A Daon White Paper

Border and Immigration Security

Trends and Initiatives

January 2009

Catherine J. Tilton

Table of Contents

1. Management Summary ... 3
1.1. Initiatives with Border Management and Immigration Security Space ... 3
1.2. Trends ... 4
1.3. Conclusion ... 5
2. Background ... 6
3. Immigration and Border Security Initiatives ... 7
3.1. Joined up Security ... 7
3.2. Whole of Government Data Interchange ... 8
3.3. Regional Security and Commerce Considerations ... 8
3.4. International Interoperability ... 9
3.5. Integrated Multi-Biometric and Biographic Watchlists ... 9
3.6. Automated and Supervised Biometric Clearance ... 10
3.7. Identity Management Models ... 10
3.8. Identity Lifecycles ... 11
4. Immigration and Border Security Trends ... 13
4.1. Information Sharing & Interoperability ... 13
4.2. Evolving System architectures ... 14
4.2.1. Embracing SOA ... 14
4.2.2. Multi-Application Infrastructures ... 14
4.2.3. Vendor/Technology Independence ... 15
4.2.4. Biometric Middleware Functionality ... 15
4.3. Multi-Modal Biometrics ... 16
4.4. Hybrid Identity Models ... 17
4.5. Privacy and Security ... 17
4.6. Programme Approaches and Timelines ... 18
4.7. Programme Phasing ... 18
4.8. System Phasing ... 19
Background on the Author – Catherine J Tilton ... 20

© Copyright 2009 Daon

1. Management Summary

The stakeholder agencies involved in immigration and border security globally are continuously looking to increase civil security while achieving cost savings and process efficiencies. New global requirements place increased demands on immigration and border security solutions in terms of size, scope, and complexity. Increased information sharing is necessary at agency, national and international levels and modern solutions have moved beyond enforcement to be much more flexible to evolve with business objectives.

This has led to number of global Immigration and Border Security trends and initiatives which enhance and modernise the business approach. Some examples of these include:

- Biometric verification to expedite known travellers through border control points
- Effective and flexible biographic and biometric watch lists to enable greater efficiency and thorough security processing
- International and inter-agency information sharing, including reciprocal arrangements for processing frequent travellers and passengers from visa waiver countries
- Fraud prevention in critical processes such as immigration and citizenship using biometric identifiers
- Identifying duplicate identities within identity repositories using biometric identifiers

The purpose of this paper is to examine some of the important initiatives and trends related to the use of biometric identifiers and identity management technology.

1.1. Initiatives within the Border Management and Immigration Security Space

The following initiatives are being observed in Border Management and Immigration agencies globally:

- Joined Up Security - Many governments have already adopted “joined up” strategies through merging of agencies or effective sharing of data through systems connectivity to achieve greater security benefits.
- Whole of Government Data Interchange – Exchange of identity information among police, intelligence, centralised criminal systems, immigration, passports and visas, border management/control and social security enables more efficient processing of cases.
- Regional Security and Commerce Considerations - Along with trade comes the need to facilitate the movement of people among co-operating nations by convenient and accurate identification of travellers. Specifically, economic blocks or trade partners with a high proportion of international travellers want to facilitate commerce and expedite traveller processing.
- International Interoperability - Bilateral interoperability and data exchange agreements can be extremely useful in both facilitating travel and in identifying persons of interest.

© Copyright 2009 Daon

- Integrated Multi-Biometric and Biographic Watch lists - Coordination, integration and consistency checking of biographic and biometric watch lists enable more accurate searching at checkpoints.
- Automated and Supervised Biometric Clearance - Passports are becoming more favourable than secondary token or token-less clearance processes. They provide the basis for automated and semi-supervised clearance as travellers already need to carry travel documents at border crossings, avoiding the need for new enrolment processes.
- Identity Management Models - Either a central Identity Management System or Identity Hubs can serve as a "gateway" for handling identity service requests from external sources.
- Identity Lifecycle - Managing the identity life cycle can reduce the incidence of misidentification and allow government personnel to deal with people in the proper way, according to their status and history. Recording of staff ID at each decision point in dealing with a client also provides significant benefits in terms of audit trails, investigations and deterring fraud.

1.2. Trends

The approach to using new technology is now more sophisticated and ensures that process efficiencies, cost savings, enforcement and civil security are balanced requirements of new programmes.

