerous initiatives in this market outside the e-Passport application.

2008 secure contactless shipments million units	Memory	Microprocessor
Financial services	-	100
Government - Healthcare	200	60
Transport	160	30
Others	50	30
Total	410	220
TOTAL	630	

Source Eurosmart, données d'Avril 2009

Totalling the use of both contact and contactless integrated circuits by government for non-e-Passport identity applications shows that 330 out of 390 million chips in 2008 were already being used in "below-the-water" applications, not as highly visible as e-Passports. Like an iceberg, 90 percent of the chip volume is unseen because it is scattered across different geographies and varieties of applications, including driving licenses, healthcare cards, electronic benefit transfer (EBT) cards, residence permits, vehicle IDs and others.



Early deployments

Chip-based identification documents have existed for the past 15 years, starting in Mendoza province, Argentina with the first chip-based driving license in 1994. That application was already designed to manage value-added data, such as the insurance company name, the owner's name and address and the possibility to record infractions. By the late 1990s, deployments of other applications appeared in some emerging countries, such as to identify vehicles in El Salvador, and to identify military personnel in Peru. At the same time, some very well thought-out projects were developed in Western Europe, such as the French and German healthcare cards.

These early deployments clearly showed the benefits of using chips to combine the security of tracking and matching individuals with additional variable data that could be written and modified as needed. The CONASUPO (Compañía Nacional de Subsistencias Populares) project, for example, deployed more than five million cards to mothers of low income families in poor states in Mexico. The mothers were entitled to receive a certain weight of

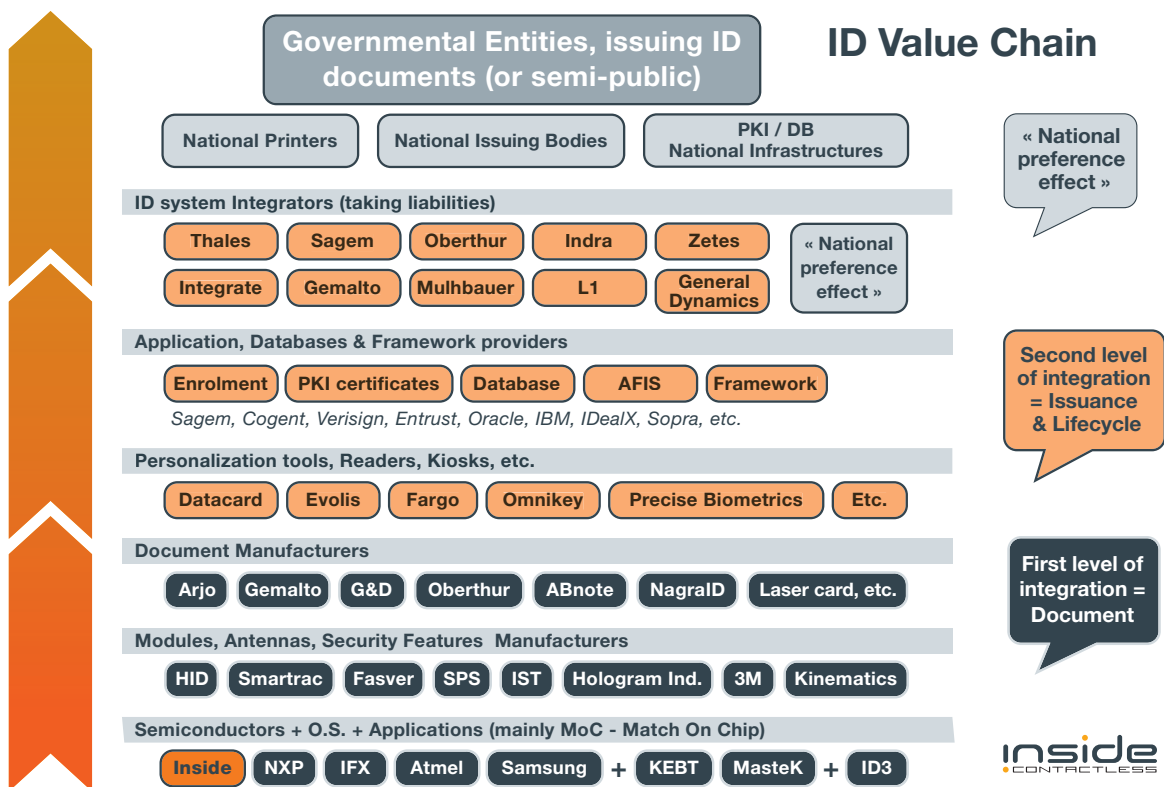
tortillas and volume of milk per month. This monthly food distribution depended on the number of children, and the mothers also needed these cards to enable their children to get vaccinations and attend school. Because many of the distribution sites, hospitals and schools were not online, this program was managed locally by enabling handheld readers to change data in the ID cards' chips. If needed, these readers could also upload statistics necessary for the countrywide monitoring of the program. This early example very clearly showed that using chips could increase the level of security over simple barcoded documents, as well as the additional value of the chip in managing the program.

Identification ecosystem

Compared to the SIM market, the identification ecosystem has many more participants. In the SIM market, scale drives down costs, and many transnational operators use the same devices and services across their territories. In identity markets, government data and legal restrictions, including the involvement of state-run printers, has caused the number of players to multiply.

An ID integrator and a document manufacturer are necessary to build a successful solution. These players can be local or global, and may choose from among many technology vendors, module and inlay providers, applet developers and service providers (for personalization or PKI infrastructure, for example) to build a solution.

The figure below, courtesy of INSIDE Secure, illustrates the mapping of the different players in the identification ecosystem.



Importance of ID integrators and Local Manufacturers & Bureaus

In many countries, the state-run printers and local personalization bureaus have been revitalized in order to cope with some of the manufacturing steps and personalization of e-Passports. Governments have made large investments in those local public companies, and public-key infrastructures have been established. These costs are not negligible, and the number of e-Passports issued per year rarely justifies this level of investment, which has been done under the pressure of ICAO standardization and the will to preserve national independence. Once these investments are made, particularly to establish the national public-key infrastructure, it is reasonable to ask how best to leverage them for broader usage. Issuing ICAO-Lite documents is a reasonable answer to this question.

