THE LEADING EDGE OF BORDER SECURITY

RECORD-BREAKING TRAVEL CREATING NEW CHALLENGES

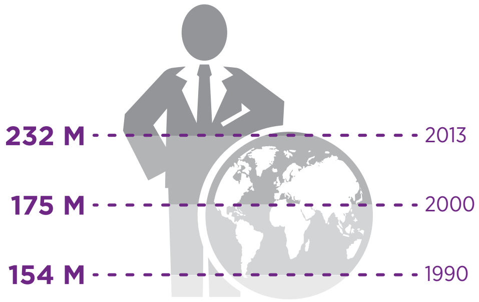
TIM KLABUNDE
Entrust Datacard; Director, Government Vertical Marketing

Entrust Datacard™

THE ERA OF THE MOBILE IDENTITY

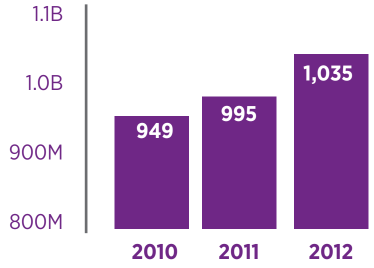
In an increasingly global market, people everywhere are moving freely across borders and around the globe at a rapid rate. In 2012, the number of people traveling internationally for business and pleasure broke the one billion mark. Another all-time high was set in 2013, and we're on pace to break that record again in 2014.[1]

Accelerating Mobility



International Migration

The number of international migrants worldwide reached an all-time high in 2013 and continues to grow rapidly.



International Tourist Arrivals

International tourist arrivals exceeded 1B for the first time in 2012.

In the past decade, technology advancements have transformed consumer expectations. Our new "instant society" empowers consumers with extreme convenience and anytime, anywhere access. People expect no less as they migrate and travel for business or personal pleasure. These heightened expectations extend to all of their increasing interactions with their governments — from crossing borders, to voting, to accessing public services. As part of this, citizens expect their government services to be linked — from demanding that their driver's license, national ID and passport share common issuance and management structure, to expecting that their government healthcare system talks with the social security administration.

[1] United Nations, Department of Economic and Social Affairs, Population Division. Trends in International Migrant Stock: The 2013 Revision

Striving to meet these expectations for their citizens and facing new levels of complexity, we've seen the growth of e-Government services that leverage mobile technologies and online channels. Today, all 193 U.N. member nations have a digital presence, with more than half offering at least one-third of their services online and two-thirds offering mobile apps to give citizens on-the-go access.[2]

Because of this, the need for secure identities is at an all-time high. As we cross-borders, vote and access e-government services, security, efficiency, cost and program risk are all factors that governments need to efficiently address.

This new world requires governments to elevate the importance of trusted identity as they balance the demand for convenience with the need for efficiency and security. As citizens demand more from their governments, it's important to create a seamless connection between securing citizens and societies and delivering government services.

Nations are now looking at the whole ecosystem that can help them enable secure identities. It is no longer about individual pieces of a program — the entire end-to-end security of a document, process, and interoperability of the program requires embedded security features to ensure a protected ecosystem and, ultimately, a protected identity.

[2] United Nations 2014 survey

THREE KEY ELEMENTS OF A CITIZEN-CENTRIC SOLUTION

As nations around the world consider solutions for the identity challenges of an increasingly changing world, consensus has centered on three key elements needed for success:

- **Unified Identity:** The need to structure identity around a single record of authority binding digital identity to the person — and link this unified identity to a variety of credentials.

- **Whole Government/Common Portal:** The need to create a common portal, giving citizens a single access point and a convenient dashboard for a breadth of service offerings on both the federal and state level.

- **Information Privacy:** Citizen confidence in a government's respect of personal privacy is key to government trust. Successful solutions must utilize a strong security framework that holds attribute data distinctly, with secure linkage to central identity.

EVOLVING IDENTITY SOLUTIONS FOR TRAVEL & BORDER CONTROL

Managing the movement of a billion people across the world's borders has exponentially increased the need for new security features. Beyond the record-high numbers, new threats continue to emerge, undermining traditional ways of creating secure identities.

