Macrothink Institute™

Business and Management Horizons
ISSN 2326-0297
2013, Vol. 1, No. 1

Connected Government: An Exploration of the UAE's Identity Management Integration Strategy

Ali M. Al-Khouri

Emirates Identity Authority, Abu Dhabi, UAE

E-mail: ali.alkhouri@emiratesid.ae

Received: March 5, 2013 Accepted: March 27, 2013 Published: April 1, 2013

doi:10.5296/ bmh.v1i1.3463 URL: http://dx.doi.org/10.5296/ bmh.v1i1.3463

Abstract

The subject of connected government is coming once again to the forefront of national development priorities around the world. This stems from the need to address various local and global necessities in light of the changing landscape of the new digital world we live in today. In a connected government context, public service agencies are needed to act as a single enterprise so that citizens feel they are being served by one organization rather than a number of different public authorities. Identity management is considered here a fundamental pillar to enable such operating models and support single sign-on (SSO) and online identity validation capabilities for e-government and e-commerce environments. This article explores and describes the United Arab Emirates (UAE) government integration strategy with relation to keeping its national identity management infrastructure (population register) updated as *life events* take place. The integration strategy also aims to support federal and local government entities to verify citizen and resident information using their own applications in a secure, reliable, and integrated manner. Another expected contribution of the integration platform is to support decision-making and strategic planning dimensions of government work.

Keywords: identity management, identity lifecycle, connected government, e-government

1. Introduction

In a world characterized by rapid change driven by globalization, governments around the world are under extreme pressure to renovate their operating models and provide quality e-government services with secure interconnected systems and applications (Dunleavy et al., 2008; OECD, 2011; Saha, 2012). Despite the enormous number of strategic projects and gigantic investments, governments around the world have been facing challenging times to achieve interconnection between their "silo living" backend systems (Backman, 2009; Bertucc, 2008; Kubicek et al., 2011; O'Brien, 2012). Governments' attention have been shifting lately toward a "*whole-of-government*" approach that focuses on the provision of services at the front end supported by integration, consolidation, and innovation in back-end processes and systems to achieve maximum cost savings and improved service delivery (UNPAN, 2008).

In the past ten years or so, many governments have launched modern identity management programs in an attempt to address a number of national priorities (Al-Khouri, 2012a). Among these are objectives related to building an infrastructure to support the authentication of online users. These programs are also based on a strong belief that a robust and secure government-owned identity management system is crucial in addressing many of today's needs and challenges. This is to say that such identity management systems can be designed and architected to develop digital identities and online identity validation capabilities to support e-government and e-commerce environments (Al-Khouri, 2012b).

However, the primary focuses of these programs, from our reading and knowledge in the field, have been on the enrolment of the population and the issuance of smart identity cards but without sufficient attention to the overall management of the identity lifecycle. This is to say that, once a person is enrolled, his or her personal data may change, e.g., legal residency status, education, marital status, etc. Such updates are considered critical in such programs to fulfilling their mandate of being the primary reference for personal data.

One of the internationally recognized countries for its innovative and state-of-the-art identity management programs that have recently drafted a strategy to address this particular need is the United Arab Emirates (UAE). Having completed the enrolment of the population, the UAE government has recognized that it is imperative to maintain an up-to-date national population register. To achieve this strategic objective, the government has conducted a detailed analysis of how citizen and resident information can be updated instantaneously as life events take place. This article aims to outline the UAE's government integration strategy to enable a connected government concept and to support its federal e-government strategy. The explored integration strategy is, in principle, related to identity life cycle management.

The article is structured as follows. In section 2, we shed light on some of the global trends with regard to identity management and enterprise integration, as well as some key challenges faced by governments in this field of practice. In section 3, we provide information about the UAE national identity management infrastructure and the government's need to architect an enterprise integration strategy to keep the population register up to date. In section 4, we provide an overview of the UAE integration strategy, objectives, and

priorities. In section 5, we describe the integration framework adopted by the UAE government and briefly describe the integration models, services, architecture, and governance aspects. We also address a high-level plan and the phases of the on-boarding of government entities, and we outline key projects and initiatives and the roadmap set for the implementation of the integration strategy. In section 6, we present some key success factors identified by the government to ensure a successful implementation, and we conclude the article in Section 7 with some perspectives.

2. Global Trends of Identity Management and Enterprise Integration

Governments around the world have been very much attracted to national identity programs (Al-Khouri, 2012a; Al-Khouri, 2012c). These programs are globally justified on the basis of building identity management systems to achieve two primary objectives: to support national security and improve access to services. Many countries have initiated smart identity card programs in the last decade, with the total value of those projects exceeding $24 billion. Further, more than 15 countries are in the process of upgrading their current identity cards to biometric-based systems.

Around the world, governments are struggling to maintain an up-to-date national population register to provide the different government entities with accurate information on citizens and residents. Typically, a citizen or resident will require multiple identification and supporting documents to access government-provided services. According to a recent United Nations report, even in highly ranked countries, the population and the governments are still in the process of understanding the role of national identity cards and how they can leverage such a valued asset in simplifying the lives of both the public and government entities in uniquely identifying a person and maintaining an up-to-date snapshot of information (UNPAP, 2012).

For example, in Sweden, government entities rely on bank-issued identification cards to register and apply for government services. In the U.S.A. and the U.K., different forms of ID are accepted, with the U.S.A. being more complicated given the different IDs issued at the federal and state levels with minimal integration or interoperability between the government departments. Korea and Singapore are the leading countries that have achieved a good level of success in providing a single ID that is issued to every citizen and resident, providing them with access to government services. Let us explore some common integration approaches in the next sub-section.

2.1 Enterprise Integration

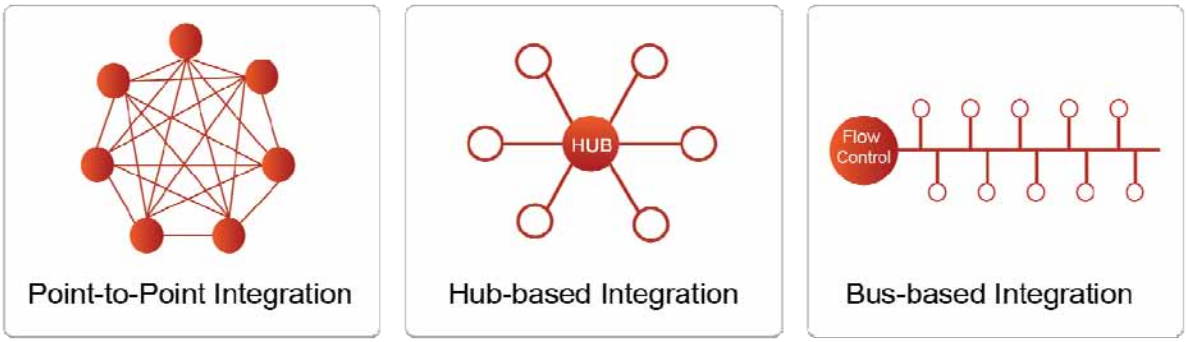

Figure 1. Integration approaches

One of the key factors to establish successful identity management is the integration between the different government entities and the entity responsible for managing identities (Bertino and Takahashi, 2010; Chappell, 2004; Williamson et al., 2009; Windley, 2005). For many years, integration has been handled at a system level where the primary focus is to identify what data is needed and how to send it to another system, creating a point-to-point integration pattern. As the number of systems grew, adding more point-to-point integration interfaces led to complex implementations and maintenance of such interfaces, presenting government entities with additional costs, limited flexibility in addressing new requirements, and other risks (Gottschalk and Solli-Saether, 2009; Pollock and Hodgson, 2004).