Additionally, many countries also are embracing the EMV migration currently underway in the payments market, fostering the emergence of local integrators able to deal with smartcard projects. All this knowledge, increasingly rooted locally and ready to be exploited, is an important ingredient for successfully deploying ICAO-Lite applications.

REQUIREMENTS FOR NON-TRAVEL APPLICATIONS

Compliance with ICAO workflow

Building upon standard ICAO workflows is very important to the ICAO-Lite approach, as it preserves the interests of all the parties involved in issuing ID documents and the rest of the identity lifecycle. It not only maintains the potential to seamlessly migrate to a fully compliant ICAO document at some later time, but also ensures all the benefits of adopting a worldwide standard.

State-run printers and personalization bureaus have already invested time, training, consultancy and more in the issuing workflows, and have achieved self-sufficiency in these processes, which is crucial for sovereign independence as well as for economic reasons. Dealing with ICAO standards prevents any proprietary software or personalization process from escaping the full control of the governmental agency in charge of issuing national ID documents.

At the same time, the ID checking workflows need to be completely standardized to avoid any proprietary blocking “hooks”. The entire reader infrastructure, maintenance contracts and software development will then be standardized, and the government can have confidence that any ICAO-certified reader purchased anywhere will also be able to read ICAO-Lite ID documents and check their authenticity without modification. Issuing agencies can leverage the experience and investments of their e-Passport-issuing colleagues, and possibly share some equipment.

ICAO standard data group definitions

The logical data structure (LDS) for storing personal data and the means to access to it are defined by the ICAO standard:

- Data is stored in an ISO 7816-4-based file system.
- Data is split into data groups (DG), and each group is stored in a transparent file (i.e., DG1=MRZ data; DG2 = facial image).
- In each data group, data is BER-TLV encoded.
- One elementary file (EF.COM) contains LDS information and a tag list.
- One elementary file (EF.SOD) contains data integrity and authenticity information.
- Only DG1, DG2 EF.Com and EF.SOD are mandatory.

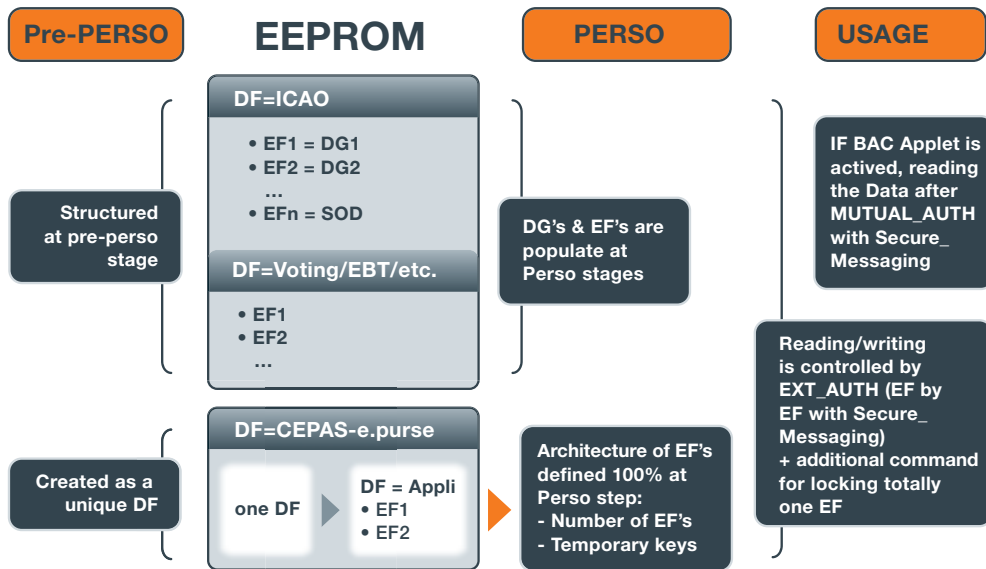
MRZ is the ID document’s machine readable zone where personal data is printed (name, surname, date and place of birth, document type and number, etc.). The correct data encoding and correct storage format are defined in the various standards documents (BSI test plans), and are certified by independent laboratories (Layers 6 and 7).

Perfectly matching the ICAO standards is an absolute prerequisite for any ICAO-Lite issuing project.

Chip lifecycle

The lifecycle of a chip for an ICAO-Lite application must be completely standardized. The various steps are summarized below.

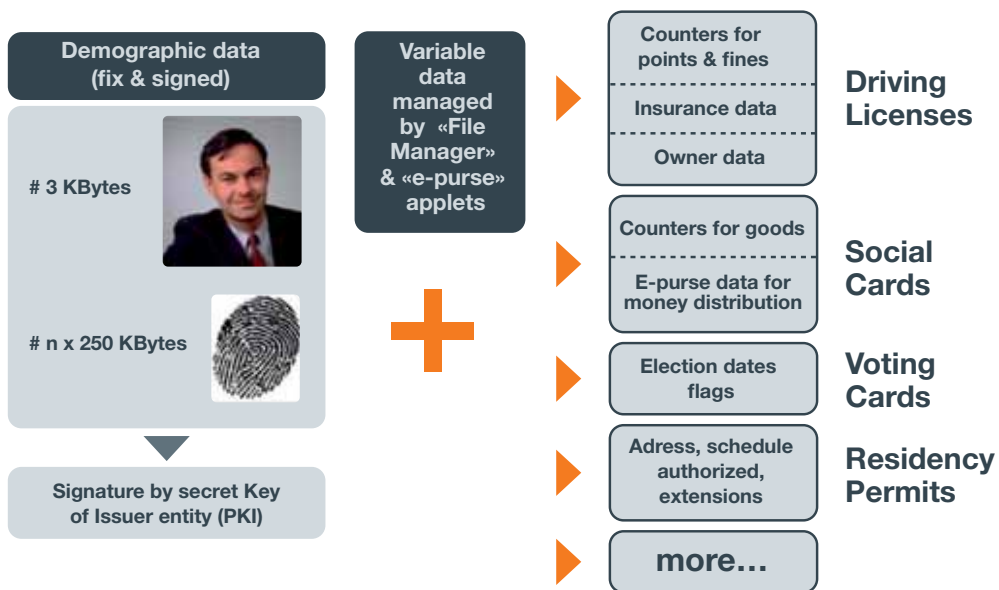
At the pre-personalization step, the memory is partitioned between the different dedicated files (DF). At the personalization step, the elementary files (EF) are populated with the information from the ID document holder according to each DF. In current usage, different data from the various parts of memory will be accessed according to the applicable security rules.