- Information Sharing and Interoperability - Interoperability requires architectural support, clear interface specifications and policy driven data exchange.
- System architectures are moving towards more open, services based architectures based on COTS products.
- Multi-Modal Biometrics – As modalities are becoming more robust, use of fusion techniques in more advanced multi-modal systems has much to offer, including improved accuracy, greater universality and better fit for purpose.
- Person and Encounter Based Identity Models - A hybrid of person and encounter based identity interaction models can give more robust identification results. Each subject is uniquely identified within the system and has a master "best information available" record but also has a set of encounters linked to that record which are searchable and retrievable.
- Privacy and Security for Citizen and Non-Citizen Data - Once a consideration primarily for citizen data, privacy and security are now also becoming a concern for non-citizen data. The traditional approach of handling citizen and non-citizen data differently is shifting towards consistently applying the appropriate protections to all persons of interest, especially since some non-citizens eventually migrate to become citizens.
- New immigration and border security programmes can be difficult to contemplate in terms of size, cost, and political risk; however, system development need not be an "all or nothing" proposition. Programme phasing is considered much more appropriate in the context of funding and business case reviews.

© Copyright 2009 Daon

1.3. Conclusion

The challenge for immigration and border security agencies is to embrace the available technology capabilities (through an integrated framework of projects to support a range of business improvements that are anchored by best practices in identity management) and use biometrics as an aid to ensuring “one person / one identity.”

Opportunities exist for modernizing existing systems, expanding applications, applying new identity technologies, and increasing inter-agency cooperation in a logical and cost-effective manner.

Effective identity management incorporating biometric functionality can be at the forefront of addressing Immigration and Border Security challenges. Next generation architectures ensure that solutions are future proofed by implementing vendor and technology independence, using a Service Oriented Architecture approach, and choosing suitable flexible identity models where biometric data becomes an extension of biographic identity data.

Innovative programme approaches including phasing and system build-out are required to align with funding challenges and to allow more fine grained business cases to be established.

© Copyright 2009 Daon

2. Background

Identity management systems incorporating biometric and identity functions are increasingly used within governments as an important tool in improving the integrity, security, and effectiveness of immigration and border security solutions. Some very *early* examples of such solutions include:

- The US INS Passenger Accelerated Service System (INSPASS) (1993) which used hand geometry to "automate inspection" of known travellers through immigration at some air and land ports of entry and used voice (speaker verification) in conjunction with RFID tags at some vehicular land crossings;
- Canadian Passenger Accelerated Service System (CANPASS) which used fingerprint and now uses iris for similar purposes;
- Singapore Immigration Automated Clearance System (IACS) (1996) which used fingerprint;
- The Israeli BASEL project (1999) which initially used facial recognition and hand geometry, later adding fingerprints, at the Palestinian border.

Since biometric and identity management technologies were initially used in these early systems, there has been significant advances in the technologies and how they are used. Table 1, below, provides a quick look at this progression and some trends which will be investigated further in this paper.

	First Generation (Early adoption)	**Following Generations (Later in adoption cycle)**	**Latest Generation (More advanced in adoption cycle)**
Business Objectives	• Process Efficiencies • Recidivist Identification	• Security • Border Control • Immigration • Process Efficiencies	• Security • Border Management • Immigration • Visa Processing • Process Efficiencies
Reference Programmes	• INSPASS • CANPASS • IACS • BASEL • Department of Homeland Security - Automated Biometric Identification System (IDENT)	• Privium (Schiphol) • UK Iris Recognition Immigration System (IRIS) • US NEXUS & US Secure Electronic Network for Travelers Rapid Inspection (SENTRI) • US Visitor & Immigrant Status Indicator Technology (US-VISIT) • Australian Customs SmartGate • Eurodac	• Japan Automated Border Control (ABC) • UK E-Borders • EU Biometric Matching System (BMS) • United States Citizenship and Immigration Services Biometric Storage System (USCIS BSS) • US Registered Traveller Program (US RT) • Australian Department of Immigration and Citizenship (DIAC)

Table 1: Progression of Border and Immigration Systems

© Copyright 2009 Daon

3. Immigration and Border Security Initiatives

In this section, some of the key Immigration and Border Security initiatives that are being considered globally are examined further, including:

- Joined up Security
- Whole of Government Data Interchange
- Regional Security and Commerce Considerations
- International Interoperability
- Integrated Multi-Biometric and Biographic Watch lists
- Automated and Supervised Biometric Clearance
- Identity Management Models
- Identity Lifecycles

As governments continue to address evolving security and business services needs, a number of these initiatives offer cost savings and process efficiencies while leveraging existing capabilities and investments.

3.1. Joined up Security

Civil security involves many different agencies and systems. These range from asylum to detention, including refugees, secondary line processing and overstays with the common thread being *identity*. This highlights the need for a single, coordinated approach to managing identities across agencies involved in border security and introduces a need for efficient sharing of identity information across systems both within an individual agency and also across different agencies. An identity of interest may exist in one system (or subject category) but not others – how can they be found?