The challenges mentioned earlier led to the introduction of hub-based and bus-based integration patterns (Li et al., 2009; Watson and Ariyachandra, 2005). See also Figure 1. In hub-based integration, government entities can connect to a central or federated hub to send and receive data between them securely through re-usable messaging and integration interfaces providing performance improvements and scalability.

Bus-based integration introduced the concept of decentralizing messaging between different applications by sending and receiving data in a similar fashion to radio technology, where government entities can connect and send information that can be received by one or many government entities without the need to physically connect to the government entity infrastructure. This provides the flexibility of sending a data set to multiple government entities using a single message.

The aforementioned patterns facilitated the integration between government entities whose focus was to send and receive specific data sets. With time, there has been a shift in emphasis from systems and data integration to overall enterprise integration with an increased focus on inter-enterprise operations, processes, and services, as depicted in Figure 2 (see also Ross et al., 2006).

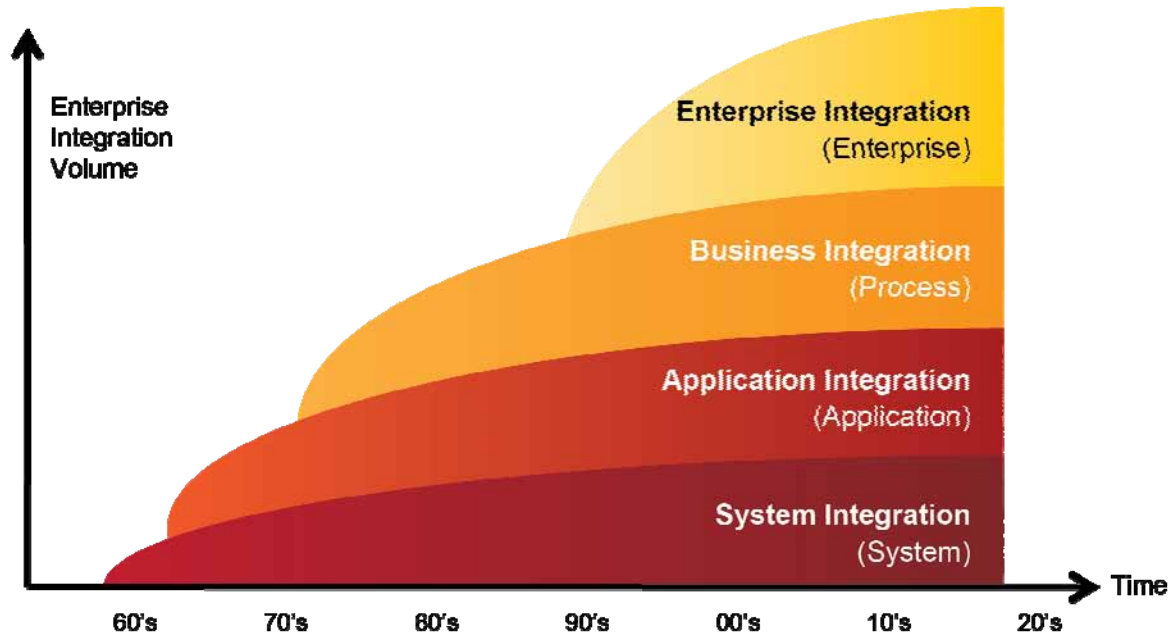

Figure 2. Evolution in integration strategies

This shift from system integration to enterprise integration provided government entities with the ability to link their integration needs with their overall strategic objectives by identifying which services a government entity can provide or need and leverage enterprise integration as a way to provide and consume these services (Daigneau, 2011; Wu, 2007).

Combining identity management and enterprise integration, global trends provide government entities with the capability to provide integrated identity management solutions that will facilitate up-to-date population registers and provide identity owners with the capability to provide innovative ID-based services to other government entities and possibly businesses.

2.2 Challenges Faced by Governments

With the global trends in mind, a number of lingering challenges still face governments in achieving integrated identity management as follows:

- Lack of a government entity responsible for maintaining a national population register;
- Data privacy and confidentiality issues;
- Lack of a clear vision and cooperation between competing government entities; and
- Lack of a government-wide integration and interoperability framework

With the aforementioned challenges identified in addition to many other factors, such as the recent economic downturn, many countries are facing a challenge to drive the notion of a connected 24-hour government.

3. The UAE National Identity Management Infrastructure

As a result of the rapid growth of the economy as well as the population over the past few years in the United Arab Emirates (UAE), the government has expressed strong determination to enhance the performance of public departments and increase efficiency in a bid to improve the coordination of and citizens' access to public services.

Among the most strategic initiatives in the UAE is the national identity management infrastructure development program launched in 2003. As part of the program, all citizens and legal residents are issued unique identification numbers and smart cards that are linked with their personal information and biometric details.

The smart identity card provides a single secure identification document. It is envisioned that the new card will further assist in streamlining and simplifying government procedures and enable the country's citizens to use the new identity card as a travel document within the GCC countries.

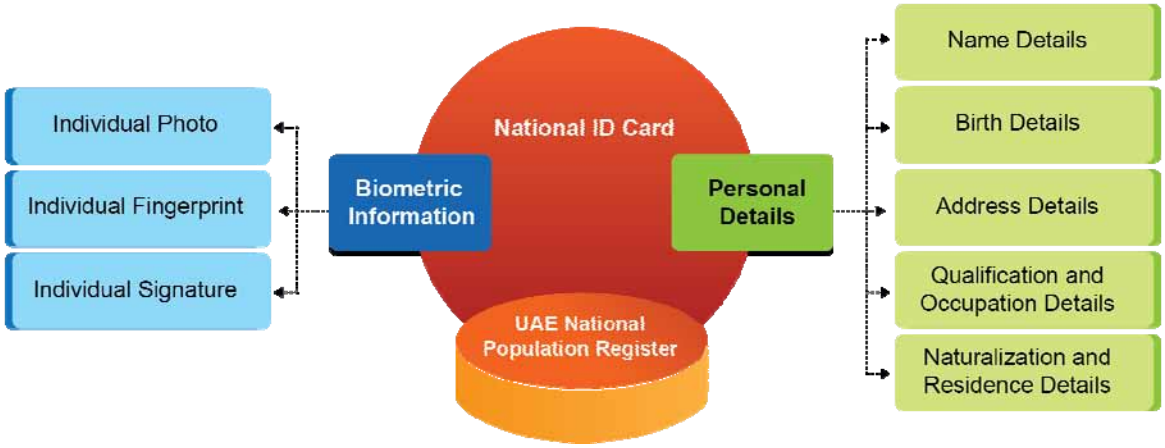

Figure 3. Identity profile

The smart identity card has the following characteristics:

- One card type for nationals and residents with personal profile information;
- All cards are PKI-enabled (digital certificate);
- Biometric data on card with "match on card" feature;
- Multiple security features (anti-fraud) built into the card; and
- Multi-factor authentication mechanisms for identity verification.

The validity of an identity card for residents is linked to the period of the residency visa permit; i.e., the expiry date as it appears on the card would be equal to the expiry date of the

visa. To enhance the value and use of the new national identity card, the government is working on using it with PKI-enabled services.

The UAE government recently announced a comprehensive Federal e-Government Strategy to promote connecting the different government entities at the federal and local levels. It sets a strategic objective of having a connected government serving the entire population, where the new identity management infrastructure is envisioned to play a fundamental role.