Partitioning the memory between static, signed data and variable data

The ability to partition the chip's memory is the entire basis of the ICAO-Lite value proposition. It means that the issuer of the ID document can define how the EEPROM memory is divided between the static demographic data, which will be signed later with the issuer's secret key, and other variable data outside the perimeter of the "to-be-signed" data. Because of this design, it is possible to construct ICAO-Lite chips that combine the ICAO signed data with points, counters, flags and other kinds of data that change during the lifecycle of the document and its interactions with readers and events. This opens the door to an endless number of possibilities, including:

- Driving licenses that can manage fines and insurance data,
- Social benefit cards that can manage statistics, counters and a small e-Purse,
- Voting cards that can manage the vote registration and flags and
- «Smart» residency permits and other types of national documents.



The ICAO-Lite document value proposition

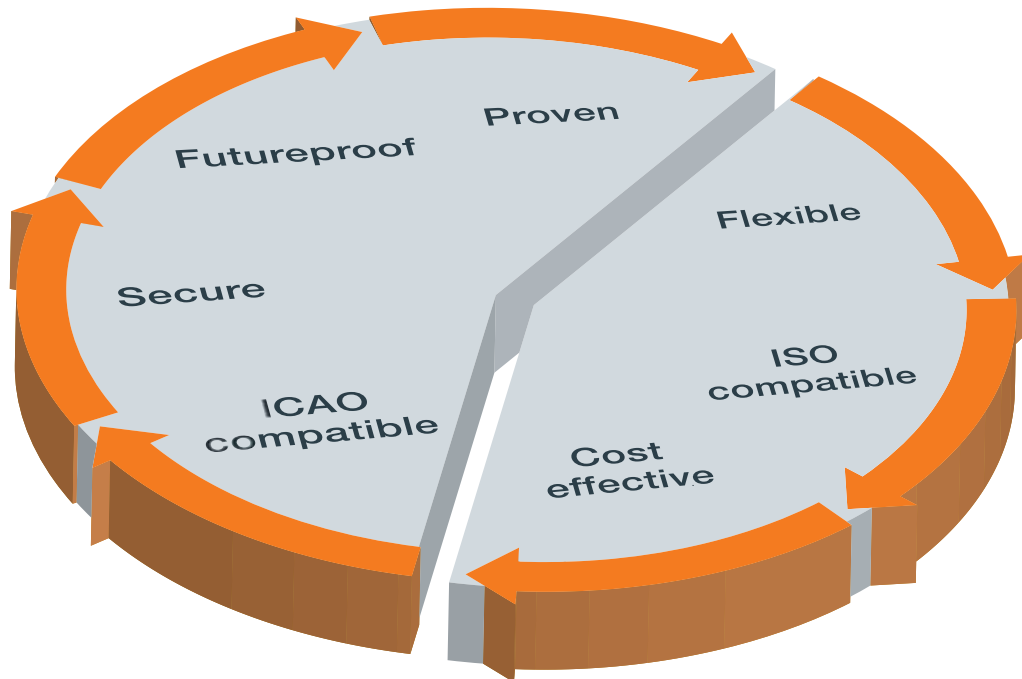
ICAO-Lite electronic ID documents offer important benefits to the various ID ecosystem stakeholders, especially the document holder. The ICAO-Lite solution is cost effective, and provides a migration path from non-electronic ID documents and fully compliant ICAO documents and solutions. The low cost of ICAO-Lite contactless microprocessors is due not only to the reduced memory size, but also to the economies of scale resulting from the huge volume of these devices employed by the banking industry, especially in the U.S., where chip manufacturers have already delivered more than 120 million units. ICAO-Lite also provides a viable migration path out of closed loop solutions (secured, hardwired logic memory based on proprietary cryptography).

The central concept of ICAO-Lite is to provide standardization and repeatability by basing its fundamentals on standards:

- A hardware platform designed to support ISO14443B-4 contactless communication protocol; allows the use of NFC for low cost mobile readers.
- A data structure compliant with ICAO recommendations; simplifies personalization and control of the document.

Moreover, the split memory usage (static, ICAO-signed data and variable data) gives document issuers flexibility to develop and load value-added applications onto the platform. Data cohabitation and integrity is guaranteed by the microprocessor and memory management unit.