Independent “silo” systems were developed to handle initial requirements and workloads and generally do so very well with respect to their original charter. However, as requirements expand, caseloads increase, and information sharing becomes more critical, the existing infrastructure cannot easily grow and adapt to the new needs and environment.

Access to identity information collected in each business transaction is required by agency officials who are tasked with assessing the information and making informed decisions at the various stages of a person’s dealings with their agency. A person may continue to deal with an agency for many years from the first application to enter a country, to applying for a work permit and residency and culminating in an application for citizenship. The only way this can be completed in an informed manner is to ensure a rigorous management system is in place that enables the officials to make decisions at each point that are correct, recorded, and then available for subsequent business transactions involving this person.

Identity information should be processed, stored, and made available in a consistent manner while retaining flexibility in business rules and support for agency-unique requirements. Cross-agency identity searches need to be supported so that all available (and appropriate) information is accessible when and where it is needed. Implementing new business use cases should be done on a case by case basis to avoid the “big bang” approach.

Identity management in immigration and border security is now a team effort for agencies involved in border security. Many governments that have already adopted “joined up”

© Copyright 2009 Daon

strategies are finding that even though merging agencies may not be appropriate for their situation, real benefits can be achieved from greater sharing of data and systems connectivity.

3.2. Whole of Government Data Interchange

The need for data interchange goes beyond agencies focused on immigration only. Today, there is a need to exchange information with and among police, intelligence, centralised criminal systems, immigration, passports and visas, border management/control and social security with a focus on the availability and analysis of data.

Why is this important?

> *"In February of this year, Oakland police and San Francisco ICE officers were contacted regarding victims of alien smuggling. Fingerprints were lifted from a suspect's car to a local motel used by the smugglers. The prints were sent to US-VISIT to be run against all latent prints and a positive match was made to a person with an immigration criminal history. He was placed on a watch list and later arrested by the border patrol in Arizona."*
>
> US Secretary of Homeland Security, Michael Chertoff in December 2007

This occurred due to the implementation of the interoperability recommendations of the 9/11 Commission. In the same speech, Mr. Chertoff described a situation in which fingerprints in the US-VISIT system were later matched against those on a car bomb in Iraq due to data interchange with the Department of Defence.

This underscores the need for the capability to easily interchange data between agencies and to configure policies for such interchange. This includes enacting routing decisions (which data can/cannot be shared), implementing format translations, and importing and interpreting received data.

The importance of appropriate security protocols to ensure access is only granted to those who need and are authorized access along with effective audit systems will help ensure that this sharing of information will be accepted by a larger portion of the public than may otherwise be the case.

3.3. Regional Security and Commerce Considerations

Another area of data interchange are those related to regional economic cooperation initiatives, such as NAFTA, EEA, EU and APEC. Along with free trade comes the need to facilitate the movement of people among cooperating nations. This, in turn, requires the ability to quickly and accurately identify these people.

Often, but not always, a visa waiver arrangement is in place either among all cooperating member states or bilaterally on a case-by-case basis. Where visa waivers exist, some standard must be in place for the issuance of passports (or other accepted travel document). Sometimes, a biometrically enabled 'border crossing card' is issued as an alternative to non-immigrant visas (for example, the US-Mexico BCC and Western Hemisphere Travel Initiative, WHTI). This generally requires cooperation between departments/ministries of commerce, immigration, and state/foreign affairs. As such, legislation is usually required along with the associated political discussions and processes. Additionally, application and adjudication processes must be defined and administrative and logistics arrangements made (e.g. at consulates or online).

© Copyright 2009 Daon

If a card is used, it may follow the ICAO 9303 TD-1 format and requirements, or could be of some other agreed-upon form. Despite the additional cost and logistics associated with a biometric enrolment, this is recommended in order to tightly bind the card and the applicant to whom it was issued. Biometric enrolment also allows use of any additional support for background checking that may be available. The use of existing travel documents will drive adoption over the use of an additional card as it avoids the need for travellers to enrol in a new system.

3.4. International Interoperability

International cooperation is also critical to border security and requires interoperability in order to exchange information with other border security programmes. Good examples of this are the EU-Biometric Matching System (EU-BMS) and Eurodac systems which exchange information on visa and asylum applicants.

Bilateral agreements are extremely useful in both facilitating travel and in identifying undesirables and those requiring detention. Such agreements could be put in place to allow exchange of information with existing/emerging border systems such as US-VISIT.

3.5. Integrated Multi-Biometric and Biographic Watchlists

One particular area in need of coordination and integration is that of watch list management. Any process that requires vetting, adjudication or entry/benefits decisions generally requires a watch list check – biometric and/or biographic. Rather than a hit or miss approach to populating and searching these watch lists, a more structured methodology and infrastructure is warranted. Watch lists may have different criteria and content depending on their purpose.