By adopting cutting-edge and innovative technologies in this promising national program, the government is keen to make it play an active and central role in supporting the development initiatives of the country. Among the primary contributions of this program is the development of a business intelligence system around population demographics to support decision-making and strategic planning in the country. Another strategic objective aims to develop and improve existing service delivery models through advanced identity authentication capabilities and facilitating e-government and e-commerce.

3.1 The Need for Enterprise Integration

With the core identity management infrastructure in place and the UAE population fully enrolled in the Population Register, the following challenges were identified in maintaining an up-to-date and accurate national population register:

- Keeping the ID card and the personal profile information updated per the life events in the citizen/resident life cycle;
- Managing the card life cycle in synchronization with the identity life cycle; and
- Keeping the population register updated in near real time.

The primary reasons behind these challenges were seen to be twofold:

- Clear identification of the sources of information, and
- Lack of integration between the different government entities and the ID-issuing authority.

Considering these challenges, the government commissioned a comprehensive study to address these challenges, focusing on the development of an enterprise integration strategy bringing together the different sources of information.

3.2 The State of Person Profile Information in the UAE

The UAE government has categorized the personal profile information into six key domains:

- **Core Identity**: Citizens' and residents' core identity information, such as name, residence and naturalization status, biometric data, digital certificates, and ID card numbers
- **Employment**: Data providing information about current occupation and employment status
- **Health**: Life information, including birth details
- **Academic**: Education details of schooling and higher education and related information

- **Legal**: Judicial information, including marital status

Based on the aforementioned key domains, it was essential to hold workshops with over 20 federal and government entities from the seven emirates to understand their role in maintaining such information, the business processes in relation to the feasibility of adoption of the national ID, and the technology used to maintain and store such information.

The outcome of this exercise was a detailed study in the integration of these government entities for managing the personal profile information in the National Population Register managed by the ID-issuing authority. The following diagram shows the mapping of the person information to the federal and/or emirate government entities:

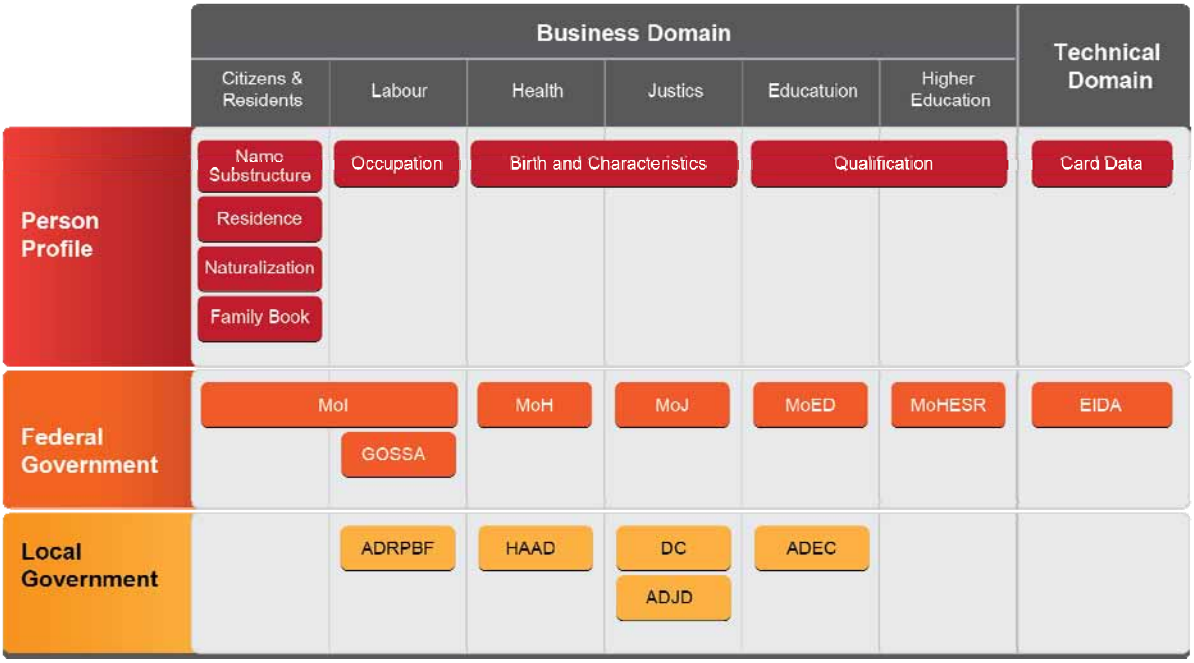

Figure 4. Data ownership among government entities

4. Integration Strategy Overview

With the results of the study highlighting the different data sources for person profile information, the government has formulated a comprehensive approach to develop an enterprise integration strategy and meet its strategic objectives.

The enterprise integration strategy was designed to be in complete alignment with the overall identity-issuing authority's business strategy and objectives. The integration strategy formulated the integration strategic objectives and outlined the priorities of the integration components.

A comprehensive enterprise integration strategic framework was also developed to define the key components to develop an agile and practical integration strategy that will have an

overarching contributional impact on the identity-issuing authority's overall business strategy.

This integration strategy led to a set of initiatives covering the people, process, technology, and on-boarding of government entities into the enterprise integration initiative. Each of the initiatives was prioritized and used to define an enterprise integration roadmap that was actionable and executable. The following diagram depicts the methodology adoption for the integration strategy development.

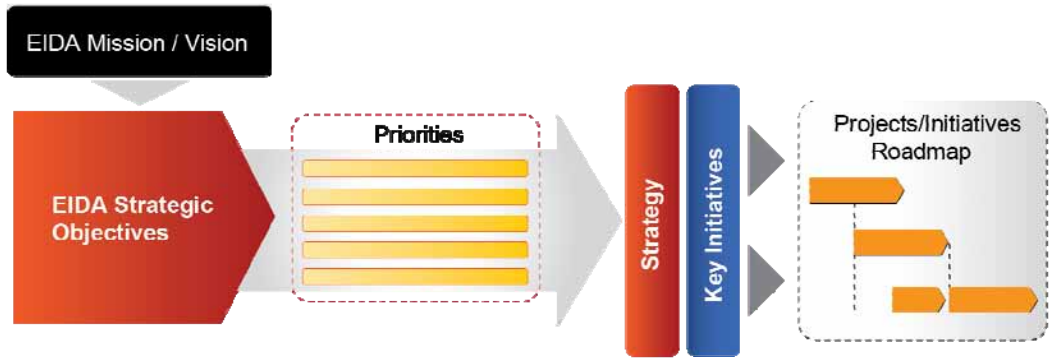

Figure 5. Integration strategy development process

4.1 Integration Strategy Objectives and Priorities

The enterprise integration strategy was architected to achieve the strategic objective of implementing an integrated and up-to-date secure national population register and deliver ID management services to UAE federal and local government entities through a flexible and adaptable service-oriented architecture.

The enterprise integration strategy was thus stated with the following objectives:

1) Provide a **secure, scalable, and flexible business platform** that supports the enterprise integration of the national population register, ID validation, and federated identity services based on the Emirates ID card and enterprise applications.

2) Provide **proactive life events services** enabling identified data owners to update and propagate person profile changes to update the national population register.

3) Provide **person profile data services** to e-government programs across different Emirates, authorized government entities, and authorized businesses.

4) Provide **population register data replica services** to authorized government entities and security organizations; provide statistics data to Department of Statistics for population statistics reports.

5) Provide effective **Web-based dashboard and management capability** for monitoring and managing the business enterprise integration.

