FAL/12-WP/39
20/11/03

FACILITATION (FAL) DIVISION — TWELFTH SESSION

Cairo, Egypt, 22 March to 2 April 2004

Agenda Item 2: Facilitation and security of travel documents and border control formalities
2.2: Biometrics
2.3: Crew identity documentation

ACCESS CONTROL IN AIRPORT RESTRICTED AREAS USING BIOMETRICS

(Presented by Canada)

1. INTRODUCTION

1.1 This paper describes Canada's initiative to develop the Restricted Area Identification Card (RAIC). Using biometric technologies to create a secure credential card for individuals accessing restricted areas of airports, the RAIC initiative will also create one central database to which all selected Canadian airports can access to verify the validity of any card issued in Canada. The RAIC initiative is intended to complement or replace the existing restricted area pass systems currently used in Canada.

1.2 Cardholders, by the nature of their employment (such as flight crews, mechanics, compliance inspectors), require access to restricted areas at multiple airports across the country. Currently there is no automated process in place that allows one airport authority to establish the positive identification of the cardholder and the validity of the card at the moment of presentation if this card were issued by another airport authority.

1.3 The RAIC initiative is important for airlines, airports and security organizations because it will create a streamlined system for cardholders to move through restricted area airports, facilitate the completion of the transaction by airport authorities, while enhancing the level of security in restricted areas of airports.

1.4 Although the RAIC is a document of entitlement for individuals accessing restricted areas of airports and not a travel document, the approach used in the development and implementation of the RAIC is of interest to the Facilitation Division since it can be applied to any travel document initiatives using biometric technologies. The approach promotes interoperability on a number of levels, interoperability of technologies which encompasses interoperability of business requirement and legacy systems, as well as global interoperability should it be required.

2. DISCUSSION

2.1 The mandate

2.1.1 On 5 November 2002, the Minister of Transport directed the Canadian Air Transport Security Authority (CATSA)[1] to develop and implement an enhanced airport restricted area pass program. Biometric technologies were specified as a security enhancement, considered desirable for this system.

2.2 Domestic consultations

2.2.1 CATSA worked in partnership with the regulatory authority, Transport Canada, to develop the framework for RAIC through an extensive consultation process with all stakeholders. A technical working group was convened in January 2003, including representatives of both airport authorities and the airline industry, to develop the technical parameters of the programme. Following this, a broader assembly of interested parties, including labour groups and law enforcement officials were consulted on the policy issues relating to this programme.

2.2.2 Interoperability of technologies was identified as a prime consideration by stakeholders and has been a main driver in the development of the programme. This requires addressing multiple dimensions of interoperability, beyond the strict definition of technological interoperability that speaks to the ability of a system to use the parts or equipment of another system. The RAIC must extend principles of interoperability to address the commercial, security and other business needs of stakeholders, ensuring that their existing applications and processes are integrated within the scope of the programme.

2.3 International considerations

2.3.1 To build a strong foundation for its RAIC programme, Canada has consulted a number of countries. In this regard, meetings were held with airport authorities in France, the Netherlands, and the United Kingdom. The programme will comply with the US government's Smart Card Interoperability Standard, although one component of that standard is not yet commercially available.

2.4 The RAIC Process - Verification & validation

2.4.1 The first phase of the process is the positive verification that the cardholder is the person to whom the airport authority issued the RAIC. This positive verification process is completed by comparing a live biometric sample, from the cardholder, with the biometric template that is stored in the RAIC. A positive match of these samples will establish that the person offering the sample is the same person enrolled in the programme. It is important to emphasize that this process does not identify the cardholder amongst a group of people: it merely establishes that the cardholder has supplied a live sample that matches the information that was stored on the card at the time of enrollment.

2.4.2 The second phase of the authentication process is the establishment that the RAIC is valid at the moment of presentation by the cardholder. The validity of the RAIC will be established by conducting a query of a centralized database containing the unique identifying number of all valid cards.

---

[1] CATSA, a federal Crown Corporation, was established on 1 April 2002 in response to the events of 11 September 2001. It is a not-for-profit corporation and reports to Parliament through the Minister of Transport. In addition to developing a restricted area identification card, CATSA is responsible for implementing the following key air transport security activities: (1) pre-board screening of passengers and their belongings; (2) security screening of checked baggage at designated airports; (3) on-board security services, which are delivered by Aircraft Protective Officers in the Canadian Air Carrier Protective Program; (4) providing contributions to selected airport authorities to offset the cost of airport policing related to civil aviation security; (5) screening of non-passengers.

2.4.3 Combining the actions described above will allow the airport authority to ensure that the cardholder who is requesting access to the restricted area had successfully established the need and the right to access a restricted area, at the time of enrollment.

2.4.4 It is within these programme parameters that CATSA strives to maximize interoperability.

2.4.5 To address the issue of interoperability, Canada is not only integrating existing systems but also promoting a modular programme structure. The modular approach will permit scalability to meet present and future technical and business needs, and will also allow a measure of flexibility to allow for adjustments to or elimination of legacy systems which are incorporated into the programme at the initial stages should the airport authorities wish to make these changes. There are four areas of the programme which will be developed with this modular approach.

a) the card and readers;

b) the enrollment application and related programmes;

c) the biometric technologies; and

d) the database structure.