Watchlist Content

Some watchlists may simply consist of facial images. Others may contain a name and biographic details. In still other watchlists (e.g., deportee) a full set of fingerprints may be available.

Watchlist Population

Some watchlists may contain known or suspected terrorists only, while others could include wanted persons, children of parents in dispute, violent criminals, or sexual registrants, and yet another may cover immigration violators or refused visas.

Watchlist Use

Certain transactions might search all watchlists while others may search a subset. Different thresholds might apply for different transactions. When multiple modalities or information types exist, the possibility of rules-based fusion exists as well. Response times and assigned priority also vary by transaction types – e.g., those at ports of entry requiring a much faster response than for a visa application.

It is important to construct systems to ensure the maximum time possible is available to search against these watch lists in order to produce a result that can be practically used; for instance, getting a result before the person of interest has disappeared into the general population.

© Copyright 2009 Daon

Given these variations, a system must support multiple (or partitioned) watchlists of various types, and multiple modalities (e.g., biographic, face, fingerprint; possibly even latent fingerprint) and these need to be managed through business rules and configurable policies.

A process for populating the watchlists is important, as is synchronization when multiple, distributed watchlists are used. Flexibility is the key in order to accommodate additional lists or changing criteria in future.

3.6. Automated and Supervised Biometric Clearance

Automated clearance systems aim to facilitate the passage of legitimate travellers, increase processing efficiency, and allow more attention to be paid to those travellers remaining. Automated Clearance systems are generally not intended to replace immigration officers, but provide a mechanism to prioritize their attention to manual/supervised clearance and passenger profiling, thereby allowing a single officer to supervise multiple e-Gates. For these reasons, such systems are growing in implementations.

Programme participants need to be thoroughly vetted to determine a risk level. This vetting process may include various background checks, travel history, and an in-person interview. Subsequently, the programme applicant needs to be biometrically bound to an identity record (and document) such that a rapid and accurate biometric verification can be performed at the border (primary inspection).

Depending on the country's policy and the biometric(s) used, a document or credential may or may not be required. For example, a highly accurate iris system can perform a 1:N identification of participants quickly without the need for a claim of identity (such as a passport number). Other systems favour the use of either an existing document (such as a passport/e-passport) or newly issued credential (such as a smartcard) with the biometric securely stored in that document/credential. In general, a document like the passport/e-passport is favourable because it is a document most travellers are already carrying while travelling. Further, 1:1 verification is much faster and requires fewer resources than either issuance of cards or use of 1:N identification.

As an alternative to using a locally stored biometric, the system may use the unique document/credential ID as a pointer into a central database of biometric records. Multiple biometrics can be used to allow for user preferences and to broaden usability, or to allow different biometrics to be used for background checking versus verification purposes.

Programmes may cover only returning nationals or may also include frequent travellers from other countries, the latter possibly involving reciprocal agreements. For example, the US Global Entry system, initially rolled out for US citizens, is considering joint statements of cooperation with the Netherlands, Germany, and the UK.

3.7. Identity Management Models

Due to the evolutionary nature of system development and the unique requirements of different agencies, identity-related data is held in many different government systems. This results in both duplication of data and "hidden data". Data associated with a given identity is held in one system while another system, which also holds data for that identity, is completely unaware of the existence of the first system's data. This data may be biographic or biometric, older or newer, consistent or conflicting.

© Copyright 2009 Daon

It is desirable that identity data be synchronized and accessible across agencies involved in border security. This can be accomplished via a central identity repository or through distributed repository architectures.

In the central scheme, existing databases are consolidated into a single (high availability) master data repository that each system can access in support of their business processes. This minimizes data duplication and synchronization issues, and allows for strong security measures to be implemented. On the other hand, some cultures object to what is seen as large scale aggregation of personal data, whether citizen or non-citizen.

In the distributed architecture, data exists in multiple systems, but the various systems can search and access data in other systems (though linkages) according to business rules and policies. This is arguably more technically complex to manage and maintain, but could require less immediate changes to the various systems involved while also avoiding the aggregation concern. It usually involves some degree of data duplication, but this can be minimized by design.

One consideration is how services are defined and provided. It is desirable that a service layer be implemented that supports both a common set of independent and reusable services as well as a set of custom services for unique business needs. The expensive alternative is having each system provide its own unique set of services and unique interface processing for each system with which it needs to exchange information.

It is easy to see how this can be achieved in a central scheme, but it is also possible in a distributed system if a “services hub” is used with each (client) system subscribing to the hub. The hub then consolidates and routes identity service requests across the enterprise. The hub concept can also be used as a transitionary mechanism – where over time the capabilities of the hub are expanded until it “becomes” the central identity management repository itself, subsuming data responsibilities over time as client systems are modernized or in some cases phased out.

