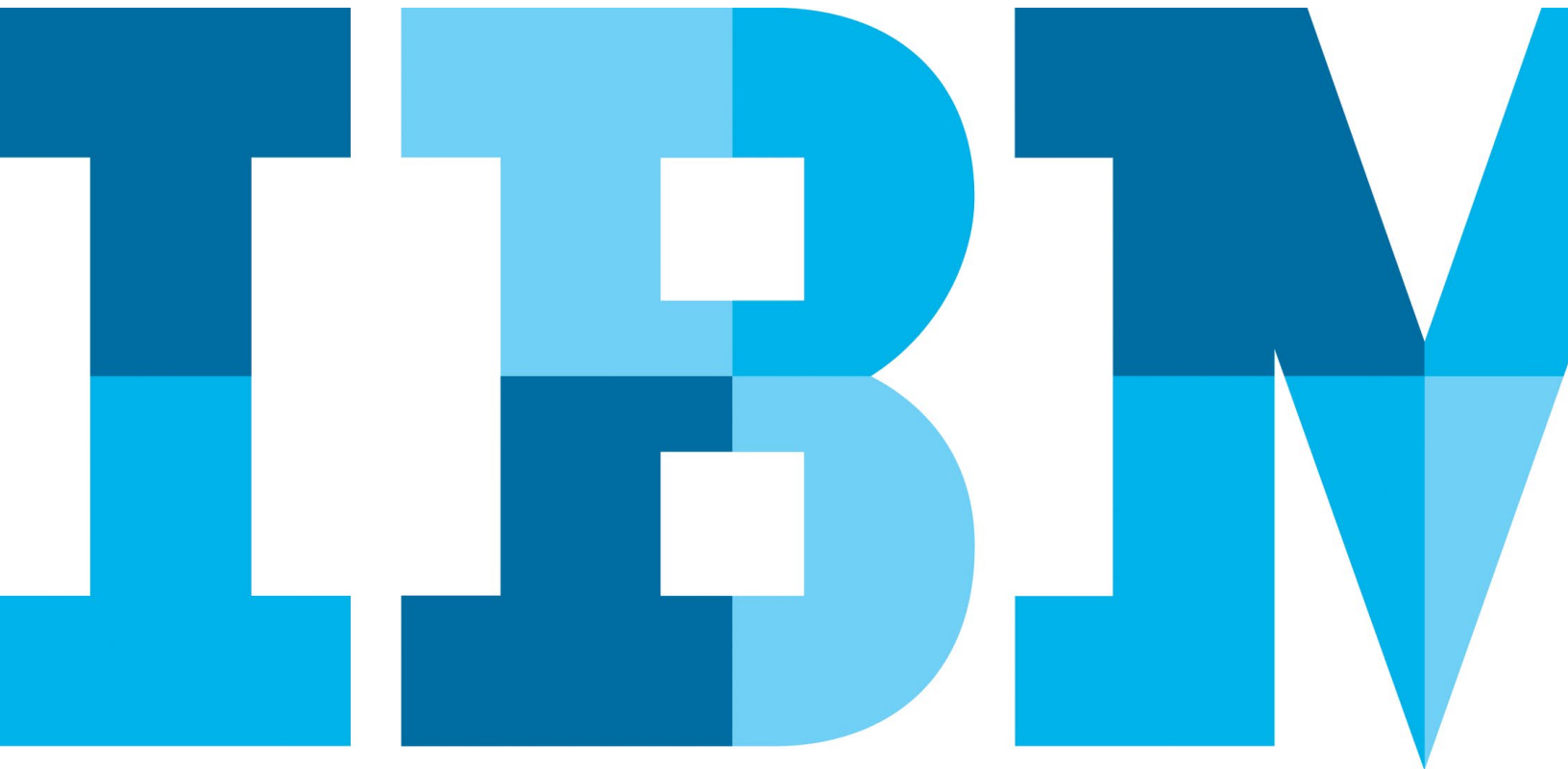


Borders 2020

An IBM perspective on “Halt! Who goes there?” border controls



Contents

- 2 Defining the problem: How do you reconcile security with facilitation?
- 2 What is being done to address the issue?
- 5 What should be done: A road map for the future
- 7 The future of secure border travel

One of the obstacles preventing fast and secure border control is that a frontier security process that has been used for hundreds of years still underpins many border management systems: the gatekeepers are still shouting “Halt! Who goes there?”

