

THOUGHTS WITH IMPACT - PART 1

Critical Insights from Government Projects

Dr. Ali M. Al-Khouri



A Series of Published Papers

THOUGHTS WITH IMPACT - PART 1

Critical Insights from Government Projects

Dr. Ali M. Al-Khoury

A Series Of Published Papers in International
Journals and Conference Proceedings

Critical Insights from a Government Projects
Emirates Identity Authority
Abu Dhabi, United Arab Emirates

First Version Printed in 2008
Second Version Printed in 2012

ISBN978-9948-16-736-5



Preface

This book represents a collection of published research articles in several international journals and magazines during 2007 and 2012. They cover various projects in the government field, and more specifically those in the GCC countries.

To allow better reading, papers included in this book were grouped into four research categories: project management, projects evaluation, electronic services, and technology implementations. These papers offer a variety of researched topics in the government context. They represent experimented practices in the field of public sector management and the implementation of advanced technologies in government sittings.

These papers are also distinguished from those available studies in the existing body of knowledge conducted in the Middle East. Research studies in this region are normally conducted by researchers who are very much interested in the academic rigor, rather than its practicality. Also very limited information is normally exposed and distributed about government projects which are by and large characterised to be classified, which makes existing research studies lack some fundamental understanding of issues that makes up the bigger picture.

The research work in this book was written by senior government officials and practitioners. They bring forward key critical insights from several strategic government initiatives, general management frameworks, imperative thoughts, reflections, and fundamental lessons learned. This should allow management to deepen their understanding of such projects and practices and better manage the associated risks.

In short, the intention of this work is to support the development efforts in organisations in the GCC countries and contribute to the advancement of the researched fields overall.

I hope that you will find this book immensely approachable and practical.

Dr. Ali M. Al-Khour

2012



Contents

Project Management

Projects Management in Reality Lessons from Government IT Projects	1
An Innovative Project Management Methodology	39

Projects Evaluation

UAE National ID Programme Case Study	55
Using Quality Models to Evaluate Large IT Systems	81

Electronic Services

Electronic Government in the GCC Countries	117
--	-----

Technology Implementations

Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics	165
IRIS Recognition and the Challenge of Homeland and Border Control Security in UAE.....	189

Projects Management in Reality

Lessons from Government Projects ¹

Ali M. Al-Khouri

COPYRIGHT © 2012 BUSINESS & MANAGEMENT REVIEW

ABSTRACT: This article presents some practical insights and challenges encountered during the implementation of major IT projects in the government sector in Arab countries. The primary purpose of this article is to point out the identified pitfalls to the existing body of knowledge from a practitioner's standpoint, as many of the articles published in this regard are published by vendors, consultants, or academics. Each item is discussed to highlight how it impacted the management and the overall performance of projects. They are believed to contribute significantly towards the successful management and implementation of projects, and as valuable lessons that should be recorded in an organisation's knowledge and watch list repository.

Key words: *Project Management; Project Failure.*

¹ Al-Khouri, A.M. (2012) "**Projects Management in Reality: Lessons from Government Projects,**" *Business & Management Review*, Vol. 2, No. 4, pp. 1-14.

* This article first appeared in 2008: Al-Khouri, A.M. (2008) "**Why Projects Fail? The devil is in the detail,**" *Project Magazine* [Online]. Available from: www.projectmagazine.com.

1. INTRODUCTION

IT IS widely accepted in the literature by both academics and practitioners that information technology projects have very high failure probabilities and that between 60 to 70 per cent do actually fail. Many other researchers argue that the actual figure might be far more frightening since many organisations tend not to disclose such experiences, due to fear of criticism by audit or the media (Collins, 2006; Cross, 2002; Fichter, 2003).

Perhaps this may be attributed to the fact that current information technology is more complex and diverse than several years ago as it is moving out of the back-office and into more mission-critical business process e.g., customer interfaces, electronic commerce, supply chain management, etc. (Gartner Group View, 1999). Besides, many researchers pointed out that many of today's failures are avoidable (Avison & Wood-Harper, 1990; Bentley, 2002; Berkun, 2005; Broder; 1999; Curtis, 1998; Lam, 2003; Radosevich, 1999). They argue that many of the projects fail because of foreseeable circumstances and that organisation's need to give careful attention to several factors to reduce failure.

The findings of this article correspond with the often quoted statement in the literature contributing to failure and that is related to the fact that organisations tend to treat IT projects from purely technological perspectives, and do not give much attention to other organisational issues. Almost all challenges and pitfalls reported in this article were organisational issues related to management and people. Figure 1 provides an overview of the pitfalls.

The identified elements hindered the progress of projects and delayed them from hitting the planned go-live milestones repeatedly. The

elements pointed out here are considered to be some valuable lessons learned during the implementation of several government IT projects and that if understood thoroughly could minimise the potential problems with the management and resultant delays in similar projects elsewhere and smooth their implementation.

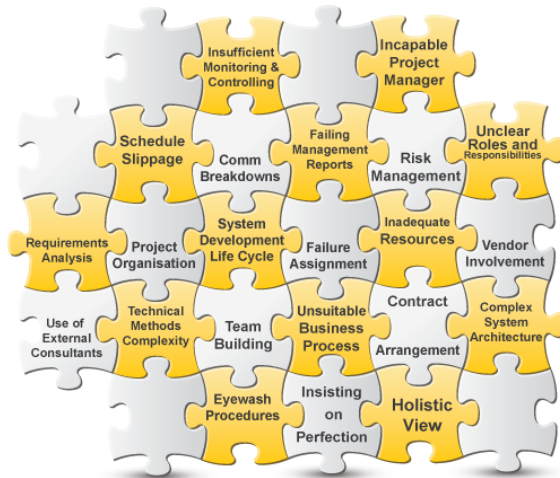


Figure 1: Projects Pitfalls Overview

They need to be comprehended and understood by the key stakeholders in projects and organisations, and not only the project management professionals. The following sections look at each encountered project pitfall individually.

2. HOLISTIC APPROACH IN PLANNING THE PROJECTS



One of the key problems with especially IT projects is the fact that the basic business principles associated with each project are sometimes underestimated or totally ignored. The reason often being a total lack of knowledge or ignorance in regard to the simple principles of sound Public Administration.

No project can be implemented in a smooth and time scale manner if the total business process is not determined or comprehended up front. This entails the identification in detail of the different processes, supporting legislation, rules and regulations to be applied, what will be required in terms of finance, human resources, accommodation and related requirements.

The IT divisions should only be tasked with execution once these basics have been determined. For example, once the different processes required by the project are determined in detail by the business experts, it becomes easy to determine the required skills necessary to attend to all the different aspects of the project.

Personnel working on the projects should therefore consist of a blend of business as well as IT experts. Decisions regarding the business issues will

be taken by business experts and not vice versa. IT experts will therefore be given a clear indication of what is required by the business experts and can apply their expertise to execute it in the best possible way. Through this interaction between the business and IT experts the best possible solutions and/or decisions will be implemented.

As a result of poor planning, all the relevant aspects of the project are not taken into consideration, resulting in unrealistic target dates being set. Often when these target dates are not reached, a scapegoat is searched for to carry the blame. It is in this instance very often seen that the magnitude of a project is underestimated to such an extent that unrealistic timeframes and closing dates are set for the project. This is typically the result of inexperienced persons planning a project.

Without a clear understanding of what the project entails, it is often found that the wrong skills are appointed or they are appointed at a very late stage in the project and there is always the tendency from these appointees to re-invent the wheel. This results in endless disagreements from both sides and causes delays without real value being added to the project. It is therefore of the utmost importance to appoint the required skilled personal on the business and IT sides from the outset, in order to avoid these fruitless differences and delays.

Provision is sometimes not made in advance to accommodate equipment, personnel working on the new project and for the public to be served in a user friendly environment. This also leads to endless delays and deadlines have to be postponed on a continuous basis.

There should also be a clear line of communication between the project management and the sponsor of the project. Without that, vital information is sometimes "withheld" from the sponsor or his decisions are anticipated only to be rectified once he becomes aware of it.

3. THE DILEMMA OF DETERMINING REALISTIC TIMEFRAMES



In almost all of the implemented large scale projects, each conducted review of the projects schedule confirmed a delay of several weeks and in others months related to the target date for the formal project kick off. The following factors were the prime delaying factors that obstructed the ability to maintain the published schedules:

- The amount of work that had to be performed was underestimated and the process to be followed was not clear,
- Underestimation of the requirements of the projects up front often leads to an inappropriate solution offered by the Vendors. This solution is then included in the contract and vendors are often, with good reasons, reluctant to deviate from the contract for a fear of scope creep. The requirements should therefore be absolutely clear and signed off by a skilled business expert who should take responsibility for the project. The proposal and associated contract should likewise cater in detail for all these requirements. This will

ensure changes to the system and contract will be restricted to an absolute minimum,

- The identification of project activities was not easy and the time required for their accomplishment was too short,
- The approval of system specifications took longer than specified. This was mainly due to an unrealistic date set for this as a result of inadequate specifications, the complexity of the system and also to the unavailability of business experts, some project staff and IT experts for decision making which consequently caused a postponement in the deliverables' dates for many specification documents and project activities,
- Far too much emphasis was often placed on the security of the systems from an IT perspective resulting in a closed system being developed by the vendors. The systems were therefore difficult to operate, not user friendly to the public and it was very difficult to affect any changes at a later stage,
- Team members not skilled for the task were sometimes compelled to take important decisions on certain issues only for these decisions to be revisited. An example is when IT experts have to make business related decisions and business experts have to make decisions on technical issues,
- Decisions were sometimes taken in good faith by management team members only to be reversed when more senior members or the project sponsors become involved. It was therefore of the utmost importance to ensure that decisions on critical issues were cleared with higher authority before it was implemented. There should be a structured way in which these issues are dealt with.

- vendor system development process was complex and could not address ad-hoc modifications to the system,
- outstanding contractual issues that could not be resolved at the technical levels took longer periods until they were resolved on the executive management level,
- the legal requirements for some organisational aspects related to sharing of data with other government organisations ran through long government cycles,
- recruiting the required staff was a big challenge especially for those jobs requiring highly skilled and knowledgeable candidates and was often finalised at a very late stage;
- communication and coordination with other government entities were a daunting activity and the delays in reaching consensus and getting approvals had an impact on the completion of project activities, and
- Consultants working on the projects were often experts in specific areas of the IT environment but regarded themselves as universal experts even in advance business processes. This resulted in the system often being steered into a closed and secure IT project with little room for change. This was especially a problem as some consultants were part of the team negotiating contracts with vendors. Further, western consultants had a tendency to cleverly, but purposefully, add additional requirements to the system which were time consuming, resulting in endless discussions and more than often required a rework of the system. This caused "legitimate" delays and extended the project to an extent where the contract of the consultant also needed to be extended for a further period of time.

Besides, project managers tend to either produce plans that were too broad in scope, with insufficient detail or which were too detailed. Large projects had detailed schedules. However, it was found impractical to use detailed plans for reporting to the steering committee executives, where they were usually interested in whether or not the project was on target, and they could not see this in the mass of detailed activities.

This requirement was sometimes difficult to obtain as project managers tried to hide the potential delays from the top management. It is however of the utmost importance to timeously provide the sponsors of the projects with detailed information outlining problems when experienced in order for informed decisions to be taken at the highest level. If not, these problems will be identified later with inevitable consequences.

In general, the process followed in the projects was more of planning the project activity-by-activity. The assumption was that as soon as the sub-projects were started, more information will become available about the other activities. We call this '*management-by-luck*'. So not surprisingly, the project managers were often sucked into a spiral of planning and re-planning, as they ceased to manage their projects and the plans lost credibility.

Our close observations of the projects show us that the project management teams did a good job in the upfront planning process, but then were not able to manage the projects effectively from that point on. This included problems managing scope change, resolving issues, communicating proactively and managing project risks.

One explanation for this setback lies in the fact that even though in many projects the roles and responsibilities of the project teams were

clear, their decision authority was often limited due to the level of influence and decision power of the project members.

There was also a tendency in the projects to focus on deadlines and perform target-led planning approaches. Too much attention was given to such dates. This affected the performance of the project members. By being concerned only about a point that lies far into the future, the project members felt that there were plenty of time to do the work. Consequently, the project activities were delayed and took longer than anticipated.

Project Managers should realise, at an early stage already, if a project was underestimated, has too many built-in security features, when inadequate system provision was made by the vendor as a result of the underestimation of the project or deadlines cannot and will not be met. They should then advise the management and the sponsor of the project accordingly and also advise on a possible new strategy. By not doing so, the eventual problems are just postponed with tremendous costs and frustration.

For instance, when the steering committees or the top management were presented with the project schedule, they presumed that it must have been possible to do the work more quickly and in shorter periods. One motive behind such slashing was to please the project sponsor and to inform him that the project was on track.

To make the plan attractive, the project managers then reduced the estimates of work content and duration, and then convinced themselves and the steering committees that the new estimates can be achieved. Tragically, it did not, and the projects generated plans that were the unbending evidence to prove the failure of such planning practices. This has had serious implications for some of the projects.

There was also tendency to plan the projects as if the outside world did not exist. The project schedule lacked any slack or a contingency timeframe. Many of the project activities were extended due to the unavailability of staff for reasons such as holidays, sick leaves, training courses and seminars and of course those skilled staff members that were appointed very late.

As it is the case in any project, project progress was dependent on certain decisions being made within the organisation. It was common not to give proper attention to the political factors underlying the decision coming from the top, and to underestimate the time required to study and implement such actions.

The result was that insufficient time and resources were given for many tasks. Sufficient time was not allowed for some important activities, which later impacted negatively on the schedule. Critical tasks were done inadequately and were redone. All these identified factors affected the planned activities, and required another re-planning activity to happen. As indicated earlier, project managers were sucked in re-planning their plans repeatedly.

4. VENDOR LACK OF INVOLVEMENT IN PROJECT MANAGEMENT



Vendors often underestimated the value of participating in the project management process. They sometimes obstructed the concept of providing an onsite project office with a team to manage the account (contract) and the project on an ongoing basis. To a large extent, vendors were seen to play a passive role in the projects, limiting their involvement and responsibility to the implementation and delivery of the system.

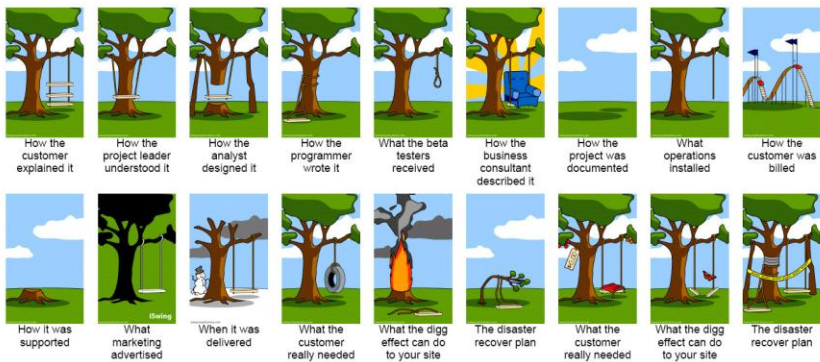
Therefore, projects were primarily managed by the client's own resources and/or the consulting companies, thus it was always a one-sided project management activity, with minimal input and cooperation from the vendors. The vendors, therefore, were constantly trying to stick to their proposed solutions in terms of the agreed contract and it was always difficult to obtain the required co-operation.

In fairness to the vendors it should be realised that changes involve development work which could be time consuming and costly and if not limited to the essential it may easily become an ongoing process which will lead to the vendor not making any profit.

Despite the fact that it was in the vendors' own interest to work very closely with the clients in order to focus on the same goal as a team, it was a common view that their responsibility was limited to the development of the system, and not the management of the other projects' activities. This created a communication gap in the projects, as it also contributed to delays in other projects activities which subsequently took longer periods to be completed.

5. REQUIREMENTS ANALYSIS

Project Management Crash & Burn 101



Even until the final stages of the implementation phases of many projects, requirements were still not 100% finalised. The systems first presented for testing were implemented in versions. Technical teams normally accepted the systems because of the management pressure to meet operational deadlines.

One understating we developed for the reasons of un-finalised requirements until then was due to requirements being not properly captured and envisaged from the beginning. In projects, there will always be cases where requirements change and/or new ones are discovered after the ideas are conceptualised and materialised into a tangible system (see also: Avison & Fitzgerald, 2003; Checkland, 1999;

Checkland & Holwell, 1998; Curtis, 1998; Mumford, 1986; Wilson, 1990), and there must always be a change control process to manage such changes to the system.

It was the fact that the vendors in many projects took a big bang approach at very complex systems and expected that there will be no or very little comebacks in terms of changes to such systems. Instead of working closely with the clients and providing ongoing feedback and involvement into the development process (especially the user interface), it was often a one-sided effort that took place by the vendors own technical staff.

Though requested many times, some vendors did not see any point in presenting their approach to explain to the clients how they intend to capture the requirements during the pilot implementation and their overall development strategy from that point. In many other projects, vendors view was centred around the concept of 'tell me your requirements, and we will develop it for you'. This resulted in many heated discussions between the clients and the vendors especially when the latter were requested to put forward business and technical solutions to certain requirements during the projects.

One of the solutions presented by some client project teams to overcome this difficulty was to have a fulltime requirements specialist on site at the clients' place during the pilot phase and specification of the next version of the system. This solution was not welcomed by the vendors, and was seen as an added cost to the projects and that they could not afford this because of the project delays and their current losses as a result. Perhaps the following sections give more explanation for the inability to clearly capture and finalise requirements.

6. SYSTEM DEVELOPMENT LIFE CYCLE



Any development project, however small, needs to go through iterations (Avison & Fitzgerald, 2003; Checkland, 1999; Curtis, 1998; Wilson, 1990). This is to evaluate whether the client's requirements and expectations have been met and whether the developed system is optimal, efficient and without bugs (ibid). Iterations are not supposed to be a nice-to-have but rather a necessity in any development project (Avison & Fitzgerald, 2003; Crain, 1992; Curtis, 1998; Harry, 1997; Olle et al., 1991).

Some vendors seemed to like the idea of a single iteration of the system, with a user interface which was developed in isolation. Although some implemented systems went through one technical iteration, it was a common view of the technical committees that only once the public has become involved with the systems, can the final iteration be developed for the first working production version.

The importance of this should be viewed against the backdrop of the fact that in some instances it was a completely new service that was rendered to the public for the first time and ample provision should have been made for possible changes resulting from the public's interaction with the system.

The time it took the vendors to make the changes to the system was of concern in many projects. There were too many channels to go through in order to get a change made to the system. Although this was healthy in a very rigid and robust environment with long time scales, it was believed by all the projects teams that a public system will not tolerate such delays.

One of the recommendations put forward was that the vendor either moves a group of the developers to the client on site in order to handle minor changes to the system on a very short turn-around time or that the client employs some of the vendors' developers directly for a period based on a time and material principle. This again was not seen of value to the vendors and that the clients were overreacting!

Either way, the systems could not accept changes through a project basis and major version evolution process, and there was a need to have a mechanism to implement minor changes on very short notice in the form of service or feature packs.

The technical committees throughout the period of the projects criticised the vendors' approach to project management and system development. For instance, from a project management point of view, many of the vendors did not make any effort to explain their project management methodology despite the continuous requests from the clients.

In addition, the project deliverables were arranged and structured in a 'lot' format where the phases were clear-cut. The rigid linear approach adopted by some vendors to develop their systems, was based on the concept of executing the project phases in a sequential fashion, with outputs from each phase triggering the start of the next phase, and with the assumption that business requirements once "work-shopped" and documented, were finalised.

This development process might have been appropriate to some project areas, but not to the development of public systems where it not only involves certain end-users operating the system, but in fact a quite big portion of the public. This development approach was envisaged to be appropriate by the vendors because it was thought to give them the possibilities to detect requirements quickly and meet the constraint that projects were supposed to be completed in agreed timeframes.

Although the linear approach can be useful as a framework within which the main activities and phases may be organised, the vendors needed to incorporate iteration into their system development process to address the problem of incorrect requirements and changing requirements due to user uncertainty. The vendors' approach must have taken into account that requirements usually change as the projects progresses and as the users come to understand the implications of the requirements.

The iterative approach was underestimated to address the fact that users do not have a fixed requirement at early stages of the project and that experimentation with a real system enables users to better define, refine, and communicate their requirements (Avison & Fitzgerald, 2003; Checkland, 1999; Crain, 1992; Curtis, 1998; Harry, 1997; Olle et al., 1991; Wilson, 1990). However, revising the development approach was

observed to be associated with extra cost which the vendors were not willing to consider as an option at all.

We need to refer back to the fact that it is widely known in the field of information technology that the rigid linear approach to systems development has been the prime factor behind the failure of many IS/IT systems because of its rigidity and the assumptions behind the arrangement of its phases. The IT divisions are sometimes unfairly blamed for the failure of projects while it is indeed a failure on the part of the business divisions not clearly indicating the business requirements which should be met with the associated IT project.

7. USE OF EXTERNAL CONSULTANTS



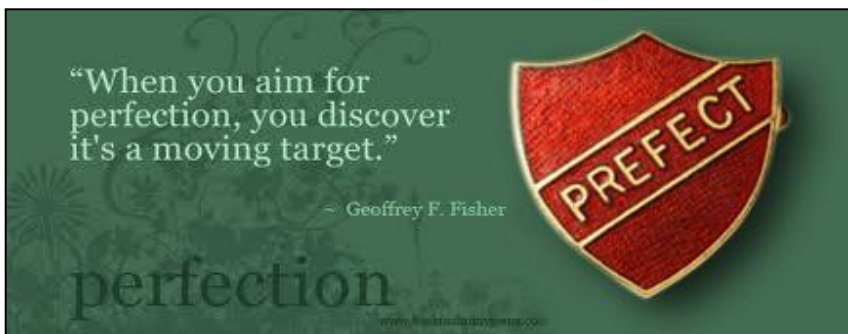
It was realised that the steering committees and top management did not always understand the depth of the changes required. Senior executives rarely concerned themselves with the details of the projects. Therefore, they hired consulting companies and sometimes individual consultants too to deal with these details.

This again had a great impact on the project triangle in respect to the cost of obtaining those new consultants. It was also found that those

consultants caused several delays to the project since they required a great deal of time to analyse management requirements, and come up with their solutions.

Time and cost were not seen by the executive management to carry the same value as the quality of the final product which they were more interested in. The next section provides some examples from the implemented projects.

8. INSISTING ON PERFECTION



There was a great tendency by some highly ranked projects members to insist on identifying every conceivable risk and controlling all possible deficiencies. This led the team to study and review project specifications and other technical documentations to a great extent of detail, as some activities in large projects took almost a year to finalise in order to accommodate the different view points. From our viewpoint, the process and activity were straightforward and it did not require much experience to setup.

There was often a tendency in the project to over emphasise the technical aspects and ignore the organisational aspects. People find it easier to imagine the concrete, technical tasks rather than the abstract,

organisational ones (Berkun, 2005; Burnes, 2004; Kerzner, 2004; Keuning, 1998).

Workshops around technical specifications also tended to take a long time to get finalised, where many project members were very much keen to enter into discussions on technical matters and to initiate solutions, before even being clear on the purpose of such deliverables and what it was meant to achieve. All this, in turn, had a great impact on the project plan and the planned go-live date.

In an attempt to understand and provide an explanation for such behaviours, this aspect was investigated further. It was found that the projects involved staff coming from very technical and operational backgrounds.

It is this fact that operationally minded project members often tend to load more and more weight onto the project, as they can think of hundreds of enhancements that, in their minds at least, must be made (Lam, 2003; Marrison, 2002). In fact, this added more value and strengthened the project and its specifications, but it also crippled the projects and seriously impacted the projects triangle (cost, quality/specification, and time). This goes to say that identifying each change and tracking its impact on the project triangle was a major challenge to the actual project management exercise.

Another explanation found for such behaviour was that people normally seek, unconsciously sometimes, to establish their identity via the project they were involved in (Marrison, 2002; O'Toole & Mikolaitis, 2002).

It was found that some members tried to make their individual mark on their projects by championing such causes as new ideas and approaches to project specifications, methodology and quality

assurance programs. In one project, *a member was insisting to change a particular product specification where if done, the product would have lost its international certification!*

Some of the consultants working on some IT projects, with the knowledge and support of senior management, indeed made the project their own and wanted to steer the project and in the process prescribe to project managers and team members which direction should be followed. This resulted in heated arguments with resultant delays and the postponing of decisions as further deliberation with higher management is often required.

9. CONTRACT ARRANGEMENT



Many disputes took place with vendors during the projects, and many of them were due to the contracts being unclear about the development methodology of the system, as the contract articles were interpreted in different ways. All contracts were well written from a legal perspective; however, it lacked the technical details.

The project deliverables in some contracts were organised in a 'lot' format. This was based on the traditional linear system development approach that some vendors were never willing to change or compromise as explained earlier. The projects scale and complexity did not allow this area to be addressed thoroughly at the time of writing the contracts.

10. COMPLEXITY OF THE TECHNICAL METHODS

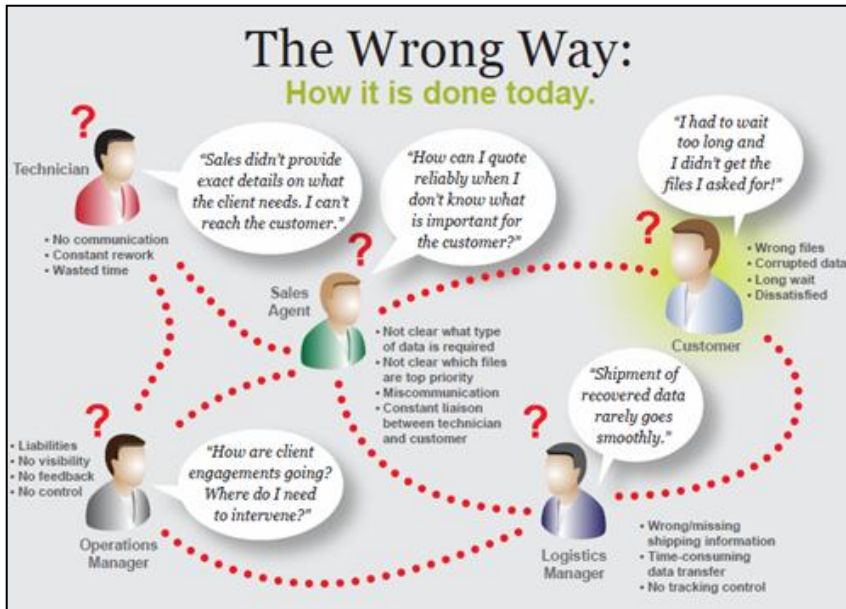


Methods and tools employed by the vendors to describe the project processes and technical aspects carried a lot of jargon which was found to be difficult to comprehend by the project teams who in turn created a lot of confusion and hampered communication and cooperation. Project members found many business processes very ambiguous and not clear at certain deliverables acceptance stages, where even sometimes the vendors own staff had difficulty in making them explicit.