Either the central system or hub can also serve as a “gateway” for handling identity service requests to/from external sources.

An example of such a repository is the USCIS biometric storage system. This system holds over 53 million subject biometric records of the Citizenship and Immigration Service and is expected to manage all biometric background checks in the future (i.e., routing and tracking such checks to the FBI and US-VISIT).

3.8. Identity Lifecycles

An identity has a life cycle. It is established, certain information is associated with it, it is verified at various points and times, and a history is developed for it. Once an identity is registered within a business system, that identity is linked with events, activities, documents, and information as the subject interacts with the system (or cooperating systems) over time. For example, the status of an individual may transition from an asylum seeker, to a resident, to a citizen. Interaction events may include such things as a border crossing, document issuance, or watch list addition.

Managing the identity life cycle can reduce the incidence of misidentification and allow government personnel to deal with people in a manner appropriate to their status and history. Recording of staff ID at each decision point in dealing with a client also provides significant benefits in terms of audit trails, investigations and deterring fraud.

© Copyright 2009 Daon

A critical element, and a foundational one for biometrics in particular, is the anchoring or fixing of an identity at a point in time, precluding the ability of a person known to the system to later assume another identity. Once fixed, this identity is uniquely enumerated and all subsequent contacts with that person can be linked back to that single, unique ID. This can then support, for example, a case management or other encounter-based system. Further, the unique identity identifier can link together events across multiple, cooperating systems.

Case workers can use this information to perform their tasks in an informed manner and identity can be dealt with at a business level.

© Copyright 2009 Daon

4. Immigration and Border Security Trends

Traditionally, business cases were evaluated based on a technology's contribution to enforcement and civil security – "the mission". The approach to using new technology is now more sophisticated and ensures that process efficiencies, cost savings, enforcement and civil security are all addressed equally within the business case for new programmes or existing programme enhancements.

In this section, some of the key Immigration and Border Security technology trends are outlined further, including:

- Information Sharing and Interoperability
- Evolving System Architectures
- Multi-Modal Biometrics
- Hybrid Identity Models
- Privacy & Security
- Programme Approaches and Timelines
- Programme & System Phasing

The approach has shifted from creating a business case that fits the 'new' technology to analysing the business outcome.

4.1. Information Sharing & Interoperability

Due to the narrow capabilities needed and technology available, early generation identity systems were often built as "closed systems" for very specific requirements with little need for sharing of information externally. However, as border and immigration issues have come to the forefront of national, regional and global security, the need to share and exchange information has become critical. In addition, as identity systems grow exponentially, the need to share rather than duplicate data for efficiency reasons has also developed.

Information sharing falls into the following main categories:

- Cross-programme - Within a given agency, there may be a need to share information between projects or programs (e.g., between visa issuance and asylum systems).
- Inter-State – State/provincial governments typically have law enforcement responsibility and need to be able to share information collected with other State and Federal systems to allow many stakeholders to carry out their responsibilities.
- Cross-agency - Within a government, a need generally exists to share information between departments or agencies (e.g., between border control and law enforcement).
- International - Allied nations, regional pacts, or bilateral agreements frequently necessitate the exchange of data between countries.

Interoperability is the key to the success of any data exchange. Interoperability requires both architectural support and clear interface specification including data formatting and security. Policies and procedures for the handling of exchanged data must also be in place.

© Copyright 2009 Daon

Partially as a result of this need, the development of identity standards has accelerated. With regards to biometrics, in addition to the ICAO standards, relevant biometric, ID/smartcard, and security standards have been developed in ISO (i.e., JTC1 SC37, SC17, and SC27). Although these go a long way towards the achievement of interoperability in terms of technical specifications, it is important to note that they do not guarantee it in and of themselves.

Examples of data sharing and interoperability include:

- The EU-VIS/BMS system in which the EU members will share visa application information to address the "visa shopping issue" and the existing Eurodac system which performs a similar function for asylum seekers.
- The US-VISIT/IAFIS interoperability initiative in which data is shared (and cross-matching performed) between entry, watch list, and criminal fingerprint databases, resulting in over 15,000 wanted criminals being identified by 2006 (including the DC snipers).

4.2. Evolving System architectures

System architectures have been moving from proprietary client/server software applications that are built around and tightly coupled with the selected technology towards more open, services-based architectures based on COTS products and infrastructure. Some observed trends in this area include:

4.2.1. Embracing SOA

The inherent characteristics of SOA provide benefits such as service/component reuse, scalability, interoperability, flexibility, and maintainability. This has been the case with most of the leading biometric systems modernization projects. Some examples are the European Union Biometric Matching Systems (supporting 70 million biometric records and associated search requests across 22 member states) and the United States Citizenship and Immigration Services (consolidating 53 million biometric records from multiple systems while building SOA-based interfaces to external biometric systems such as US-VISIT and FBI).