This paper offers an approach to how governments and the transportation industry can address the problem by adapting new processes and technology. It focuses on aviation, but the concepts apply to other modes of international transport that involve a reservation or advance payment, such as rail and sea travel.

It suggests that, in the future, visitors will not be told to halt for risk assessments and identity checks, but will keep moving because border officials will know what risks they present before they reach the frontier. “Come in. We know who you are.”

Defining the problem: How do you reconcile security with facilitation?

Every time a border is crossed an individual is taking an opportunity. It may be an opportunity for business, pleasure, improved economic circumstances, or the opportunity to escape from conflict, political and religious persecution or famine.

Border crossings may also be vulnerable points in a nation’s frontier. They are threatened by smugglers, traffickers and terrorists who present themselves and their cargo as legitimate to enter the country illegally.

Evidence of this mixture of opportunity and threat is presented most vividly in a modern international airport, where luxury retailers and business lounges co-exist with security checkpoints and armed guards. Behind the scenes, border management systems are attempting to balance two completely opposite objectives: they must protect the nation from unwanted guests while simultaneously welcoming valued visitors.

Reducing immigration controls to improve facilitation may allow people to enter illegally or allow criminals to exploit weak border controls to extend their networks and cause serious problems for their hosts. Tightening controls often has an immediate effect at the border. Visitors can wait for hours to see an officer for a 30-second interview and document check.

An increase in physical security controls is likely to increase the time passengers spend in lines. In many airports, the stringent physical security check means it can take an hour to pass airside. The X-ray processing of all objects that are brought airside by travelers causes delays and frustration for passenger, the airport and airline, but without this process, there is an increased risk of objects likely to cause a disturbance entering the aviation system.

Unless something changes, the process will cease to function effectively, damaging trade and tourism, and giving encouragement to those who promote global disharmony.

What is being done to address the issue?

The problem is not being ignored. Governments and the transportation industry are improving border security and facilitating travel. Some initiatives are discussed in the following sections.

Increasing capacity

The most widespread approach to addressing the problem had been to improve security by tightening the checking processes and by dedicating more resources to the process: everybody gets checked, and some people get checked more than others. These

one-size-fits-all security and immigration processes rely on increasing the capacity of lanes, security staff and scanning technology to meet demand. However, a solution that depends on increasing staff may become inefficient, because systems designed to support peak loads only use a fraction of their capacity during off-peak hours. Security controls that rely completely on people may also be vulnerable to lapses of concentration, corruption, human errors and occasional industrial relations problems.

Automation and registered traveler programs

In the last decade, the commercial success of the Privium project at Schiphol airport in Amsterdam encouraged many airports to partner with host governments to install automated security and border control gates. Automated biometric recognition gates are now installed in many airports around the world. This technology uses iris, face and fingerprint recognition in online modes, which match the subject with a database, and offline modes, matching travelers with their passports or identity cards, to support both private sector and government schemes.

The value proposition is the same across all types of gates. Most border crossings are made by low-risk frequent travelers; if these people can be diverted to automated gates, border guards can focus on the infrequent or unregistered travelers. This means low-risk travelers flow through low-cost automated gates and people who need to be risk assessed are met by a skilled border guard. In this way, security and facilitation are simultaneously improved.

Many countries are now implementing registered, sometimes referred to as “trusted,” traveler schemes. To enroll, the passenger provides their biographic and biometric details to the scheme provider, who then checks eligibility. Once admitted into the scheme, the traveler may use dedicated, automated border gates on arrival and an expedited security check on departure.

There is currently very little interoperability between the schemes. In the arrivals hall of some airports, visitors are greeted by an array of automated gates that are used by separate commercial and government schemes. Harmonization is underway, but the treaties that allow a citizen vetted by one nation to gain automatic entry to another require complex negotiations, and that takes time.