Importance of ID integrators and Local Manufacturers & Bureaus



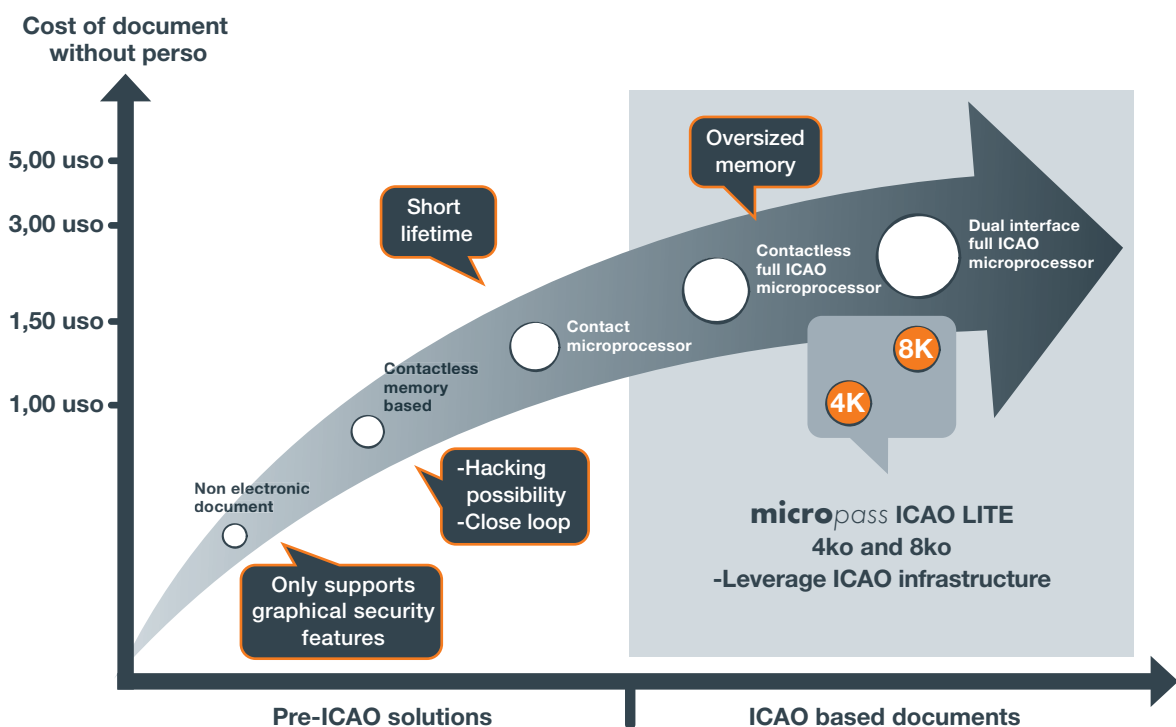
Price positioning versus other solutions

Identification documents not dedicated for travel purposes have to be issued with a target price that balances the cost of the applications with the cost to citizens. Mandatory citizen documents, such as national identity cards, driving licenses or healthcare cards, must be affordable for everyone.

In addition to providing tamperproof ID to each citizen, an ID document should offer additional new services based on Internet access. But non-electronic documents can't support this even though their cost is very low (about U.S. \$0.50 for a blank document without graphical and electrical personalization). Full ICAO chips have been deployed on a large scale in e-Passports and offer a strong platform for supporting new services alongside identification, but the chip cost (minimum U.S. \$2.00 for the smallest EEPROM memory) is prohibitive for manufacturing ID documents despite their cutting-edge capabilities.

Multi-application microprocessors supporting the ICAO-Lite logical data structure offer a cost-effective alternative (U.S. \$1.00 to \$1.50) that can jumpstart the spread of electronic ID documents. The key elements to achieving this target price range are:

- Contactless payment industry leverage,
- Antenna assembly technology, and
- Document material definition.



The price range is also targeted to compete with contactless solutions based on proprietary cryptography and ISO 7816 contact-only documents, which both present weaknesses regarding lifetime and security.

Full standards compliance

Unlike memory chips, high-capacity barcodes and other technologies, contactless microprocessor chips used for transactional applications are governed by strong inter-industry RF communications standards, as well as by data exchange protocols. ISO 14443 A/B defines close proximity protocols used mainly in payment and mass transit applications, whereas ISO 15693 is used for applications where the distance between reader and chip are much greater, such as for access control and vehicle ID. The ISO 7816-4 standard defines an inter-industry command set which will be used to personalize documents using traditional industry equipment without any need for proprietary modules or add-ons. In "9303 Machine Readable Official Travel Documents" (Part 3, published in 2008), ICAO decided to standardize the biometric passport logical data structure (LDS) and access commands. Data is stored on the contactless chip using an ISO 7816-4-based file system, and is organized in data groups (DGs).

Near field communication (NFC) operates at 13.56 MHz for use over short distances. It has been recognized as a second-generation standard for RFID technology (smartcard / RFID tag) by the International Organization for Standardization, and is expected to be used widely in various electronic devices in the near future. NFC is able to exchange (read and write) data with any device supporting the following standards:

- ISO 14443 type A
- ISO 14443 type B
- Sony FeliCa™

The NFC standard was registered as ECMA-340 with ECMA International on December 2002. On December 2003, it earned the internationally recognized ISO/IEC 18092 standard. In January 2005, an expanded NFC standard was established as the internationally recognized ISO/IEC 21481 standard.

The NFC stack is the basis for the full standardization ecosystem. The data link layers, such as the control system for when radio waves collide and the physical layers such as the modulation scheme and coding, are shared layers. The NFC stack prescribes device to device communication, reader mode (i.e. tag reading) and card emulation. Supported protocols are illustrated in the following figure:

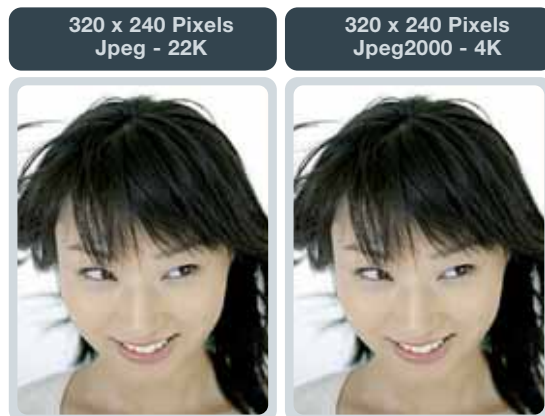
NFC stack		
Device to device	Reader mode	Card emulation
ISO18092	Felica ISO14443 A&B ISO15693*	Felica ISO14443 A&B

Note that ISO15693 is considered an option.

NFC is a compelling technology for deploying low-cost, interoperable readers for movable checkpoints. The most obvious application is the mobile phone, due to its constant technological update, secure element embedding capacity (to host keys, applications, etc.) and over-the-air connectivity.