Methods of forging and altering passports are becoming more sophisticated, and there is a rapidly growing market for stolen identity documents — which can be used by imposters or altered by talented counterfeiters — with Interpol's Stolen and Lost Travel Documents database now including more than 30 million documents (passports, visas, etc.) from 167 countries. Other easy-to-forge identity documents like birth certificates are being used to obtain legitimate passports — in these cases making it nearly impossible to identify fraudulent documentation.

New strategies for addressing these challenges are centered on three types of identity documents:

Passports

The passport remains the de facto form of identification for international travel, and there is no indication that this will change anytime soon. However, led by European nations, we're seeing a global shift to ePassports, with 101 countries now issuing these more-secure documents and 81 percent of new passports issued now including a smart chip.[3] New ePassport technologies are further enhancing high-security authentication for travelers.

National ID/Driver's Licenses

National IDs are following a similar trend, with experts forecasting that by 2015, the majority of the world's nations will be issuing eIDs.[4] Already, more than 62% of national IDs issued include some form of biometrics.[5] Continued innovation will expand the capabilities of these "smart" eIDs — enhancing the specificity of credentials linked to the card and adding new applications utilizing high-end contactless technology.

Mobile Credentials

As the applications of mobile technology grow more diverse and in-demand, mobile credentials are a new frontier with great promise. Mobile payments are projected to grow from $235 billion today to $721 billion in 2017[6] — and this growth is especially concentrated in emerging economies, where traditional identity documentation is often nonexistent. This is driving the development of sophisticated mobile credentials that can be used to grant both physical and logical access to secure environments. We may soon see the adoption of mobile credentials as an acceptable form of identification for travel within the borders of a country — around the U.S. or across Canada, for example.

[3] United Nations 2014 survey
[4] Acuity Market Intelligence Report
[5] Need source
[6] PewResearch

PREVENTING WEAK LINKS

When thinking about securing these types of identity documents, it's important to avoid the tendency to focus on just the security of the end-user credential and/or document. An identity solution, in general, is only as secure as its weakest link — and in today's world, that weak link could be a person, a process, a physical or a digital asset.

Governments can take steps today that will help alleviate and mitigate the risk of fraud and false identification as citizens and consumers travel, cross borders, vote or access e-gov services. These include:

Secure Databases

Securely bind the physical identity to the cyber or online identity. The database is a critical resource that can help safeguard borders and travel — when properly used — to assess and verify passengers. Enforce credential-based strong authentication for e-services, leverage the trusted identity profile and work to maintain the chain of trust.

Train Field Officers/Agents

Ensuring that those vetting passengers have the proper training and know what to look for in both arrival and outbound travelers is important. This helps with the noticing of behavior and body language clues, understanding the technologies and electronic components of smart credentials, etc.

Outbound Validation

Proper electronic validation — of both incoming and outgoing passengers — provides high assurance of the integrity and authenticity of the document and allows complete, closed-loop tracking of travelers, significantly mitigating the threat of forgery. While the potential for technology failures is always a possibility, it still provides the means to appropriately process travel documents for secondary inspection.

Advanced Identification Technology

Continuous advancement in technology will be key for identifying passengers. In particular, biometrics of the individual such as fingerprints or even facial recognition could be used. Leveraging these advanced biometric technologies can further mitigate the impersonation threat.

Physical Security of Documents

The physical security features of these documents are essential to validation. Tools like Datacard® Security at Time of Personalization™ can complement supply chain security by reducing the value of blank documents. Variable security features added during the personalization process make fraud more difficult, requiring not only the raw materials, but access to, and understanding of, these personalization technologies. Examples include: the Datacard® PersoCurve™ security feature, Laser Engraving, 3D photos and UV Fluorescence.

BEYOND THE CREDENTIAL: END-TO-END SECURITY

The emerging trends discussed above are all promising new ways of providing citizens with secure credentials that enable efficient and convenient travel.

