Deloitte.

Next Generation Smart Border Security

Ability. Quality. Delivery.

October 2013

Table of contents

Introduction

The migration of people and the movement of goods across borders have become increasingly difficult to track and manage in globalized economies. Cross-border passenger travel is a vital part of the way of life in the European Union (EU), and border crossings – both through the Union's exterior borders, and within internal borders between member countries – is key to facilitating passenger travel via air, land, and water. The Schengen Area enables travellers to move freely between internal borders without additional screening. As part of the Schengen agreement, however, external borders must be strengthened, which heightens the need for modern technology to support the safe and efficient screening of people entering this special zone. Further complicating this need, the amount of people coming through major global checkpoints is growing. More than 210 million passengers passed through UK airports in 2010, and between 2011 and 2012, Australia processed more than 31 million international air and sea passengers. That number is expected to reach 50 million by 2020. Each individual represents a myriad of data points, ranging from demographics, travel patterns, visa authorizations, employment and education history, and criminal background. Risk-based decision making is key to operating a safe, secure, and efficient automated border security system that leverages this and other data to make informed decisions about where to focus border security resources, while ensuring smooth border crossings for legitimate travellers.

Cross-border passenger travel is essential to the objectives of the European Union and the fundamental freedoms of movement of people and goods. By utilizing risk analytics, a registered traveller program and an entry/exit system that enables low-risk passengers to travel easily while providing enhanced scrutiny for those travellers who pose higher security risk, can be implemented efficiently.

Context

In order to effectively meet the dual objectives of facilitating access of eligible travellers while mitigating security concerns, the EU must have a system in place that enables targeting at border crossings to identify travellers which present the highest risk. An Automated Border Control (ABC) system can facilitate this risk-based border security, but in order to be successful, the system must be supported by strong data management processes, analytics capabilities, and most importantly, an understanding of the characteristics that signal crossings that are likely to present potential security risks to the EU. By understanding the current state of passenger traffic traveling into and out of the EU, it is possible to establish a baseline for what constitutes "normalcy" in border crossings, thereby identifying those crossings that extend outside of the normal and may present a risk to security. By establishing the ability to identify tourists, regular crossings of business travellers, and other border crossings that benefit the European economy as innocuous and, therefore, requiring a lower level of scrutiny, a potential entry/exit system and registered traveller programme that enables the EU to focus its resources on crossings into or out of Europe that may threaten security, can be designed. This baseline information serves a dual purpose of not only enabling high-risk crossings to undergo additional scrutiny, but also shortens the time safe travellers spend at entry and exit points.

According to this baseline for safe or "normal" transit across the EU external border, an understanding of the composition of target groups can be built. The relevant authorities can then identify and analyse the behaviours of risk or target groups and design a registered traveller programme based on these parameters as a foundation. By collecting data and information on risk groups such as where they are geographically located, how they travel, and what economic and social drivers impact their choices, the EU can develop an ABC system that employs risk analytics to improve effectiveness and efficiency.

This type of system has been successfully implemented outside the EU. Australia employs an intelligence and risk-based approach for border security, based on an understanding that the majority of travellers and goods do not present a high risk. The system analyses advanced traveller data prior to arrival to determine if the traveller possibly presents a security threat, enabling passengers with an Australian or New Zealand passport identified as low risk to self-process their entry using the system. SmartGate scans passengers and utilizes biometric data to determine if a secondary scan is necessary – rendering entry simple and efficient for the majority of passengers. Furthermore, in 2010, the Australian government invested a 48 million Euro to introduce a biometric-based visa system used only for certain non-citizens. These steps have enabled Australia to focus security efforts on passengers who pose a potential security risk, while allowing low-risk passengers to enter with minimal interference, through automated, biometric screening. The system's use of risk-based analytics has been a success and can be replicated with the right balance of data, intelligence, and technology (Australian National Audit Office 2012).

Risk strategy

Once passenger data is understood, it can be used to generate an integrated and dynamic risk model that addresses specific risks and their priorities. A true risk prioritization framework must take into account new and emerging threats based on actual and anticipated events, while weighting accordingly based on the likelihood of the event occurring and the government's tolerance for risk. Identification and prioritization of these threats comes through robust integration with intelligence and targeting capabilities. Border control organizations from the Member States and Frontex should engage with intelligence agencies early and often in order to work towards coordinated efforts to enable smart borders.