Structured diagrams such as data flows (DFD's) if developed would have eased the illustration of the logical relationships and the flow of data and processes in the system. However, some vendors' reply was that this was not needed. The projects' members and the end-users

continued to struggle to find out how the system and its sub-components worked. This led the projects' teams to develop their own versions of data flow diagrams and charts based on their own interpretation of the business process and system behaviour.

11. UNSUITABLE BUSINESS PROCESS



In many projects, the systems functionalities were very much determined by the consulting companies and the individual consultants who all came from western countries and underestimated many cultural aspects. It is worth to mention, that the projects were operated more as an IT PROJECT from day one with much emphasis on security and technical aspects.

An IT solution was always the approach to any business problem that came to the fore. This was why there were so many unsolved issues in all the projects from a business perspective during the walkthroughs of the system and the pilot operation which required many manual

organisational procedures be adopted to cover up systems deficiencies. That the vendor not being able or willing to affect changes that were identified in a timely manner, further aggravated this.

12. COMPLEX SYSTEM ARCHITECTURE



Many of the developed systems lacked flexibility in terms of their ability to allow ad-hoc programming changes to be made to its structure to reflect the requirements. The systems were developed in such a complex way that made technical, business, and other system behavioural changes very daunting to the vendors, as they struggled to figure out how to manage and implement such changes.

In fact, adjustments to the system were always an issue and in the most instances impossible to perform. The complexity challenge was due primarily to the overuse of security functions, and complex programming structures which considerably reduced system flexibility, and increased its intricacy.

13. COMMUNICATION BREAKDOWNS



Language in the projects was clearly an issue and many misunderstandings were the result of language constraints. The agreed communication language both verbal and written between the project parties was English.

However, it was important to consider in some projects that the clients and the vendors had different mother tongues. The vendor experienced difficulties when participating in or facilitating workshops with staff members who were not trained to conduct such sessions (e.g., training and testing); who were not fluent in English and who usually got emotionally involved in serious discussions, arguments, and conflicts on many occasions, because of language barriers and misinterpretation of conversations.

14. FAILURE ASSIGNMENT



In some projects, management's attention was shifted away from primary project performance factors and was focused on finding someone or some group to blame for the continuous project delays. The focus was often not on error detection, prevention, or even mitigation. It was on failure assignment, leading to more disputes over culpability between the clients and their consulting companies.

More time was spent wrestling with disputes, and less time on managing the project. Instead of focusing on the project processes and deliverables (the main task that they were brought in for), some individually hired consultants also played a key role in supporting the client to fight with the consulting companies. These fights with the consulting companies allowed some vendors in turn to have a tranquil and stress-free time throughout the projects.

15. RISK MANAGEMENT

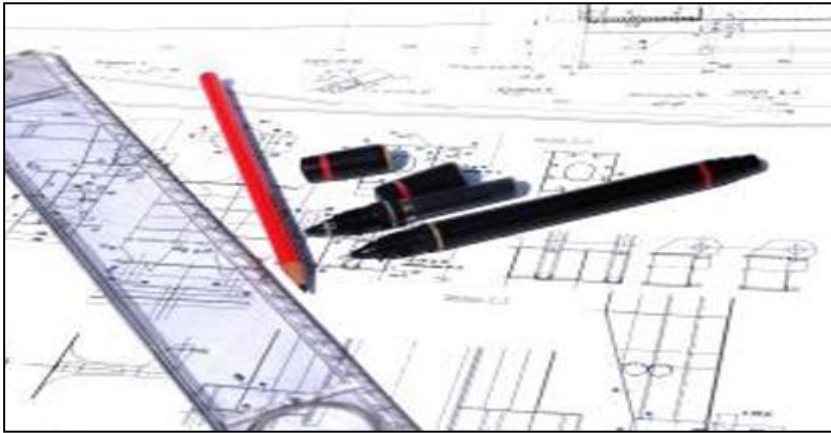


In projects, the risk assessment process is performed not simply to reveal potential risks, but to point out the types, locations, and strengths of controls needed (Gilbreath, 1986). Risk management is the ability to recognise a threat, accurately assess its implications and develop approaches to mitigate the risk in a cost-effective manner (Crouhy et al., 2001; Lam, 2003; Marrison, 2002; Wideman, 1998).

A general analysis of the risks associated with the projects was performed at an early stage of the projects to identify them and scope their potential impact. During the initiation of the projects, the projects teams were able to foresee the risks involved with quite a bit of detail. After that, however, the vision and the value of the predictions concerning risk diminished.

One reason was that the projects teams were exhausted by the daily workload and the long working hours. Their thoughts and concerns were more directed towards completing those assigned tasks. Thus, little or no time was given to perform the much needed risk assessment throughout the project.

16. PROJECT ORGANISATION



People are, without a doubt, every project's most valuable and most perishable resource. They demand to be managed, and their management is usually the biggest challenge to project success (Berkun, 2005; Binney & Williams, 1997; Burnes, 2000). Failure to clarify responsibilities and the principles of cooperation result normally in resources that are unavailable when required (Finney, 1999; Frame, 1999).

It was found that roles and responsibilities were not allocated according to individual strengths and expertise, but was based on their positions in the organisations. Not much attention was given to setting up good communication systems. There was a clear need to setup a useable collaboration environment where project members can have access to project information and can communicate with each other through out.

17. UNCLEAR ROLES AND RESPONSIBILITIES



All projects had a defined structure. However, it did not clearly define the roles and responsibilities of all project members. This led to reduced project momentum and resulted in the loss of valuable project time discussing principles that should have been clarified at the outset.

Many of the project members wasted time doing work that was not their responsibility, especially the consultants. This pitfall would have been avoided by having a clear responsibility chart. The lack of a formally appointed "owner" in some projects had a severe impact on the overall projects progress and performance, as projects members ceased to work in harmony and their efficiency dropped.

18. TEAM BUILDING



A motivated team in which all members are equally involved and can rely on each other is a key factor for success (Larsen, 2004). Organisations therefore need to devote time for the planning and development of a positive project culture (Harry, 1997; Ives & Olson, 1985; Newman & Sabherwal, 1996). People management was not an easy task in all projects. Projects members and teams had different starting points and personal aims. Most of the project teams included equal levels of senior managers and decision influencers.

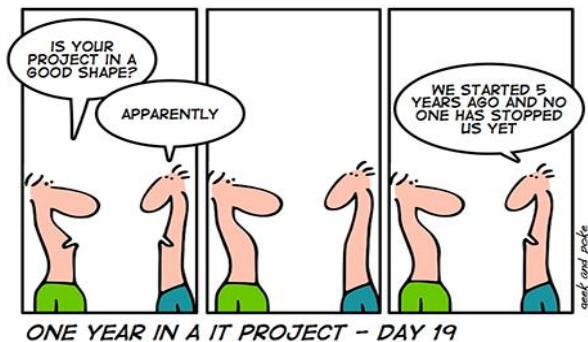
This caused a lot of conflicts at different stages in the project as many of them were not all working by the same rules and procedures and had their own agendas. This again, weakened cooperation and reduced the potential for project members to benefit from each other. It also reduced the projects managers' flexibility as it was hard to transfer people from one activity to another.

19. INADEQUATE RESOURCES



For any business endeavour to succeed it must be blessed with the right amount of resources at an acceptable level of quality and skills (Hitchin & Ross, 1994). The rate of recruitment of staff in all projects was far too slow to bring the necessary staff in a broad spectrum of the vital positions to the level of knowledge required by the requisite dates. The workload (managerial and operational) continued to be done by a group of people too small in number and not all of them were dedicated to the projects.

20. THE INCAPABLE PROJECT MANAGER



Managing complex large-scale projects requires organisational and technical skills (Huber, 2003; Mullaly, 2003; Schneider, 1999). It requires

dealing effectively with new technology, new business processes, and changes in organisational structures, standards, and procedures (Harry, 1997; Ives & Olson, 1985; Newman & Sabherwal, 1996). Unless the project manager is sensitive to the impact of each of these elements on the project as a whole, he or she is likely to get caught in conflict situations (ibid).

The beginning of all projects was a honeymoon period, when all projects members felt great about the project. It was when the project teams began to develop substance in its recommendations that difficulties arose. The project managers were supposed to be convincing and persuasive; to sell the overarching goals to obtain the continuous support of the project members. The problem was that the project managers, often from the consulting companies, were viewed in some projects, as the persons standing next to and supporting the vendors.

Some project managers and in an attempt to hide their project management shortcomings, were always trying to involve themselves in diminutive activities that could have been accomplished by the most junior staff in the projects. There were also those moments, when the project managers became frustrated with the project teams and began to think of them as people who needed to be disciplined and made to pay attention to the project and started reporting them to the steering committees.

The workshops were sometimes turned into a war room, where the noise level was high, especially that of the project managers, who should have been maintaining control. Partly they were incapable of controlling the teams because of the equal power of the technical

teams. This set up an increasingly negative atmosphere in the projects. It seemed the projects were heading towards serious trouble.

Few project managers decided to leave the projects shortly before the first pilot operation start date. Although some senior team members took their positions upon their leave, it was apparent that they left behind a gap in knowledge in many project areas that they accumulated during their assignment. Those projects went through a struggle for a while until the new members built up the required knowledge.

21. EYEWASH PROCEDURES



One common element seen in many projects is the adoption of what are so-called eyewash procedures that do not give meaningful directions, or guidelines (Gilbreath, 1986). One may argue that as long as these procedures do not prevent performance, understanding or control of project work, they present little problem (*ibid.*). However, what usually occurred in the projects was just the opposite: confusion, and wasted resources.

The consulting companies presented “oodles” of procedures that were supposed to be followed in the projects. In reality, only few were followed e.g., change requests, meeting minutes, risk sheets, to name a few. The fact that there were too many procedures and templates confused many projects members and led them to develop their own ways of doing things. This again created more confusion especially since some projects documentation followed different standards.

22. FAILING MANAGEMENT REPORTS



Information plays a dual role in any project, that of a valuable resource and an essential tool. Management reports are only as good as the information they contain and that information has value only when it promotes analysis (Garreth et al., 2000; Gilbreath, 1986; Laudon & Laudon, 1998; Mullins, 1996; Wysocki, 2000). It does not matter how they are structured, how frequently they are produced, or how many ways

they can slice and graphically depict the information pie, reports that do not promote analysis do not deserve management attention (ibid.).

For long periods, the projects monthly reports produced by the projects did not carry the desired quality of information to enable the steering committees to maintain an overview of the projects' progress or to understand the potential risks the projects may have been heading towards. In fact, the submitted reports were lengthy and contained lots of data that led the steering committee to abandon reviewing the monthly reports altogether.

23. CONCLUSION

Project management is a research topic on which there is much literature written about. However, recent studies show that the failure rate in the IT industry is still a continuing story. No overarching framework or methodology to guide projects to success has yet emerged. This paper presented some lessons from many governments IT projects where the challenges reported herein obstructed the maintenance of the projects triangle of project schedule, budget and quality in equilibrium.

The reported pitfalls were almost all organisational issues related to management and people. Thus, these factors need to be comprehended by both project management professionals and key executives/owners in organisations.

REFERENCES

- [1] Avison, D.E. & Wood-Harper, A.T. (1990) *MultiView - an exploration in information systems development*. USA: McGraw Hill.
- [2] Avison, D.E., Fitzgerald, G. (2003) *Information Systems Development: Methodologies, Techniques and Tools*, 3rd ed., McGraw-Hill, London.
- [3] Bentley, C. (2002) *Practical PRINCE2*. USA: The Stationery Office Books.
- [4] Berkun, S. (2005) *The Art of Project Management*. USA: O'Reilly.
- [5] Binney, G. & Williams, C. (1997) *Leading into The Future: Changing The Way People Change Organisations*. London: Nicholas Brealey Publishing.
- [6] Broder, J.F. (1999) *Risk Analysis and the Security Survey* (2nd Edition). Boston: Butterworth-Heinemann.
- [7] Burnes, B. (2004) *Managing Change* (4th edn). London: FT Prentice Hall.
- [8] Checkland, P. (1999) *Systems Thinking, Systems Practice*, Chichester: John Wiley & Sons.
- [9] Checkland, P. and Holwell, S. (1998) *Information, Systems, and Information System: Making sense of the field*. Chichester: John Wiley & Sons.
- [10] Collins, T. (2006) "Government IT: What happened to our £25bn?" IT Management, Politics & Law, *ComputerWeekly.com* [Online]. Available from: <http://www.computerweekly.com/Articles/2006/10/30/219476/government-it-what-happened-to-our-25bn.htm> [Accessed 13 November 2007].
- [11] Crain, W. (1992) *Theories of Development: Concepts and applications* (3rd Edition). New Jersey: Prentice Hall International.
- [12] Cross, M. (2002) "Why government IT projects go wrong," *Computing*, [Online]. Available from: <http://www.itweek.co.uk/computing/features/-2072199/whygovernment-proje-cts-wrong> [Accessed 12 June 2007].
- [13] Crouhy, M., Mark, Robert & Galai, D. (2001) *Risk Management*. USA: McGraw-Hill.
- [14] Curtis, G. (1998) *Business Information Systems: Analysis, Design, and Practice* (3rd Edition). USA: Addison-Wesley.
- [15] Fichter, D. (2003) "Why Web projects fail," *Online* (July/August), Vol. 27, No. 4, pp. 43-45.
- [16] Finney, R. (1999) 'Monitoring an Active Project Plan', *Information Technology Management WEB* [Online]. Available from: <http://www.itm-web.com/essay012.htm> [Accessed 12 Dec 2007].

- [17] Frame, J.D. (1999) *Project Management Competence*. Jossey Bass: San Francisco.
- [18] Gareth, R., George, J.M.; Hill, C.W.L. (2000) *Contemporary Management* (2nd Edition). USA: McGraw-Hill.
- [19] Gartner Group View (1999) "Are all IT projects doomed for failure," *Asia Computer Weekly*, Singapore (September), p. 1.
- [20] Gilbreath, R.D. (1986) *Winning at Project Management: what works, what fails and why*. New York: John Wiley & Sons.
- [21] Harry, M. (1997) *Information Systems in Business* (2nd Edition). Great Britain: British Library Cataloguing in Publication Data.
- [22] Hitchin, D. & Ross, W. (1994) *Achieving Strategic Objectives: The Role of Human Resources and Organisational Development*. USA: Addison Wesley Longman Publishing Co.
- [23] Huber, N. (2003) 'Hitting targets? The state of UK IT project management', *ComputerWeekly*, (November 5).
- [24] Ives, B. & Olson, M.H. (1985) "User involvement and MIS Success," *Management Science*, Vol. 30, No. 5, pp.586-603.
- [25] Kerzner, H. (2004) *Advanced Project Management: Best Practices on Implementation* NJ: Wiley & Sons, Inc.
- [26] Keuning, D. (1998) *Management: A Contemporary Approach*. London: Pitman Publishing.
- [27] Lam, L. (2003) *Enterprise Risk Management: From Incentives to Controls*. NJ: Wiley & Sons, Inc.
- [28] Larsen, E.R. (2004) 'People: The Key to Successful Project Management', *Chemical Engineering Progress* (September), Vol. 100, No. 9, pp. 55-8.
- [29] Laudon, K. & Laudon, J. (1998) *Management Information Systems – New Approaches to Organisations & Technology*. New Jersey: Prentice Hall, pp. 334-379 & pp. 624-653.
- [30] Marrison, C. (2002) *The Fundamentals of Risk Measurement*. USA: McGraw-Hill.
- [31] Mullaly, M.E. (2003) 'The Accidental Project Manager: Coming In From the Cold', *gantthead.com* [Online]. Available from: <http://www.gantthead.com/article.cfm?ID=165059> [Accessed 10 Nov 2007].
- [32] Mumford, E. (1986) "Participation in Systems Design: What can it Offer", paper presented at SERC/CREST Advanced Course, Loughborough University.

- [33] Newman, M. & Sabherwal, R. (1996) 'Determinants of Commitment to information Systems development: a longitudinal investigation', *MIS Quarterly*, Vol. 20, No. 1.
- [34] Olle, T.W., Hagelstein, J., Macdonald, I.G., Rolland, C., Sol, H.G., Van Assche, F.J.M. & Verrijn-Stuart, A.A. (1991) *Information Systems Methodologies: A Framework for Understanding* (2nd Edition). Wokingham: Addison-Wesley.
- [35] O'Toole, W. & Mikolaitis, P. (2002) *Corporate Event Project Management*. NJ: Wiley & Sons, Inc.
- [36] Radosevich, Lynda, Measuring Up: the importance of metrics in IT project management, *CIO Magazine*, CIO Communications, Inc., September 15, 1999.
- [37] Schneider, P. (1999) 'Wanted: ERP People Skills,' *CIO*, March 1, 1999, pp. 30-37.
- [38] Wideman, R.M. (1998) *Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities*. USA: Project Management Institute.
- [39] Wilson, B. (1990) *Systems: Concepts, Methodologies and Applications* (2nd Edition). Chichester: John Wiley & Sons.
- [40] Wysocki, R.K., Beck, R., & Crane, D.B. (2000) *Effective Project Management*. New York: John Wiley.

An **INNOVATIVE** Project Management Methodology ²

Ali M. Al-Khouri

COPYRIGHT © 2007 WARWICK ENG CONFERENCE

ABSTRACT: This paper presents a project management methodology - developed part of an engineering doctorate research at Warwick University - for managing strategic and large scale IT projects. The methodology was mainly tested in 4 countries. The research demonstrated that by following a formal structured methodology, governments will have better visibility and control over such programmes. The implementation revealed that the phases and processes of the proposed methodology supported the overall management, planning, control over the project activities, promoted effective communication, improved scope and risk management, and ensured quality deliverables.

Key words: *Project Management; Project Methodology.*

² Al-Khouri, A.M. (2007) "**A Methodology for Managing Large-Scale IT Projects.**" *Proceedings of Warwick Engineering Conference*, Warwick University, Warwick, United Kingdom, pp.1-6.

1. INTRODUCTION

RECENT studies estimated that the cost associated with implementing large scale government IT projects to scale up to multi-billion US dollars (Fontana, 2003). Obviously, the nature, size and complexity of these projects raise their failure probabilities. This is in reference to the accepted phenomenon in the literature by both academics and practitioners that information technology projects have very high failure chances and that between 60 to 70 per cent do actually fail. Many other researchers argue that the actual figure might be far more frightening since many organisations tend not to disclose such experiences, due to fear of criticism by audit or the media (Dorsey, 2004; Fichter, 2003).

By and large, the knowledge required to succeed with IT is complex and rapidly changing. It is noted that the examples in the existing literature are rarely of the size and complexity of those executed in the government sector. Proceeding without understanding and managing the risk inherent in such projects will obviously lead to higher probabilities of failure.

This paper presents an overview of a project management methodology that was implemented in 4 countries, to support the management and control of the project phases. This paper is structured as follows. First some recent studies on the IT projects failure are highlighted along with the factors leading to such results. Then the field of project management is briefly explored to pinpoint the need for a methodological approach to managing large IT projects. The process followed, underlying principles, and an overview of the proposed methodology phases are provided next. A synopsis on the implementation of the methodology and its value are outlined in the following two sections, and the paper is then concluded.

2. IT PROJECTS FAILURE

In line with the above statistics, it is estimated that between 20-to-30% of industrialised country government IT projects fall into the total failure category; 30-to-60% fall into the partial failure category; and that only a minority fall into the success category (Heeks, 2003). Studies indicate that large-scale projects fail three to five times more often than small ones (Charette, 1995).

Such failure can impede economic growth and quality of life and that the cost of failure may become catastrophically excessive as societies come to rely on IT systems that are ever larger, more integrated, and more expensive (ibid). Many researchers pointed out that a lot of today's failures are avoidable and that many of the projects fail because of foreseeable circumstances and that organisations need to give careful attention to several factors to avoid failure (Avison & Wood-Harper, 1990; Bentley, 2002; Berkun, 2005; Broder, 1999; Curtis, 1998; Lam, 2003; Radosevich, 1999).

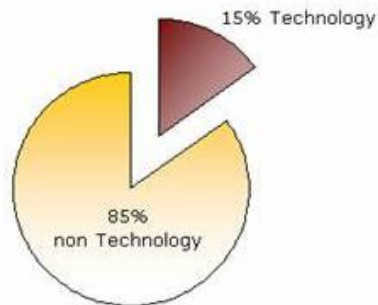


Fig. 1: Critical Success Factors - Technology Vs. Non-Technology

Among the widely quoted factors contributing to failure is that organisations tend to treat IT projects from pure technological perspectives, and not give much attention to other organisational and

management issues. The literature shows that technology can contribute as little as 15 percent to the overall success of projects (see also Figure 1), where as the remaining 85 percent is dependent on bigger organisational issues related to people, data, and management.

Research points to the fact that one of the principle causes of information system failure is when the designed system fails to capture the business requirements or improve the organisational performance. Figure 2 below illustrates an example of how a user's requirements might be interpreted, not only at the requirements analysis stage but throughout the project.

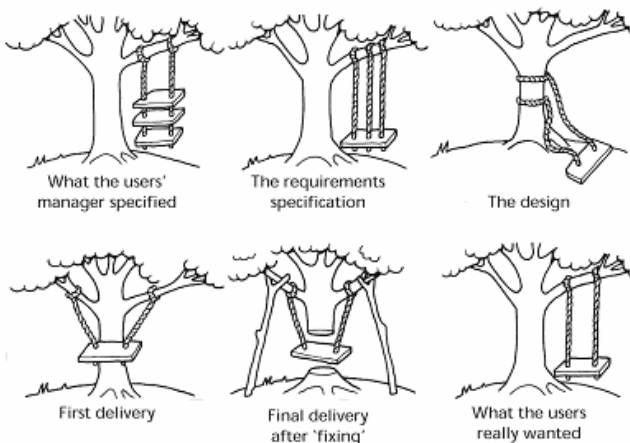


Fig. 2: interpretation of user requirements

3. PROJECT MANAGEMENT

The argument of this research undertaking has been mainly to advocate that by following a disciplined methodology that sets

standards for all phases of the project is more likely to increase the success chances. Project management is viewed as the art of defining the overall management and control processes for the project (Devaux, 1999; Garton and McCulloch, 2005; Stankard, 2002).

Project management worked with differing degrees of success, in different industries, different organisations, and on different projects. What is undeniable is that industries have been much more successful when project management is used than when it was ignored (Devaux, 1999; Ireland, 1991).

A project management methodology that takes into account the success and failure factors in the field of IT projects are more likely to increase the success probabilities of the project (see for example: Avison & Fitzgerald, 1998; Curtis, 1998; Flynn, 1998).

Looking at the existing available methodologies, the literature perceives the field as a jungle with large and confusing variety of approaches in existence (Avison & Fitzgerald, 1998). It is estimated that over a thousand brand name methodologies exist world-wide (Jayaranta, 1994). Charvat (2003) found in an analysis of 18 different methodologies that:

- (1) some focus purely on the technology itself,
- (2) others focus more on a generic project management approach

As such researchers argue that organisations need to carefully assess the methodology based on the organisational requirements and that it is the project size and complexity which necessitates the use of the *fitting* methodology (Berkun, 2005; Charvat, 2003; Radosevich, 1999; Verrijn-Stuart, 1991; Gilbreath, 1986). From a practical point of view,

there is no one methodology that guarantees success, but rather by employing one, an organisation will have a structured set of concepts to handle each step - from understanding the business requirements to the development of the system - in the project (Avison & Fitzgerald, 1998; Crain, 1992; Curtis, 1998; Harry, 1997; Ives & Olson, 1985; Newman & Sabherwal, 1996; Olle et al., 1991).

The following section describes the process followed in the development of the methodology that was later implemented to manage the UAE programme.

4. CRAFTING THE METHODOLOGY

Researchers have continuously emphasised the need for organisations to seriously analyse failed or out-of-control IT projects, and the associated challenges. Nonetheless, research to date has found no single explanation for system success or failure. Nor does it suggest a single or a magic formula for success.

Successful projects	<ul style="list-style-type: none"> • User Involvement • Executive Management Support • Clear Statement of Requirements • Proper Planning • Realistic Expectations
Challenged projects	<ul style="list-style-type: none"> • Lack of User Input • Incomplete Requirements & Specifications • Changing Requirements & Specifications • Lack of Executive Support • Technical Incompetence
Failed projects	<ul style="list-style-type: none"> • Incomplete Requirements • Lack of user involvement • Lack of Resources • Unrealistic Expectations • Lack of Executive Support • Changing Requirements & Specifications • Lack of Planning • Didn't Need it Any Longer • Lack of IT management • Technical Illiteracy

Table 1: indicators found between and successful and failed projects

However, it has found different elements leading to project success or failure. These elements were more or less presented in the Standish Group *CHAOS 2001* report as shown in Table 1. Mapping these factors from Standish report to the literature, the most common factors that contributed to project success or failure were:

- Management Commitment
- Business Strategy Focus
- Requirements Definition
- Complexity Management
- Changing targets
- Formal Methodology
- Project Management
- Planning
- User Involvement
- Risk Management

These factors were taken into consideration when designing the methodology. In the development and implementation of the methodology, the underlying principles were based on theories and practices coming from two subject areas:

- (1) Project management, and
- (2) System development.