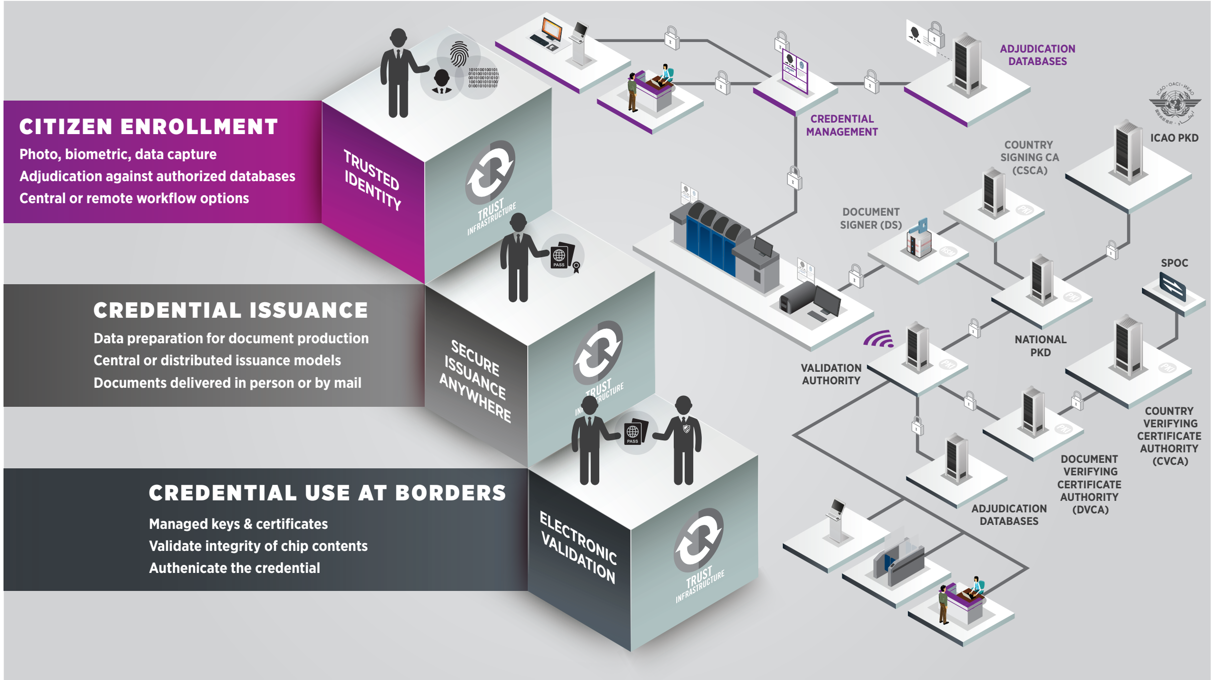
But, let's not forget the key element of looking at the entire ecosystem. When governments start looking at the entire program — from enrollment and issuance to management and validation, it tends to become more difficult to ensure all pieces work together to create a secure environment.

Industry leaders like Entrust Datacard provide new ways to help ensure that end-to-end security in the full ecosystem.

That means building a trust infrastructure that combines physical, electronic and digital security features to support the entire identity lifecycle — from citizen enrollment and credential issuance, to managing physical as well as digital credentials like PKI and digital certificates, to authenticating identities and validating access and interactions — all while intelligently identifying suspicious and fraudulent activity.

By leveraging the end-to-end security of a trust infrastructure, today's governments can effectively combat the growing threats to identity documentation. But more importantly, they can answer the heightened expectations of their citizens — offering greater convenience and easier travel — while enhancing efficiency and minimizing costs.

Building Secure Ecosystems



CITIZEN ENROLLMENT

Photo, biometric, data capture
Adjudication against authorized databases
Central or remote workflow options

CREDENTIAL ISSUANCE

Data preparation for document production
Central or distributed issuance models
Documents delivered in person or by mail

CREDENTIAL USE AT BORDERS

Managed keys & certificates
Validate integrity of chip contents
Authenticate the credential

ABOUT ENTRUST DATACARD

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information, visit www.entrustdatacard.com.