To achieve the above objectives, the following priorities were identified:

- Ensure that the enterprise integration strategy and roadmap defines end-to-end architecture and solution implementation with minimal dependency and risks to achieve a successful implementation.
- Build an enterprise integration function that enables capability building for planning, management, operations, and support of enterprise integration.
- Consider leading enterprise integration patterns from leading vendors available in the market to implement the complete enterprise integration that can be modular and scalable.
- Leverage existing IT systems, IT infrastructure and security, and data center as well as other existing systems from other stakeholders effectively.
- Adopt an appropriate approach to implementing and operating the required enterprise integration and its platform through qualified and experienced system integrators and solution providers to deliver.

Based on these objectives, an integration framework has been designed and adopted to achieve effective integration, which is discussed next.

5. Integration Framework

The framework for the enterprise integration strategy was based on the identity-issuing authority's corporate business strategy and objectives as the main drivers with consideration for enterprise integration best practices, enterprise integration technologies, and on-boarding external and internal entities on the proposed integration platform. Also, the framework ensured alignment with the internal ICT department initiatives and current environment. The resulting enterprise integration strategic objectives and priorities were defined across a number of enterprise integration strategic components, as shown in Figure 6 below.

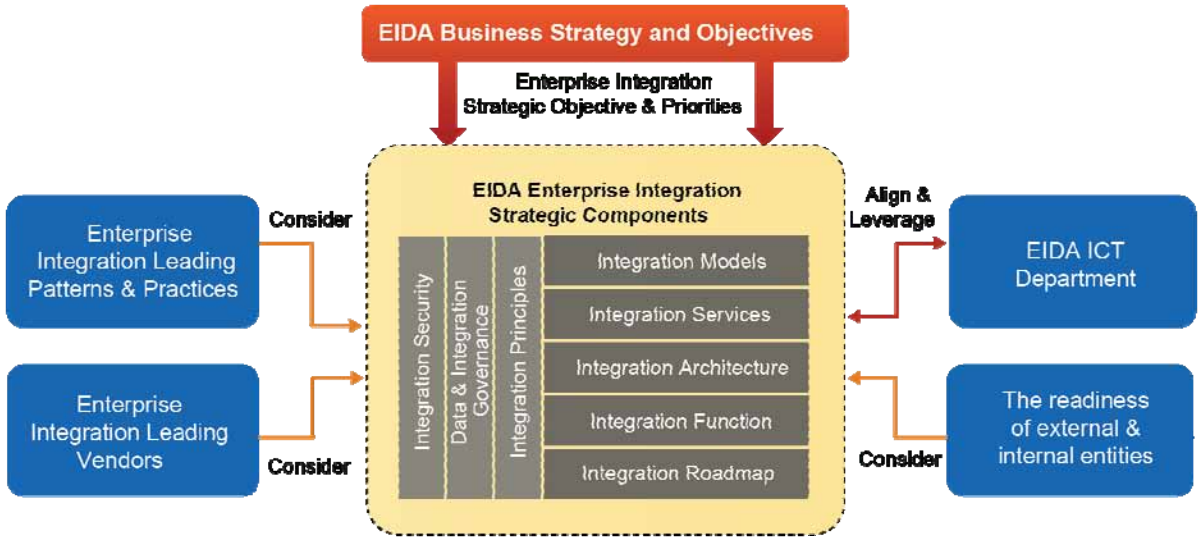

Figure 6. Enterprise integration strategic components

The enterprise integration strategic framework components were defined as follows:

- **Integration Models:** Defines the multiple integration models to government entities to access the services provided by the enterprise integration platform.

- **Integration Services:** Defines the business services providing integration capabilities to the national population register required to maintain an up-to-date national population register and services where government entities and potentially business to access the register. The technical services facilitate the platform and application services and the internal and external integration at the identity-issuing authority.

- **Integration Architecture:** Defines the required technology architecture including the needed applications, integration, data, infrastructure, and security to fulfill enterprise integration needs.

- **Integration Function:** Defines the required enterprise integration organization and structure to support the roll-out of the enterprise integration strategy.

- **Integration Roadmap:** Defines the detailed roadmap to implement the enterprise integration strategy covering the people, process, technology, and government on-boarding initiatives.

- **Integration Security:** Defines the security requirements for state-of-the-art security measures covering integration services access and authorization, data encryption, and secure transport.

- **Data & Integration Governance:** Defines the service, data, and security governance measures to support the enterprise integration unit and its function.

- **Integration Principles:** Defines the general integration principles that are the rules and guidelines for the integration, platform standards, change management, and others.

5.1 Integration Models

Various integration models needed to be supported by the integration platform to meet possible business and functional requirements and to provide various options for external entities to connect through the four distinct models of integration that were developed for the implementation of the integration strategy. See Figure 7.