> *"BMS requires the highest levels of availability and security, in addition to providing state-of-the art biometric matching at a competitive cost. The selected team used a COTS-based approach that minimized schedule risks and achieved a highly competitive price. Best of all, the resultant BMS architecture is flexible enough to accommodate future requirements as policies and business processes evolve over time."*
>
> Dr. Frank Paul – heading large-scale IT system development in the European Commission's Directorate-General Justice, Freedom and Security.

Of particular interest is the fact that the US Federal Bureau of Investigation (FBI) has mandated such an architecture for its Next Generation Identification (NGI) system which will replace its current AFIS capability.

4.2.2. Multi-Application Infrastructures

Rather than building silo systems, each with their own infrastructures, there is a trend towards use of a central infrastructure for multiple applications. This not only supports such goals as elimination of redundant and/or isolated "stovepipe" systems and managed data

© Copyright 2009 Daon

sharing and synchronisation, it also maximises investments in identity infrastructure through reuse rather than duplication. Following this trend will enable an agency's central infrastructure to support multiple business function applications internally and then easily extend this support to another agency's applications.

Leading examples of multi-application systems supported by a single infrastructure include the Qatar and Japan border control and eGate systems. The EU BMS is designed and planned to support other applications beyond the initial visa system (e.g., Schengen, Eurodac, and IRT). DIAC's Biometric Authentication Management System for asylum, refugees, and foreign fishermen also falls into this category.

Figure 1 illustrates the multi-application infrastructure deployed in Qatar. It demonstrates how the system supports multiple biometric modalities across multiple applications including border control, citizen identity, and law enforcement.

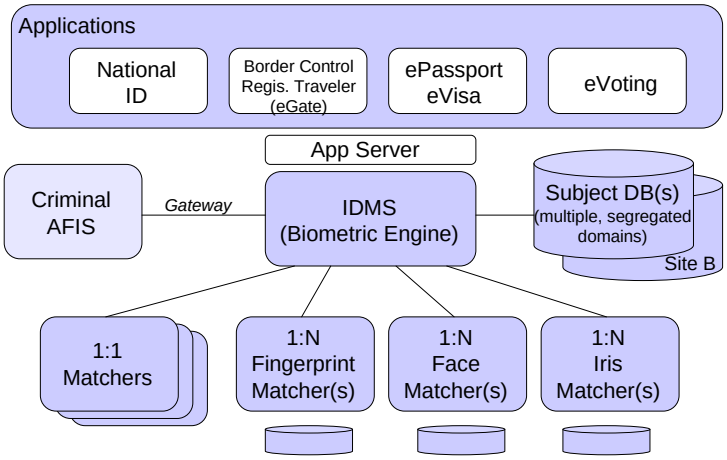

Figure 1 - Multi-Application Architecture of Qatar

4.2.3. Vendor/Technology Independence

Instead of building a system around the identity management technology, modern systems are decoupling the business application from the underlying technology. The aim is to avoid vendor and technology "lock-in" which limits future flexibility and drives up life-cycle cost. This is particularly relevant to biometric solutions. In modern systems, a layered architecture is preferred and allows for both vendor and technology (including modality) independence. This provides the flexibility to respond to changing requirements and to take advantage of technology enhancements more readily. The ability to "mix and match" components allows for the addition or substitution of technologies (e.g., adding facial recognition to a fingerprint system), improvements in accuracy through fusion, and re-competition for incremental increases in capacity.

4.2.4. Biometric Middleware Functionality

In many ways as a result of these architectural trends, identity systems are now incorporating "biometric middleware" functionality at the heart of their technical architectures. This allows the decoupling of the business application layer from the biometric matching layer. This layer can now form the central infrastructure for managing all identity-related capabilities and resources, becoming an "identity management platform" for biographic and biometric data. Today, there are COTS products offering this functionality which are highly configurable for

© Copyright 2009 Daon

addressing individual system requirements. These products offer Web Services integration, multi-application support, and vendor independence. In fact, all of the systems shown in the "advanced" column of Table 1 implement a biometric middleware functionality using COTS products.