Efficient photograph storage

Most electronic passports embed EEPROM chips with a minimum 44 KB of memory in order to store data, especially cardholder photographs. The total amount of memory required for photographs depends on the size and resolution of the photographs. Photos are captured during the enrollment phase of the document lifecycle, and are immediately converted into compressed JPEG format.



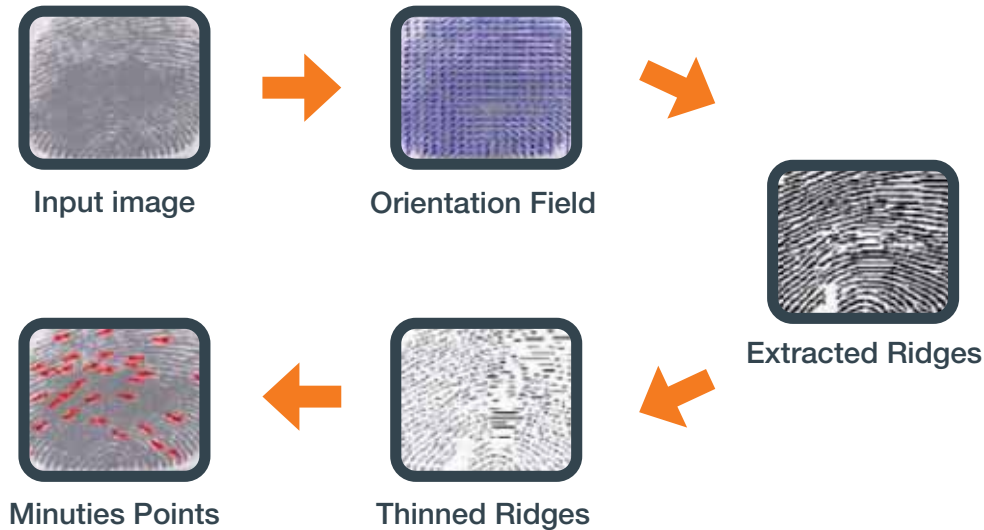
The rapid increase in the number of web sites, users and data flows since 2000 has led to new compression algorithms that have drastically reduced the size of data objects (without losing quality) to reduce bandwidth requirements. The JPEG2000 algorithm is an improved version of JPEG compression that gives the smartcard industry a new tool for embedding quality ID photographs with a small footprint.

The figure above shows the comparison between JPEG and JPEG2000 compression results. Using JPEG2000, it becomes possible to store significantly detailed facial photographs into only 4 KB of memory, which is suitable for use with an 8-KB microprocessor chip. It is also possible to both reduce the resolution and boost the compression rate to go beyond 2 KB and use even smaller 4-KB microprocessor chips. Quality criteria are mainly determined by the application, and should be weighed for contactless microprocessor platform selection.

Match-On-Chip option reduces risk of stolen checking stations

Biometric checking through a template comparison mechanism uses extraction algorithms to convert live, captured fingerprint images into templates used for comparison with a reference one. The process flow for comparison is:

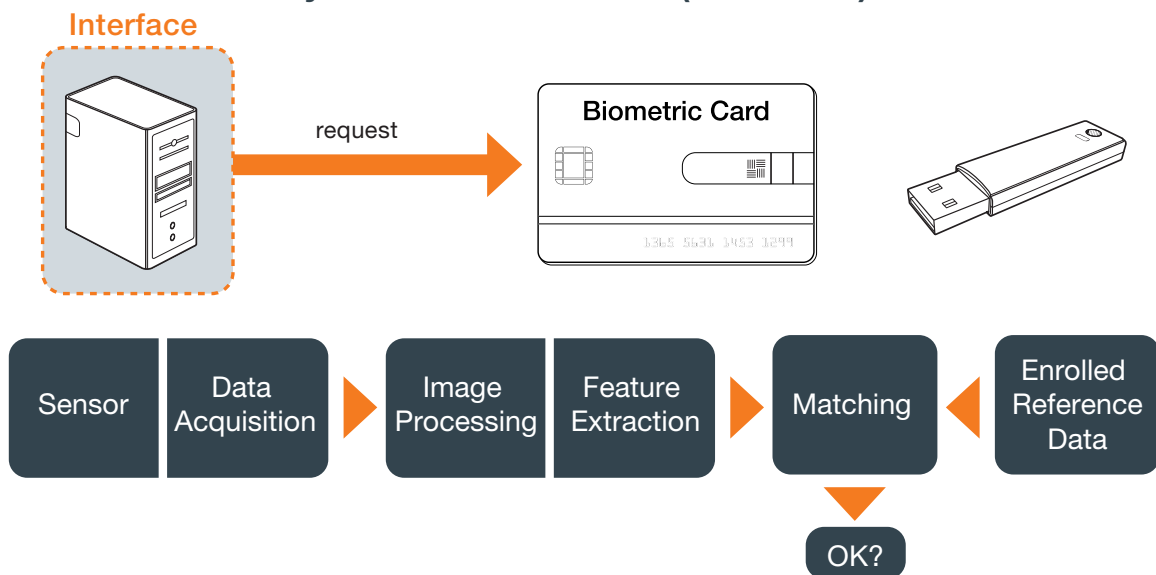
- Fingerprint acquisition and processing
- Template extraction
- Comparison with reference template
- Approval or denial



Fingerprint capture is done using a reader (thermal, capacitive and optical are most popular), which returns an image of the fingerprint. The frame is immediately converted into a template by extracting the minutiae points using the following process:

The comparison algorithm checks both templates by analyzing each minutiae point. It could be run in either the fingerprint reader or the smartcard. The first method is referred to as match on board, while the second method is called match on card. The match-on-card option is very valuable for ICAO-Lite documents because it results in a higher level of security because that no biometric data ever leaves the card. That critical data only belongs to the document holder, avoiding the risks related to a stolen control station.