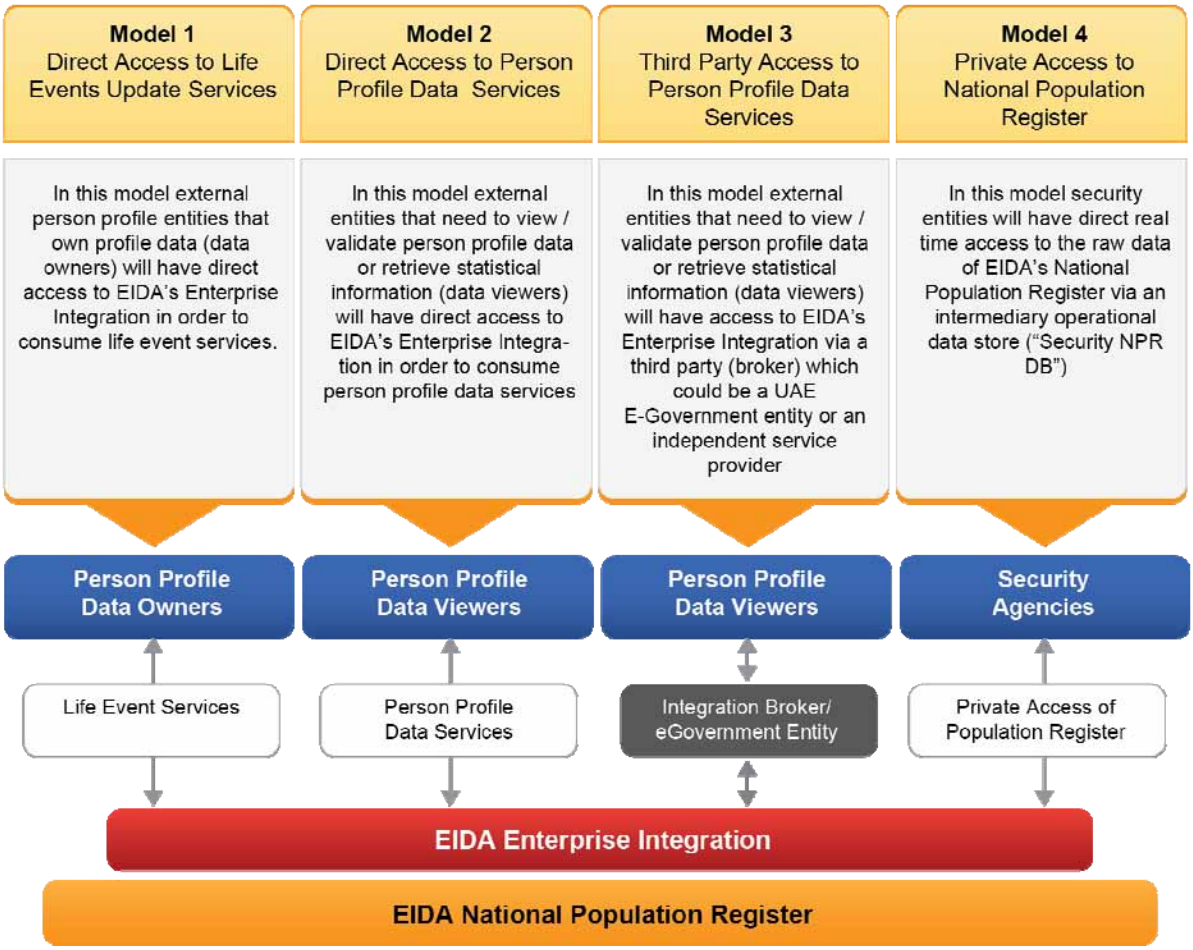

Figure 7. The four integration models

5.2 Integration Services

The enterprise integration needed to be supported by a series of business integration services that allow external entities to integrate with the national population register systems. The business services taxonomy was organized into several service groups to provide integration capabilities to the national population register. These services were mainly post-issuance services, i.e., services that could be provided after a national ID number and ID card were issued. Figure 8 below shows the various business integration services groups:

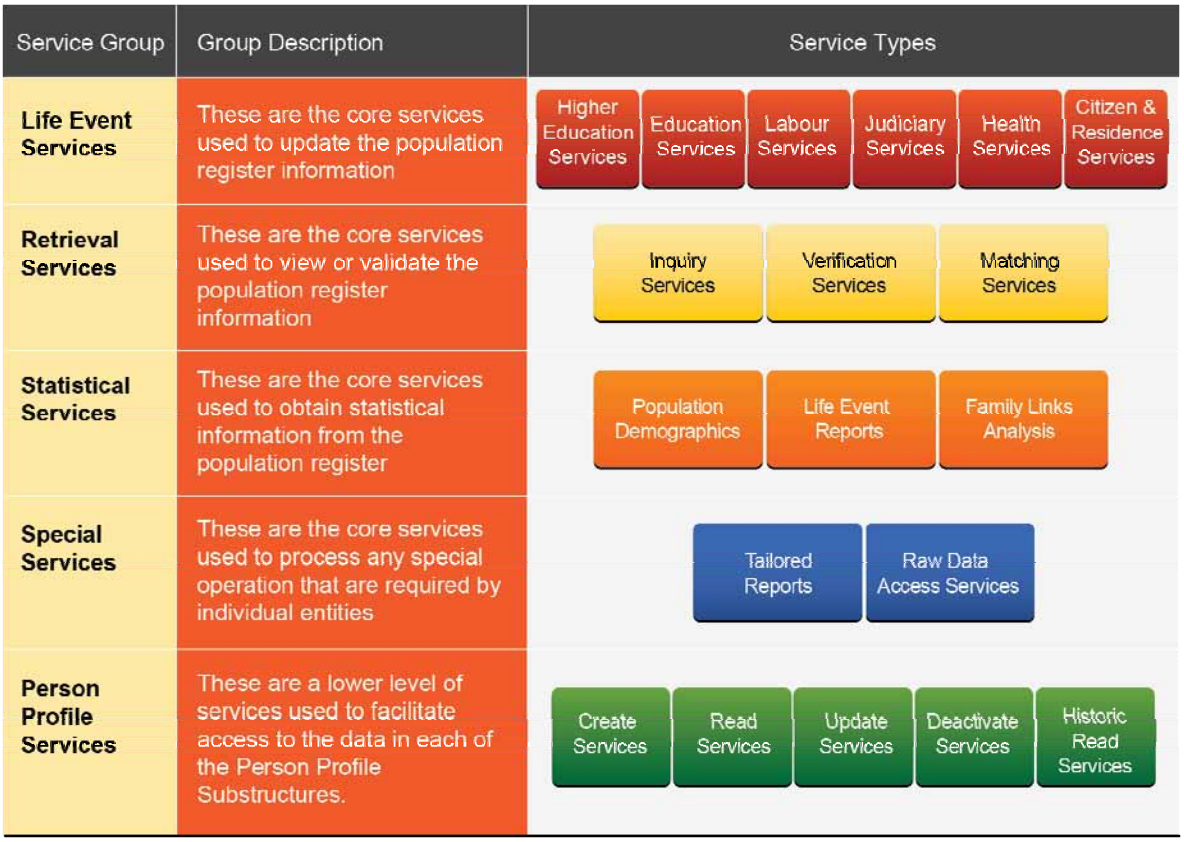

Figure 8. Business integration service groups

5.3 Integration Architecture

To enable seamless, secure, and flexible integration within the internal environment and between the external entities, a standards-based and an SOA-based enterprise integration were seen as important to implement to enable the functionality of the integration platform. A reference architecture was developed as depicted in Figure 9 below.

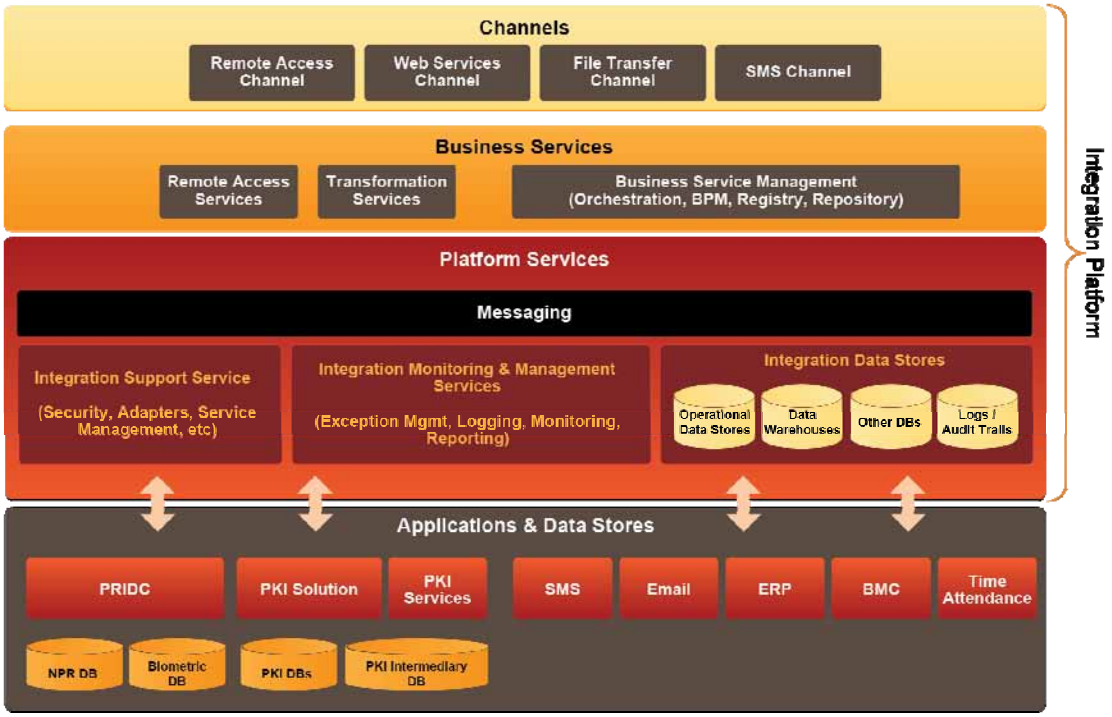

Figure 9. Integration platform architecture

Each of the four reference architecture layers is described in Table 1.