Multiple data sources, when combined, can be assessed using powerful analytics to identify and act on areas of potential threat as identified through the risk strategy.

However, data analysis and risk modelling, once initiated, will likely result in the realization that the available data and intelligence does not provide all of the information required to make informed decisions. A strong risk strategy implies a continuous feedback loop – as new information needs are identified, law enforcement, intelligence agencies, and policy makers must work together to determine what methods can be put in place to make sound assumptions, and work collaboratively to identify new processes and policies to continue to collect different forms of intelligence or data elements to improve decision making.

A strong risk strategy implies a continuous feedback loop.

Risk management

Understanding key characteristics and indicators in travel data can unveil deviations and patterns that form the basis of risk profiles. Leading edge technology has enabled new capabilities in data mining that outperform previously available statistics and risk modelling methods. One such development is Advanced Knowledge Discovery (AKD), a methodology which uses supervised machine learning to discover hidden combinations of influencing factors that can be used to detect, describe, explain, and quantify zones of risk, fraud, and propensity to specific behaviours that may indicate a suspicious traveller. Data is run through rule algorithms that produce understandable business rules to determine where problems are and better track movement in and out of a country.

Nascent activity, by its nature, is hard to discover. In order to detect and then isolate this activity, a rich and structured data ecosystem is needed. Internal factors in a single data set may not be sufficient to explain behaviours, but complex combination with exogenous data may prove extremely insightful. Treating each attribute as a factor, and isolating specific combinations of factors, enables the identification of high-value clusters – often times detecting weak or hidden signals that were not obviously apparent through basic analysis of trends and correlations – from which risk profiles can be defined. Such risk profiles may lead border agents to better target high risk travellers based on complex patterns that take into account multiple factors (including dates, origins, destinations, time of day, and frequency of travel).

Smart Border Analytics Tool

The Smart Border Analytics Tool provides enhanced information on the migratory patterns of individuals entering and exiting the Schengen Area through the use of "big data" and geospatial capabilities. It leverages AKD technology to be able to provide dynamic modeling and simulation of border security scenarios. Visualization levers show visa types, visa status, immigration clusters, and demographic information for immigrant populations It is fully customizable to incorporate various structured and unstructured data sets, including government data sources, commercial transportation information (i.e. airlines), law enforcement information, and open-source data.

Migration of People

- What are the common visa types that are typically used to illegally cross the border?
- What are the primary countries of origin for illegal migrants?
- Where are illegal migrants travelling within the country and can clusters be identified within certain regions?

Information management

Agencies collect a wide range of "big data" that capture different facets of the migration of people and movement of goods across the border, and governments have an opportunity to address critical border security and immigration by using border analytics to turn this data into insight. For risk models and data mining to be effective, they must be underpinned by strong information management. AKD modelling has the ability to analyse huge amounts of "big data", processing millions of records of all types of data (including numeric, symbolic, and text values) with an unlimited number of variables. For data to be made available for use in this type of complex analysis, it must be properly stored, cleansed, and validated.

Multiple data sets – often with different underlying data structures – must be consolidated and maintained in a single location. Data management should also take into account the integrity of the processes by which the data is collected, the validation through which missing values or inconsistency in data sets is detected, and the data warehouse structures through which data is stored and accessed (or exported) for use with analytics tools.

Data protection and privacy

The risk management tool will use personal data from different sources. The quality of the risk analyses will to a high degree be dependent on the type and quality of data that will be possible to input into the system, which will vary between Member States and authorities. Furthermore, EU and national data protection and privacy legislation will need to be respected in relation to the processing of available data. In the EU, the use of personal data is restricted by Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. More specifically, collecting and processing personal data of individuals is limited for explicit and legitimate purposes, including situations where data is necessary to perform tasks of public interests or tasks carried out by government, tax authorities, the police or other public bodies (The European Parliament and the Council of the European Union 1995). Further provisions are established in the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which covers data that are used to prevent, investigate, detect or prosecute a criminal offence or of executing a criminal penalty (The European Parliament and the Council of the European Union 2008). The Commission recently proposed a new data protection legislative framework and any processing of data for the purpose of the risk analyses will need to respect the relevant existing or new legal texts.