System-on-Card/Token (2002/2005)



ADDING VALUE TO DOCUMENTS AND PROCESSES

Broader usage than travel

The objective of e-Passports and national ID cards used as travel documents is to allow the document holder to leave one country and enter another, and prove their identity during the journey. This is the primary objective for travel documents, and particularly for e-Passports. This objective makes interoperability the primary requirement. Just as important, the security and authenticity of the documents are prerequisites for any solution brought to the marketplace. Lastly, the speed of checking the ID document, particularly the electronic portion, is also of paramount importance, as high levels of security and checking cannot be allowed to slow down the border crossing process.

For many years, travel documents without electronic chips have been used as proof of identity for many other applications, such as opening a bank account, taking an exam, etc. As a consequence, it is evident that a chip-based travel document will also find identity applications beyond its original intent. Even without becoming a true multi-application document, these additional applications will nonetheless piggy-back onto these documents.

Universal reading of static and variable data

Reading and checking with NFC phones

The lack and the cost of a reading infrastructure is the first barrier to overcome to multiply the use cases and add value to ID documents. Depending on the application, this could be much more than just reading and checking the authenticity of the chip. Some variable data may need to be modified or updated on the fly in a completely mobile environment. For example, a driving license needs to be checked by police while on a road, and may require the addition of penalty points or the management of a fine. Being able to perform these activities with a commercial NFC phone equipped with an appropriate secure element -- a tamper-proof silicon chip that protects the encryption keys and computes the necessary algorithms -- instead of a dedicated and costly handheld terminal would greatly benefit the widespread deployment of electronic and automated controls.

Multi-step checking: visual, chip read, remote server access

Based on the previous example, it is possible to establish some guidelines for a gradual approach to checking ID documents:

1. In an initial, routine verification step, security is borne by visual inspection of the document.
2. If any doubts arise from step one, then reading the chip locally will be necessary. This could be performed with a handheld reader or, as previously described, by an NFC phone. This second verification step allows the personal information printed on the document to be compared with the same data recorded in the chip.
3. If further verification is required, the same NFC phone could be used as a bridge to communicate with a remote server via GPRS/EDGE/3G. The secure element embedded in the phone is used in the authentication processes and to establish a secure channel between the ID document and the remote server.

With the gradual verification process, clerks handling the process can concentrate on the more dubious cases, and easily decide when to escalate.

Remote ID checking via Internet, NFC phones or USB keys

Using an ID document online is another anticipated benefit of e-citizen life, and is expected to grow significantly in the coming years. This could be achieved with an NFC phone paired via Bluetooth with a PC, or by using a USB contactless interface, as shown below:



The NFC phone and the USB key could be used to establish a secure path/tunnel between the contactless chip embedded in the ID document and a remote server, which could perform some kind of authentication or approval of services, or simply register the e-signing.

ROM-based applets for managing variable data

The ability to store applets in the ROM portion of the ICAO-Lite chip that are triggered on demand by applications is the driver behind adding value to ID documents. For each application, applets can manage, read, compute and store variable data in the unsigned memory partition. All the transactions, security and data logging are completely compatible with and similar to those of the smartcard industry. The strength of the ICAO-Lite is in combining the two parts of the memory; the first being static and signed by the ICAO standard, and the second being variable and managed by the same standards of the smartcard industry.

File manager and BAC and EAC mechanisms

The file manager is the basic applet for managing data in any application. It includes all the basic APDUs (commands) for managing files and data, from the security aspects (authentication process, secure channel, etc.) through the operational aspects of computing cryptography (3DES) and manipulating files and data under the to-be-set security rules. This applet covers as much as 80 percent of the cases and requirements for non-travel applications. The file manager is a 100-percent standard ISO applet, compatible with all the standard readers deployed for smartcard applications. The commands used for protecting access to the data, both static and variable, largely rely on the file manager applet. They are BAC (basic access control) and EAC (extended access control), which authenticates the reader before allowing it to retrieve some information. Development kits are widely available to help with building and testing applications.

E-Purse

For some targeted value-added applications, such as social benefit programs, the use of the e-Purse mechanism could bring additional benefits because debiting and crediting the e-Purse adds robustness to the transaction flows. The e-Purse has some interesting features, such as a debit and credit journal and compatibility through existing e-Purse standards. One such e-Purse standard is CEPAS (Contactless e-Purse Application Specification), which has already been widely deployed in Asia. Interestingly, CEPAS is the backbone of the SSID specification, a Singapore standard for identification based on the ICAO e-Passport specifications, and is deployable with ICAO-Lite standard chips. Other solutions can be implemented to leverage infrastructure already deployed, ensuring compatibility with the secure access modules (SAMs) in the readers.

Match on chip

The capability to link an ID document with its holder based on biometric technology is one of the most promising value-added applets. This verification method establishes the physical presence of the individual, facilitating proof of identity, and making the ID document a truly personal token.

With match on chip, all matching decisions are made inside the ID chip; hence, ID document integrity is preserved. The match-on-chip applet performs the biometric matching (usually of a fingerprint) inside the environment of the chip's secure operating system. Match-on-chip functionality allows:

- Personal control of a certificate
- Guaranteed cardholder presence
- The ID document to be the master of the transaction
- The issuer to be the source of trust
- The ID document to be the issuer representative

Clearly complementing and not competing with automated fingerprint identification system (AFIS) databases, match on chip is employed in situations where creating a centralized database isn't useful and would be a waste of time and resources. For social benefits applications, for example, it is often important to be able to deliver services to the right person without having to (or being able to) check their presence in a centralized, online database. Being able to compare the biometric template captured on the reader with the template stored within the chip enhances security and privacy. Additionally, ISO standardization recently has been solving many interoperability issues in that field. Finally, the scalability of the solution is an advantage, especially in geographies lacking telecommunications infrastructures.

Travel cards and pre-registered travelers programs are also excellent targets for this technology. Ultimately, match on chip could be used in many local services, public transport and all areas where a group of individuals have access to free or advantageous services.