Electronic authorities to travel

Some countries, notably the USA and Australia, collect passport information directly from potential visitors and check them against watchlists before they begin their journey. If they are cleared to travel, they receive an Electronic Travel Authority (ETA) approval from Australia or Electronic System for Travel Authority (ETSA) approval from the USA. The approvals are valid for one or two years, and a fee is charged. By processing passport checks before the passenger reaches their destination, the host country only needs to check that they have a valid permit to enter when they reach the border. This reduces queues and improves border control because the long wait time to process the passport check is done in advance.

ETA and ESTA approvals can be regarded as short-term visas for certain visitors, reassuring the airline that the passenger is unlikely to be denied entry on arrival. However, their similarity to visas can make implementation politically uncomfortable. If a country feels visa control is being imposed on their citizens, they may retaliate. Because ETA and ESTA approvals are based only on passport information, risk assessment is reduced to watch-list checking rather than the comprehensive economic and social assessment that takes place during a visa application.

Countries may be able to achieve the same result with less political fallout by implementing an authority-to-carry (ATC) scheme, which is less like a visa and more like an advanced clearance scheme. ATC uses reservation details provided by the airline rather than basic passport information provided by the passenger, and so supports a more comprehensive risk assessment.

Passenger risk assessment

Many governments are collecting information found in airline reservation systems and departure control systems to identify persons of risk before, during and occasionally after they travel.

Governments identify known persons of interest when they intend to travel by looking through passenger data to find their names or document numbers. They also identify people who may present a possible security risk because their travel patterns have proven to be risky in the past.

Benefits of passenger risk assessment

Risk assessment in advance helps security officials answer questions at the border. If this takes place before the passengers arrive at their destination, people can be identified in transit and their interception planned before they arrive. If the assessment takes place before they leave, passengers who present a risk can be denied permission to travel.

This risk assessment helps immigration officers differentiate between passengers who may require heightened checks and those that present no risk. In this way, facilitation at the airport may also be improved because investigations can be focused on those who present a risk, reducing wait time for the majority of travelers.

Passenger risk assessment can improve detection rates for customs enforcement officers because their attention can be directed towards passengers who have travelled using a classic smuggling method of operation. It helps the officers demonstrate objectivity in their intervention process, because their natural instincts can be augmented with logical analysis.

Limitations of passenger risk assessment

Passenger risk assessment is an effective security and facilitation tool, but it has limitations. One of the problems is the data collection process. Airline messages are designed to help the travel industry manage a passenger's journey; they are not intended to

feed a government risk assessment process. Messages arrive from a variety of sources in varying formats, and data quality is poor. In many cases, airline data arrives too late to prevent unwelcome travelers from reaching the border.

Another issue is the effectiveness of the risk assessment process. Analysis systems use name matching and rules-based techniques to process millions of messages every year. No system is 100 per cent accurate, and in large volumes, small inaccuracies can generate a lot of exceptions. This causes false positives, mistakes and repeated risk assessments for the same passenger. While the analysis of millions of messages can be automated, the decision to intervene must remain with a human agent. They can become overwhelmed with the volume of alerts that require their intervention.

If the process of data collection and risk assessment is made more reliable, border control policies based on risk assessment could become more acceptable to governments. For example, if the border agency is certain that no one on an aircraft presents an immigration or security threat, everyone could be waved through without being checked again. Removal of border checks would be the ultimate boost to facilitation.

Summary of what has been done to date

Many of today's schemes are attempts to improve on the old "Halt! Who goes there?" process. Authority to travel, passenger risk assessment and registered traveler schemes are making improvements to the problem by attempting to understand who is coming here before they reach the border.

However, all of these initiatives are actually building blocks of an integrated solution. It may be possible to achieve significant improvements in security and facilitation without considerable investment by realigning the technology to support a new border management process.

What should be done: A road map for the future

Most people crossing a border are law abiding and honest. Border management should be processing such people with the lightest and least expensive touch possible. Border control is like looking for a needle in a haystack. Therefore, it makes sense to build mechanisms for getting rid of the hay so that the needle is easier to find. Rather than increase capacity in the old system, it's possible to rearrange the steps to implement a new, more effective system by doing the following:

- Assess risk on departure
- Identify them on arrival

This simple realignment of steps has immense consequences for the border management system. The logical conclusion is that almost everyone passing through immigration at an international airport has already been accepted by the host country, because, if they were not welcome, they would not have reached the border.