4.3. Multi-Modal Biometrics

More and more programmes are opting for a multi-biometric system rather than a single modality or are designing their systems to enable the inclusion of additional biometrics at some point in the future. This is partly because newer modalities are becoming more robust and thus feasible for use and because of advances in fusion techniques, but also due to the following benefits of multiple biometrics:

- *Purpose fitting*. Some biometrics work better for a given function, application, or environment than others. A system that can support multiple biometrics allows use of the best biometric (or set of biometrics) for a specific purpose. For example, one biometric may be better for outdoor environments than others more suitable for indoors, while another may be better for time consuming background checking rather than high throughput verification. In some scenarios, cultural requirements need to be taken into account especially with respect to facial recognition.
- *Improve accuracy*. Each single biometric exhibits its own accuracy performance in terms of false match and non-match rates (under given conditions). Combining biometric modalities can reduce these error rates below those of either modality used in isolation. For example, the fusion of fingerprint and facial scores has been shown to work well together. This can also be true for multiple algorithms for the same modality, if sufficiently different.
- *Universality*. Every biometric has some measurable failure to enrol rate. That is, some segment of the population is unable to enrol or consistently acquire samples of usable quality. This may be due to age, occupation, disability, or other factors. Use of more than one biometric can broaden the population of those who are able to successfully use or be processed within the system. For example, a person with severe cataracts who is unable to enrol their irises may be able to enrol their face or fingerprints.
- *Increase security*. Use of multiple biometrics, or a biometric with another type of authentication (e.g., smartcard), increases the number of authentication factors, and thus the difficulty of attack. This is also one of the countermeasures against sensor spoofing.

Systems that require background or watchlist checking in addition to an operational verification component will frequently choose to enrol one biometric (e.g., fingerprints) for the background checking function but another biometric (e.g., face or iris for known travellers) for operational use. Fingerprints are often the common thread between law enforcement, intelligence and border systems. This is because the use of fingerprints is well understood, as they have been in operational use for decades and are accepted as a reliable legal basis for identification. However, an additional biometric has advantages such as dealing with failure-to-acquire situations.

© Copyright 2009 Daon

4.4. Hybrid Identity Models

Traditional identity management systems are person-centric. That is, they maintain a single, unique view (set of information) of each individual subject. As new information becomes available, previous information is updated or replaced. For example, a single master set of fingerprints may be maintained for a given, uniquely identified subject.

An encounter-based model, on the other hand, maintains records for each encounter with an individual. Usually, and where possible, these encounters are linked to a unique identity (typically through a biometric match). This is also known as "Identity at Event" as initially piloted within DIAC. This model is valuable in case management environments.

An example of an encounter-based application is the ability to confirm with confidence at each step of the process an applicant's identity when dealing with a government agency (e.g., the application, interview, medical check, departure check, arrival at border check and then all internal business transactions with a government agency such as Immigration). An example of this is the US-VISIT IDENT database which retains data, including biometrics, for each entry into the country.

An example of a person-centric application is the provisioning of a biometric authentication / access control system.

In immigration and border management applications, the trend is towards a hybrid model. That is, each subject is uniquely identified within the system and has a master "best information available" record, but has a set of encounters (also uniquely identified) linked to that record which are searchable and retrievable.

4.5. Privacy and Security

As identity systems, including those with biometric content, are growing in size and visibility, the privacy and security of these systems is receiving more scrutiny. When systems were smaller and more closed, these issues were not seen to be as critical as they are now becoming. The level of privacy required also varies from country to country and the requirements in each country can be quite different. Although the benefits of open architectures and information sharing (as discussed above) are great, they also create challenges to maintain the security and integrity of the system and to ensure the privacy of personal information.

The trend in this area is to address these issues early in the programme – from both the policy and technical aspects. Privacy Impact Assessments (PIAs) are being adopted as is the development of Privacy Policies. Both address the information to be collected; its update, retention, and destruction; its access and sharing; and its protection.

The encryption of biometric data in transit, in operation and at rest (particularly within central databases) is becoming the norm. Best practice also includes limiting data collected to the minimum needed without adversely impacting functionality – i.e., only sufficient data to meet mission requirements and to prevent misidentification and false hits.

Once a consideration for only citizen data, privacy is now also becoming a concern for non-citizen data. The traditional approach of handling citizen and non-citizen data differently is shifting towards consistently applying the appropriate protections to all persons of interest.

© Copyright 2009 Daon

4.6 Programme Approaches and Timelines

New immigration and border security programmes can be difficult to contemplate in terms of size, cost, and political risk. However, system development need not be an "all or nothing" proposition. Projects can be sized and phased to meet programmatic needs in these areas. Table 2 provides some comparative system scopes.

Type	Cost range	Timeframe
Focus on business improvements through a single project.	$2-10M	6 mo – 1 yr
Delivery of multiple business outcomes through a range of projects.	$10-50M	1-2 yrs
Integrated framework of business improvements	$50-100M	multi-year

Table 2: System Scopes

4.6.1 Programme Phasing

Programmes typically move through a series of phases from initial concept to final deployment and operation. At each step, decisions are made based on available data as to whether or not to continue forward and if so, which direction to move both technically and programmatically. As funding, design, and implementation decisions are made, options are narrowed.