Other applets

In general, there is no limit to adding specific applets to ICAO-Lite ID documents to create added value. Some can be very specific and private, while others can be broad and standardized. Obvious applications are public transit and e-services, which could range in scope from very local (one city, on campus) to nationwide.

ISO 15693 compliance for convergence with access control and ticketing

In many situations where ICAO infrastructures have been deployed, airports being the most common, travel documents are being checked in sensitive areas where security levels are high, especially in terms of controlling access to these areas. Because of this, it is natural to expect there to be a convergence between ID document verification and access-control operations. In light of this, the ICAO-Lite chip's ability to operate with the ISO protocol 15693 (vicinity) becomes a compelling added value because it increases the reading distance slightly, and ensures backward compatibility with the large majority of readers that have adopted this protocol currently deployed in the field.

Convergence with payment cards

Opportunities also exist for convergence with payment cards. This is probably most relevant in emerging countries, where the percentage of the population with access to banking services is very low. Two main drivers are meaningful for these situations:

1. **Biometry:** Many future holders have the same last name derived from their paternal ancestors (patronym) and limited education for managing their first account. For identity purposes, biometrics is the best technology to deal with this.
2. **National-backed scheme:** The natural path for providing a larger portion of population with access to banking services is to first start with social benefit or pension distribution. To control this, governmental agencies are creating virtual accounts at large public banks and delivering ID documents or ATM-like cards to pensioners to provide access to the funds. Later, the government will enact some laws requiring the payment of salaries only by electronic means, extending these accounts to a broader range of the population. In general, these ATM-like cards are not linked with an international system, and have more of the characteristics of an ID document than anything else.

These two drivers are creating a large opportunity for convergence between the payments and the ID sectors, as it is the state or a delegated governmental agency that is acting as the domestic system.

CONSEQUENCES FOR THE DOCUMENT DEFINITION

Chip size

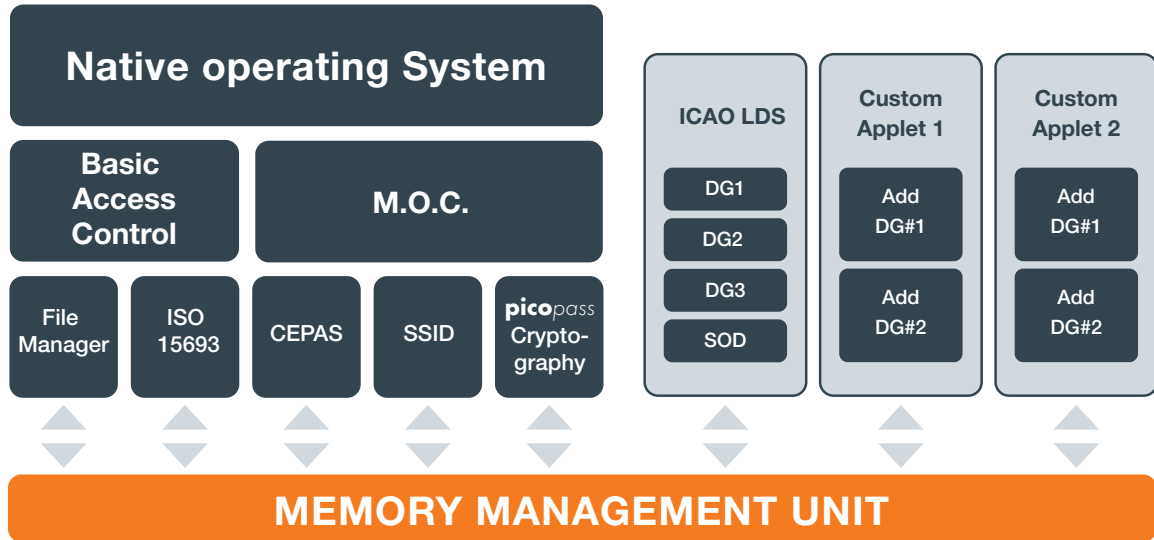
The various classes of ID documents will have different requirements for the size of the chip. The ROM size required will depend on the number of applications to be resident and eventually triggered. The EEPROM size required will depend on how much static, signed data and variable data needs to be stored, and represents the core of the document as a secured container of demographic data.

For the ROM part, it is likely that a size between 64 and 96 KB will be enough to store the various applets needed by the specific applications to be used during the lifetime of the document. This is good news, as this size range is typical of lower-cost microprocessor platforms. In certain situations, the global ROM space could be partitioned into different blocks, as, for example, one block of 64 KB and two blocks of 16 KB for a total of 96 KB. The advantages of this partitioning are the ability to power only part of the memory for better performance and run applications in each block independently for greater security.

For typical ICAO-Lite applications, we anticipate an entry-level market requiring 4 KB of EEPROM, probably dedicated to single-use documents, such as travel cards, with a biometric template stored in the document. With 4 KB of EEPROM, the price points are very competitive and become the main driver to justify the migration from pure plastic document to electronic ones. The next level will be in the 8-10 KB range, allowing easier use of multiple data groups combining compressed photos, biometric templates and the necessary demographic data.

Example of an ICAO-Lite ROM and EEPROM structure

Shown below is a typical profile for an ICAO-Lite implementation. The structure of the ROM memory is on the left side and the structure of the EEPROM memory is on the right. The ROM contains the operating system, typical ID applications such as the basic access control applet or the match-on-card applet, plus a suite of applets and primitives used to support the functions of the ID document. The EEPROM primarily contains the LDS structure, i.e., the data groups of static, signed data, as well as the SOD, a digital signature based on the document's LDS contents. Additionally, the EEPROM contains the variable data corresponding to the value-added applications.



FUTURE EVOLUTION

E-citizen documents and e-signing

Although the ID document was originally intended to prove identity, it has also become a mechanism for obtaining a variety of benefits and services from public administrations or their equivalent. This trend started in the early 21st century when the first initiatives combined identification with controlling the delivery of public services. As this trend continues, there will be additional needs to:

- Automate some administrative processes, such as signing tax declarations, receiving non-pledge certificates, consulting the points balance on a driving license, and many other uses.
- Sign and track transactions for the purpose of non-repudiation, uploading statistics and acknowledging the receipt of benefits and services.