In addition to the above elements, the methodology has been developed to address the core needs identified for supporting and improving the following:

1. concept development
2. overall project portfolio management
3. management of stakeholders expectation
4. analysis of requirements
5. quality of output
6. utilisation of resources
7. communication and management reporting
8. project control and risk management
9. knowledge management

A two-staged project management methodology consisting of nine phases was developed depicted in Figures 3 and 4. The methodology is composed of the following interlinked processes:

1. initiating processes
2. planning processes
3. executing processes
4. controlling processes
5. closing processes

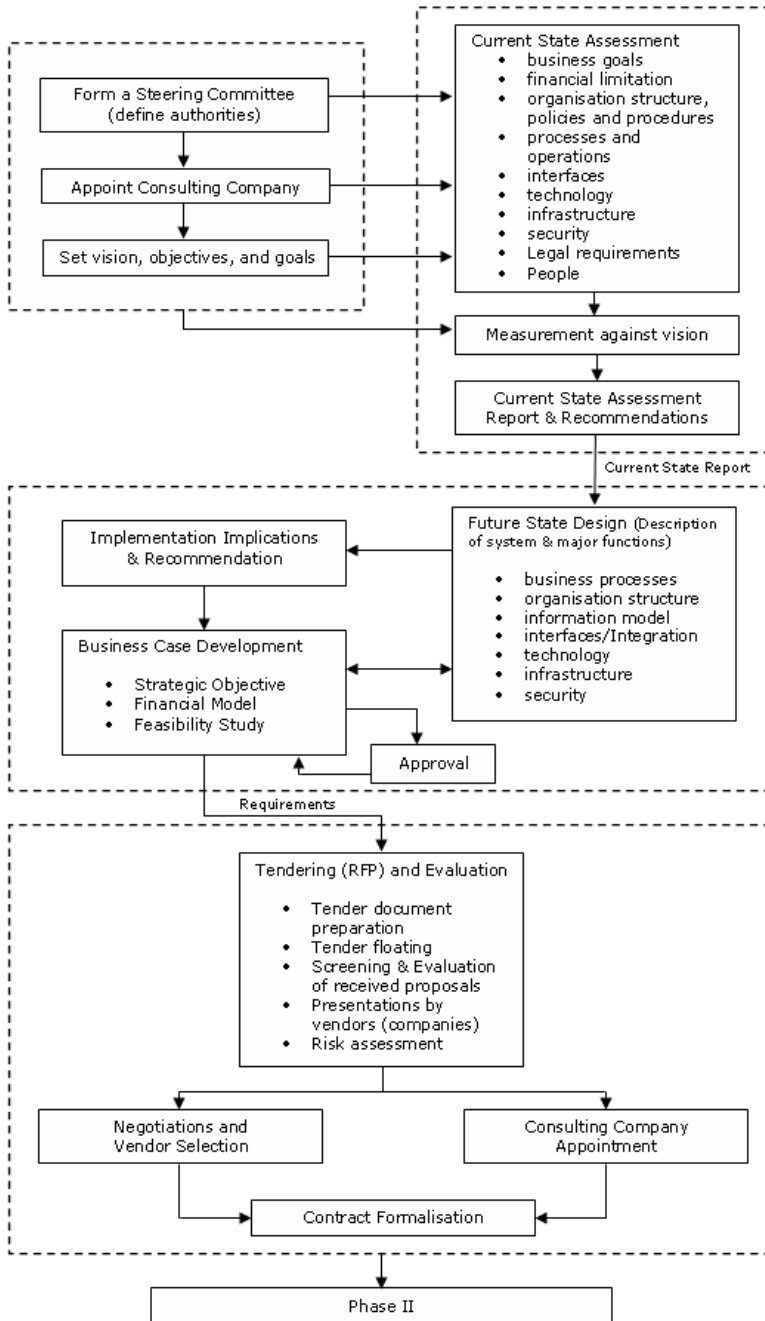


Figure 3: Phase one of the proposed methodology

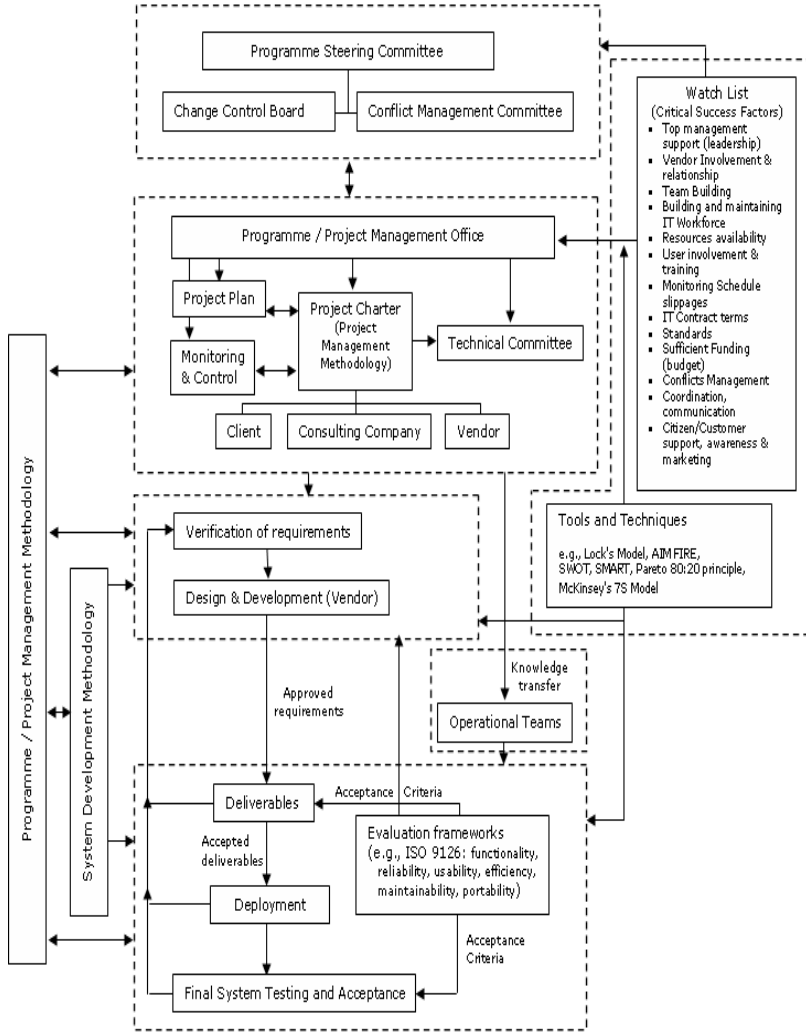


Figure 4: Phase one of the proposed methodology

5. APPLYING THE METHDODOLOGY

The methodology was mainly tested in 4 large government projects. Presentations in conferences and official delegation visits to many countries worldwide contributed to the overall enhancement and

supported the value of the methodology. The model was refined at several stages to address common problems identified during the implementation, and the feedback from the government officials and experts in the field.

The implementation of the methodology has revealed the following contributions to the overall project management practices:

1. agreed and articulated project goals and objectives
2. staged and controlled phases with sign-offs
3. regular reviews of progress against plan, scope, quality.
4. supports project and management status reporting
5. global overview of the project processes, beginning and end of the project, and all the work in the middle
6. strong management control through clear change control and conflict management procedures
7. promoted the involvement of management and stakeholders at different stages of the project
8. clear focus on defining system requirements
9. capturing and sharing of lessons learned
10. improved project control – evaluate and measure performance based on the defined scope, schedule, budget, quality of deliverables.
11. transparent project management practices
12. risk management
13. handled project complexity

14. virtuous communication channels among the project stakeholders

Twelve consideration areas that governments need to heed during the course of the scheme implementation were also identified:

- Having clear goals
- Appointing a project director
- Setting up a project management office
- Assessing project managers skills (leadership skills, communication, negotiation, delegation, problems solving, change management, etc)
- Develop stakeholders commitment
- Dealing with project team anxiety
- Team assembly
- responsibility assignment (RA) through RA Matrix
- Monitoring, evaluation and control
- Performance observation
- Planning and communicating
- Skilled team members
- Flexibility of the project plan

6. SIGNIFICANCE AND VALUE OF THE METHODOLOGY

The implementation results of the systems, and the feedback from the government officials and experts in the field indicated the value and significance of the methodology. The methodology was noted to incorporate flexible and easy to understand principles of project management to improve the planning and control of the government schemes.

There was also a common view that the phases and processes of the methodology improved the overall visibility and control of the project activities, promoted effective communication, supported scope and risk management, and ensured quality deliverables. One could still argue that multiple data from multiple case studies would have provided better indication of the reliability and value of the development methodology. However, governments' policies especially in this kind of projects do not allow close involvement or data dissemination. In fact, government projects are tend to be hidden from the public domain in many countries.

The nature of strategic and large scale IT programmes carries much higher confidentiality rating. Nonetheless, to prove real usefulness and contribution as a standard for managing such programmes, it would require a significant period of time to gather objective quantitative data from different experiments. Nevertheless, the methodology takes an advantage over the existing standard methodologies in the fact that it has been applied and customised to 4 international projects. The appreciation and feedback from the 4 countries, government officials worldwide, and experts in the field demonstrates the usefulness of the methodology too.

7. CONCLUSION

Following best practices or a particular project management methodology or framework, cannot make projects *failure proof*. To succeed, a successful project needs much more than a cookbook approach specially when implementing large scale projects. There are many issues that require management attention and a comprehension

of their possible impact is considered essential to increase the chances of a successful endeavour.

This research attempted to add value to the limited knowledge currently available to practitioners and researchers about project management methodologies, and introduced a new test PM methodology in four large scale government IT programmes. Project management was found crucial to exist in large and complex projects where attention was required to analyse and carefully respond to the implications of the slightest change.

It is important for management to realise that every project is unique, and that by repeating old experience or practices from similar past projects will not help to accommodate the ever changing landscape of today's projects. Successful implementation requires clear business process, the ability to manage the system's flexibility, and the ability to cope with high complexity levels (Frame, 1999; Garton & McCulouch, 2005; Gilbreath, 1986).

Above and beyond, successful implementation requires superior skill in a variety of generic business, communication, and organisational skills, in addition to knowledge of the deployed technologies (Haller, 1998; Ireland, 1991; Kerzner, 2004; Page, 2002). Under these circumstances, project management is argued to be essential to achieve better visibility and control over projects.

REFERENCES

- [1] Avison, D.E. & Wood-Harper, A.T. (1990) *MultiView - an exploration in information systems development*. USA: McGraw Hill.
- [2] Bentley, C. (2002) *Practical PRINCE2*. USA: The Stationery Office Books.

- [3] Berkun, S. (2005) *The Art of Project Management*. USA: O'Reilly.
- [4] Broder, J.F. (1999) *Risk Analysis and the Security Survey* (2nd Edition). Boston: Butterworth-Heinemann.
- [5] Charette, R.N. (1995) 'Why Software Fails, *IEEE Spectrum*' [Online]. Available from: <http://www.s-pectrum.ieee.org/sep05/1685> [Accessed 01 01 2007].
- [6] Charvat, J. (2003) *Project Management Methodologies*. New Jersey: John Wiley & Sons.
- [7] Crain, W. (1992) *Theories of Development: Concepts and applications* (3rd edition). New Jersey: Prentice Hall International.
- [8] Curtis, G. (1998) *Business Information Systems: Analysis, Design, and Practice* (3rd Edition). USA: Addison-Wesley.
- [9] Devaux, S.A. (1999) *Total Project Control*. New York: John Wiley & Sons.
- [10] Dorsey, P. (2000) 'Top 10 reasons why systems projects fail,' [Online]. Available from: <http://www.dulcian.com/papers> [Accessed 03 02 2007].
- [11] Fichter, D. (2003) 'Why Web projects fail', *Online* (July/August), vol. 27, no. 4, pp. 43-45.
- [12] Fontana, J. (2003) 'A national Identity Card for Canada' [Online]. Canada, House of Commons. Available from: <http://www.parl.gc.ca> [Accessed 03 03 2007].
- [13] Frame, J.D. (1999) *Project Management Competence*. San Francisco: Jossey Bass.
- [14] Garton, C & McCulloch, E, (2005) *Fundamentals of Technology Project Management*. USA: McPress.
- [15] Garton, C. and McCulloch, E. (2005) *Fundamentals of Technology Project Management*. USA: Mc Press.
- [16] Gilbreath, R.D. (1986) *Winning at Project Management: what works, what fails and why*. New York: John Wiley & Sons.
- [17] Haller, R. (1998) *Managing Change*. London: Dorling Kindersley.
- [18] Harry, M. (1997) *Information Systems in Business* (2nd edition). Great Britain: British Library Cataloguing in Publication Data.
- [19] Heeks, R.B. (2003) 'Most eGovernment-for-Development Projects Fail: How Can Risks be Reduced?' *IDPM i-Government Working Paper*, 14, [Online]. UK: University of Manchester. Available from: <http://www.ed-exchange.org/eGov/faileva-l.htm> [Accessed 02 04 2007].

- [20] Ireland, L.R. (1991) *Quality Management for Projects and Programs*. USA: Project Management Institute.
- [21] Ireland, L.R. (1991) *Quality Management for Projects and Programs*. USA: Project Management Institute.
- [22] Ives, B. & Olson, M.H. (1985) 'User involvement and MIS Success', *Management Science*, vol. 30, no. 5, pp.586-603.
- [23] Jayaratna, N. (1994). *Understanding and Evaluating Methodologies: NIMSAD A Systemic Framework*. London, MacGraw-Hill.
- [24] Kerzner, H. (2004) *Advanced Project Management: Best Practices on Implementation*. NJ: Wiley & Sons, Inc.
- [25] Lam, L. (2003) *Enterprise Risk Management: From Incentives to Controls*. NJ: Wiley & Sons, Inc.
- [26] Newman, M. & Sabherwal, R. (1996) 'Determinants of Commitment to information Systems development: a longitudinal investigation', *MIS Quarterly*, vol. 20, no. 1.
- [27] Olle, T.W., Hagelstein, J., Macdonald, I.G., Rolland, C., Sol, H.G., Van Assche, F.J.M. & Verrijn-Stuart, A.A. (1991) *Information Systems Methodologies: A Framework for Understanding* (2nd Edition). Wokingham: Addison-Wesley.
- [28] Page, S.B. (2002) 'Project Management Methodology: The Key To Becoming a Successful Project Manager', *gantthead.com* [Online]. Available from: <http://www.gantthead.com/article.cfm?ID=135300> [Accessed 10 04 2007].
- [29] Radosevich, L. (1999) 'Project Management Measuring UP', *CIO* [Online]. Available from: http://www.cio.com/archive/091599_project.html [Accessed 10 01 2007].
- [30] Stankard, M.F. (2002) *Management Systems and Organisational Performance: The Search for Excellence Beyond ISO9000*. USA: Quorum Books.

Paper

3

UAE National ID Program ³

... a case study

Ali M. Al-Khouri

COPYRIGHT © 2007 WASET.ORG

ABSTRACT: This article provides some insight into the implementation of the national ID programme in the United Arab Emirates (UAE). The fundamental aim is to contribute to the existing body of knowledge in the field, as it sheds light on some of the lessons learned from the programme that is believed to widening the knowledge horizons of those involved in such initiatives

Key words: *National ID; Identity Management.*

³ Al-Khouri, A.M. (2007) "UAE National ID Programme Case Study," International Journal Of Social Sciences, Vol. 1, No. 2, pp.62-69.

1. INTRODUCTION

MANY countries around the world have either implemented, or are in the process of embarking on national ID projects. The key motives behind such initiatives is to improve the identification and authentication mechanisms in order to reduce crime, combat terrorism, eliminate identity theft, control immigration, stop benefit fraud, and provide better service to both citizens and legal immigrants (see for example: [1],[2],[3],[4]).

In view of the fact that these projects are unique undertakings and involve a degree of uncertainty and risk, national ID programmes are perceived to carry a high level risk and that more knowledge needs to be acquired to understand the complexity of these types of endeavors. In this regard, this article aims to present a case study of the implementation of an ID card programme in the UAE, and to highlight some of the lessons learned which, if considered, are most likely to support the planning and execution of similar initiatives.

This article is structured as follows. First, some primary information about the programme, its strategic goals and objectives are presented. The technologies employed and the enrolment process are explained next. A short overview of the enrolment strategy is provided and then the lessons learned are presented which concludes the paper.

2. UAE ID CARD PROGRAMME

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 co-ordination of and the citizen's access to public services.

The project which was kicked off in June 2003, aimed to develop a modern identity management system with two strategic objectives addressing security and economical requirements (see also Figures 1 and 2). The security objective evolves around the necessity of the government to have an integrated population register that will become the central reference point for the whole government for the purpose of population identification and service delivery.

By employing the necessary technologies, the project develops a trusted and robust identity verification infrastructure to enhance homeland security and help the government in protecting individuals against the ever increasing crime of identity theft.

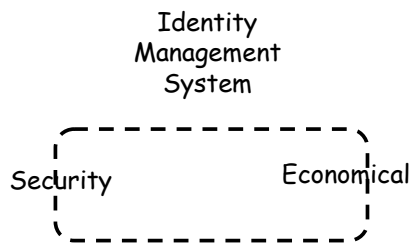


Fig. 1: project strategic goals

The second strategic goal of the project evolves around supporting the government's economy. One of the key requirements in this goal is to support the country's digital economy by building a national e-authentication infrastructure which should become the basis and the backbone for e-government services and e-commerce initiatives.

Besides, having a centralised and integrated population register will assist in planning and utilising resources as it should provide timely, accurate, and statistical information for strategic decision making and

long term planning with respect to education, healthcare, town planning, transport requirements, energy, etc.

Another side of this objective aims to unify the existing cards in the country such as driving license, labour card, health card, and other 'entitlement'⁴ cards. This will also have a profound impact on the economies of scale in the management and production costs of such cards.

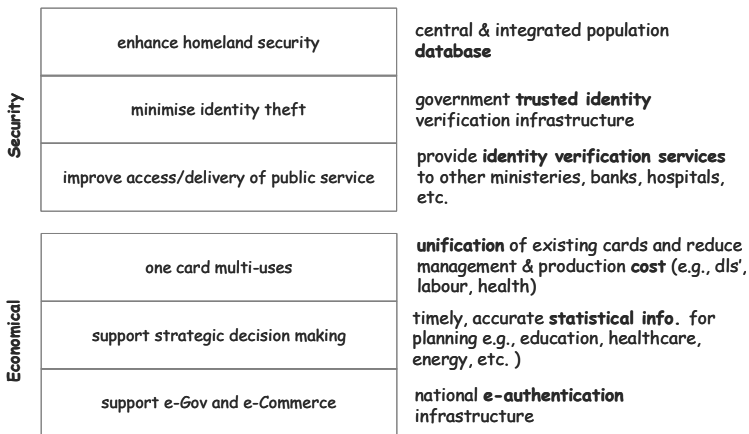


Fig. 2: security and economic objectives

3. KEY OPERATIONS OF THE NATIONAL ID SYSTEM

The national ID system incorporates the latest technological advances. It is designed based on a 4-tier web-based architecture and complies with the latest industry standards such as ICAO for card design, x.509 for

⁴ There are two main types of identity documents used in many countries. The first are often referred to as "foundation" documents, and they include birth certificates and immigration records. These primary documents are used to obtain documents of the second type, "entitlement" documents, such as passports, drivers' licences and other government issued documents.

PKI, and ISO 17799 for IS security policy. The system guarantees secured communication throughout the system's national network structure by using Virtual Private Network (VPN) technology and an associated technical Public Key Infrastructure (PKI).

The fingerprint-based biometry provides the means to ensure a single identity for each applicant and to authenticate the identity of the ID card bearer. In principle, the national ID system is designed to provide three primary operations as depicted in Figure 3.

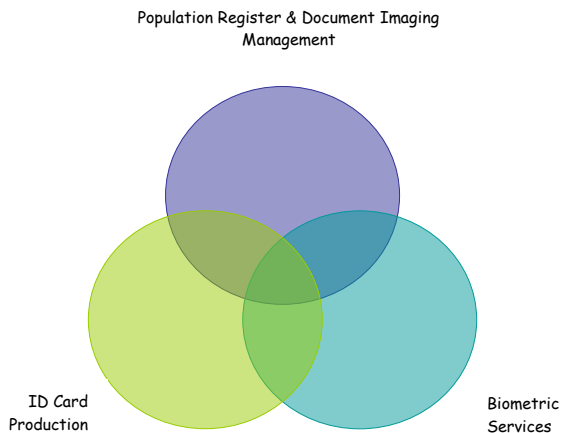


Fig. 3: primary operations of the national id system

3.1 Population Register and Document Imaging Management (PRDI)

The National ID system maintains the Population Register that records information about every UAE citizen and legal resident registered on the system and assigns a unique Identification Number (IDN) to each person. The system is currently sized to manage five million records.

It provides the means to record events such as births, marriages, divorces and deaths, as well as the updation of variable (constantly changing) information such as address, education, employer, etc. The National ID system also stores images of the official support documents presented during the application for an ID card or on events declaration on the Population Register.

3.2 ID Card Production

The National ID system includes a process for the enrolment, processing, production and delivery of ID cards. This process is adapted for the first application for an ID card including the renewal of an expired ID card or the replacement of a damaged, lost or stolen ID card. The ID card produced by the national ID system includes biometric fingerprint-based authentication capabilities and uses a public key infrastructure (PKI) that is adapted for future e-government and e-commerce usage.

3.3 3 Biometric Services

The national ID system provides a complete range of biometric functions using fingerprints and palm prints. The system encompasses an Automatic Fingerprint and Palm Print Identification System that provides person identification, authentication, crime solving and crime linking services. These services are used to guarantee the applicant's identity using the ID card and to ensure that a person is issued with one and only one ID card. The full set of biometric services is also used for law enforcement purposes.

4. ID CARD

The ID card is identical for both UAE citizens and residents in terms of card design and displayed data. The card validity period is set for 5

years for citizens, and is linked to the residency permit validity for residents. The ID card includes a digital certificate with PKI capabilities. This feature constitutes one of the basis for future online identification, authentication and transactions to support e-government and e-commerce.

chip data
digitally
signed &
encrypted



Overt:

- Guilloches & Rainbow
- Ghost image
- Holographic overlay
- Variable fine lines
- Special Raster
- UV ink
- Rainbow printing

Covert:

- Micro text
- Hidden text
- UV

Fig. 4: UAE id security features

As depicted in Figure 4, it contains many security features which will make it very difficult if not impossible to forge the card and will allow in most cases a trained card acceptor to identify a faked ID card even on face value.

The digital security on the ID card chip in terms of the used signature and encryption features is accorded to the highest international security levels. In terms of the IT security in the contact chip, the UAE ID card follows the highest electronic standards, based on the use of asymmetric encryption and digital signature.

5. IMPLEMENTATION STAGES AND THE ENROLMENT STRATEGY

The system was implemented mainly in three phases (see also Figure 5):

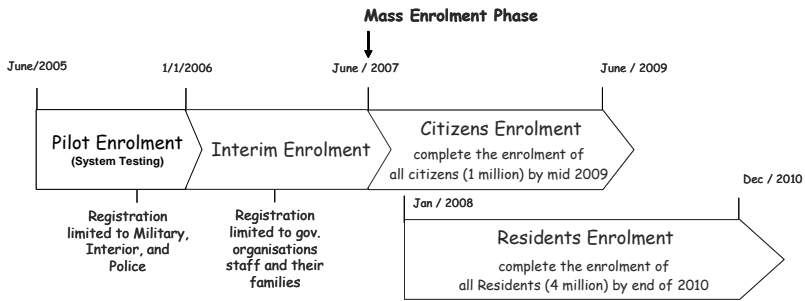


Fig. 5: enrolment plan

5.1 Pilot Enrolment:

The first live enrolment began in June 2005 as a pilot phase in an attempt to test the system and its capabilities. This was considered to be a good starting point since many technical and business process related issues were identified that needed the system to cater for. The enrolment was stopped for more than two months to upgrade the software of the overall system to reflect the new identified requirements.

5.2 Interim Enrolment:

Although the system was ready for the mass enrolment phase towards the end of 2005, the enrolment was limited to the registration of staff of government organisations where registration centres were available, due to the incompleteness of the construction projects of the majority of the registration centres across the country.

5.3 Mass Enrolment Phase:

The registration in this phase was linked to the obtainment of certain services from the government sector such as the renewal of vehicles and passports for citizens, and the renewal and issuance of residency permits for residents. With a 3 year enrolment strategy, the project aims to register the whole population of the country by end 2010.

The registration process of those new births and new residents is planned to take place directly through the Ministry of Health and Ministry of Interior who will interface with the national ID database that will initiate automatic requests such as first ID card application, card issuance, ID card renewal and replacement, and population register events declarations such as marriage, divorce, birth, etc.

6. ENROLMENT PROCESS

Taking into consideration the criticality and importance of the enrolment process as the new national ID card will become the source document to prove an individual's identity, a robust registration process was put in place to ensure comprehensive identity verification prior to the issuance of the ID card (see also Figure 6).

Applicants are supposed to come to any of the available registration centres with the supporting documents (application form⁵, passport and family book for citizens). The applicant goes through a three staged (12 to 17 min) process at those centres. In the first office, the particulars completed on the application is scanned into the system through the 2D barcode on the form and verified against the immigration system of the Ministry of Interior online.

⁵ The application form is also available for download from the Internet.

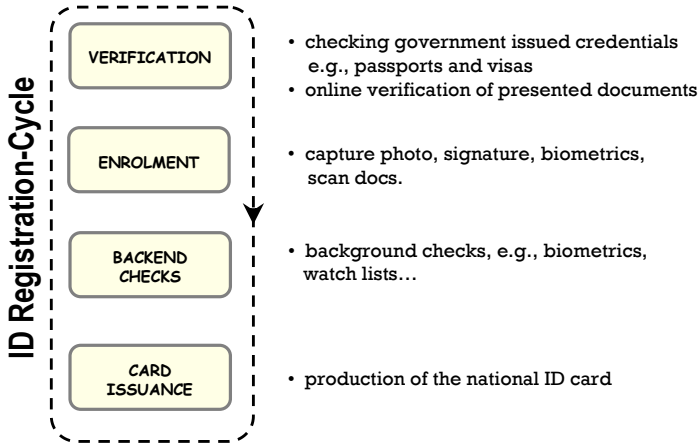


Fig. 6: registration and card issuance process

The applicant then moves to another station where his/her photo is captured, a signature acquired using an electronic pad (which is then digitised into the system), and some supporting documents are scanned in. He then goes through the last station where his/her 10-fingerprints are captured (slaps, rolled, palm and writers' palm).

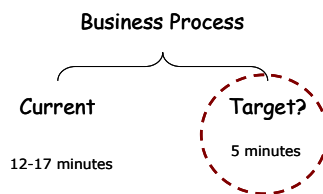
The applicant is then given a receipt indicating the date he/she must return to collect his/her card or that it will be sent to him/her through a registered courier.

The choice of card delivery is left to the applicant. Before the card is printed, there are other processes that run at the backend for further investigation. A biometric check is performed against civil and forensic fingerprint databases to ensure that the person has not been registered in the system previously, and is not wanted by the police authorities. In normal cases, cards are printed and distributed within 48 hours.

7. LESSONS LEARNED

This section provides a review of the current business operations in the UAE national ID card programme and presents some of the identified process improvement areas. The proposed changes are seen as key factors to increase public acceptance and project success chances.

7.1 Registration Process



It was a concern from the early days of the project that the enrolment process involved many activities that required the project members to radically review and improve. The review exercise revealed that the average enrolment process could be completed in less than 5 minutes rather than the current 17 minutes without any big impact on the project objectives if only two enrolment activities were re-engineered: (1) the registration form and (2) the biometrics captured.

7.1.1 Registration Form

The registration form throughout the project life cycle went through many iterations in an attempt to reduce the amount of data needed for the enrolment. It started with an 8-page document, and was reduced to 6, and then to 4 pages. The form which was a pre-requisite to initiate the registration process was viewed as:

- too lengthy
- required considerable time to fill

- some information was not readily available
- was sometimes filled incorrectly
- large number of resident applicants are illiterate
- considered to be the enrolment's bottle neck

The reason for its design and the large number of data required was to achieve the objective of producing statistics about the population of the country. The review process indicated that there was a vision mix-up between the two requirements of building a statistical database and the other objective of enrolling the whole population of the UAE and producing ID cards for them. This was a clear confusion among many members and stakeholders of the project to aim to achieve these two objectives at the same time.