Table 1. Reference architecture layers

Layer	Description
Channels	This layer is the presentation layer of the enterprise integration. It allows external entities to use the identity authority's services through various channels such as Web services, file transfer (FTP), and remote access.
Business Services	This layer provides the functionality for service modeling, service orchestration, SOA governance, transformation, and remote access (needed for *special* security operations) where all services provided to government entities are defined and maintained
Platform Services	This layer is the key enabler of SOA-based enterprise integration. It provides messaging capabilities, integration services (adapters, APIs, etc.), monitoring and management services, and data services (ODSs, DWs, and DBs) to facilitate internal and external integration.
Applications & Data Stores	This layer is not considered a part of the enterprise integration to be implemented. This layer contains applications and data stores that will be integrated with each other via the enterprise integration, as well as facilitating external entities' integration for the purpose of accessing the population register.

5.4 Integration Governance

The enterprise integration governance model was needed to ensure control over the life cycle of services exposed through the platform and consumed by the different stakeholders. Enterprise integration governance defines and enforces policies related to service contracts, data quality, data and information privacy protection, authorized access to services, non-repudiation, and logging. For the successful implementation and operation of enterprise integration, these governance principles needed to be adhered to. The diagram below illustrates the data and integration governance principles that needed to be defined and enforced to control access to the enterprise integration platform.

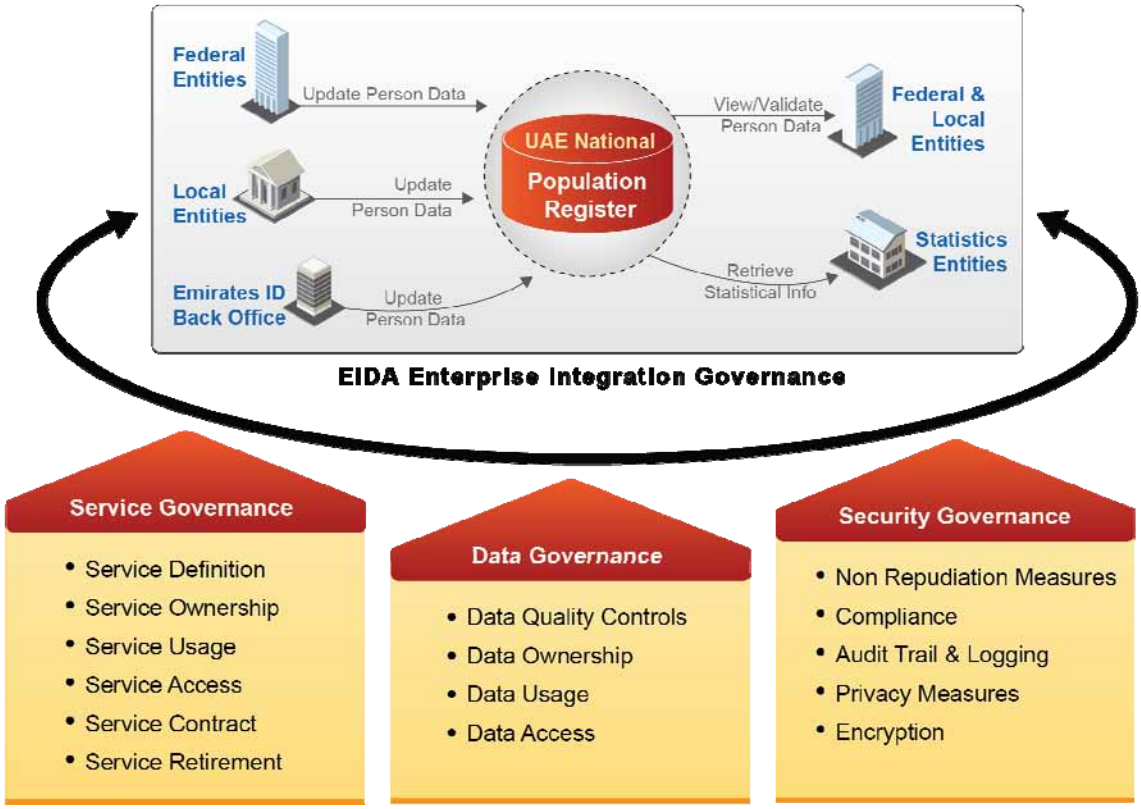

Figure 10. Data and integration governance principles

5.5 On-Boarding of Government Entities

To ensure a structured deployment process, a comprehensive approach needed to be defined that will clarify the process of on-boarding government entities and confirming their readiness, service development, service testing, and launching of the integrated services. See also Figure 11.

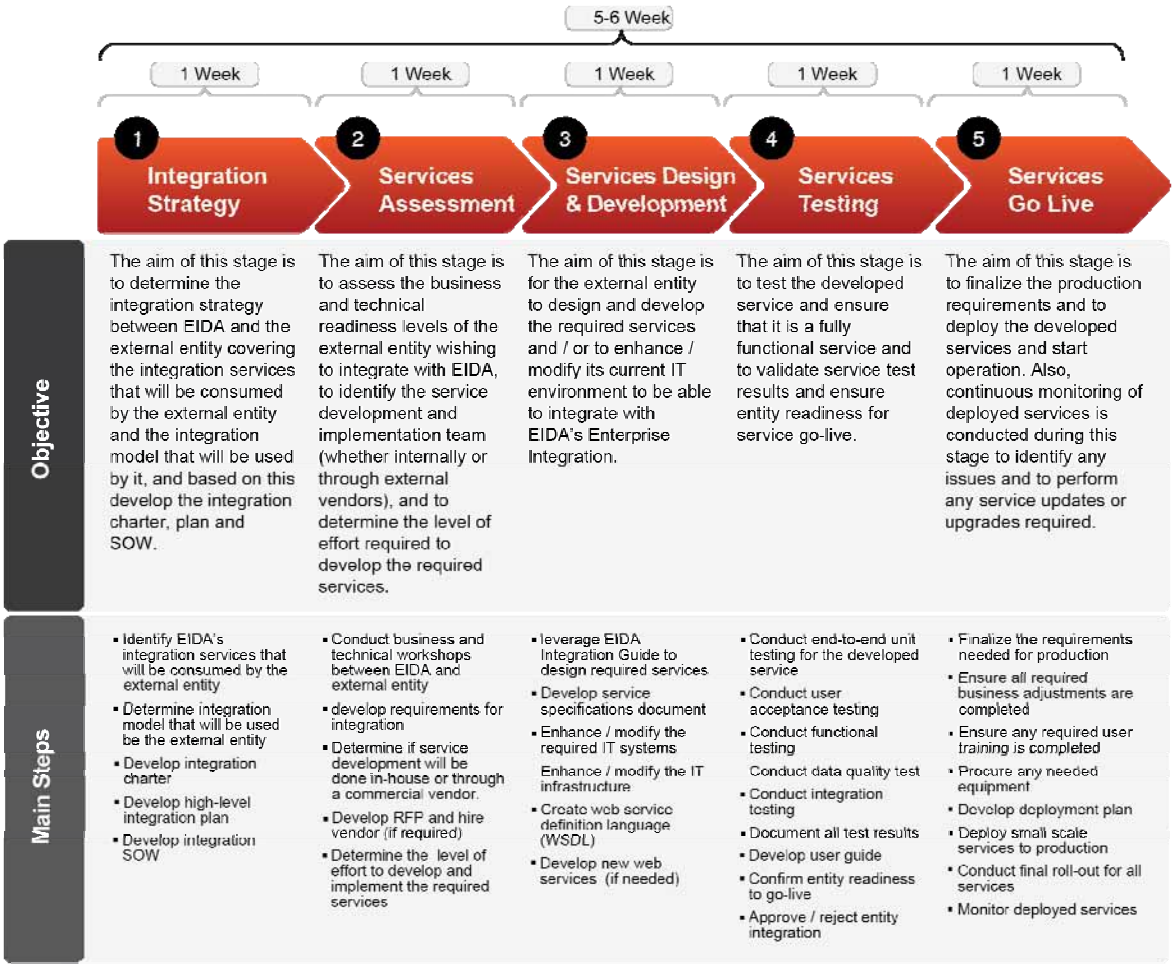

Figure 11. High-level plan phases for on-boarding of government entities

5.6 Integration Strategy Key Projects and Initiatives

The successful implementation of the integration strategy required the project team to undertake a number of initiatives/projects across four key domains: people, processes, technology, and external entities. Below are the identified key enterprise integration implementation initiatives/projects.