This realigned process would consist of an early risk assessment followed by a series of identity checks as the traveler moves through the system. Risk assessment is expensive and time consuming. Identity checks based on biometrics and electronic passports are becoming more affordable, and can be performed almost instantaneously. By spending more time on a thorough risk assessment earlier in the process, governments can save money by mainly conducting identity checks as the passengers approach and cross the border.

How do we build systems that “decide once—check many”?

As with the other approaches detailed in this white paper, “decide once—check many” walks a fine line between economic feasibility, customer facilitation and technical ability. The sections that follow examine the issues presented by this approach.

Know your customer

Customer relationship management systems have existed in the private sector for decades. Consumer-facing organizations track buyer behavior and offer customized service that is likely to lead to happier customers. The prime objective for governments when managing their borders is something similar. They need to assess what a passenger is likely to do there based on previous travel histories and current travel plans. They can identify those passengers who require further assessment and conduct an interview before departure. They can also recognize their frequent customers who can be admitted with minimal checks.

Our initial view would be to start a passenger movement history file of all visitors, recognizing that the travel histories would initially be incomplete, but would fill up over time. Advanced passenger information will provide notice of a border crossing. As people enter the country, their details can be recorded. Over time their travel pattern can be stored and used for basic risk assessment.

Having identified the best way of collecting data from airlines, we would then suggest expanding the system to passenger name records (PNRs) and introducing appropriate forms of watchlisting, checking, and rules-based analysis. This system will support the “decide early” concept. It can also be used by visa issuing agencies and by law enforcement agencies for checking names and passports against watchlists at the border. Immigration officers find it very useful to know whether their interviewee is a genuinely new client, and not a persistent entrant attempting access with a new set of credentials.

The creation of a mandatory record of who has crossed their borders may present data protection issues for some countries, but being able to cross the border quickly may encourage regular travelers to opt in.

Decide early

Systems need to provide a near-instant view of an individual's risk potential at their first point of contact. Are they on a watch-list? Is there anything in their journey or history that raises suspicion? No? They are therefore cleared for entry and marked as "cleared." When the person identifies themselves as this cleared individual, there is no need to repeat the risk assessment.

To conduct this pre-arrival assessment, governments are increasingly collecting travel industry data—a PNR and advance passenger information (API)—from carriers. Checking and analyzing such entry and exit data can be largely automated. This represents the most likely route for making border control more effective and lower cost. Experience suggests that the data is most valuable if it is combined so that API and PNRs are used together.

Getting accurate data about all border crossings will take a number of years, so it is sensible to think in terms of the continuous development of enhanced controls, measuring results and checking to see what works, rather than implementing a predefined solution, designed without the benefit of any practical experience.

Designing the frontier for high-speed identity checking

As progress is made towards an automated process for checking people in advance, physical border controls only need to confirm that a person is who they claim to be and implement the decision made earlier when the traveler's information was checked. We see three parallel approaches for developing appropriate physical controls:

1. Support the development of frequent traveler schemes. This requires a number of actions by governments:
 - Offer a service to background check people who enroll in private, registered traveler schemes. Giving a well-developed mechanism for checking people in advance of their arrival, this check would simply be the normal check done when an individual travels.

- Consider how such schemes should be audited to ensure they are, and remain, appropriate.
- Implement joint action between governments and the travel industry to create standards that allow separate schemes to interoperate. The advantage of this approach is that industry bears all the cost and competing schemes ensure innovation and value for money, particularly when new technologies become available.

2. Automatic biometric gates are not automatically successful.

While the business case for automated gates is clear cut, it requires careful installation in order to be realized. The hardware may cost less than the salary of an immigration officer to install, but the gates' large number of moving parts makes them relatively expensive to maintain and, incorrectly positioned, they can be underused. A program to implement automatic gates should proceed cautiously to confirm how best to manage and supervise the gates, and identify where and why they add value.