For these reasons, we can anticipate that simply verifying the integrity of the data stored in the ICAO-Lite chip or using some of the certificates or keys securely stored in that chip won't cover all these needs. It will also be necessary to generate a genuine e-signature in the chip, which will require an RSA (or elliptic curve) co-processor.

Such e-signature-capable ID documents have already been deployed in national projects in Japan, Malaysia, Brazil and several countries in Europe and elsewhere, and the scope of these projects may be either more limited e-citizenship schemes or comprehensive multi-application national ID documents. Today, these projects are probably beyond the capabilities of a very low-cost ICAO-Lite implementation, which is based on less expensive silicon platforms. But it is likely that asymmetric cryptographic management will soon be available in a broader range of these platforms.

Today, the two limitations for integration into an "ICAO-Lite" solution are:

- Cost of the hardware (silicon platform with crypto co-processor)
- Cost of the infrastructure for managing the keys issued to citizens, as well as the dynamic interoperability of these keys for various services, and depends on how advanced each country is in that process.

Match on chip for Internet remote access, travel cards, etc.

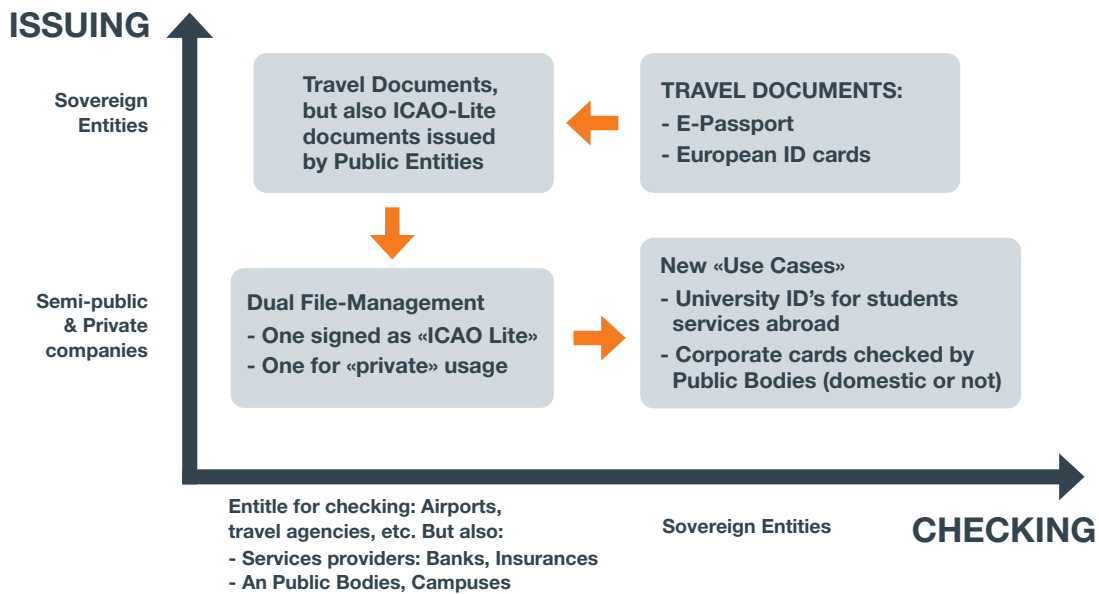
We believe strongly that self identification using match-on-chip technology will drive a large number of ICAO-Lite documents to be issued over the coming years. This will apply to many applications combining identity check with access control and self-identification using ATMs, kiosks and other terminals. In these applications, the individual is using their ID document for self-identification, which then allows them to open a door, access private information, use a computer or perform some other workflows.

This method for delivering information or initiating a workflow could be extended into a more private environment with remote PCs. In that case, the individual would use a contactless-enabled PC (some such devices have already started to ship) or a USB-linked device (USB keys, smartcard readers) to create a secure channel to the ICAO-Lite document with match on chip. Then, using the fingerprint reading capability of the PC itself or an add-on reader, it is then possible to perform a biometric check to authorize remote access to a website or other remote resources.

Extending use to semi-private and private entities

We conclude our discussion of the global interest in leveraging ICAO standard flows by envisioning some ways to extend its use. Starting with the simple case of an e-Passport, which was originally developed primarily as a way to ensure security and interoperability when crossing international borders, there are already situations in which an entitled entity, such as a travel agency or an airline, is able to read and check the e-Passport for its own purposes. This is an elegant way of increasing the value of the document and integrating this value into a semi-private or private workflow.

Some workgroups are already working on ways to help develop the business case for emerging countries interested in leveraging their public investment in this technology for the benefit citizens and the private sector. For example, a bank branch would be able to check the authenticity of an e-Passport before allowing an individual to open a bank account. In this way, the government's investment in security is clearly injected into a process benefiting the bank.



When the ID document is an ICAO-Lite document issued by a semi-public or a private entity, the use cases could be expanded even further because the schemes for distributing the public keys used to verify issuing entities' digital signatures can be more flexible than those described in the ICAO standard. Because an ICAO-Lite document partitions the memory and manages variable data, the document can be verified by private entities because it supports ICAO standard checks while enabling private interactivity with the stored data for other purposes.

To close the loop, now imagine the reverse scenario, with an ICAO-Lite document issued by a private entity being checked by a public one. An example would be a student ID issued by a university in one country being checked by a public sector (health for example) in another country before providing services guaranteed to students internationally.

In closing, we believe ICAO-Lite solutions will find many new and varied applications while maintaining its advantage of providing a solid, standards-based, common platform for interoperability, and will extend beyond the public arena to adoption by semi-public and even private bodies. With its unique combination of a standards-based approach and powerful development tools, we believe the ICAO-Lite model will prove to be the right solution for many of the identification issues facing a variety of organizations today.