Informing operational decisions

Finally, intelligence-driven, risk-based decision making methods need to be operationalized and leveraged to enable more efficient and effective resourcing and traveller flow at the border. Determining which transactions hold the highest risk and need to be prevented or mitigated, while enabling low-risk travellers to cross borders more efficiently, is a key consideration for border services agencies today. Policy makers and border stakeholders are keen to learn more about the patterns, trends, and forensic analysis of the legitimate and illicit traveling population. Once sufficient data is collected to populate the information ecosystem and build comprehensive traveller profiles, it can be used to inform both operational decisions and risk management and mitigation. This information will be integral to determining which transactions carry the highest potential risk.

Continuous tuning of analytics tools and the risk profiles they generate can be used to dynamically inform operational decision and policy changes. Operationally, border staff can leverage this data to reduce wait times for the bulk of travellers crossing the border who would be classified as low-risk. Analysis of high-frequency periods would enable border staff to better manage throughput by determining the appropriate number of border services officers, automated border gates, and additional operators required during peak times. Such efficiencies allow low-risk travellers to pass through border security more quickly and be processed automatically, while enabling border staff to focus on the higher-risk transactions, directing those passengers to be further screened by border services officers.

Data can also be used to support strategic decision making among government policy leaders. Data can be input into a variety of visualization and geospatial tools. Visualizing patterns of risk and how they trend and change over time can provide concrete understanding for educated management decisions and policy making. Leveraging a highly immersive visual environment to sort through complex data and manipulate "what-if" scenarios can further support this decision and policy making. Such environments provide a collaborative workspace in which leaders engage together in exploring innovative ideas, using analytics tools to visualize the implication of potential operational or policy decisions as they are considered.

Conclusion

Analytical techniques are the underpinnings of successful automated border control. Methods such as predictive modelling, whereby patterns found in historical and transactional data are used to identify risks, can be used for traveller segmentation. Further, the bi-directional, real time collection of data enables anomalies to be detected instantaneously, enabling emerging threats to be identified before a traveller has crossed the border. The large volume of data collected to populate the information ecosystem can be augmented further by social network analysis, geospatial information, and shared data from other countries, including entry and exit data.

Data analytics will help speed the legitimate flow of people across the border and allow border officers to focus efforts where issues are more likely to occur. However, given the volume of data and complexity of the analysis required, this stage may create a bottleneck. In order for a data analytics strategy to be successfully executed, it will require an integrated capability across border services organizations. A significant focus needs to be placed on information sharing between and among national and local government agencies. Joint policies, operational programs, and training will need to be implemented to facilitate efficient and effective collaboration. This will also require standardization of the data collected to expedite the processing of travellers.

Works cited

- Australian National Audit Office. *Processing and Risk Assessing Incoming International Air Passengers. Audit Report*, Canberra, ACT: The Publications Manager, 2012.
- The European Parliament and the Council of the European Union. *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.* Official Jounal L350, 2008: 0060-0071.
- The European Parliament and the Council of the European Union. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of persoanl data and on the free movement of such data.* Official Journal L 281 (The Publications Office), 1995: 0031-0050.

Contacts

Sean Morris
Global Leader, Migration and Border Management
+1 571 814-7640
semorris@deloitte.com

Paul Adamson
Director, Border Management
+44 20 7007 4180
padamson@deloitte.co.uk

David George
Asia-Pacific Leader, Global Migration and Border Management
+61 396 716 133
davidgeorge@deloitte.com.au

Marc Atallah
Director Analytics
+33 140 884 331
maatallah@deloitte.fr

Alex Haseley
Senior Manager, Global Migration and Border Management
+33 155 616 399
ahaseley@deloitte.fr

Katarina Bartz
European Regional Coordinator, Global Migration and Border Management
+49 403 2080 4902
kbartz@deloitte.de

Heather Reilly
U.S. Immigration Policy and Solutions Lead
+1 (571) 814-7964
hreilly@deloitte.com

Stanislaw Bochnak
Director Consulting
+48 22 511 01 15
sbochnak@deloittece.com

Lauren Ross
Manager, U.S. Immigration Policy and Solutions
+1 (410) 340-1052
lauross@deloitte.com