Automated border gates would mainly be used by returning nationals, using their standard electronic passport via face or fingerprint verification. In Europe the chip on the Biometric Residents Permit (BRP), now being issued by all member states is technically the same as the passport chip. This means that BRP holders could use the same gates. Indeed, third-country nationals could be invited to buy a BRP, or its technical equivalent produced by the same process, to facilitate their travel around Europe, and this might be a useful interim solution to the need for a Registered Traveler program. Elsewhere in the world, holders of old-style passports could also buy an electronic border pass to use automated border gates.

3. Consider delegating identity checking to carriers

The airlines' successful introduction of e-ticketing has improved the experience of most passengers by replacing a cumbersome paper-based transaction with a convenient and

simple process that saves time and money for both airlines and passengers. The system's security depends on tight identity controls using the passenger's travel document, normally a passport, at check in and the boarding gate. As airlines are now routinely checking passports at a number of points in their process, why not make that identity check part of the immigration process?

The advantage is clear. If the government decides that the passengers on a flight present no risk, and the airline confirms their identity, why do they need to see an immigration officer on arrival? Pre-assessed passengers could be diverted to a "smart zone" and "waved through" immigration without delay. Business travelers may pay a premium and provide more personal screening information to fly on a "smart zone" flight.

Airlines often struggle to establish the identity of passengers due to data entry errors, multiple versions of the same name and the complexity of group bookings, code shares and last-minute changes. To add immigration checks onto the standard process may simply be too risky, but the advantages of improved facilitation justify investigating an enhanced process.

Enhancements may include capturing biometric data as part of the check-in or boarding process and sending it to the destination government. In order to support fast entry, this biometric check could take place before travelers reach the border. The airline could be more certain of the identity by receiving confirmation from the government that an individual passenger is cleared to travel—and that they are genuinely the person who has been cleared.

Clearly such an approach would be risk-based and the airline processes would need to be audited. But rather than have a system that treats everyone as the exception, early risk assessment allows trust to inform the process and efficiencies to be introduced.

Delegating checks to carriers involves some unexplored compromises. It will never be universal; it's easy to identify high-risk countries for which this approach would be unacceptable. It can't happen until there is sufficient experience with the centralized checking process. However, we think that carriers would be receptive to working with governments on such schemes because of the advantage it provides to their customers.

The future of secure border travel

Our view is that it is best to think in terms of establishing a system for recording passenger movements and building appropriate links to other border management systems over time. As the passenger movement history develops, a growing number of passengers will be recognized at the border as "repeat customers" and confidence in the risk assessment will increase. We recommend that a system be dedicated to the passenger history function; combining multiple purposes on a single database is often more expensive than it first appears, and this system will become highly used, as it answers the first question asked: "Have we seen you before?"

Many problems of border management are due to adherence to the travel process of "departure, arrival, risk assessment, decision." Risk assessing everyone in real time at the border causes long lines and impacts trade and tourism. It may even contribute to illegal migration, because people who make it all the way to the physical frontier are more likely to be admitted than if they had applied for entrance in their homeland.

The future of secured, facilitated travel depends on each journey being regarded as a cycle of travel planning, risk assessment, decision making, departure, arrival and return. Risk assessment before departure means that unwelcome people should not travel. Attempts to do so will be met by barriers at each stage of the process; ticket purchase without pre-clearance, check-in without a valid travel document, boarding without a valid ticket, and document combination and entry at the destination without a passport or visa will be very difficult indeed.

However, for those who are prepared to be risk assessed before travel by their intended hosts, their travel experience could be very different. The businessperson who flies monthly would be a member of the frequent-traveler scheme at his or her nearest airport. This traveler would pass through most airports almost without stopping until reaching the aircraft, facilitated by pre-flight risk assessments by the government, commensurate security checks by the airport and automated recognition by the airline.

The potential items on the road map that we have described should all be incremental in nature. It is our strongly held view that the IT systems to support them would also best be developed incrementally. All of the approaches in this document depend on collaboration between governments, the transportation industry and technology providers. As a leading provider to most governments and the transportation sector, with extensive partnerships with technology providers, IBM is well placed to contribute to making this vision a reality.

For more information

To learn more about this issue, please contact your IBM representative or IBM Business Partner, or visit the following website: <http://bit.ly/CustBorders>

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing



© Copyright IBM Corporation 2016

Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.



Please Recycle