The recommendation from the review exercise was that the implementation of the project must take place in three stages as depicted in Figure 7. In the first stage, the project must attempt to (a) enrol the population for the new ID card with a minimal set of data as depicted in Figure 8 below. As only primary identification data will be required for first time enrolees, the application form was suggested to be eliminated and rather make use of the existing electronic link with the Ministry of Interior's database to obtain and verify data.

Then stage two and three must run in parallel. In stage two, efforts must be directed towards promoting (and enforcing) the presentation of the new ID card for identity verification and as a pre-requisite to most often visited government services by the population.

Those organisations then need to maintain the new ID numbers in their databases, which should be used when moving to stage three of the strategy which requires the national ID database to interface and integrate with such databases. Provided the link is in place, a proper

data warehouse can be built that is up-to-date and more reliable for generating statistical reporting purposes as it will obtain information from primary and trusted sources.

Names	Name (Segmented)	Name
	Gender, DoB, Marital St.	Gender, DoB, Martial St.
Passport	Nationality	Nationality
	Passport No, Place of issue, Issue and Expiry dates	Passport No, Place of issue, Issue and Expiry dates
	Unified No	Unified No, Sponsor Name
	Family ID, Book No	Residency File No, Issue and Expiry dates
Address	Emirate	Emirate
	City	City
	Mobile phone	Mobile phone

Fig. 8: primary identification data captured for first enrolment

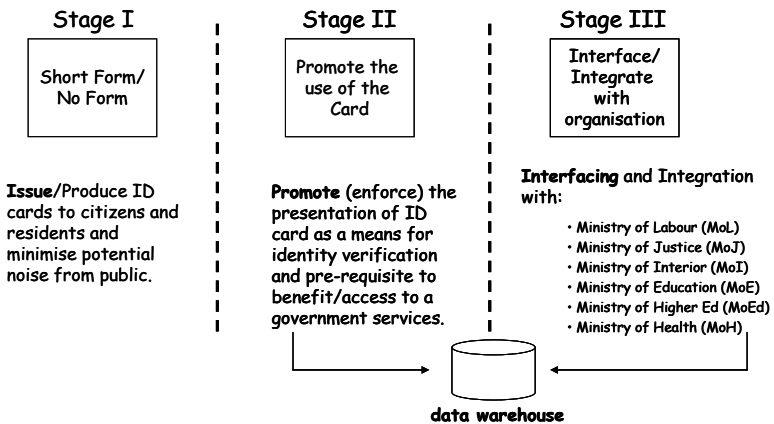


Fig. 7: project implementation stages

7.1.2 *Biometrics captured*

The enrolment process required the capturing of all fingerprints (i.e., slaps, rolled prints, palm, writer's palms) a process taking around 6 to 10 minutes to complete.

On the system level, only rolled fingerprints were used for identification, where slaps and palms were stored for criminal search by the Ministry of Interior.

The review recommendation suggested to only capture the flat prints and use smaller acquisition devices (just the slaps and the two thumbs), and to capture other fingerprints at a later stage only if needed.

It was recommended that a second biometric must be introduced to complement the fingerprint biometric and enhance the FTE⁶, FAR⁷, FRR⁸ rates. The second biometric was recommended to be more of a real time application that could be used in mass population areas such as airports. Both biometrics were seen as easy to operate and will cut processing time to less than 2 minutes.

7.1.3 *Biometrics quality*

Shortly after the introduction of the pilot phase of the programme it became abundantly clear that the quality of fingerprints taken by operators will have a determining effect on the classification,

⁶ Failure to Enroll: when the system fails to enroll an applicant largely due the poor quality of the biometrics being captured.

⁷ False Acceptance Rate(also referred to as False Match Rate): is an incorrect identification or failure to reject an imposter (Imposter: is a person trying to submit a biometric in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrollee).

⁸ False Reject Rate (also referred to as False Non-Match Rate): is the failure to identify or verify a person.

identification, and authentication of applicants. Apart from possible shortcoming in the operating system itself the percentages of failure to enroll (FTE), false rejection rate (FRR), and false acceptance rate (FAR) may increase dramatically if operators are not properly trained in the art of taking fingerprints.

Failure to enroll due to operator failure may for example result in false demographic information. The lesson learnt therefore was that a very high premise should be placed on a comprehensive operator training programme. It was also realised that results of biometric hits should be closely monitored to determine the performance of the system in terms of the quality of these results.

A clear indication of unacceptable system performance would be if a too long hit list is required to identity hits or if the real hit constantly appears very low on this long hit list. While it can be argued that the hit list can be shortened by tuning the applicable threshold, it will then mean that real hits that appear low on the hit list will not be identified if the systems performance is not improved.

There is obviously a very close relationship between the quality of fingerprints taken and the performance of the system. It was however realised that the introduction of a second biometric will complement the fingerprint biometric and will basically balance any shortcoming.

The re-engineering of the above two enrolment processes provided a saving in the office space, equipment and staff required for enrolment as the original enrolment process was divided into three stages as depicted in Figure 9. The reason for the three office design was mainly to segregate duties, and manage the daily in-flow of applicants and shorten the waiting time.

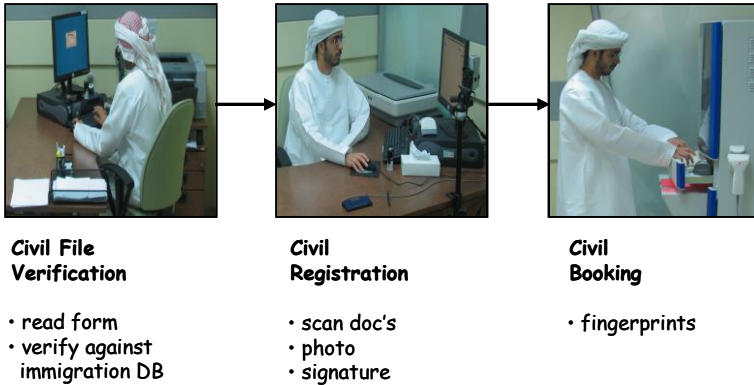
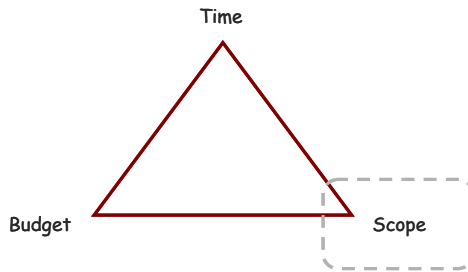


Fig. 9: registration procedures

It was therefore recommended to enhance the system to perform the enrolment process through a single workstation. This was viewed to radically support the enrolment strategy, in which smaller devices can be used to carry out the registration, and enhance the portability of the system for wider deployment in areas such as setting up permanent and temporary registration offices in traffic departments, immigration, municipalities, schools, companies with a large number of staff members, etc.

7.2 Scope Creep



Scope creep is a term used to describe the process by which users discover and introduce new requirements that are not part of the initial planning and scope of the project. As widely quoted in the literature, many doubt a limited and specified scope for national ID programmes, as the nature and high cost of such projects are likely to yield and encourage the expansion of its functions [5],[6],[7],[8].

The project management literature also indicates that coping with changes and changing priorities are the most important single problem facing the project management function [9],[10],[11]. Indeed, changing targets all the time, would obviously take any project nowhere.

In the UAE ID programme, project performance was monitored and measured regularly to identify variances from the project plan. It was supported with a formal and well-defined process to control and manage the changes being requested to the project scope and objectives during the project lifecycle. See for example Figure 10 that depicts an example of one of the change control policies.

Despite all the efforts put into managing and controlling change, the changes introduced and processed dragged the project schedule far

away from the original target date. It was common during the different implementation stages of the programme to change the scope to either add new or change agreed functions, which obviously had severe impact on the implementation project plan and budget. Examples of such changes included the shifting from centralised card printing to decentralised, upgrading the card technology, changing card design and displayed data, upgrading database technology, etc.

	Type of Change			
	Technical nature (No financial impact)	Technical nature (With financial impact)	Contract Scope (No financial impact)	Contract scope (Financial Impact)
Steering Committee	Accept or Reject	Analyse and Recommend	Accept or Reject	Analyse and Recommend
Change Control Board		Reject or Recommend to Project Sponsor		Reject or Recommend to Project Sponsor
Project Sponsor		Approve or Reject		Approve or Reject

Fig. 10: change control authorities

Another example of such changes to project scope was related to the perception of the multi-purpose functionality. Several attempts were made from certain key stakeholders of the project to expand the card applications during the execution phase that had severe impact on the project progress.

It took some time for them to realise the importance of limiting the purpose of the card as an identity document in the first phase of the project and that efforts must rather be concentrated on the enrolment of the population and the issuance of the new ID card.

Indeed, a multi-purpose card was one of the objectives of the project, but not in the way it was comprehended. The Multi-purpose term stated in the objectives was used to explain that the card can replace other identity documents when it comes to the verification of identities. Since the card was obligatory to the total population of the UAE, the provision was that the new ID card can replace such cards if the other entities use the new ID number in their databases as a primary number to retrieve individual records.

The management of scope in the UAE ID card was clearly one of the biggest challenges that required the project core team to spend a lot of time and effort to clarify the feasibility of such actions to the upper management. Finding the right communication approach was key to managing scope creep.

7.3 Too Much Security

It was during this evaluation phase of the project (discussed next) as well as the experience gained after the introduction of the pilot phase that it was realised that far too much emphasis were placed on security issues which rendered the operating system a closed system which required costly and extreme efforts to affect even simple changes. Needless to say that required changes to the system became a very cumbersome task with unacceptable cost and time frames associated with each change.

This resulted in a strained relationship with the vendor as these delays were perceived by the client as to reflecting on a possible inability or lack of co-operation from the vendor. It was later on realised that the system security, security during the enrolment process and security around information included in the card itself should not be of such

extent that it places a stranglehold on the flexibility to change and the user friendliness of the system.

While security features built into the card body could be as inclusive as is required, the personal information of the applicant stored in the security portion of the card should be protected but should be freely available to authorised users.

7.4 Evaluation Framework

Since the UAE national ID system was provisioned to become the most critical system in the country as the main central hub for population identity cross checking and service eligibility (i.e., online with 24/7 availability requirement), it was important that the overall system goes under a thorough quality evaluation.

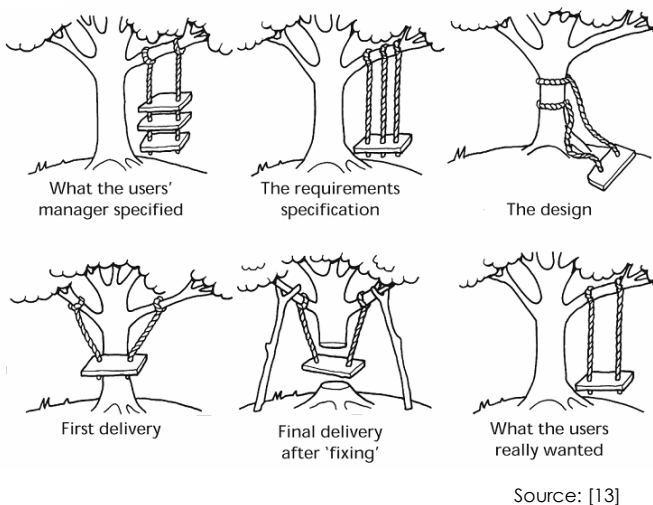


Fig. 11: An example of varying interpretations of user requirements

As widely quoted in literature that one of the principle causes of information system failure is when the designed system fails to capture the business requirements or improve the organisational performance (see for example: [12],[13],[14],[15],[16]. Figure 11 shows an example of how a user's requirements might be interpreted during the lifecycle of a project which is not really far from being true in many of the IS projects implemented around the world.

During the UAE programme implementation there was no clear communication of the development standard followed by the vendor, which created confusion among the project team members when it came to individual deliverable acceptance, as well as the final acceptance of the system.

In general, the project team, with the workload and responsibilities put on them, seemed to be overloaded and to have scattered visions of how things should be done and achieved. Everybody wanted the project to be concluded as quickly as possible and was seemingly very impressed with the work produced by the vendor.

At the very late stages of the project, the core project team employed ISO 9126 standard for the purposes of software quality and the overall system architecture evaluation (see also Figure 12).

The evaluation study contributed significantly in identifying many of the system deficiencies that required the vendor to address prior to the final acceptance and handover of the system. Besides, the use of quality framework provided a very useful and supportive methodological approach for going about software quality assessment. It acted as a comprehensive analytical tool and provided a more thorough view of the system's strengths and weaknesses.

It addressed a wide range of quality characteristics of the software products and processes enabling better description of software quality aspects and its importance. Arguably, if used as a guide in an early stage of the project it could have provided a sound basis for informed and rational decision making which could have contributed significantly to the delivery of a system which is properly addressing user requirements.

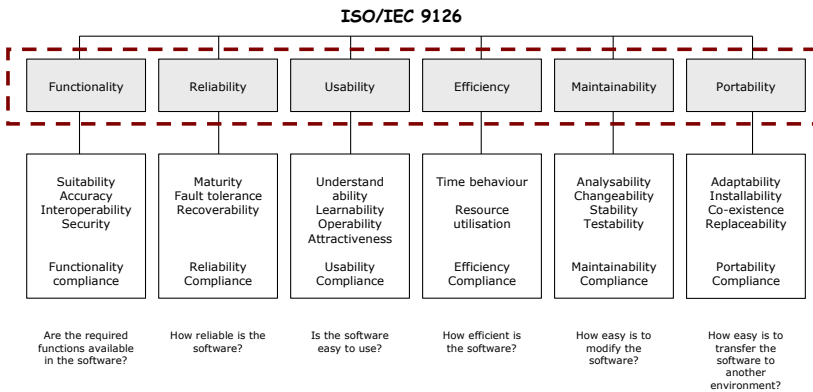


Fig. 12: ISO-IEC 9126 quality model

8. CONCLUSION

Not much has been written about National ID systems implementation from a practitioners' point of view. The literature was found to be full of articles from the private industry discussing advanced technologies and what can be achieved through them. This article adds to the current body of knowledge in the field, and is believed to assist in widening the thinking circle of those who are wearing similar hats.

As indicated in this paper, much could indeed be achieved through national ID programmes. However, agreed vision and thereafter proper planning is essential to succeed with such projects. It took quite some time before the team started to agree on the fact that the first phase of the project should focus on the enrolment of the whole population and the issuance of the new ID card.

National ID programmes and because of their nature, are perceived to invest quite significantly in technology upgrade and R&D departments for future developments in areas related to identity management and to keep up with the ID industry developments and standards. It was learned that new functionalities and upgrades must be thoroughly studied and researched to eliminate unnecessary changes during the execution phase.

As it is becoming the trend, such programmes need to put much effort in promoting e-identity and e-verification services using the new ID card. It would be interesting to measure the impact of national ID programmes on the overall government economy, as it would obviously promote electronic transactions and would also encourage government organisations to streamline their operations and make use of the secure (e)verification infrastructure that it will provide.

7.5 Further Research

Further research and practical work in this field may further contribute to the body of knowledge. Areas in which further research may yield valuable insights and better understanding are:

- 7.5.1 similar studies of national ID implementations that could show the appropriateness of the items presented in the lessons

learned, and the degree to which it can support similar initiatives,

- 7.5.2 an investigation of the suitability of quality models in national ID programmes and projects of such nature and its impact on the project success rate.

ACKNOWLEDGEMENT

The author would like to thank Mr. Gawie von Wielligh for his review feedback that improved the overall structure and quality of this paper.

REFERENCES

- [1] [L. Goldman, "Chips with everything," *Occupational Health*, vol.56, no. 4, pp.12-3, April 2004.
- [2] H. Knight, "Anti-Fraud: The road to a national ID card is paved with pitfalls," *The Engineer*, London, p. 25, December 2003.
- [3] W. Matthews, "ID card plan assailed," *Federal Computer Week*, vol. 16, no. 4, p.16, February 2002.
- H. Michael, "Identity cards: Why bother," *The Economist*, London, vol. 335, no. 7916, p. 50, May 1995.
- [4] R.A. Clarke, "The Resistible Rise of the National Personal Data System," *Software Law Journal*, vol. 5, no.1, pp.33-36, 1992.
- [5] R.A. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues" [Online]. Australia, The Australian National University, 1994 Available: <http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html#PPI> [Accessed 15 09 2006].
- [6] J. Fontana, "A national Identity Card for Canada" [Online]. Canada, House of Commons, 2003. Available from: <http://www.parl.gc.ca> [Accessed 02 08 2006].
- [7] A.M. Froomkin, "The Uneasy Case for National ID Cards as a Means to Enhance Privacy" [Online]. USA, University of Miami School of Law, 2002. Available: <http://www.la-w.fm> [Accessed 02 10 2006].
- [8] G.R. Heerkens, "Project management: 24 lessons to help you master any project". New York: McGraw-Hill, 2005.

- [9] J.R. Meredith, & S.J. Mantel, "Project management: a managerial approach," 2nd ed. New York, NY: John Wiley & Sons, Inc, 2003.
- [10] R.G. Reiss & F.N. Spon, "Project Management Demystified: Tools and Techniques," New York: McGraw Hill, 1995.
- [11] D.E. Avison & A.T. Wood-Harper, "MultiView - an exploration in information systems development." USA: McGraw Hill, 1990.
- [12] P. Bocij, D. Chaffey, A. Greasley, & S. Hickie, "Business Information Systems: Technology, Development and Management for the e-business," 2nd ed. New York: Prentice Hall, 2003.
- [13] W. Crain, "Theories of Development: Concepts and applications," 3rd ed. New Jersey: Prentice Hall International, 1992.
- [14] G. Curtis, "Business Information Systems: Analysis, Design, and Practice," 3rd edition, USA: Addison-Wesley, 1998.
- [15] M. Harry, "Information Systems in Business," 2nd ed. Great Britain: British Library Cataloguing in Publication Data, 1997.

Using **Quality Models** to Evaluate Large IT Systems ⁹

Ali M. Al-Khouri

COPYRIGHT © 2007 WASET.ORG

ABSTRACT: This article presents findings from the evaluation study carried out to review the UAE national ID card software. The article consults the relevant literature to explain many of the concepts and frameworks explained herein. The findings of the evaluation work that was primarily based on the ISO 9126 standard for system quality measurement highlighted many practical areas that if taken into account is argued to more likely increase the success chances of similar system implementation projects

Key words: *National ID system, Software Quality, ISO 9126.*

⁹ Al-Khouri, A.M. (2007) "**Using Quality Models to Evaluate National ID systems: the Case of the UAE,**" *International Journal Of Social Sciences*, Vol. 1, No. 2, pp.117 -130.

* The content of this article was partially presented at an international conference: Al-Khouri, A.M. (2006) "**Using Quality Models to Evaluate Large IT Projects,**" *Proceedings of World Academy of Science, Engineering and Technology*, Vienna, Austria, Vol. 21.

1. INTRODUCTION

THE United Arab Emirates (UAE) have recently initiated a national ID scheme that encompasses very modern and sophisticated technologies. The goals and objectives of the UAE national ID card programme go far beyond introducing a new ID card document and homeland security [1].

To increase its success, the government is pushing for many innovative applications to explore 'what can be done with the card'. Examples of such possible applications of the card ranges from using it as a physical identity document to prove identity, to linking it to wide range of government services, with the vision of replacing all existing identity documents (e.g., driving license, labour card, health card, etc.) with this new initiative.

From such perspectives, it becomes critical that such systems maintain a high level of quality. Quality models can play a good role as useful tools for quality requirements engineering as well as for quality evaluation, since they define how quality can be measured and specified [2]. In fact, the literature reveals that the use of quality frameworks and models may well contribute to project success, as it enables the early detection and addressing of risks and issues of concern at an early stage of the project (see for example [3],[4],[5]).

This article attempts to provide a short evaluation of the population register software (referred to in this article as PRIDC – population register and ID card) implemented part of the national ID card project in the UAE to pinpoint areas of possible improvements.

The article is structured as follows. The first section provides brief background information about the concept of software quality and

measurement standards, with focus on ISO 9126 framework. The next section presents the methods employed to obtain data based on which the system was evaluated. The next few sections provide an overview of the PRIDC system, its components, its development lifecycle approach, results obtained from the previous tests, and mapping these latter set of data to ISO 9126 quality attributes. The paper is then concluded with some reflections on the areas that need to be considered when pursuing similar evaluation studies with a focus on national ID systems.

2. SOFTWARE QUALITY

It is becoming a common trend for IT projects to fail. The rate of failure in government projects is far higher than those in the private industry. One of the main causes for such failures was widely quoted in the literature to be related to poor user requirements resulting in a system that does not deliver what was expected from it (see also the statistics presented in Figure 1 from the recent Standish Group study).

Standish Study Results:	
51%	of project failed
31%	were partially successful
Failure causes:	
13.1%	In complete requirements
12.4%	Lack of user involvement
10.6%	Inadequate resources
9.9%	Unrealistic user expectations
9.3%	Lack of management support
8.7 %	Requirements keep changing
8.1%	Inadequate planning
7.5 %	System no longer needed

Fig. 1: Standish group study results

The CHAOS survey of 8000+ projects found that of the eight main reasons given for project failures, five are requirements related. Getting

the requirements right is probably the single most important thing that can be done to achieve customer satisfaction. Figure 2 depicts further reasons for such failures [6]. Many of these failures are argued to could have been prevented with requirements verification and the adoption of quality assurance frameworks [4],[7].

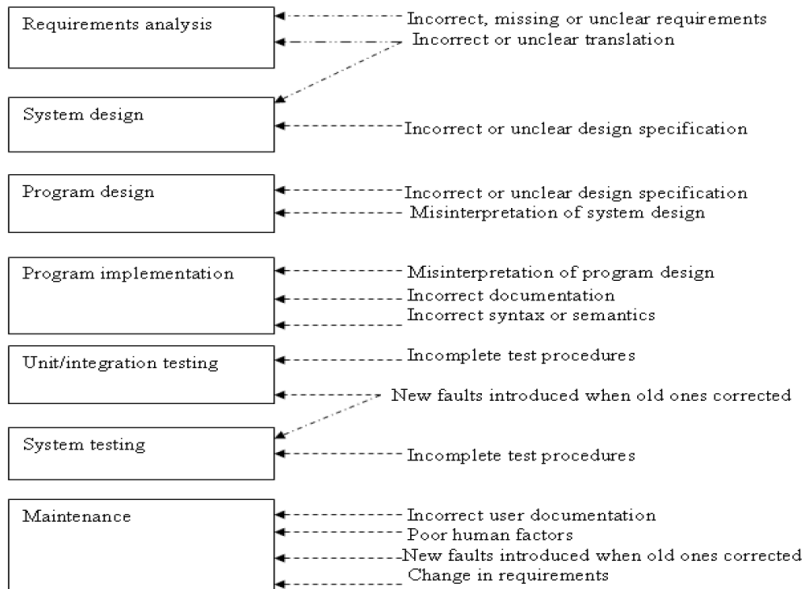


Fig. 2: causes of faults during development

Source: Adopted from Pfleeger (2001)

In general terms, there are three different approaches to system quality assurance:

1. Product Certification

An independent party (or a QA company) conduct a limited exercise in verification, validation and / or test of the software components.

2. *Process Audit:*

An independent party conduct and assessment of the development process used to design, build and deliver the software component.

3. *User Satisfaction:*

Analysis of the actual behaviour of the software.

Since the objective of the evaluation study in this article here is to judge whether the given implemented system has met the requirement of product quality, the third category approach was defined as the boundaries for the evaluation taken place in this study.

2.1 Quality Measurement Standards

Software quality assessment is attracting great attention as the global drive for systemic quality assurance continues to gather momentum e.g., pressures of consolidations, mergers, and downsizing, emergence of new technologies [8].

Of the very initial works conducted in the field of software quality assessment was done by B. Boehm and associates at TRW [9] and incorporated by McCall and others in the Rome Air Development Center (RADC) report [10].

The quality models at the time focused on the final product and on the identification of the key attributes of quality from the user's point of view. The assessment framework was later improved; consisting of quality attributes related to quality factors, which were decomposed into particular quality criteria and lead to quality measures (see Figure 3).

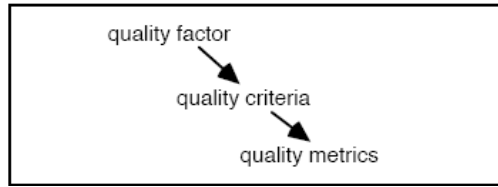


Fig. 3: Boehm quality model

Attempted standardisation work over the intervening years resulted in the Software Product Evaluation Standard, ISO-9126 (ISO/IEC, 1991). This model was fairly closely patterned after the original Boehm structure, with a six primary quality attributes that were subdivided into 27 sub-characteristics as illustrated in Figure 4.

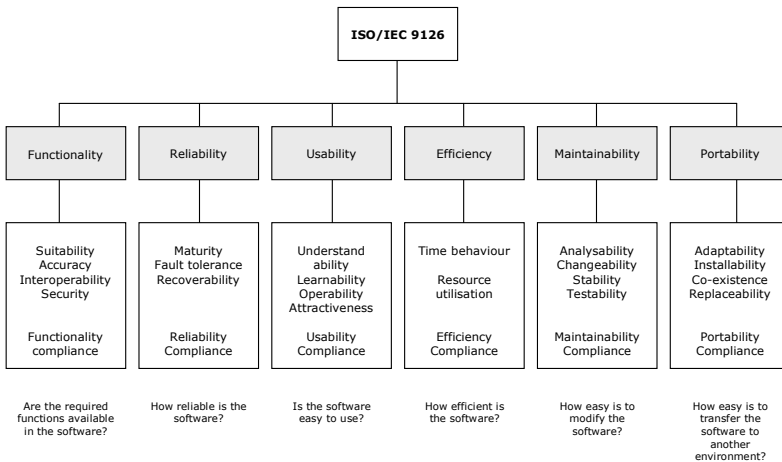


Fig. 4: ISO/IEC 9126 standards characteristics

However, the standard was criticised to provide very general quality models and guidelines, and that they are very difficult to apply to specific domains such as components and CBSD (see for example:

[11],[12]. However, this is believed by others to be in fact one of its strengths as it is more adaptable and can be used across many systems [13],[14]. To solve this problem ISO/IEC 9126 has been revised to include a new quality model which distinguishes between three different approaches to product quality:

- (1) External Quality metrics – ISO TR 9126 -1: a result of the combined behaviour of the software and the computer system and can be used to validate the internal quality of the software;
 - (2) Internal Quality metrics – ISO TR 9126 – 3: a quantitative scale and measurement method, which can be used for measuring an attribute or characteristic of a software product;
 - (3) Quality in use metrics – ISO TR 9126 – 4: is the effectiveness, productivity and satisfaction of the user when carrying out representative tasks in a realistic working environment. It can be used to measure the degree of excellence, and can be used to validate the extent to which the software meets user needs.
- Figure 5 depicts the relationship between these approaches.