Figure 12. Key enterprise integration initiatives/projects

Each of the above initiatives and projects has been defined, highlighting the needed resource requirements, estimated duration, and interdependencies.

5.7 Integration Strategy Roadmap

With the enterprise integration strategy set to be executed over a three-year period, a comprehensive enterprise integration implementation roadmap was crafted to execute the defined initiatives/projects with the following key objectives to be achieved in each year:

- **Year 1:** Evaluate and select the right technology vendor to implement the integration platform and define the integration function requirements to support its implementation.

- **Year 2:** Implement the necessary strategy initiatives to kick-start the integration platform and on-boarding of government entities while setting up the necessary integration function to support its implementation.

- **Year 3:** Focus on adding more government entities as part of the integration strategy and provide the necessary support to operate, maintain, and support the integration platform.

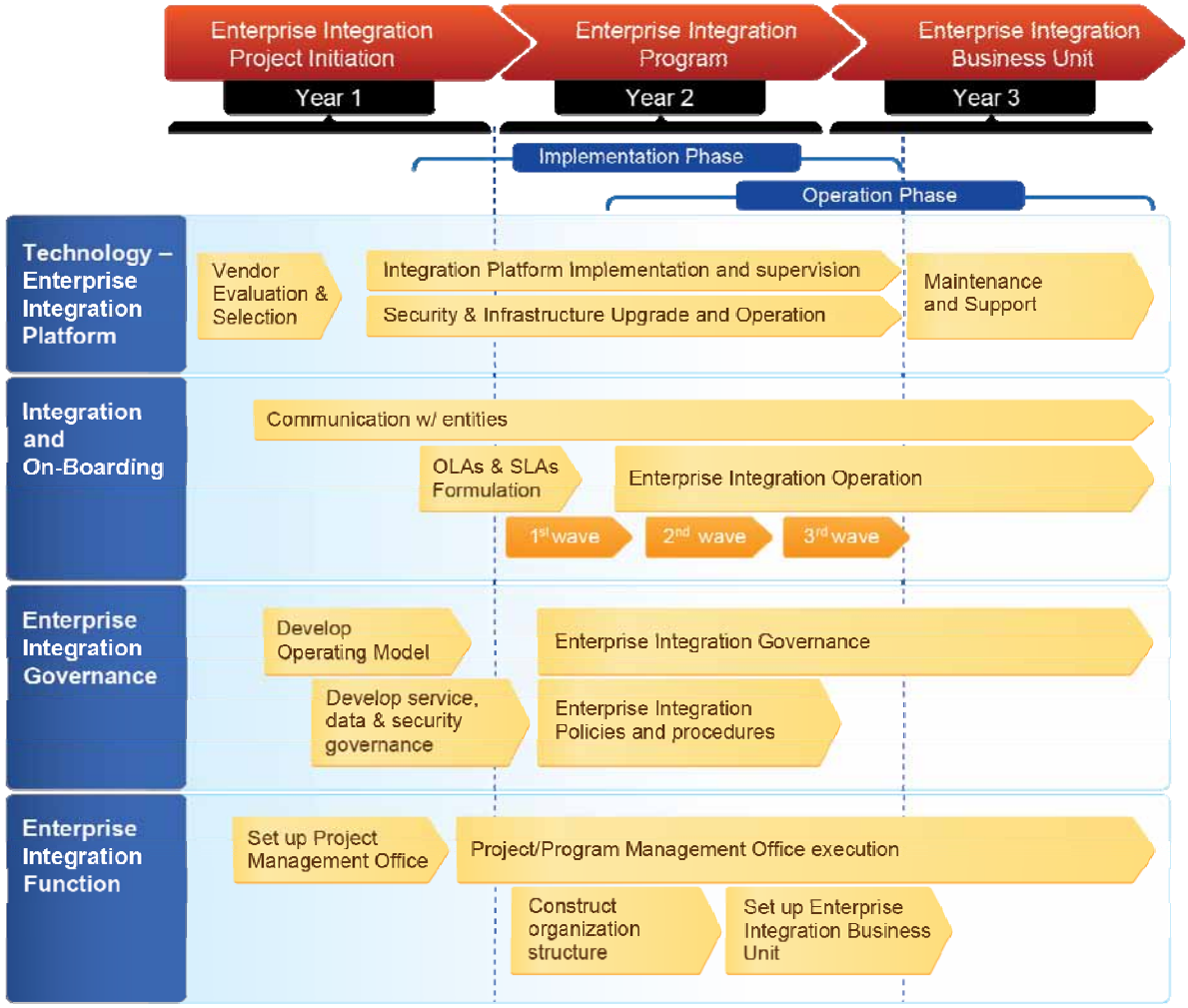

Figure 13. Enterprise integration implementation roadmap

6. Key Success Factors

To achieve a successful implementation of the enterprise integration strategy, the government identified the following key success factors that needed to be dealt with vigilantly:

- **Promotion** of the integration strategy to UAE federal and local government entities through the adoption of a well-defined communication plan and awareness campaigns.
- **Adoption** of the new smart ID card by government entities/citizens/residents by requiring the presentation of an ID card when requesting services.
- **Adoption** of an ID number as part of person profile by data owners would support and enable integration between the identity-issuing authority and the government entities.
- **Provide comprehensive services** to UAE federal and local government entities.
- **Ensure secure access** to the national population register to promote confidence and adhere to data privacy and confidentiality best practices.
- Robust **integration on-boarding approach** and **dedicated on-boarding team** to help and support government entities in integrating with the national identity management system.

7. Summary and Discussion

A national identity management program is characterized by the scope of the identity profile of an individual. One of the key factors to establish a successful identity management infrastructure is the level of integration between the different government entities (e.g., data owners) and the entity responsible for managing identities (e.g., Identity Authority).

In the case of the UAE, the early work of integration was handled at a system level where the primary focus was on identifying what data is needed for ***creating*** the identity profile. The integration focus at the time primarily dealt with how to collect information from a single system (i.e., the Ministry of Interior). The integration was more of a point-to-point integration pattern between the Interior and the Identity Authority.

Over the past years and prior to setting up the new integration strategy in the UAE, the number of systems that needed to be connected with (i.e., data owners), has grown exponentially, and thereby adding more point-to-point integration interface requirements. This has led to complex integration implementations. On the other hand, the maintenance of such interfaces presented the *identity authority* with additional costs, limited flexibility in addressing new requirements and related risks. This in turn led the UAE to study different topologies of integration such as hub-based integration and bus-based integration.