The card and readers

2.4.6 The RAIC is a smart card which stores the cardholder's biometric information required for the positive verification process. To allow for integration with access control legacy systems, the 125 kHz proximity technology must be a component of the card. Almost all Canadian airports, as most airports around the world, use this technology in their access control systems. This technology does not encrypt the communication between the card and the reader and the cost of replacing the readers at both the points of access to and the doors within the restricted area to accommodate encryption technologies would be prohibitive. As a primary security enhancement, however, RAIC will enable the airport authority to replace the readers at points of entry to the restricted area with readers that will offer encrypted communication with the smart cards.

2.4.7 Canada intends to include both contact and contactless[2] chips on the smart card when it is fully deployed. The biometric templates will be stored on these chips. Compliance with ISO standards will be required to ensure the cards and readers will be compatible with or upgradable to be compatible with the next generations of hardware and software. These measures, taken together, will allow us to meet our desired level of interoperability.

The enrollment application

2.4.8 In the deployment of the RAIC, a common enrollment application will be delivered to each issuing airports to assure compliance with data fields constituting the common denominators of the programme. The enrollment process must also address the business needs of the individual airports. Each airport requires supplemental information, such as the condition of employment and the location of the workstation, to allow for the proper management of compliance with the terms and conditions of issuance.

2.4.9 The enrollment application will be developed to enable communication with the existing data structures at each of the airports. This link will serve two purposes: first, it will allow the programme to make use of existing access control databases which house the information on all current pass holders; second, this link will ensure that there is no need to duplicate the data entry process - all information from

[2] Contact chips require the card to be inserted into a reader and are used for logical access, that is, access to data. Contactless chips only require that the card is placed near the reader and these are typically used for physical access.

the enrolment will be transferred to the airport authorities database, thus eliminating the need for the airport authority to reenter common data and also allowing for the creation of a common data file between the airport authority and the central database.

2.4.10 Communication between the access point to the restricted area and the centralized database will also be required. The biometric template of each RAIC applicant will be stored in the central database. When a request for a RAIC is processed, a search of the central database will be conducted to ensure that no unauthorized duplicate cards are issued by an airport authority. The enrollment application will be modular in that it will contain several biometrics using the one which is consistent with the practices of a particular airport and scalable to allow for the integration of solutions to the future needs of any or all of the stakeholders.

The biometric technologies

2.4.11 The first phase of the RAIC programme will be implemented as a pilot project using fingerprint and iris recognition technologies. The technologies will be deployed at two major airports and the test period will allow Canada to appreciate the effectiveness of the technologies and the preference of the end users. Although the algorithms related to each of the biometric technologies is proprietary, CATSA believes that programme interoperability can be reached by employing multiple biometric templates on the same card.

2.4.12 This approach requires that one of the biometric technologies be designated as the reference biometric, that will be readable at all sites. The reading of the reference biometric template (fingerprint) will serve as a secure breeder document to allow for enrollment in the local biometric system, such as an iris scan system.

The database structure

2.4.13 Canada will deploy an information technology infrastructure to support the process for establishing the validity of the RAIC. The database will be located at CATSA headquarters and centrally managed. Using the CATSA wide area network, the database will be replicated to local servers at the airports. All communication between the database and external servers or databases will be done through an ODBC (Open Database Connectivity) link. All systems interfacing with the CATSA database will be required to be ODBC compliant, allowing for system integration and process interoperability.

Privacy issues

2.4.14 One of the first decisions taken in the development of the RAIC programme was that the biometric information required for the positive verification process, would be stored on the card rather than in the central database. In fact, as little biometric information as possible is actually kept centrally. This means that the programme takes only a portion of the fingerprint, looks for patterns, and assigns numeric factors to the patterns. It is this string of digital attributes that are stored, not the image of the fingerprint and it is impossible to reverse engineer these digital attributes to create a fingerprint. The programme is currently undergoing a Privacy Impact Assessment. Privacy Impact Assessments ensure that privacy is considered throughout the design or re-design of programmes or services in Canada. The assessments identify the extent to which proposals comply with all appropriate statutes. The end result of the Privacy Impact Assessment is assurance that all privacy issues have been identified and resolved or mitigated.

3. CONCLUSION

3.1 CATSA believes that the RAIC programme will be a significant enhancement to the security measures in place at Canadian airports, allowing for interoperability with systems in place at airports and systems being developed by other interested parties that are related to air transport security.

3.2 By adopting a modular approach to building the RAIC programme Canada can be assured that if a component of the programme becomes redundant, it can simply be removed. If a new business need surfaces, a component can be added to meet the new requirement. A constant commitment to interoperability and compliance with recognized standards will allow the RAIC programme to become and remain a significant security enhancement.

4. ACTION BY THE DIVISION

4.1 The Division is invited to note this paper and recommend inclusion as appropriate in ICAO guidance material.

— END —