In brief, internal metrics measure the software itself, external metrics measure the behaviour of the computer-based system that includes the software, and quality in use metrics measure the effects of using the software in a specific context of use.

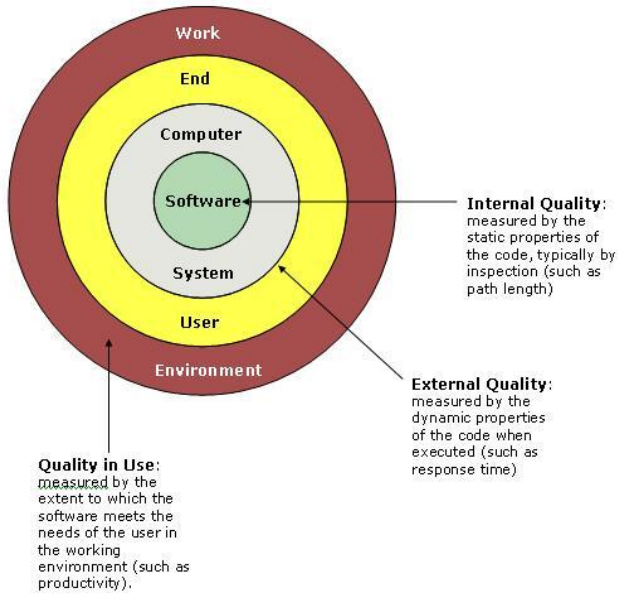


Fig. 5: relationship between internal quality, external quality and quality in use

Appropriate internal attributes of the software are prerequisites for achieving the required external behaviour, whereas external behaviour is a prerequisite for achieving quality in use (see also Figure 6).

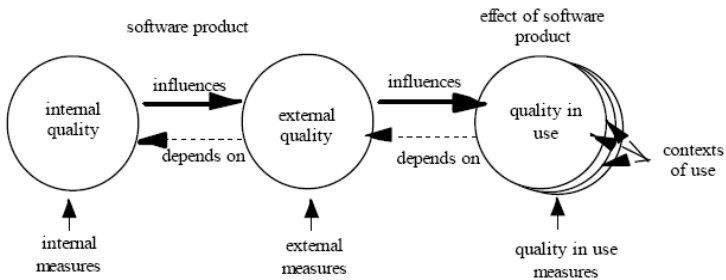


Fig.6: approaches to software product quality

It is also worth to mention that a new project was launched called SQuaRE - Software Product Quality Requirements and Evaluation (ISO/IEC 25000, 2005) - to replace the above but follow the same general concepts of 9126 standard (see also Figure 7).

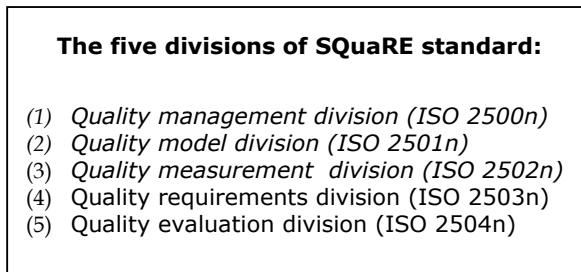


Fig.7: SQuaRE standard

Nonetheless, research and practical work shows that the assessment of the quality of a software component is in general a very broad and ambitious goal [11].

Recent research also shows that these characteristics and sub-characteristics covers a wide spectrum of system features and represent a detailed model for evaluating any software system as Abran et al. [15] explain:

"...ISO 9126 series of standards even though it is not exhaustive, this series constitutes the most extensive software quality model developed to date. The approach of its quality model... is to represent quality as a whole set of characteristics... This ISO standard includes the user's view and introduces the concept of quality in use."

3. METHODOLOGY

"If you chase two rabbits, both will escape."

Chinese Proverb

ISO 9126 quality characteristics and sub-characteristics were used to evaluate the national ID system. In this investigation several evaluation methods were employed. Following were the prime sources of information for the evaluation study:

1. information gathered from the test sessions took place during the acceptance of the project deliverables;
2. observation of the system environment (both at the central operational and registration centres);
3. by means of recording the author's own experience as the Director of the Central Operations sector, and head of the technical committee overseeing the implementation of the programme.

In general, the evaluation was qualitative in nature. In carrying out the evaluation and recording the findings, the PRIDC system went through two types of testing; functional and technical.

3.1 Functional Testing

This is an application level testing from business and operational perspective. It is conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. Often called black box testing, this type of tests is generally performed by QA

analysts who are concerned about the predictability of the end-user experience. During the deliverables acceptance, the national ID system was tested with black box testing procedures (that focuses on testing functional requirements and does not explicitly use knowledge of the internal structure) as per the test plan designed by the solution provider. No change was allowed by the vendor to the test plan as they wanted to narrow down the scope of testing, and limit it to the test cases developed by them.

3.2 Technical Testing

This is the system level testing. It tests the systems, which are supporting or enabling to run the Functional Applications. With general perception of QA, the COTS are not seen to be required to test but they need to be audited for the configuration and deployment set-up. Generally, white-box testing (also called as glass, structural, open box or clear box testing) was considered here by the technical team to test the design of the system that should allow a peek inside the 'box', as this approach focuses specifically on using internal knowledge of the software to guide the selection of test data.

White-box testing requires the source code to be produced before the tests can be planned and is much more laborious in the determination of suitable input data and the determination if the software is or is not correct. It is worth mentioning that a failure of a white box test may result in a change which requires all black-box testing to be repeated and the re-determination of the white box paths. For this obvious reason there was always negligence from the vendor to initiate a white-box testing. It must also be heeded that neither black nor white box testing can guarantee that the complete specifications have implemented and all parts of the implementation have been tested.

To fully test a software product, both black and white box testing are required. While black-box testing was limited by the test plan documents provided by the vendor, the white box testing was not possible to perform since the source code was still not handed-over to the client at the time of writing this study. However, all the architectural component of the national ID Sub-systems which were selected and assembled from the COTS were assessed and audited to their configuration and deployment set up. Having addressed the evaluation methods, the following sections describe the details of the work carried out in this study.

5. PRIDC SYSTEM AS A COMPONENT-BASED SYSTEM

"For more than a decade good software development practice has been based on a "divide and conquer" approach to software design and implementation. Whether they are called "modules", "packages", "units", or "computer software configuration items", the approach has been to decompose a software system into manageable components based on maximizing cohesion within a component and minimizing coupling among components."

(Brown and Wallnau, 1996, p.414)

5.1 What is a component-based software (CBD)?

Component-based software development (CBD) is an emerging discipline that promises to take software engineering into a new era [16]. Building on the achievements of object-oriented software construction, it aims to deliver software engineering from a cottage industry into an industrial age for Information Technology, wherein software can be assembled from components, in the manner that hardware systems are currently constructed from kits of parts (ibid).

Component-based software development (CBSD) shifts the development emphasis from programming software to composing software systems as it embodies the 'buy, don't build' philosophy espoused by [17]. See also Figure 8. The concept is also referred to in the current literature as component-based software engineering (CBSE) [18],[19]. It principally focuses on building large software systems by integrating different software components and enhancing the overall flexibility and maintainability of the systems.

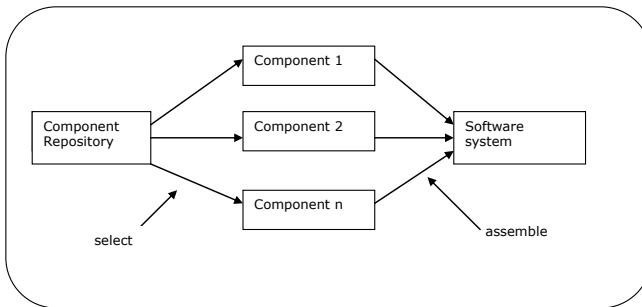


Fig. .8: component-based software development.

If implemented appropriately, the approach is argued to have the potential to reduce software development costs, assemble systems rapidly, and reduce the spiraling maintenance burden associated with the support and upgrade of large systems [20].

[21] define component-based software development as an approach "based on the idea to develop software systems by selecting appropriate off-the-self components and then to assemble them with a well-defined software architecture." They state that a component has three main features:

1. is an independent and replaceable part of a system that fulfils a clear functions,
2. works in the context of well-defined architecture,
3. communicates with other components by its interface.

According to [22] two main advances are raising the profile of software components as the basic building blocks of software - see also: [16],[23],[24],[25],[26],[27]:

- (1) the object-oriented development approach which is based on the development of an application system through the extension of existing libraries of self-contained operating units, and
- (2) the economic reality that large-scale software development must take greater advantage of existing commercial software, reducing the amount of new code that is required for each application.

Component-based development approach introduces fundamental changes in the way systems are acquired, integrated, deployed and evolved. Unlike the classic waterfall approach to software development, component-based systems are designed by examining existing components to see how they meet the system requirements, followed by an iterative process of refining requirements to integrate with the existing components to provide the necessary functionality [22].

5.2 Component-based software development lifecycle

The component life cycle is similar to the life cycle of typical applications, except in implementation and acquisition phases where the two life cycles differ. The life cycle of component-based software

systems can be summarised as follows:

1. *Requirement analysis*: a process of defining and understanding the activities that the information system is meant to support;
2. *Software architecture design*: a process of developing detailed descriptions for the information system;
3. *Component identification and customisation (implementation)*: a process of formalising the design in an executable way by acquiring complete applications or components through purchase, outsourcing, inhouse development, component-leasing etc;
4. *System integration*: a process of adjusting the system to fit the existing information system architecture. This can include tasks such as adjusting components and applications to their specific software surroundings,
5. *System testing*: a process of identifying and eliminating nondesirable effects and errors and to verify the information system. This can include both user-acceptance- and application integration-tests,
6. *Software maintenance*: a process of keeping the integrated information system up and running. This can include tasks such as upgrading and replacing applications and components in the information system. It also includes performing consecutive revisions of the integrated information system.

Having shortly highlighted some background information about the concept of component-based development and lifecycle, the next

section takes a snapshot of the PRIDC system and maps it to component-based software.

5.3 PRIDC System development life cycle

Broadly speaking, the development of the PRIDC system in general can be described to have incorporated the following two approaches:

1. the development of a uniquely tailored information system (population register) to enable the registration of population into the system in accordance to the pre-defined business requirements, and
2. the integration of several application/hardware package to achieve the desired functionality requirements e.g., biometrics, PKI, smart cards.

For the purpose of benchmarking PRIDC system development lifecycle, a framework proposed by [28] for quality assurance of component-based software development paradigm has been adopted in this study. The framework contains eight phases relating to components and systems that provide better control over the quality of software development activities and processes:

1. *Component requirement analysis.*
2. *Component development.*
3. *Component certification.*
4. *Component customisation.*
5. *System architecture design.*
6. *System integration.*
7. *System testing.*
8. *System maintenance.*

The details of this benchmarking are presented in the following section.

5.4 A comparison of PRIDC system with ISO standard.

PRIDC systems Lifecycle is currently based on project implementation phases. The Project implementation is executing in Lot-wise as framed in the contract. A comparative study of PRIDC Systems Life Cycle with ISO 12207 standard can be presented as below:

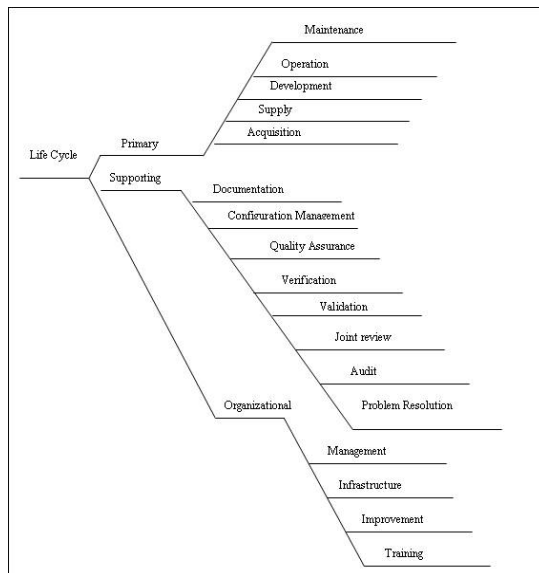


Fig. 9 ISO 12207 standard¹⁰

¹⁰ ISO Standard for system implementation.

In 1987 ISO and IEC(International Electrotechnical Commission) established a joint Technical Committee (JCT1) on Information Technology. In June 1989, the JCT1 initiated the development of ISO/IEC 12207, on software life cycle processes to fill a critical need. The ISO was published August 1,1995.

TABLE 2: Comparison of PRIDC System with ISO 12207 Standard

No	ISO 12207	PRIDC System Life cycle
1	Primary life cycle processes	
1.1	Acquisition process	All lots of Category A.
1.2	Supply process	All lots of Category D.
1.3	Development process	All lot of Category B.
1.3.1	Process implementation	All lots of Category C.
1.3.2	System requirement analysis	All lots of Category A.
1.3.3	System architectural design	All lots of Category B.
1.3.4	Software requirement analysis	The solution provider internal process.
1.3.5	Software architectural design	The solution provider internal process.
1.3.6	Software detail design	The solution provider internal process.
1.3.7	Software coding and testing	The solution provider internal process. EIDA had done few of such testing.
1.3.8	Software integration	The solution provider internal process.
1.3.9	Software Qualification testing	The solution provider internal process.
1.3.10	System integration	The solution provider internal process.
1.3.11	Software qualification testing	The solution provider internal process.
1.3.12	Software installation	The solution provider internal process.
1.3.13	Software acceptance Support	Lot 12 and Lot3 testing
4	Operation Process	Need to define.
5	Maintenance Process	Need to define.
6	Supporting life cycle processes	
6.1	Documentation process	Done as a part Project deliverable.
6.2	Configuration management process	Done as a part Project deliverable.
6.3	Quality assurance process	Not done as a part of Project contract.
6.4	Verification process	Can be considered, Lot 3 system compliance test.
6.5	Validation process	Can be considered, Lot 12 system compliance test.
6.6	Joint review process	Can be consider – program management meeting.
6.7	Audit process	Need to perform.
6.8	Problem resolution process	Need to perform.
7	Organisational life cycle processes	
7.1	Management process	EIDA needs to perform.
7.2	Infrastructure process	EIDA needs to perform.
7.3	Improvement process	EIDA needs to perform.
7.4	Training process	Done as a part of Lot 3 – Admin Training.

5.5 ISO 9126 and PRIDC mapping

Following is a summary of the evaluation results as per the ISO 9126 quality attributes.

Functionality	the degree of existence of a set of functions that satisfy stakeholder/business implied needs and their properties. Overall, in terms of number of changes requested on the system, as illustrated in Table 1.10, there were more than 213 modification items in the form of 53 change requests (23 major changes) passed to the vendor to implement. This was the first functional test results with the first version of the PRIDC system. This is a significant amount of modifications and it clearly implies that there was a big gap during the system requirement analysis and capturing phase.	
Suitability	Can software perform the tasks required? The degree of presence of a set of functions for specified tasks (fitness for purpose)	checked against specifications & feedback from registration centres.
Accuracy	is the result as expected? The degree of provision of right or agreed results or effects	checked against specifications. Test cases were developed by the test team of the vendor. Besides, there were many other cases that were not tested for accuracy but encountered later after the release of the software.
Interoper-ability	Can the system interact with another system? the degree to which the software is able to interact with specified systems (i.e. physical devices)	checked against specifications. However, the system was designed to be a closed architecture, as interoperability with future systems was seen to be of big concern.
Security	Does the software prevent unauthorised access? a set of regulations for maintaining a certain level of security; degree to which the software is able to prevent unauthorised access, whether accidental or deliberative, to programs and data (i.e. login functions, encryption of personal data etc).	checked against specifications and in accordance with the Information Security Policy The PRIDC system is a critical system for the country, thus important security features were incorporated into the system to ensure high confidentiality, integrity and authenticity of the data. The security is built around the following main rules: • Strong authentication of the operators (each end-user will use both password and fingerprint to logon onto the system),

		<ul style="list-style-type: none"> • Network security using Virtual Private Network (VPN) + Demilitarised Zone (DMZ) and Secure Socket Layer (SSL) over Hyper Text Transfer Protocol (HTTP), • Strong physical protection of the Central, Disaster Recovery and Service Points Local Area Networks (LAN) <p>The security scheme was implemented at 4 levels:</p> <ol style="list-style-type: none"> 1) Application level, 2) Network level, 3) System level, 4) Physical level. <p>The security features carried out at each of the above levels included a wide range of advanced international security standards and measures:</p> <p>X509 V3 certificates, X500 directory, LDAP V2 and V3, DES, 3xDES, RC2, RC4, AES ciphering algorithms (used by CISCO VPN), RSA (PKCS#1) signature algorithms, MD2, MD5, SHA1, Diffie-Hellman and RSA key exchange algorithms, pkcs#12, pkcs#7, pkcs#10, IPsec, IKE, TOO MUCH SECURITY!</p>
Compliance	the degree to which the software adheres to application-related standards or conventions or regulations in laws and similar prescriptions	checked against specifications
Reliability	the capability of the software to maintain its level of performance under stated conditions for a stated period of time (This is assessed based on the number of failures encountered per release)	
Maturity	Have most of the faults in the software been eliminated over time? the frequency of failure by faults in the software	If looked at the number of sub versions released of the PRIDC system (i.e., ver 1.5, ver 1.6 and ver3.0) as depicted in Table 1.7, the evolution of these versions was unplanned (i.e., previously not specified) versions of the system, which signifies that the immaturity of the system in terms of business requirements and needs. At the time of carrying out this evaluation, the software was still seen to require further modifications before the system can be finally accepted

Fault- tolerance	is the software capable of handling errors? the ability to maintain a specified level of performance in cases of software faults or of infringement of its specified interface; is the property that enables a system to continue operating properly in the event of the failure of some of its components.	Although the system had a centralised architecture, its architecture allowed the different systems to continue operation in the cases of failure of the central system through replication and redundant systems.
Recoverability	Can the software resume working and restore lost data after failure? the capability of software to re-establish its level of performance and recover the data directly affected in case of a failure	Databases were continuously replicated on the Disaster Recovery site. The system insured that no more than one hour of work would be lost following a database crash/failure. However, in case of a major disaster that would lead to the loss of the operational capacity of the main data centre, the PRIDC system was planned to be restarted within 24 hours.
Usability	the effort needed for the use by a stated or implied set of users.	
Understand-ability	does the user comprehend how to use the system easily? evaluates the attributes of software that bear on the users' effort for recognizing the underlain concept of the software. This effort could be decreased by the existence of demonstrations	Usability testing uncovered many difficulties, such as operators having difficulty understanding system interface, business logic and processes. With the lack of on-line help function, the GUI interface of the system did not seem to follow any clear standard, as operators started guessing what different buttons may mean. For example, two registration centre's operators deleted the files of all registered applicants on one day when they pressed the button 'Abort' to cancel an operation, where the system was performing the action of 'Delete' with the 'Abort' button. In general, Interface functions (e.g., menus, controls) were no easy to understand.

Learnability	can the user learn to use the system easily? evaluates the attributes of software that bear on the users' the user's effort for learning how to use the software	User documentation and help were not complete at the time of carrying out this evaluation. The system was not easy to learn as users had to repeat the training sessions many times as the cases of data entry errors was raising when post-audit procedures for data quality check were implemented.
Operability	can the user use the system without much effort? evaluates the attributes of software that bear on the users' effort for operation and operation control (e.g. function keys, mouse support, shortcuts e.t.c.)	The interface actions and elements were sometimes found to be inconsistent - error messages were not clear and led to more confusion and resulted in operators guessing and attempts to rectify problems which in turn led to deeper problems as the system was not designed to handle user play-around cases (i.e., to handle unexceptional errors). Some important functions such as deletion was being performed with prompt to confirmation.
Attractive-ness	does the interface look good? evaluates how attractive is the interface to the user?	the system design and screen layout and colour was not so appealing
Efficiency	Have functions been optimised for speed? Have repeatedly used blocks of code been formed into sub-routines?	
Time Behaviour	how quickly does the system respond? evaluates the time it takes for an operation to complete; software's response and processing times and throughput rates in performing its function	To be checked against specification. However, the full testing of this characteristic was not possible at the time of carrying out this study since the daily enrolment throughput was around 1200 people a day, subsequently the same figures for the card production. From a database capacity view point, the PRIDC system was dimensioned to manage records of 5 Million persons. Whereas the throughput of the system was as follows: <ul style="list-style-type: none"> • allows for up to 7,000 enrolments per day. • able to produce up to 7,000 ID Cards per day. • The Biometric Sub-System is able to perform up to 7,000 person identification (TP/TP) searches per day.

		<p>The processing operations was designed as follows:</p> <ul style="list-style-type: none"> • New enrolment: 20 minutes • Card collection: 3.5 minutes • Card Renewal: .8 minutes • PR Functions: .8.5 minutes • Civil investigation: 11 minutes • Biometric subsystem: Within 22 hours
Resource Utilisation	<p>does the system utilise resources efficiently? is the process of making code as efficient as possible; the amount of resources and the duration of such use in performing the software's function</p>	<p>This task was not possible at the time of carrying out the evaluation, since the source code was still not handed over to the client.</p>
Maintain-ability	the effort needed to make specified modifications	
Analysability	<p>can faults be easily diagnosed? the effort needed for diagnosis of inefficiencies or causes of failure or for identification of parts to be modified</p>	<p>During system installation and with the release of the software (also during business operations), undocumented defects and deficiencies were discovered by the users of the software. Those encountered faults were very difficult to analyse and diagnose even by the vendor technical team and encountered software inefficiencies usually took long time to fix, as problems were usually passed to the development team in France for investigation and response.</p>
Changeability	<p>can the software be easily modified? Changeability is the effort needed for modification, removal or for environmental change</p>	<p>The system architecture was so complex, as the word 'change to the system' meant a nightmare to the vendor. The vendor always tried to avoid changes all the time with the justification: 'the system in the current form, allows you to enrol the population and produce ID cards for them'. The client concern was that the software in its current version opens doors for many errors from user entry errors to incomplete business functions that were not captured during the phase of requirement specifications.</p>

		it is worth also to mention that changes to the system when agreed was taking so long to implement. For example, adding a field to the system (job title) took a work of 1 month to implement with an amazing amount bill.
Stability	can the software continue functioning if changes are made? the risk of unexpected effects of modifications	as mentioned above, the system complex architecture implied that a change in one place would almost affect many parts of the system. A change in one part of the system, would normally cause unexpected effects as a result of the modification.
Testability	can the software be tested easily? the effort needed for validating the modified software.	in general, system (business) processes and functions were tested against specifications. However from a technical perspective, the complex architecture of the system made it impossible to test many areas of the software. The vendor was pushing for the system to be accepted from a functional perspective (including the network setup).
Portability	A set of attributes that bear on the ability of software to be transferred from one environment to another	
Adaptability	can the software be moved to another environments? the software's opportunity for adaptation to different environments(e.g. other hardware/OS platforms	The software was designed and coded to operate within a unique environment of databases, operating systems and hardware. Most of the hardware used proprietary APIs' (Programming Applications Interface) to interface with the system. This automatically locked the system to only use the specified set of hardware but not otherwise.
Installability	can the software be installed easily? the effort needed to install the software in a specified environment	Though installation files and guides were available, the software architecture was not clear at all. All attempts made by the technical members failed in this regard. Despite the several requests, the vendor felt that the system should not be installed other than the vendor himself.

Co-existence	does the software comply with portability standards? Conformance is the degree to which the software adheres to standards or conventions related to portability	the system did not comply with any portability standards other than the vendor's own.
Replaceability	does the software easily replace other software? the opportunity and effort of using the software in the place of specified older software.	The PRIDC software was expected to take over the current population register database maintained part of the immigration system in the Ministry of Interior. However, this was a long-term objective. The software needed to go under several revolutions, before it can achieve this objective.

6. REFLECTION

"Some problems are so complex that you have to be highly intelligent and well-informed just to be undecided about them."

Laurence J. Peter

Many researchers and practitioners argue that measurement is an essential issue in project and process management and improvement from the logic that it is not possible to control what is not understood and it is not possible to scientifically understand what is not measured [4]. Using measurement practices may well increase the rate of project success to a higher level, statistically [30].

In the real world, however, this may be argued to be a valid issue at the organisation level not at the individual project level. This is to say that projects usually have very short term strategies with very tight deadlines

and tend to be the result of an opportunistic behaviour; where applying such measurement strategies may not be seen to add value, bearing in mind the time and cost associated with such measurement analysis activities. As the UAE national ID system will become the most critical system in the country as the main central hub for population identity cross checking and service eligibility (i.e., online with 24/7 availability requirement), it becomes important that the software goes under a thorough quality check.

Taking into consideration the CBS nature of the system, some components were viewed to be more critical to go under a through quality checks as a failure in different software components may lead to everything from public frustration to complete chaos when the card becomes 'the means' to accessing services. The evaluation study carried out here attempted to provide a short but thorough overview of the PRIDC system, and measure the system quality against ISO 9126 standard. Many limitations had been encountered that will help greatly the project team to address before the final acceptance of the system from the vendor.

From the evaluation, the system was found to have been developed as a component-based software system, but most importantly was observed to be a closed system. This closed architecture—although it was promised to work as prescribed in the specification documents—was viewed to likely cause the following major drawbacks in the short and long run:

1. the system supported only a few hardware vendors, as this was seen to result in the system losing certain amount of autonomy and promoting it to acquire additional dependencies when integrating COTS components;

2. system evolution was not a simple plug-and-play approach. Replacing one component was more typically to have rippling affects throughout the system, especially where many of the components in the system were black box components; and
3. the system architecture forced the client to return again and again to the original vendor for additional functionality or capacity.

The closed architecture with the different proprietary platforms it incorporated were altogether more likely to slowdown the pace of organisational business and process excellence as changes to the system would be expensive and extremely difficult to maintain.

The literature has not been kind to the closed system architectures as research show that such systems have proven to be too slow and too expensive to meet the rapidly changing market needs, as it restricts the level of quality that can be achieved [30],[31],[32],[33]. However, some vendors and service providers strongly advocate standardised systems via closed architectures. Their argument is that such architectures are so necessary in their system standards efforts and that the openness of the component-based approach leads to a chaos of choices and integration headaches, and that such architectures to address the 'security' needs.