As explained earlier in section 2, in hub-based integration, government entities can connect to a central or federated hub. This connectivity enables stakeholders to send and receive data securely through re-usable messaging and integration interfaces to a centralized data hub. On the other hand, bus-based integration introduced the concept of decentralized messaging between different applications by sending and receiving data akin to a television broadcast. This respects the fact that different stakeholders have their own databases and services, but need to share data in delivering their services effectively.

The UAE integration strategy recognized that integration is the key to not just providing an identity to an individual but also to create a complete identity profile and more importantly manage this identity profile for its currency. It is in this context that a new integration strategy has been drawn up.

The primary consideration of the UAE integration strategy is that different stakeholders (e.g., government entities) can connect and send information that can be received by one or many government entities without the need to physically connect to the individual infrastructure of the government entity. This is envisaged to provide a level of flexibility for sending data sets to multiple government entities using a single message similar to a broadcast, albeit securely. This is the basis of the UAE's new integration strategy.

It is also recognized in the UAE that the identity profile created in the national population register spans the life-events of an individual and that life-events need to be updated in real time in the population register. Accordingly, the program has identified different sources (i.e., data owners) that contribute to the personal profile (e.g., Ministry of Interior, Ministry of Justice, Ministry of Education, to name a few). The new integration strategy envisages going beyond point-to-point connectivity by providing business process integration in addition to

the technical integration with respect to data update.

The UAE integration strategy implementation is based on integrating systems for updating the population register in real-time as per the occurrence of the life-events. In the first phase of integration, there will be integration at systems level for updating the population register in real-time as life-events occur. In the second phase of the implementation, the infrastructure will provide the required business process integration to ensure the validation of the data updates coming from the identified sources of information (data owners). This will bring in the much required data governance needs and the business rules for validating the automatic data update in the national population register.

The third phase of the integration strategy implementation envisages the data subscription and data sharing services on account of an up to date population register. This will ensure that the nation as a whole is served by the current population register and will enable efficient delivery of services to the citizens from the government, securing in the knowledge that the service is being delivered to the individual who he or she claims he or she is.

8. Conclusion

This article has attempted to provide some practical insights into a government integration strategy design and architecture that aims to improve identity life cycle management. The explored initiative is believed by the UAE government to propel the country to a leading position in providing integrated identity management solution and support its strategic 2021 vision of being among the top ten countries in the world. The innovative integration strategy outlined in this article is also envisioned to enable the UAE federal government and local Emirates' strategy to achieve their objective of being a 24-hour connected government. This is likely to contribute to the UAE's prosperity and economy, providing effective, efficient, and secure government services to its citizens and residents.

A key contribution of this article is that it explores and describes the strategy from within a government setting. In light of the lack of existing research to cover this topic until now, we hope that the presented work supports the fields of both research and practice. The single case and the qualitative nature of this study are considered an obvious limitation. Therefore, more quantitative research that sheds light on wider implementations is seen as an opportunity for further research and exploration of the practices to provide a more holistic picture of the given subject.

Finally, the rapid technological advancements will put more pressure in the days to come on governments to adapt and become connected governments. This will raise the bar in the public sector to reduce costs, improve relationships, become more efficient and effective, and, most importantly, user-centric (see, for example, Noveck, 2009; OECD, 2009; Shareef et al., 2012). Similar to the private sector, governments will have hard times ahead as they will seek ruthlessly to strengthen their international competitive advantage and cope with the new digital world order.

References

Al-Khouri, A. M. (2012a). Population Growth and Government Modernisation Efforts. *International Journal of Research in Management & Technology, 2*(1), 1-8.

Al-Khouri, A. M. (2012b). PKI in Government Digital Identity Management Systems. Surviving in the Digital eID World. *European Journal of ePractice, 4*, 4-21.

Al-Khouri, A. M. (2012c). eGovernment Strategies: The Case of the United Arab Emirates. *European Journal of ePractice, 17*, 26-150.

Backman, J. (2009). Beyond Silos: Cross-boundary Internet Service Portals'. *Government Finance Review*. Retrieved December 10, 2012 from http://www.highbeam.com/doc/1G1-195266688.html

Bertino, E., & Takahashi, K. (2010). *Identity Management: Concepts, Technologies, and Systems.* Artech House Publishing.

Chappell, D. (2004). *Enterprise Service Bus: Theory in Practice.* O'Reilly Media.

Daigneau, R. (2011). *Service Design Patterns: Fundamental Design Solutions for SOAP/WSDL and RESTful Web Services.* Addison-Wesley Professional.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2008). *Digital Era Governance: IT Corporations, the State, and e-Government.* Oxford University Press, USA.

Gottschalk, P., & Solli-Saether, H. (2009). E-Government Interoperability and Information Resource Integration: Frameworks for Aligned Development. Information Science Reference. http://dx.doi.org/10.4018/978-1-60566-648-8

Kubicek, H., Cimander, R., & Scholl, H. J. (2011). *Organizational Interoperability in E-Government: Lessons from 77 European Good-Practice Cases.* Springer. http://dx.doi.org/10.1007/978-3-642-22502-4

Li, S., Hu, Y., Xie, Q., & Yang, G. (2009). Heterogeneous Information System Integration Based on HUB-SOA Model. *Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT '09).* Huangshan, P. R. China, 26-28, Dec. 2009, pp. 239-242, [Online], Retrieved December 6, 2012 from http://www.academypublisher.com/proc/iscsct09/papers/iscsct09p239.pdf

Noveck, B. S. (2009). *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful.* Brookings Institution Press.

O'Brien, A. (2012). *Business Strategy: From Silos to Smart Government – SOA in Human Services.* IDC.

OECD. (2009). *e-Government Studies Rethinking e-Government Services: User-Centred Approaches.* Organisation for Economic Co-operation and Development, OECD Publishing.

OECD. (2011). *The Call for Innovative and Open Government: An Overview of Country Initiatives.* Organisation for Economic Co-operation and Development, OECD Publishing.

Pollock, J. T., & Hodgson, R. (2004). *Adaptive Information: Improving Business through Semantic Interoperability, Grid Computing, and Enterprise Integration.* Wiley-Interscience. http://dx.doi.org/10.1002/0471714216

Ross, J. W., Weill, P., & Robertson, D. (2006). *Enterprise Architecture as Strategy: Creating a Foundation for Business Execution.* Harvard Business Review Press.

Saha, P. (2012). *Enterprise Architecture for Connected E-Government: Practices and Innovations.* IGI Global. http://dx.doi.org/10.4018/978-1-4666-1824-4

Shareef, M. A., Archer, N., Dwivedi, Y. K., Mishra, A., & Pandey, S. K. (Eds.) (2012). *Transformational Government Through eGov Practice: Socioeconomic, Cultural, and Technological Issues.* Emerald Group Publishing Limited.

UNPAN. (2008). United Nations e-Government Survey 2008: From e-Government to Connected Governance, United Nations, New York. Retrieved December 6, 2012 from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf

UNPAP. (2012). United Nations E-Government Survey 2012: E-Government for the People, United Nations. Retrieve December 6, 2012 from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

Watson, H. J., & Ariyachandra, T. (2005). Data Warehouse Architectures: Factors in the Selection: Decision and the Success of the Architectures. Retrieved December 6, 2012 from http://www.terry.uga.edu/~hwatson/DW_Architecture_Report.pdf

Williamson, G., Yip, D., Sharoni, I., & Spaulding, K. (2009). *Identity Management: A Primer.* Mc Press.

Windley, P. J. (2005). *Digital Identity.* O'Reilly Media.

Wu, R. C-Y. (2007). Enterprise integration in e-government, Transforming Government: People. *Process and Policy, 1*(1), 89-99.

Copyright Disclaimer