In the early stages, various information gathering and risk reduction approaches can be taken, such as:

- *Requests for information.* With no procurement obligation, the agency may solicit information from industry and academia to learn about feasibility, available solutions, and estimated costs. This can inform decisions moving forward.
- *Prototyping.* When more than one approach appears feasible (or to determine feasibility), small scale prototyping can be performed to prove out and compare characteristics and performance.
- *Proof-of-Concepts and Pilot systems*. Rather than bite-off a full scale system deployment, a smaller scale implementation can be built and deployed to address either a portion of system functionality or a segment of the target environment.
- *Phased procurement or build-out*. Programs can be partitioned into segments that can be procured or developed incrementally.

This allows the ability to investigate the impact of technology with a low risk to the overall programme. Lessons learnt from such activities will allow the next phase to take advantage of these lessons thereby enabling business functionality and architectural decisions to be adapted to better meet the organisation's objectives.

A variety of procurement models exist ranging from procurement through a prime contractor who leads a consortium, selection of an overall integrator, adoption of individual COTS components and direct procurements of systems and expertise.

© Copyright 2009 Daon

4.6.2 System Phasing

The "big bang" approach to system development is no longer the norm as budgets and risk concerns advise against it. Another approach is to build-out the system in phases. This is particularly applicable for layered or multi-application systems where the system can be developed in a staged manner. For example, systems typically comprise front-end applications, an IT/network infrastructure, databases, and back-end services/resources. A possible phasing of build-out could include:

- Develop overall system concept, requirements, and architecture.
- Build-out the back-end, including databases and resources needed to supply services required by the business application(s).
    - Note that this must be scalable, but not necessarily built to scale initially. In fact, it may initially address only critical services or those required by the first application to come online.
- Build the service interfaces and supporting communications network/infrastructure.
- Build and test application #1.
- After application #1 has been successfully deployed, is stable, and the need exists, build and test application #2, expanding the backend and services as necessary.
    - Note – the backend should have been built to support multiple applications and identity technologies/biometric modalities. If the first application required only a single technology while the second required either a different or additional modalities, they can be added at this point.
- Continue until all applications and supporting capabilities are in place.

This approach allows multi-year budgeting and supports a series of gated decision points. It also supports renewed competition at appropriate junctures. At any point, future plans can be postponed or modified. It should be noted, however, that this approach is dependent upon the use of a flexible, scalable architecture from the outset.

The phasing of programmes and systems ensures key benefits and return on investment can be established early, thereby building confidence in the approach.

© Copyright 2009 Daon

Background on the Author – Catherine J. Tilton

Catherine Tilton is the VP for Standards & Emerging Technologies at Daon. Catherine is a recognised leader in the field of biometrics and identity and the application of these technologies in national security systems. She is frequently sought for speaking engagements globally.

Cathy has over 25 years of engineering and management experience, including over 15 years in the biometrics industry. She has led or been involved in the design, development, and deployment of numerous biometric systems in both the commercial and government domains.

Cathy's experience includes:

- US United States Visitor and Immigrant Status Indicator Technology (US-VISIT),
- US Transportation Security Administration (TSA) – Transportation Worker Identification Credential (TWIC),
- US Department of Defence (DoD) Common Access Card (CAC) for logical and physical access,
- US Defense Information Systems Agency Common Operating Environment biometric framework, and
- FBI Automated Fingerprint Identification System - Prototype and System Design.

She is also an authority on biometric standards, serving (or having served) as:

- US Head of Delegation to ISO/IEC JTC1 SC37 subcommittee on biometrics,
- Chair of the Biometric Identity Assurance Services (BIAS) Integration technical committee at OASIS.
- Chair of the BioAPI Consortium,
- International Representative of INCITS M1 Technical Committee on Biometrics,
- Chair of INCITS Ad Hoc Groups studying integration of biometrics with the government smart card and biometrics in e-authentication,
- ISO Project Editor for ISO/IEC 19784-1, BioAPI 2.0, and BioAPI Lite,
- Active participant in the Registered Traveller Interoperability Consortium (RTIC), and

Prior to Daon, she held a similar position at SAFLINK and was a systems engineering department manager at Unisys, where she was involved with large scale electronic defence systems development. As a captain with the US Army, she was involved with R&D and testing of new communications-electronics equipment/systems. She has a BS in nuclear engineering from Mississippi State and an MS in systems engineering from Virginia Tech. Catherine has been the recipient of the Unisys President's Award for Engineering Excellence, the CTST Larry Linden Security Technology Award, and most recently, ANSI's Lohse Information Technology Medal.

© Copyright 2009 Daon