Moreover, over the long-term life of a system, additional challenges may well arise, including inserting of COTS components that correspond to new functionality and "consolidation engineering" wherein several components may be replaced by one "integrated" component. Following are further reflections on the major ISO 9126 quality attributes:

6.1 Functionality

The functionality factors were mainly checked against the system specification documents. However, it was discovered on the release of the first version of the software that many business functions were not covered in the specifications, resulting in the need for subsequent releases to address and fill the operational gaps. However, the evaluated software version in this study was not at an acceptable state, as it required additional enhancements to cover some of the additional business functions and rectify identified deficiencies, errors and bugs.

It is also worth to mention that the overemphasis of security requirements during the specification phase contributed exponentially to the existing high complexity of the overall system, and its interoperability with other sub-systems. The fundamental problem concerning software development is defined as to try to understand the customer's sometimes unspoken needs and requirements and translate these into a tangible software solution.

The literature shows that one of the principle causes of information system failure is when the designed system fails to capture the business requirements or improve the organisational performance. Researchers argue that such failures were because many organisations tend to use rule-of-thumb and rely on previous experiences [35]. The vendor adopted the waterfall system development approach when it came to user requirements analysis and system implementation.

The vendor was reluctant to make any modification to the developed system, and was presenting high cost impact on each change to it even if it was a change to modify labels of text fields on user screens. The common response of the vendor was that 'the system is developed according to the agreed specification, and any deviation from that is probably to have a cost impact.'

This attitude of the vendor opened doors for long discussion meetings and arguments around this area, and slowed down the progress of the project, as changes got parked for long periods as some got buried and lost into the huge project documents and long meeting minutes. However, system functionality is a temporary matter that can be resolved once attended to. The most critical items that needed to be addressed along with the functionality concerns were the areas discussed next.

6.2 Reliability

Software reliability is the probability that a software system will not cause the failure of the system for a specified time under specified conditions. The different tests carried out during the deliverables acceptance relied on systematic software testing strategies, techniques, and process, and software inspection and review against specifications. However, and during this study, it was found very useful to incorporate less systematic testing approaches to explore the ability of the system to perform under adverse conditions.

6.3 Usability

The software seemed to have many usability concerns as system users struggled to understand system processes and functions, as minimal user documentation were available that also did not cover the areas users needed most.

Extensive training was required to educate the users on the system, as much effort was required from the registration centre supervisors to support the users. The system was required to go through a major review to evaluate its usability. It also needed to be enhanced to follow a standard GUI methodology overall.

6.4 Efficiency

System processes and functions were checked against the time indicated in the specifications from a functional perspective. Nonetheless, code review was not possible because the source code was not handed over to the client at the time of carrying out this evaluation. Overall, the technical team had concerns about the capability of the system to provide acceptable performance in terms of speed and resource usage.

6.5 Maintainability

The complex architecture of the system made the analysis and diagnoses of discovered system faults and their maintenance so difficult where problems were usually passed to the development team in another country for investigation and preparation of bug-fix patches.

Besides, the complex architecture acted also as a huge barrier to making urgent changes to the system as it required long analysis to evaluate the impact on the different components of the software, associated with an unrealistic cost impact of implementing such changes claimed by the vendor.

6.6 Portability

The system had many proprietary API's to interface with the different components of the system, locking the system to use a specified set of hardware but not otherwise. Installation files and guides did not enable the reinstallation of the system.

Overall, the system was observed not to comply with any portability standards other than the vendor's own, which can be carried out only by the vendor himself. The vendor was asked to add APIs to the system

to allow the plug-in of new components to the system both data and hardware wise.

7. CONCLUSION

"You don't drown by falling in the water; you drown by staying there."

Edwin Louis Cole

As widely quoted in the literature, the application of software metrics has proven to be an effective technique for improving the quality of software and the productivity of the development process i.e the use of a software metrics program will provide assistance to assessing, monitoring and identifying improvement actions for achieving quality goals (see for example: [3],[4],[5],[6],[8],[9],[12], [14],[29],[35], [36],[37]. In this study, the author attempted to use the ISO 9126 quality model to evaluate the PRIDC system; mainly from a product quality angle. See also Figure 10.

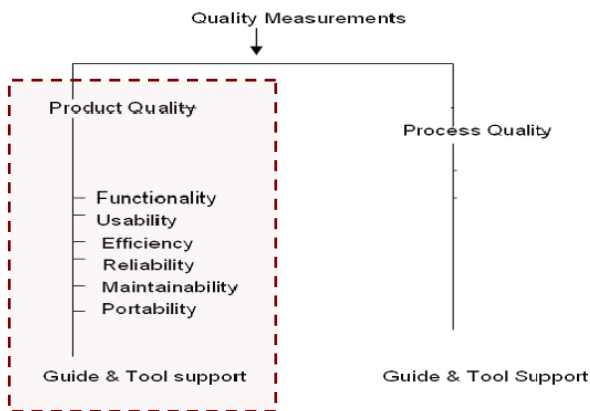


Fig. 10: software quality metrics framework - Source: [37]

The study presented in this article contributed to a great extent in spotting some of the system deficiencies that were addressed prior to the final acceptance and handover of the system. It was also the author's observation that the project team, with the workload and responsibilities put on them, seemed to be overloaded and to have a scattered vision of how things be done and achieved. Everybody wanted the project to conclude as quickly as possible as everybody seemed also to be confident of the work produced by the vendor.

The use of quality framework showed in this study can be a very useful and supportive methodological approach for going about software quality assessment. ISO 9126 framework can act as a comprehensive analytical tool as it can move beyond superficial evaluation to achieve a more thorough view of the system's strengths and weaknesses than can be provided by less systematic approaches.

When implementing big projects such as National ID schemes, project management and technical teams should use quality models for evaluating the overall architecture prior to the final acceptance of the system. As such and if used as a guide in an early stage of the project it can arguably provide a basis for informed and rational decision making and have the potential to increase the project success rate.

From a technical view point, the ISO software quality metrics may also be extended throughout the phases of software development life cycle. The framework is designed to address the wide range of quality characteristics for the software products and processes enabling better description of software quality aspects and its importance.

ACKNOWLEDGMENT

The author would like to thank Mr. Naorem Nilkumar for his contribution and the technical input that improved the overall work presented in this article.

REFERENCES

- [1] A.M. Al-Khouri, "UAE National ID Programme Case Study," *International Journal Of Social Sciences*, vol. 1, no. 2, pp.62-69, 2007.
- [2] E. Folmer & J. Bosch (2006) "A Pattern Framework for Software Quality Assessment and Tradeoff analysis," *International Journal of Software Engineering and Knowledge Engineering*, 2006 [Online]. Available: <http://www.eelke.com/research/literature/SQTRF.pdf>.
- [3] S.N. Bhatti, "Why Quality? ISO 9126 Software Quality Metrics (Functionality) Support by UML," *ACM SIGSOFT Software Engineering Notes*, vol. 30, no. 2, 2005.
- [4] E.J. Garrity & G.L. Sanders, "Introduction to Information Systems Success Measurement," in E.J. Garrity & G.L. Sanders (editors) *Information System Success Measurement*. Idea Group Publishing, pp.1-11, 1998.
- [5] R.B. Grady, "Practical results from measuring software quality," *Communications of the ACM*, vol. 36, no. 11, pp.63-68, 1993.
- [6] S. Hastie (2002) "Software Quality: the missing X-Factor," Wellington, New Zealand: Software Education [Online]. Available: http://softed.com/Resources/WhitePapers/SoftQual_XF-actor.aspx.
- [7] S.L. Pfleeger, *Software Engineering Theory & Practice*. Upper Saddle River, New Jersey: Prentice Hall, 2001.
- [8] R.A. Martin & L.H. Shafer (1996) "Providing a Framework for Effective Software Quality Assessment - Making a Science of Risk Assessment," 6th Annual International symposium of International council on Systems Engineering (INCOSE), *Systems Engineering: Practices and Tools*, Bedford, Massachusetts [Online]. Available: http://www.mitre.org/work/tech_transfer/pdf/risk_assessment.pdf.
- [9] B.W. Boehm, J.R. Brown, H. Kaspar, M. Lipow, G.J. MacLeod, G.J. & M.J. Merritt, "Characteristics of Software Quality." *TRW Software Series - TRW-SS-73-09*, December, 1973.
- [10] J.A. McCall, P.K. Richards & G.F. Walters, "Factors in Software Quality," volumes I, II, and III, US. Rome Air Development Center Reports NTIS AD/A-049 014, NTIS AD/A-049 015 and NTIS AD/A-049 016, U. S. Department of Commerce, 1977.

- [11] M.F. Bertoa, J.M. Troya & A. Vallecillo, "Measuring the Usability of Software Components," *Journal of Systems and Software*, Vol. 79, No. 3, pp. 427-439, 2006.
- [12] S. Valenti, A. Cucchiarelli, & M. Panti, "Computer Based Assessment Systems Evaluation via the ISO9126 Quality Model," *Journal of Information Technology Education*, vol. 1, no. 3, pp. 157-175, 2002.
- [13] R. Black (2003) "Quality Risk Analysis," USA: Rex Black Consulting Services [Online] Available: <http://www.rexblackconsulting.com/publications/Quality%20Risk%20Analysis1.pdf>.
- [14] G.G. Schulmeyer & J.I. Mcmanus, "The Handbook of Software Quality Assurance" (3rd edition). Upper Saddle River, New Jersey: Prentice Hall, 1999.
- [15] A. Abran, Al-Qutaish, E. Rafa, J.M. Desharnais, & N. Habra, "An Information Model for Software Quality Measurement with ISO Standards," in SWEDC-REK, International Conference on Software Development, Reykjavik, Islande , University of Iceland, pp. 104-116, 2005.
- [16] K.-K. Lau, (editor) 'Component-based Software Development: Case Studies,' World Scientific (Series on Component-Based Software Development), vol. 1, 2004.
- [17] F.P. Brooks, "No Silver Bullet: Essence and Accidents of Software Engineering," *Computer*, vol. 20, no. 4 , pp. 10-9, 1987.
- [18] A.W. Brown, "Preface: Foundations for Component-Based Software Engineering," *Component-Based Software Engineering: Selected Papers from the Software Engineering Institute*. Los Alamitos, CA: IEEE Computer Society Press, pp. vii-x, 1996.
- [19] A. Brown & K. Wallnau "Engineering of Component-Based Systems," *Proceedings of the Second International IEEE Conference on Engineering of Complex Computer Systems*, Montreal, Canada, 1996.
- [20] C. Szyperski, *Component Software: Beyond Object-Oriented Programming*. New York, NY.: Addison- Wesley, 1997.
- [21] X. Cai, M.R. Lyu & K. Wong(2000) "Component-Based Software Engineering: Technologies, Development Frameworks and Quality Assurance Schemes," in *Proceedings APSEC 2000, Seventh Asia-Pacific Software Engineering Conference*, Singapore, December 2000, pp372-379 [Online]. Available from: http://www.cse.cuhk.edu.hk/lyu/paper_pdf/ap-sec.pdf.
- [22] A.W. Brown & K.C. Wallnau, "The Current State of CBSE," *IEEE Software*, vol. 155, pp. 37– 46, 1998.
- [23] M. Kirtland, *Designing Component-Based Applications*. Redmond, Washington: Microsoft Press, 1999.
- [24] G.T. Heineman & W.T. Councill (editors) *Component Based Software Engineering: Putting the Pieces Together*. Boston, MA: Addis on-Wesley, 2001.
- [25] G.T. Leavnesn & M. Sitaraman, *Foundations of Component-Based Systems*. New York: Cambridge University Press, 2000.
- [26] R. Richardson, "Components Battling Component," *Byte*, vol. 22, no. 11, 1997.

- [27] R. Veryard, *The Component-Based Business: Plug and Play*. London: Springer-Verla, 2001.
- [28] G. Pour, "Component-Based Software Development Approach: New Opportunities and Challenges," in *Proceedings Technology of Object-Oriented Languages, TOOLS 26*, pp. 375-383, 1998.
- [29] N.S. Godbole, *Software Quality Assurance: Principles and Practice*. Oxford, UK: Alpha Science International, 2004.
- [30] L. Bass, P. Clements & R. Kazman, *Software Architecture in Practice*. Reading MA.: Addison Wesley, 1998.
- [31] J. Bosch, *Design and use of Software Architectures: Adopting and evolving a product line approach*. Harlow: Pearson Education (Addison-Wesley and ACM Press), 2000.
- [32] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, & M. Stal, *Pattern-Oriented Software Architecture: A System of Patterns*. New York: John Wiley and Son Ltd, 1996
- [33] M. Shaw, and D. Garlan, *Software Architecture: Perspectives on an Emerging Discipline*. New Jersey: Prentice Hall, 1996.
- [34] P.B. Crosby, *Quality Is Free: The Art of Making Quality Certain*. New York: McGraw-Hill, 1979.
- [35] R.G. Dromey, "A model for software product quality," *IEEE Transactions on Software Engineering*, vol. 21, no. 2, pp. 146-162, 1995.
- [36] J.T. McCabe, (1976) "A Complexity Measure," *IEEE Transactions on Software Engineering*, vol. SE2, no. 4, pp. 308-320, 1976.
- [37] K.H. Möller & D.J. Paulish, *Software Metrics*. London: Chapman & Hall Computing, 1993.

ELECTRONIC GOVERNMENT

in the GCC Countries

Barriers and Solutions ¹¹

Ali M. Al-Khouri & J. Bal

COPYRIGHT © 2007 WASET.ORG

ABSTRACT: The study investigated the practices of organisations in Gulf Cooperation Council (GCC) countries with regards to G2C e-government maturity. It reveals that e-government G2C initiatives in the surveyed countries in particular, and arguably around the world in general, are progressing slowly because of the lack of a trusted and secure medium to authenticate the identities of online users. The authors conclude that national ID schemes will play a major role in helping governments reap the benefits of e-government if the three advanced technologies of smart card, biometrics and public key infrastructure (PKI) are utilised to provide a reliable and trusted authentication medium for e-government services

Key words: *e-Government, G2C, national ID, online authentication, biometrics, PKI, smart card.*

¹¹ Al-Khouri, A.M. & Bal, J.(2007) "**Electronic Government in the GCC Countries,**" International Journal Of Social Sciences, Vol. 1, No. 2, pp.83-98.

1. INTRODUCTION

AMONG the many promises of the Information Communication Technologies (ICT) revolution is its potential to modernise government organisations, strengthen their operations and make them more responsive to the needs of their citizens. Many countries have introduced e-government programmes that incorporate ICT and propose to transform several dimensions of their operations, to create more accessible, transparent, effective and accountable government.

Evaluating current practices, recent studies show that the implementation of e-government programmes is not a simple task as many if not all governments lack the fundamental infrastructure, organisational culture, understanding and resources for a transformation of the magnitude that e-governments require. Many researchers have addressed the technical and management issues surrounding e-government projects. Many others also have demonstrated the challenges associated with the implementation of e-government programmes, and put forward recommendations to overcome them.

Despite the variety of approaches that were proposed in the literature to handling government electronic services, not one proven solution or framework to build an e-government architecture appears to exist.

The objective of this research study is to provide a short overview of the current literature in the research area and relate this information to the issues surrounding e-government initiatives. In principle, the study is designed to:

- (1) explore the potential applications of a national ID card and its suitability as a reliable medium to verify virtual online identities (if implemented with smart card, biometrics, and PKI technologies), and

(2) conduct a postal survey (followed by telephone interviews of executives) of organisations in the GCC¹² countries to understand their e-government practices and progress.

The finding of the study adds to the body of knowledge, as it draws a picture of the current practices, assesses the progress in the field of e-government and pinpoints the key obstacles and the degree to which national ID programmes can support the progress of G2C initiatives.

This paper is structured as follows. First a short overview of the current literature on e-government is provided to highlight current trends, patterns, and models for such initiatives as well as the barriers to successful implementation. The following sections establish a link between national ID card schemes and e-government by looking at the technology requirements for enabling a reliable digital ID framework that can support and enable e-government development. Then the research survey methodology is explained, findings are presented and conclusions drawn.

2. THE ILLUSION OF E-GOVERNMENT

Citizens' experience with the 24x7 world of the private sector has fuelled demands for similar experience with their governments; easy to deal with, available when you want them to be, one-stop service that is personalised with simple completion of transactions on line. This utopia bears little resemblance to most government's current capabilities; multiple agencies, multiple payment and delivery options, little coordination or standards, modest online functionality and variable

¹² The surveyed organisations in this study were all from the Southern Gulf countries; Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates often referred to as the Gulf Co-operation Council (GCC) countries.

customer service capabilities. Citizen demands are at odds with the current structure of most government agencies. Evidence is emerging however that when government does go online successfully, patterns of interaction are dramatically changed.

In principle, the literature examines e-government activities in terms of the interactions between sectors of government, businesses and citizens [1]. The matrix in Figure 1 shows the nine principle interactions. Some research studies also included employees in this spectrum. However, many researchers have considered the employee element to go under government activities.

		Recipient of Services		
		Citizen	Government	Business
Suppliers of services	Citizen	Citizen to Citizen (C2C) e.g., small advertisement	Citizen to Government (C2G) e.g., tax declaration by single person or family	Citizen to Business (C2B) e.g., job exchange by job seekers
	Government	Government to Citizen (G2C) e.g., benefit processing	Government to Government (G2G) e.g., transactions between Pas	Government to Business (G2B) e.g., procurement of PAs
	Business	Business to Citizen (B2C) e.g., Online order in a shopping mall	Business to Government (B2G) e.g., tax declaration by private organisation	Business to Business (B2B) e.g., procurement through EDI

Fig. 1: e-Government's interactions

2.1 Government-to-government (G2G)

This represents the backbone of e-government. It involves sharing data and conducting electronic exchanges between governmental departments, rather than being focused on the specific agency or agencies responsible for administering programs and policies.

2.2 Government-to-business (G2B):

It includes both the sale of surplus government goods to the public, as well as the procurement of goods and services. It aims to more effectively work with the private sector because of the high enthusiasm of this private sector and the potential for reducing costs through improved procurement practices and increased competition.

2.3 Government-to-citizen (G2C) – (the focus of this paper)

This provides opportunities for greater citizen access to, and interaction with the government. This is what some observers perceive to be the primary goal of e-government. Thus, and from G2C perspective, many government agencies in developed countries have taken progressive steps toward the web and ICT use, adding coherence to all local activities on the Internet, widening local access and skills, opening up interactive services for local debates, and increasing the participation of citizens on promotion and management of the territory [2].

Several approaches were proposed in the literature to handling electronic services. However, the literature provides not one proven solution or framework to build an e-government architecture. For this very same reason, e-government architecture development practices around the world vary according to several factors (the technical team experience, solution provider, consultants, budget, technological limitations, etc.), leaving those organisations with no choice but to go for a model and then enhance it based on new requirements and/or constraints.

To build such architectures, governments need to understand the complexity associated with the development and transition stages of e-government. One of the well-known models in the literature that outlines the stages of e-government development was developed by

Layne & Lee [3] that outlines the stages of e-government development. In moving to the first two phases, government organisations are faced with technological challenges such as those in Figure 2. Stage three and four is where governments instead of automation, they transform their services and integrate processes and functions across the different levels of the government to create an integrated information base, implementing a 'one-stop-shopping' concept for its citizens.

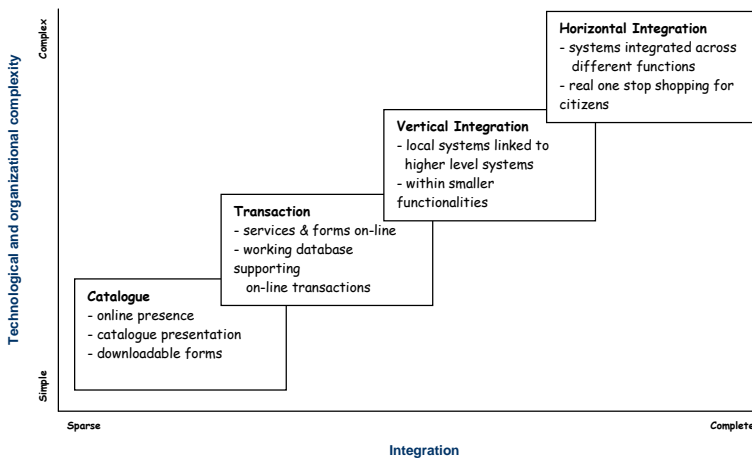


Fig 2: dimensions and stages of e-government

The model assumes that e-government initiative will require both horizontal and vertical integration; horizontal as e-government efforts must extend to all departments within a level of government (i.e., federal, state, local) and vertical as e-government initiatives must integrate across levels of government. It was observed in the literature that some researchers used Layne & Lee's four phases and interpreted them as components of a maturity model to judge the maturity of the processes of an organisation and for identifying the key practices that are required to increase the maturity of these processes - see for example [4]. By focusing on a limited set of activities and working

aggressively to achieve them, it is argued that the maturity model can steadily improve organisation-wide e-government processes and enable continuous and lasting gains in the e-government capabilities.

However, and according to various studies of e-government practices around the world, many researchers have found that such initiatives are stuck in phase one and two, far from the ideal integrated digital government [5]. Researchers have identified many technical and organisational barriers challenging e-government progress to move up the ladder to stage three and four of Layne & Lee's model (see Figure 3).

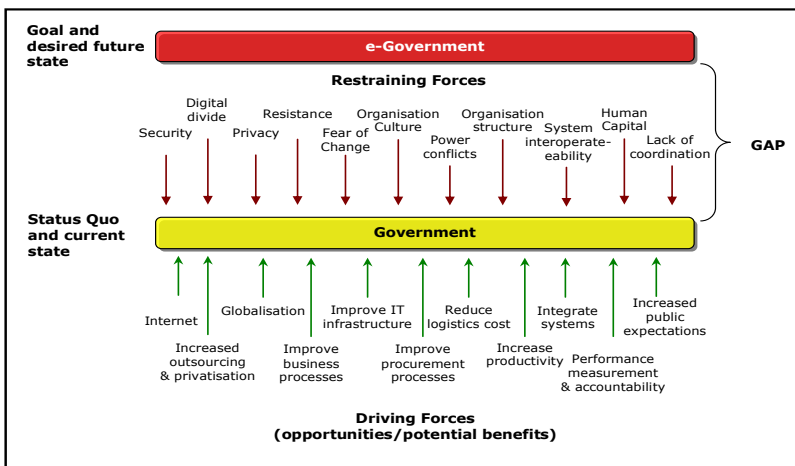


Fig. 3: e-government force analysis

It appears the current literature does not give enough attention to the need in e-government programmes for identity verification which is believed by the authors to be the foundation for G2C initiatives. It is argued by the authors that if governments are to complete phase two of the Layne & Lee (2001) model and enable a much larger and more

comprehensive set of G2C transactions to take place online, they will need to ensure that citizens have the ability to authenticate themselves online and verify their identities - see also [6]. Governments need to develop clear vision of how they intend to authenticate individuals' digital identities [7]. A digital identity is the representation of a human identity that is used in a distributed network interaction with other machines or people [8].

Their vision need to look at the different options available for building a digital identity management infrastructure that "allows transactions in which the parties are separated in time and space while retaining the ability of these transactions to contain all of the human identity based attributes that transactions between people have always had" [8]. Only with a robust digital identity infrastructure can the true power of G2C applications be released. Initiatives such as national ID projects are a key to G2C e-government progress, and a step towards building a secure digital infrastructure that can enable online identification and authentication.

The national ID project is seen by the authors as a good opportunity to build the governments' central identity infrastructure component for e-government initiatives. The next section looks at how advanced technologies can support G2C e-government and provide a robust digital ID as well as a solid foundation for developing secure applications and safeguarding electronic communications.

3. NATIONAL ID AND G2C E-GOVERNMENT

National ID programmes may well address many of the security issues related to electronic communications and the verification of online identities, provided that appropriate technologies are utilised.

This can also be realised by looking at one of the primary goals of such schemes, take for instance the UAE national ID project, which aims to improve the country's ability to accurately recognise peoples' identities through identification (1:N) and verification (also referred to as authentication) (1:1) methods as depicted in Figure 4 [9].

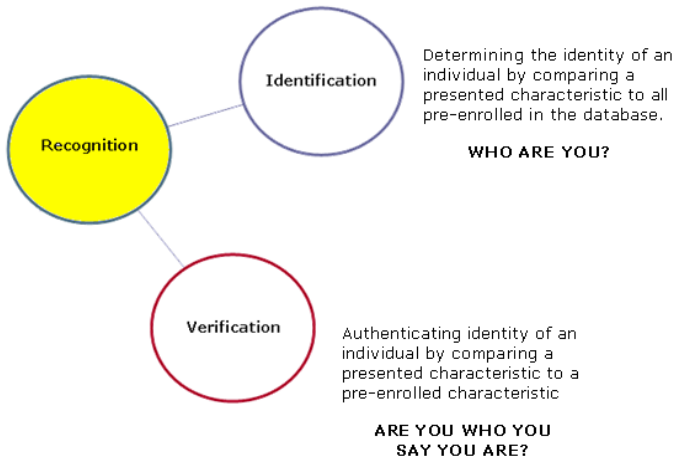


Fig 4: identity recognition

The key to G2C e-government is authentication i.e., the ability to positively identify and prove the authenticity of those with whom the government conducts business. Without authentication, other security measures put in place for many G2C transactions can be ineffective. To clarify this further, governments need varying levels of authentication strength based on the value or sensitivity of their online information or services, balanced against other considerations like usability, deployment, and budget. The discussion in this section is limited to the presentation of authentication levels that organisations may consider in their G2C initiatives and some of the advanced technologies that can make such requirements possible. It is important to heed that the

essence of G2C e-government is that transactions occur between people that are represented by machines. The anonymity of these transactions makes it more difficult to identify the parties involved and to ensure a trusted business relationship.

Since all successful business relationships are based on trust, establishing online trust should be one of the primary goals of any e-government initiative. The focus must be building a trust environment that provides a high level of data privacy, data integrity, and user authorisation. The real cornerstone of G2C e-business trust is authentication: that is, knowing with whom the government is doing business with. PKI, smart cards, and biometrics (see Table 1) are the technologies that are believed to be the key components of the trust model to address both electronic transactions security and online identity authentication.

Table 1: PKI, smart cards, biometrics

(1) Public Key Infrastructure (PKI):	state-of-art in digital authentication & overall security infrastructure
(2) Smart Card:	a plastic card with an IC chip capable of storing & processing data that may also come with optional magnetic strips, bar codes, optical strips etc. viewed as n ideal medium for national ID schemes, e-government & e-commerce applications
Biometrics:	allow to connect individuals to their credentials and therefore enables the verification (authenticate or identify) of people's identity using the unique properties of their physical characteristics

Combining these three technologies can provide the government with a three-factor authentication capability such as depicted in Figure 5:

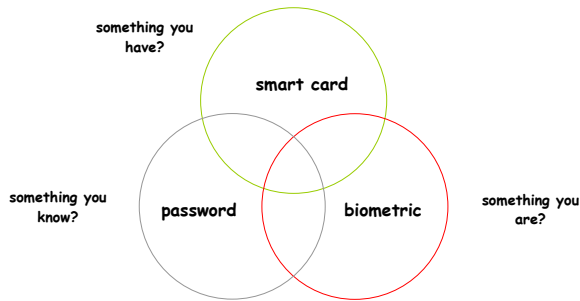


Fig. 5: three factor authentication

- (1) a password to ascertain what one knows,
- (2) a token (smartcard) to ascertain what one has/posses, and
- (3) biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is.

As such, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customers account. This would be difficult, if not totally impossible.

By requiring three forms of identification to access credentials, organisations will be able to bind users' digital identities to their physical identities which allows them to be more confident that the users are who they say they are, which should in turn give governments a high level of assurance of online identities.

The following three sections will introduce the three main technologies, namely: PKI, biometrics, and smart cards.

Due to the breadth and depth of the PKI subject, the discussion here is narrowed to address the online identity authentication issue. Several practical studies demonstrated that most of the e-government security requirements can be fulfilled through the public key infrastructure (PKI) security services.

PKI is defined as a system of computers, software and data that relies on certain sophisticated cryptographic techniques to secure on-line messages or transactions [10]. The requirements imposing the need for additional security measures are either related to the hardware/software infrastructure of the e-government platform (e.g. performance, availability, etc.), or to highly specialised-security critical applications (e.g. e-voting; anonymity, un-coercibility, etc.).

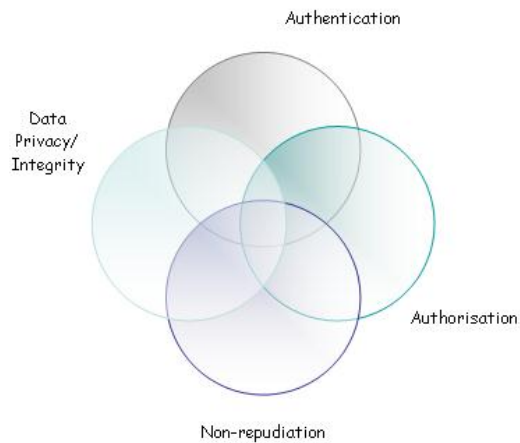


Fig. 6: PKI security framework

In principle, as depicted in Figure 6, PKI provides four key features to secure online transactions:

- Authentication — to verify the user identity prior to an online exchange, transaction, or allowing access to resources (e.g., digital certificate¹³, public key certificate, biometrics, etc.)
- Data privacy/integrity —to ensure the confidentiality of information and that data is not altered as it moves around the public Internet (e.g., encryption¹⁴).
- Non-repudiation — to prove that an individual has participated in a transaction (e.g., digital signature). Only two-factor authentication definitively binds a user's physical identity to his digital identity.
- Authorisation — to verify that the user has permission to participate in an activity, a transaction, or is allowed access to resources (e.g., cross reference public key certificate with a privilege through the use of policy management servers).

PKI provides a mechanism for binding cryptographic keys, used to encrypt and digitally sign messages, to other credentials such as name, age or place of birth from key certificates and transporting those certificates around the internet electronically.

¹³ A digital signature is sometimes referred to as an electronic signature, but is more accurately described as an electronic signature that is authenticated through a system of encryption logarithms and electronic public and private keys. A digital signature is often described as an envelope into which an electronic signature can be inserted. Once the recipient opens the document, the digital signature becomes separated from the document and the document can be modified. Thus, a digital signature only preserves the integrity of a document until it is opened.

¹⁴ Encryption is a security method that transforms information into random streams of bits to create a secret code. There is software-based encryption such as Secure Sockets Layer (SSL) or Public Key Infrastructure (PKI). Hardware-based encryption, such as smart cards, is another type of encryption.

A government agency can for example send messages using citizen's digital certificate encoded with relevant public key that only that specific citizen can open.

3.1 Biometrics

Biometric technology can be used in identity management systems to identify someone in a population (known as 1:N matching) or to verify someone against his/her own details (known as 1:1 matching). Apart from being non-transferable among individuals, biometrics do not provide data about the person; rather, information of the person.

When biometrics such as fingerprints or iris recognition is deployed in these contexts, for unique identification and for strong authentication, they provide an effective means for binding people to their identities.

In the context of a national ID scheme, the biometrics process allows a technique of padlocking the citizen to the card. In doing so, the card cannot easily be transferred to another individual. In particular, given the current focus on the use of biometrics in national identity cards, it sets out an architecture for strongly-authenticated identity cards that deliver (perhaps counter-intuitively) both enhanced security and enhanced privacy.

3.2 Smart Cards

In a smart card secure environment, users are not locked into one form of authentication, such as the ever-vulnerable password. Smart cards provide a mechanism for binding cryptographic keys to individuals, with appropriate authentication, so that when a key is used then the organisation or the individual can be certain of the identity of the person at the other end of the transaction or communication.

Mapping this to the earlier example of the government agency, when a person gets a message, he or she can put their smart card into their PC and punch in their PIN that will in turn lets the smart card use the relevant key to decode the message. Depending on the configuration, if a user loses the smart card, the card can be inoperable without the biometric.

Forged fingerprints can be weeded out with the use of the PIN. Smart cards allow on-card or off-card biometric matching. Off-card matching means that biometric authentication happens online where the biometric features are compared with backend databases.

On-card matching technology means that biometric features are compared with a stored template within the card. The template is stored exclusively in the secure smart card environment, which reliably protects sensitive personal data against unauthorised access.

On-card matching is an outstanding way of user authentication within security applications that meet the three paramount requirements of security, ease of use, and data privacy. Using the power of these three technologies, government organisations and businesses alike can use varying levels of authentication depending on the level of security required for a particular transaction (Figure 7).

Citizens with simple readers attached to their PCs (at home, work) or even kiosk machines can logon onto the government internet portal and perform various transactions online in off-card or on-card authentication modes (Figure 8).

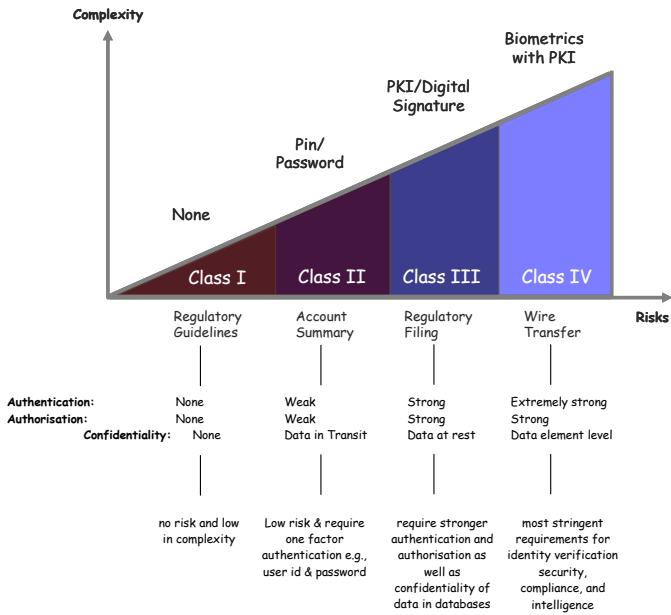


Fig. 7: an example of types of authentication for G2C e-gov services

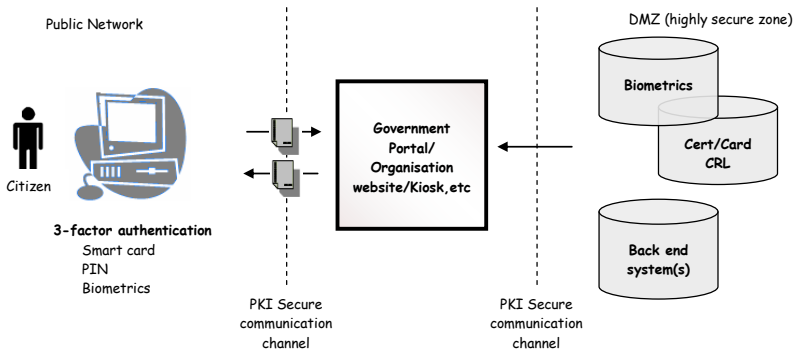


Fig. 8: conceptual model for electronic authentication

The next sections present the research methodology and the findings from a survey conducted to assess the current status of e-government projects in the Middle East.

4. RESEARCH METHODOLOGY

The data of this study were gathered by two principal methods: personal interviews and a questionnaire survey. A six-page questionnaire was designed, consisting of structured and semi-structured questions, to gather information and understand the surveyed organisations practices in the field of the e-government.

The questionnaire was first pilot tested through telephone interviews with four senior executives and two managers in two organisations - following the recommendation of [11],[12],[13]. These interviewees provided detailed feedback on the clarity of the questions and overall comprehensibility of the instrument.

The result of this pilot study led to some adjustments to the content and format of the questionnaire and terminology used in the survey. The updated questionnaire was then pre-tested on 6 interviewees in four organisations before being administered to all participating organisations (excluding those who took part in the pilot study).

A total number of 198 questionnaires (both in English and Arabic-language versions) were sent to the contacted organisations through the chief information officer or the IT/IS manager, as advised by the sites. The majority of the questionnaires were mailed to respondents with pre-paid envelopes, while the rest were either faxed or e-mailed to respondents. Sixteen questionnaires could not be delivered to the intended recipients and were returned by the postal service.

A total number of 60 questionnaire forms were returned (by postal mail and electronically), giving a response rate of 30.3%. After evaluating the responses, it was found that eight responses were unusable owing to insufficient data. The removal of these unusable responses gave a total

of 64 usable questionnaires (that is including 12 responses produced from the first pilot mailing), which represent an overall response rate of 30.5%.¹⁵

In the sample of 64 participants, 26 government organisations were represented. The characteristics of the respondents are summarised in Table 2. The country with the most participants was the United Arab Emirates with a response rate of 38.1%, followed by Bahrain with 32.4%. Table 3 gives response characteristics for each site.

Table 2: Responses by Industry

Industry (Government)	No.of organisations
Oil/Petroleum	4
Medicine/Health	3
Transportation	4
Telecommunication	3
Finance/Insurance	4
Other	8

4.1 Telephone interviews

Respondents to questionnaires were asked if they could be contacted to provide some clarifications and to be asked some additional questions for the purpose of improving the quality of research information. It was also made clear that their right to anonymity would not be affected in either case. Out of the 64 respondents, 21 agreed to be interviewed, 18 of whom were executives and department directors, and 5 senior managers.

¹⁵ The results of the pilot and final questionnaires were merged here since the changes made to the initial questionnaire were only to clear out ambiguity and change the arrangement of questions. The additional questions included in the final questionnaire were questions 27 and 28 (See Appendix B: Research Questionnaire).

The initial draft of the questionnaire served as an interview guide to ensure that all the relevant questions were asked. Semi-structured, telephone interviews (transcribed for subsequent analysis) were administered to 19 individuals¹⁶ in 12 organisations.

The semi-structured interviewing approach was developed to ensure that the research questions were properly addressed while allowing for 'probing' questions to gain even greater understanding and insight into the issues. The qualitative data obtained through telephone interviews helped to fine tune the focus of the questionnaire survey and interpret its quantitative results.

Some additional follow-up interviews were also conducted by telephone and e-mail. All the interviewees were very friendly and were willing to share their experiences and ideas. Most of the interviews lasted between 20 and 30 minutes.

4.2 Measurement of variables

The questionnaire was divided into two sections to help break the monotony, ease problems of comparison and, most importantly, enable the arrangement of the questions thematically [11].

Part I: This part was designed to be filled by the IT/IS department managers or the responsible department foreseeing the management and implementation of technology related services. The objective of this part of the questionnaire was to gain an understanding of some basic information about the IT infrastructure and technologies utilised to support the electronic strategies.

¹⁶ Out of the twenty-one respondents who agreed to be interviewed, 2 senior managers declined later without any explanation.

Part II: This part of the questionnaire was designed for all respondents.

The objective of this part was to understand the perceptions of both executives and other senior managers about e-government opportunities, obstacles and future plans as well as their level of awareness.

Site (Distributed/ Returned/ %)	Functional areas of returned surveys (self-reported)	Hierarchical levels of returned surveys (self- reported)
Bahrain (34 / 11 / 32.4%)	Corporate Mgmt 3 IS/IT 3 Human Resources 1 Planning & Development 1 Finance 1 Missing Id's 2 Total 11	Executive 6 Senior/mid mgr. 3 <u>Missing Id's</u> 2 Total 11
Kuwait (29 / 8 / 27.6%)	Corporate Mgmt 2 IS/IT 2 Human Resources 1 Planning & Development 1 Finance 1 <u>Missing Id's</u> 1 Total 8	Executive 3 Senior/mid mgr. 4 <u>Missing Id's</u> 1 Total 8
Oman (31 / 9 / 29.0%)	Corporate Mgmt 3 IS/IT 2 Human Resources 1 Planning & Development 1 Finance 1 <u>Missing Id's</u> 1 Total 9	Executive 4 <u>Senior/mid mgr.</u> 5 Total 9
Qatar (36 / 9 / 25.0%)	Corporate Mgmt 2 IS/IT 2 Human Resources 2 Planning & Development 1 Finance 1 <u>Missing Id's</u> 1 Total 9	Executive 4 Senior/mid mgr. 3 <u>Missing Id's</u> 2 Total 9

Saudi Arabia (38 / 11 / 28.9 %)	Corporate Mgmt	3	Executive	4
	IS/IT	1	Senior/mid mgr.	6
	Human Resources	1	<u>Missing Id's</u>	1
	Planning & Development	3		
	Finance	2		
	<u>Missing Id's</u>	1		
	Total	11	Total	11
United Arab Emirates (42 / 16 / 38.1 %)	Corporate Mgmt	6	Executive	9
	IS/IT	1	Senior/mid mgr.	6
	Human Resources	2	<u>Missing Id's</u>	1
	Planning & Development	3		
	Finance	1		
	<u>Missing Id's</u>	3		
	Total	16	Total	16
(210 / 64 / 30.5 %)	Total	64	Total	64

Table 3: Survey response characteristics by region

5. RESEARCH FINDINGS

The following table summarises the research findings.

<p>1. How important do organisations perceive online presence and e-government initiatives?</p>
<p>Out of the 26 surveyed organisations, 20 had internet websites, 4 were planning to develop one, two indicated that they "have no intention of developing one," with the justification that they had no interaction with citizens. Overall, all respondents perceived e-government as a concept that gives them an opportunity to revolutionise their organisations.</p>
<p>2. Major Driver for e-Government projects?</p>
<p>Customer expectations and Internal efficiency/cost reduction were found to be the most common drivers for e-government projects.</p>
<p>3. What plans/strategies do organisations have, to go about e-government projects?</p>
<p>None of the responding organisations indicated to have an e-government strategy but rather a set of guidelines and short term plans. These plans focused on augmenting internal operations, where G2C was left down to the operational departments to implement. In most of the cases, IT departments were tasked to champion such projects.</p>
<p>4. Impact of e-government on organisations operations?</p>
<p>e-government was viewed to enable the government to appear as one unified organisation and provide seamless online services.</p>
<p>5. What is the greatest obstacle to e-government initiatives as viewed by organisations?</p>
<p>Security was found to be a major concern. Ability to verify online identities was the seen to be the biggest obstacle when it came to G2C transactions.</p>
<p>6. Can national ID projects support e-government projects?</p>
<p>Many have viewed national ID projects to be mainly addressing homeland security issues and to replace existing cards such as driving licence, health card, bank cards, etc. However, a common view was that their governments, whether through a national ID or other programmes, must put a solution in place to address the need of online authentication of individuals, to support e-government progress.</p>

Table 4: Summary of research findings

1. How important do organisations perceive online presence and e-government initiatives?

The results of the survey revealed that almost 77 percent of government organisations that responded had an internet web site (See Figure 9). Out of the twenty three percent of the respondents who responded "no" to having a web site, more than 66 percent planned to create a web site by this year or early next year.

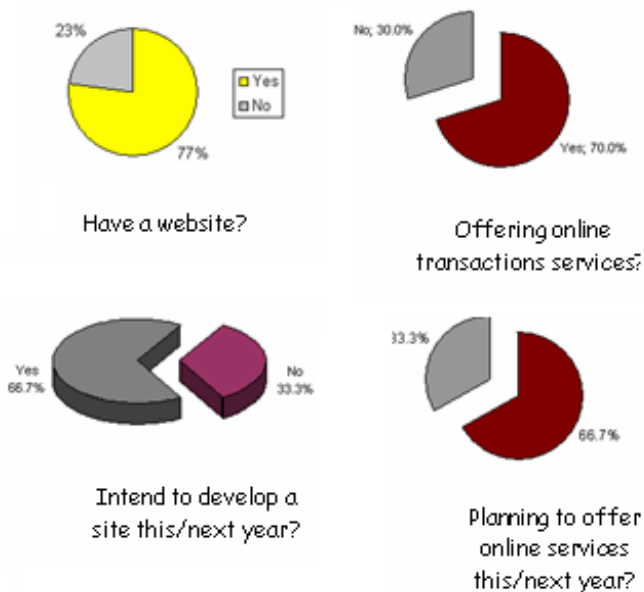


Fig. 9: online presence

Out of the two organisations that did not have websites, one executive claimed that they did not see the need to have a website because of the nature of the services of their organisations which requires the physical presence of the citizens/customers. The other executive claimed to "have no intention of developing one, because of online security concerns."

On the other hand, around 57 percent of those who responded to have a web presence indicated to have automated online services such as payment of fees, bills and fines (see Figure 10). Only three (21.4%) organisations indicated to have integrated their systems for limited online functionalities. This supports the findings of previous studies that most of the organisations are still in the cataloguing and transactional phases of Layne and Lee model.

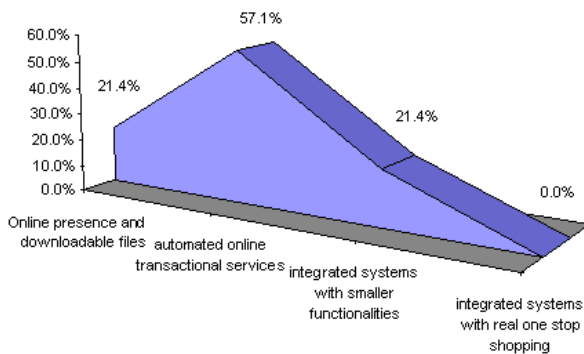


Fig. 10: Organisations own perception of their own electronic operations

2. Major Driver for e-Government projects?

The majority of the respondents (85.9 percent) indicated that the major driver for e-government projects was the (1) growing expectations of citizens for online services and (2) internal efficiency and cost reduction (see Figure 11).

Though not in the form of policies or legislation, responding organisations also reported that a significant amount of pressure is being applied by the government to better coordinate business process and information flow among ministries and local departments.

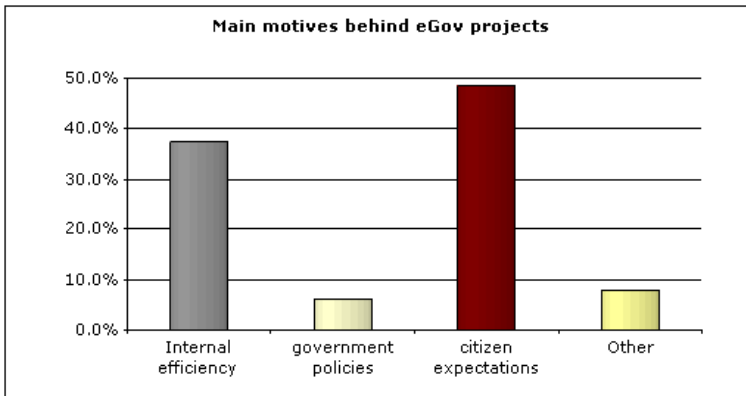


Fig. 11: main motives behind e-government projects

Many of the interviewed executives said that because of the above two drivers for e-government, their organisations are in the process of planning to integrate stovepipes of automation and support collaborative business processes and streamline business operations.

Yet others expressed concerns over the ability to effectively integrate their systems and technically collaborate with other government organisations because of technical and security constraints.

Sixty seven percent of respondents agreed with the statement that "online government services must be customer-centric". The 21 percent of respondents who answered "no" to this statement indicated reasons such as confidentiality of records and current policies to hinder such concepts (see also Figure 12).

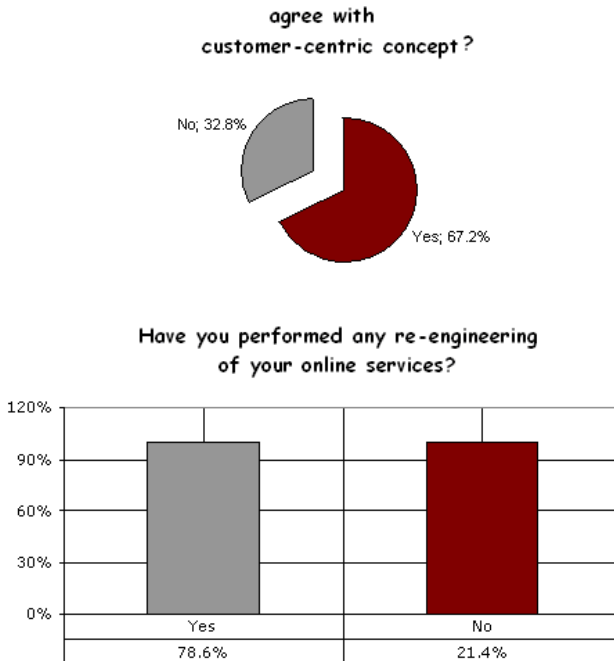


Fig. 12: re-engineering and customer-centric services

Many of them have also expressed their concerns about their inability to automate many of their services and put them online since identity verification was a prerequisite function, as one IT director explains:

"with the pressure we have from the top management to improve performance and offer online services, we are still struggling to address the online identity verification issue."

As depicted in Figure 13, out of those organisations who indicated to have a website, 26.7 percent indicated that they have an IT infrastructure that can support limited online service plans. Not very surprisingly, 73.3 percent responded "no" to having one.

With follow up phone calls to people in both categories, they indicated that they have invested in many advanced technologies to secure their services from any misuse, but the authentication of online identities was considered to be the lacking element in all organisations that made their infrastructure incomplete when it came to G2C transactions.

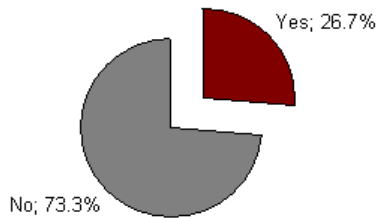


Fig 13: IT infrastructure readiness

3. What plans/strategies do organisations have, to go about e-government projects?

Only 26.9 percent of respondents indicated that they have an e-government plan but not a strategy and that 61.9 percent of them tasked information technology departments to create such plans and carry out the implementation (see also Figure 14).

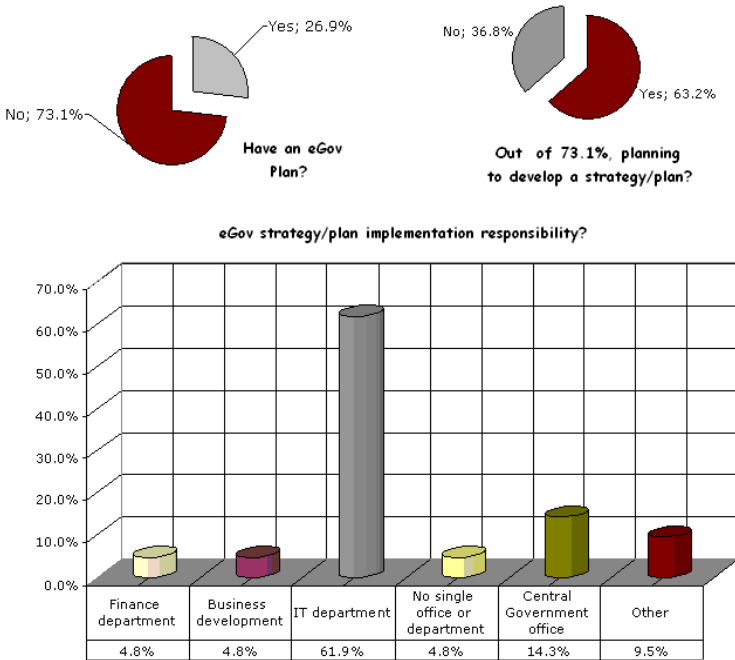


Fig. 14: e-government strategy

Two of the organisations indicated to have no clear vision or plan regarding their e-government, and said that they are in the process of appointing a consulting company to develop an e-government roadmap for their organisations.

During the course of interviews with the executive management it was found that almost all organisations had a draft blueprint for going about e-government programs. However, they claimed that those strategies do not address the one-stop-shopping concept, and it focuses more on internal organisational efficiency. Overall, many of the current e-government plans and strategies were believed not to address the G2C aspect, and are left to the ministries and other government departments to address.

Some organisations indicated that the information technology departments have better understanding of what e-government involves, as one explains: "the IT department knows more about these technological projects. " We tasked them to coordinate with other departments to create e-government plans. In this way, the other departments can focus on their core business." (Translated from an interview) This was a common and shared view among many of the interviewed executives.

This is also cited in literature as one of the key reasons that system projects fail. Information technology people tend not to know much about the business goals and strategy. Hence organisations get IT systems that are not aligned with the business strategy; a most common cause for project failure.

4. Impact of e-Gov on organisation's operations?

More than 30 percent of organisations indicated that e-government projects have increased the demand on forward thinking management and technical staff. It was also cited that such demand and skill shortages in different management and technical fields put upward pressure on wages. Follow up phone calls were made to get some clarification from those who reported a reduction in the number of staff as a result of e-government programmes.

The feedback received was that some of the re-engineering activities automated many of the internal processes reducing the size of the work forces. However, they also indicated that e-government projects have placed greater emphasis and demands on the need for solid project management and business process analysis skills, as well as the technical staff who can manage and administer complex technical systems.

It was also indicated during the interviews that many of the e-government projects caused a sharp rise in the use of outside contractors and consulting companies due to the complexity of the projects and to meet pressing deadlines. There was also this common view among many of the participants that e-government can improve the traditional service channel strategies, which enables governments to appear as one unified organisation and provide seamless online services. The following factors were also among the cited impacts of e-government as captured during the course of the interviews (see also Figure 15):

- improving business productivity (simplification of processes)
- efficiency and improvements in processing internal activities as well as public administration operations
- reducing expenditures through savings on data collection and transmission
- sharing of data within and between governments
- promoting information society
- public management modernisation and reform
- enabling citizen engagement
- promoting open and accountable government
- prevent corruption as it promotes more transparency

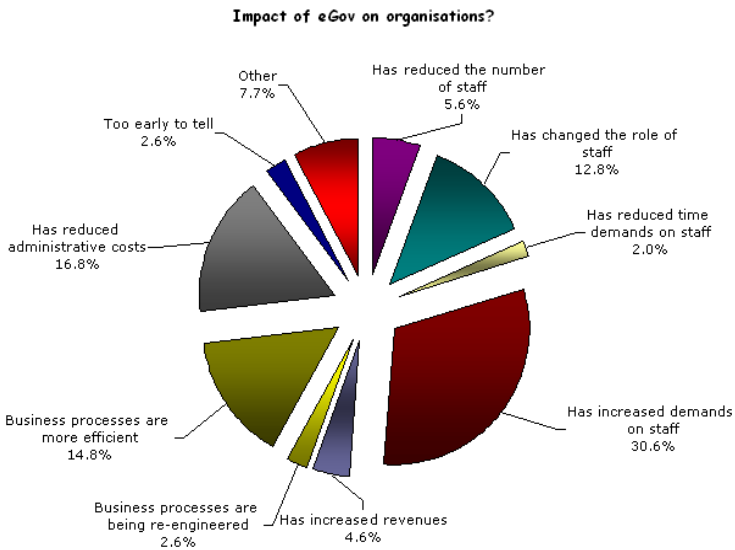


Fig. 15: e-government impact on organisations

5. What is the greatest obstacle to e-government initiatives as viewed by organisations?

Quite surprisingly, not one organisation indicated public concerns over their privacy to be an obstacle to e-government projects. Perhaps, this may be due to the culture and demographic nature of the studied countries. However, most organisations indicated to be using secure socket layer (SSL¹⁷) capabilities to ensure the privacy of information especially for financial transactions and the transmittal of sensitive information.

¹⁷ with SSL, data is encrypted, or scrambled, prior to sending it and then decrypting it on the receiving end. By encrypting the data as it travels the Internet, it is virtually impossible for the transaction to be translated if intercepted.

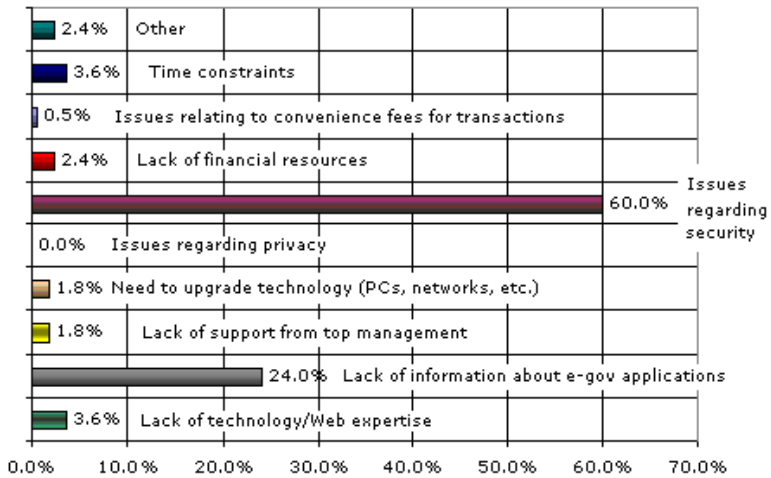


Fig. 16: e-government obstacles

As depicted in Figure 16, the majority of respondents (60%) considered security issues to be the primary obstacle to their e-government projects, whereas 24 percent indicated lack of strategic direction and information about e-government applications to be the second most concerning and challenging issue. It was obvious that security was a common concern among the interviewed executive management in all surveyed organisations.

Although organisations indicated to be using many security technologies, online identity verification was stated as the biggest concern that led to slow down their "e-services plans" where identity assurance was required. This finding is consistent with the findings of Javelin Strategy & Research's 2005 Identity Fraud Survey Report published in 2005¹⁸.

¹⁸ Javelin Strategy & Research's 2005 Identity Fraud Survey Report. Published in January 2005, this report was co-released by Javelin Strategy & Research and the Better Business Bureau, and served as an update to the Federal Trade Commission's (FTC) 2003 Identity Theft Survey Report.

Other organisations have indicated that although some services require authentication of their identities, and because of the pressure of the top management, they are offering those services online, but using intermediaries such as postal or courier services to authenticate peoples' identities before delivering government documents/products to them.

As a part of the study, the online identity problem was further investigated. The interviews showed that many of the surveyed organisations faced transactions where people presented false credentials or those belonging to others to take advantage of some of the services the government provides. Three organisations have indicated that they have pulled back some of the online services they provided on the Internet after discovering that some people provided false credentials to gain access to sensitive information and benefit from some of the government online services. This area was noted as a common concern at some sites, as one executive said:

"Though we have invested a great deal in information technology and communication security, we are being challenged with attempts from some people trying to play around and take illegal advantage of the services we offer on the Internet."

Another Interviewee said:

"we definitely need an identity management solution that guarantees to us the identity of those interacting with us online. Putting legislation in place that criminalises identity theft activities could be one part of the solution. But bear in mind that all those who perform such activities know that they are breaking the law. We need a mechanism to authenticate those people online."

More than 50% of the respondents indicated to be utilising personal details or passwords to authenticate online individuals (see also Figure 17). None of the respondents indicated to be using PKI or biometric technologies for their online services. However, many of the IT

department executives indicated that they are currently studying the possibility of introducing PKI and smart card technologies to address this growing area of concern.

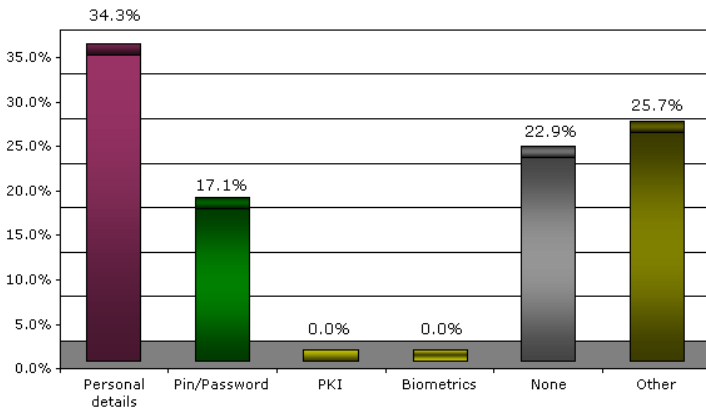


Fig. 17: utilised technologies for virtual identity authentication

6. How can national ID projects support e-Gov projects?

Though with some variations in the confidence level, more than 55 percent of respondents seemed to have confidence in biometrics to address the need for online verification. Around 38 percent had some doubts about its suitability for online usage, whereas less than 7 percent indicated to have no confidence at all (see also Figure 18). It was also found that during the interviews that some organisations were using smart cards and biometrics for authentication applications both for internal access control purposes, as well as for some public services such as airports¹⁹.

¹⁹ In Dubai International Airport in the UAE, the electronic gate (e-Gate) project was launched in 2002 to allow frequent flyers fast access through electronically controlled gates. This fully automated passport control system replaces manual checks with proximity smart card and fingerprint technology to identify and clear registered

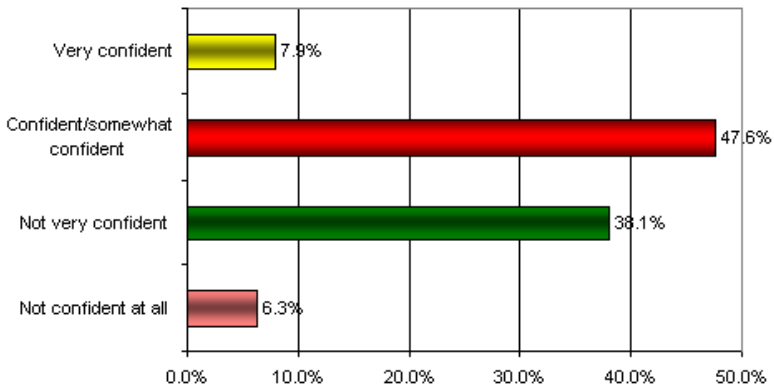


Fig. 18: level of confidence in biometrics

As depicted in Figure 19, more than sixty-four percent of respondents viewed national ID projects to more likely address homeland security than (online) identification of people.

Only 29.7 percent indicated that they think national ID projects will support e-government projects, and 51.6 percent indicated their lack of knowledge in this regard.

passengers. It is also the intention of the government to use the new national ID card, and the (thumb prints) stored in the chip of the smart card for auto immigration clearance without the need for registering for e-gate service anymore.

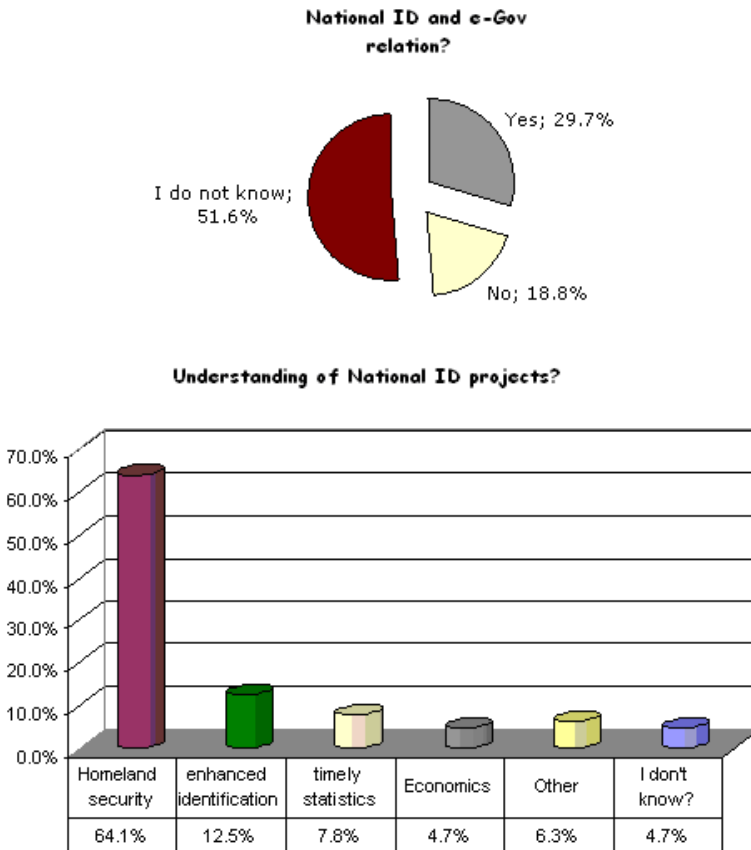


Fig. 19: Awareness of the relationship between national ID projects and e-government

Many of the interviewed executives believed that their governments need to put in place appropriate mechanisms to identify people online, as one executive explains:

"I agree with the fact that the government has the responsibility to provide its population with identification means that proves their identities and who they are. Today, there is pressure from the top to automate our operations and put the 'e' in our services. Whether through a national ID or other programmes, the government should provide the people with an 'e' identity that we can use to authenticate them online" (translated from the interview).

A common view among the interviewees was also that the new smart ID card will allow the citizens and residents to authenticate themselves in an easy and completely secure electronic way whenever they access e-government applications. Another claimed advantage of the new card was that it will allow individuals to put their own electronic signature to digital documents such as declarations or application forms, which will have the same value and legal status as the documents that are nowadays signed by hand.

6. DISCUSSION & CONCLUSION

The findings of this study are seen to be critical and have several implications for practitioners specially if attempting to understand some practices related to G2C e-government in the GCC countries. Overall, the findings in general suggest that organisations need to have a more global view of what e-government is all about as many organisations tasked their IT departments to champion e-government projects. E-government was seen more of an automation activity.

This study shows that G2C e-government initiatives in the surveyed countries, is progressing but in a slow motion because of the lack of a trusted and secure medium to authenticate the identities of online users. In the surveyed organisations, many managers stated that the lack of a reliable authentication medium is preventing them from enabling many of their services to online state.

Consistent with the literature, the analysis of questionnaire responses and data collected from interviews with managers revealed that, passwords remains one of the most popular approaches used currently to address online authentication requirements.

With little variations in the perceptions of their impact, many of the obstacles to e-government presented earlier were highlighted by management in the surveyed organisations as so.

Security and overall system integration were by far the most widely quoted obstacles. Many of the interviewed management indicated to have computerised almost all their administrative functions, and in many cases their core business and support functions as well. Many organisations indicated that they had formed review committees to review their corporate plans and facilitate communication between departments and to oversee the overall programme implementation. However, they appeared to have no structured approach to e-government strategy formulation and development.

Though each organisation had constituted a body in the form of committee or department to carryout the 'e-readiness' assessment and thereafter draft a strategic plan for the implementation of e-government, it seemed according to the interviewed executives to focus merely around G2G operations. The G2C was left to the individual ministries and departments to implement.

6.1 The smart ID card & e-Government

As viewed by many of the survey respondents and interviewees, governments must take the responsibility of putting in place a reliable identity management infrastructure. With the rapid evolvement of technologies, governments need to introduce new and stronger means of identification and authentication for its population.

Traditional paper and conventional ID cards do not cope with the nature of e-government environment which requires advanced

technologies to authenticate virtual identities over the web. Electronic authentication must be viewed as a fundamental part of the security infrastructure needed for the safe delivery of online government services that gives both the user and the service provider the confidence in the identity of the other party in a transaction. It is argued by the authors that initiatives such as national ID card schemes can very well address this requirement and can bring answers to many of the security concerns. The UAE national ID programme is a good example, as it aims to build a robust and secure national identity infrastructure.

The roll-out of this new national identity card in the UAE will mark a major milestone in the development of e-government due to the nature of technologies it utilises e.g., biometrics, smart cards and public key infrastructure. The use of these technologies is seen to provide a more secure and reliable G2C electronic authentication services. Indeed, such schemes would pave the way for greater penetration and usage of government services and reap the promising benefits of e-government. It cannot be re-emphasised much more that for governments to fulfil their critical functions, they must be able to authenticate their citizens' claims about their own identities and characteristics [14]. As digital government becomes a reality, the need for reliable digital identifiers becomes increasingly urgent (*ibid.*).

6.2 Further research

This study was aimed only at organisations in the GCC countries. However, additional work must be carried out if a better understanding of worldwide e-government programmes is to be established. Some areas in which further research may yield valuable insights for more comprehensive understanding and assist management in determining optimal courses of action are:

- (1) a follow-up study in the same countries with a larger sample of organisations to gain insight into their perspectives and practices in the field of e-government development and implementation and to test the findings of this study,
- (2) a similar study should be conducted in other countries that could show the findings reported here are indeed generalisable and might increase the robustness of the findings,
- (3) a study to shed light on the different views on power and control in organisations in relation to e-government adoption from both theoretical and empirical perspectives,
- (4) a field research for testing the impact of each identified obstacle to e-government programmes. This, in turn, should give a greater understanding of those obstacles and pave the way to put forward appropriate and/or develop frameworks that can overcome such obstacles.
- (5) understanding of the suitability of the national ID card with further detail as an authentication medium of online users.

As explained earlier, the authors intend to carry out a short practical study on the use of national ID card (item 5 above) as a medium for online identity verification, in a separate study.

ACKNOWLEDGMENT

The authors would like to thank those who participated in the survey. They also would like to extend their gratitude the reviewers who provided feedback that improved the overall structure and quality of this paper.

APPENDIX: RESEARCH QUESTIONNAIRE

Purpose

The purpose of this questionnaire is to investigate issues related to field of e-Government and its practices in GCC countries as part of a research project. This form is also available on the Internet for electronic submission. The web site can be found at: <http://www.alkhouri.itgo.com/research/questionnaire.ht-ml>. If you have any queries about this questionnaire or need additional information, please contact the researcher through the following e-mail address: alkhouri@itgo.com.

Date: _____
Name: _____
Position: _____
Organisation: _____
Telephone: _____

e.g., you may not provide your telephone number if you prefer and/or any of the other information.

All information will remain strictly CONFIDENTIAL

Part A: This section is to be completed by IS/IT managers.

1. Does your organisation have an Internet website?

Yes / No *(Delete as appropriate)*.

If "No", then do you intend to develop a website by this year or early next year? otherwise, go to question 2.

Yes / No *(Delete as appropriate)*.

2. Are you offering any online transactional services?

Yes / No *(Delete as appropriate)*.

If "No", are you planning to offer any online service(s) by next year? otherwise, go to question 3.

Yes / No *(Delete as appropriate)*.

3. Have your organisation performed any re-engineering of the manual processes/services before offering it/them online?

Yes / No *(Delete as appropriate)*.

4. How do you perceive your organisation on-line services in the following categories?

a. Online presence and downloadable files *(Please tick as appropriate)*.

b. automated online transactional services

c. integrated systems with smaller functionalities

d. integrated systems with real one stop shopping

Other

(Please specify)

5. What security methods do you use to secure online transactions?

a. Personal details *(Please tick as appropriate)*.

b. Pin/Password

c. PKI

d. Biometrics

e. None

Other

(Please specify)

6. Does your organisation have an IT infrastructure that supports your online services plans?

Yes / No *(Delete as appropriate)*.

If "No", then please clarify, otherwise go to question 7.

Part B: This section is to be completed by all.

E-government is the delivery of services and information, residents, 24 hours a day, seven days a week.

6. *From your current work position, what do you think are the main motives behind e-government initiatives in your organisation?*

- a. Legislative requirements [] *(Please tick as appropriate).*
- b. technology advancements []
- c. efficiency []
- e. cost effectiveness []
- f. services to citizens []
- g. constituent/(citizen) demand []
- h. Don't know []

Other

(Please specify)

7. *Do you agree that government services must be customer-centric?*

Yes / No

please specify why?

8. *Does your organisation have an overall e-government strategy and/or master plan to guide its future e-government initiatives?*

Yes / No *(Delete as appropriate).*

If 'no,' are you planning to develop a strategy/plan in the next year? otherwise, go to question 9.

Yes / No *(Delete as appropriate).*

9. *Who has overall responsibility for implementing this strategy or plan or currently looking after eGov initiatives? (Check only one)*

- a. Finance department [] *(Please tick as appropriate).*

- b. Business development []
- c. IT/IS department []
- e. No single office or department []
- f. Central Government office (specific Ministry or government department) []

Other _____
 (Please specify) _____

10. How has e-government changed your local government? (Check all applicable)

- a. Has reduced the number of staff [] (Please tick as appropriate).
- b. Has changed the role of staff []
- c. Has reduced time demands on staff []
- e. Has increased demands on staff []
- f. Has increased revenues []
- g. Business processes are being re-engineered []
- h. Business processes are more efficient []
- i. Has reduced administrative costs []
- j. Too early to tell []

Other _____
 (Please specify) _____

11. Please give an indication of your level of satisfaction with the services provided by your own organisation?

(Check only one, on a scale of 1 - very unsatisfied – to 5 - very satisfied)

Very unsatisfied 1 2 3 4 5 very satisfied

12. Which if any of the following barriers/obstacles to e-government initiatives has your local government encountered? (Check all applicable.) rate 1 to 7

- a. Lack of technology/Web [] (Please rate as appropriate).

- expertise
- b. Lack of information about e-gov applications []
- c. Lack of support from top management []
- e. Need to upgrade technology (PCs, networks, etc.) []
- f. Issues regarding privacy []
- g. Issues regarding security []
- h. Lack of financial resources []
- i. Issues relating to convenience fees for transactions []
- j. Time constraints []
- Other _____
- (Please specify) _____

13. In your opinion, what is the purpose of national ID projects?

- a. Homeland security [] (Please tick as appropriate)
- b. enhanced identification environment []
- c. timely statistics []
- e. Economics []
- f. I don't know []
- Other _____
- (Please specify) _____

14. If a biometric were used in these situations, how confident would you be that this technique would guarantee the identity of online users?

- a. Not confident at all [] (Please tick as appropriate)
- b. Not very confident []
- c. Somewhat confident []
- e. Very confident []
- Other _____
- (Please specify) _____

15. Do you think that if appropriate technologies such as PKI and biometrics were utilised, the national ID project will support your eGov

initiatives by means of providing a safe and secure verification environment?

- a. Yes (Please tick as appropriate)
- b. No
- c. I don't know

16. What would be the purposes of a national identity card?

- a. To prevent identity theft? (Please tick as appropriate)
- b. For voting purposes?
- c. To combat terrorism?
- e. To facilitate international travel?
- f. To replace many documents with a single card?
- g. To access government services?
- h. To combat illegal immigration?

Other

(Please specify)

17. If you have any additional comments, which you feel would be helpful to this study, in particular, any difficulties, important factors or considerations which have not been mentioned, please state them here.

18. If you have any additional comments, which you feel would be helpful to this study, in particular, any difficulties, important factors or considerations which have not been mentioned, please state them here.

If your answer is Yes, please make sure that you have included your telephone number at the front sheet.

We are very much grateful indeed for your help. Please return the completed questionnaire in the stamped addressed envelope provided to:

Ali M. Al Khouri, P.O.Box: 27126, Abu Dhabi, United Arab Emirates

Thank you once again for completing this questionnaire.

REFERENCES

- [1] A. Chadwick and C. May, "Interactions between states and citizens in the age of the internet: e-government in the United States, Britain and the European Union." *Governance: an International Journal of Policy, Administration and Institutions*, vol. 16, no. 2, 271-300, 2003.
- [2] S. Graham and A. Aurigi, "Virtual Cities, Social Polarisation, and the Crisis in Urban Public Space." *Journal of Urban Technology*, vol. 4, no. 1, 19-52, 1997.
- [3] K. Layne, and J.W. Lee, "Developing Fully Functional E-Government: A Four Stage Model," *Government Information Quarterly*, vol. 2, 122-36, 2001.
- [4] P.J. Windley (2002) "eGovernment Maturity" [Online]. USA: Windleys' Technolometria, Available: <http://www.windley.com/docs/eGovernment%20Maturity.pdf>.
- [5] P.R. Devadoss, S.L. Pan & J.C. Huang, "'Structurational analysis of e-government initiatives: a case study of SCO," *Decision Support Systems*, vol. 34, 253-269, 2002.
- [6] A. Leigh & R.D. Atkinson, *Breaking Down Bureaucratic Barriers: The next phase of digital government*. USA: Progressive Policy Institute, 2001.
- [7] P. Windley, *Digital Identity*. USA: O'Reilly Media, Inc, 2005.
- [8] Digital ID World (2004) 'What is Digital Identity?' [Online]. Digital World. Available from: http://www.digitalidworld.com/local.php?op=view&file=aboutdid_detail.
- [9] A.M. Al-Khouri, "UAE National ID Programme Case Study," *International Journal Of Social Sciences*, vol. 1, no. 2, pp.62-69, 2007.
- [10] C. Lambrinouidakis, S. Gritzalis, F. Dridi, & G., Pernul, "Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy'," *Computer Communications*, vol. 26, 1873-1883, 2003.
- [11] G. Hoinville and R. Jowell, *Survey Research Practice*. London: Heinemann Educational Books, 1978.
- [12] A.N. Oppenheim, *Questionnaire Design, Interviewing and Attitude Measurement*. London: Pinter, 1992.
- [13] M. Shipman 'Information through asking questions', in *The Limitations of Social Research* (third edition). London: Longman. pp. 78-115, 1988.
- [14] L.J. Camp (2003) 'Identity in Digital Government - A research report of the digital government civic scenario workshop' [Online]. Cambridge, USA, Kennedy School of Government. Available: <http://www.ljean.com/files/identity.pdf>.

DIGITAL IDENTITIES and the Promise of Technology Trio: PKI, Smart Cards & Biometrics ²⁰

Ali M. Al-Khouri & J. Bal

COPYRIGHT © 2007 SCIENCE PUBLICATIONS

ABSTRACT: This article looks at one of the evolving crimes of the digital age; identity theft. It argues and explains that if three key technologies were implemented together namely biometrics, smart cards, and PKI, then they can deliver a robust and trusted identification and authentication infrastructure. The article concludes that such infrastructure may provide the foundation for e-government and e-commerce initiatives as it addresses the need for strong user authentication of virtual identities

Key words: *identity theft, e-government, G2C, online authentication, biometrics, smart cards, public key infrastructure.*

²⁰ Al-Khouri, A.M. & Bal, J. (2007) "**Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics,**" *Journal of Computer Science*, Vol.3, No. 5, pp.361-367.

* The content of this article partially was presented at a national conference: Al-Khouri, A.M. and Bal, J. (2005) "**Identity theft and the promise of the technology trio,**" *Proceedings of 3rd Safety & Security Conference*, Abu Dhabi, United Arab Emirates.

* This paper was quoted in the: Summer '07 Intelligence section in *MIT Sloan Management Review*.

1. INTRODUCTION



“Someone got my Social Security number off the internet and stole my identity. Thank God — I hated being me!”

IDENTITY theft has become the fastest growing crime in the world ^{[1][2]}.

Undoubtedly, the expansion and increasing sophistication of identity theft threatens the adoption of many strategic information technology (IT) initiatives such as e-government and e-business ^{[3][4][5]}. Identity theft is an activity that takes place when an individual's personal details are taken over or stolen by someone else in attempt to impersonate him/her and have access to particular information or service, perform financial transactions, or even commit crimes. Identity theft has many and increasing links to organised crime.

As recently as 10 years ago, people would research to find someone who had died before they ever had a job. They would then apply for a copy of birth certificates in the names of those dead people, and use it to obtain other ID documents. However, with the advances in the field of information technology, identity theft has become much easier. For instance, more than 30 internet websites offer fake ID's for sales from as little as \$40 for a social security card, \$79 for a birth certificate and \$90 for a driving license from any US state.

Websites such as www.fake-id.org and www.phonyid.com offer driving licenses with similar security features issued by the US government from all the 50 US states for \$100 each, as well as Canadian ID's. Several hundred dollars buys one a complete ID set, including a military ID and a college diploma. Use of false identification is considered to be a significant threat to homeland security as well as personal and financial security of citizens. It is not easy to gauge the amount of identity fraud at this moment of time, however, the minimum cost to the economy in some countries is in excess of \$40bn per annum according to some official studies carried out (see for example: Federal Trade Commission report released in 2004; UK Cabinet Office report released in 2002).

According to Gartner's recent study, about 15 million Americans were victims of fraud that stemmed from identity theft in the period from mid-2005 and mid-2006^[6]. This represented an increase of more than 50 percent from the reported 9.9 million in 2003 by the Federal Trade Commission. Current research and studies refer to the advances and spread of computer technology as the main factor behind this dramatic increase in identity theft ^[7]. The literature shows that identity theft and fraud levels are increasing throughout the world (e.g., Canada, Australia, Britain, and Japan) with gigantic costs to victims and business^[8]. Some countries have introduced identity theft legislation that recognises such crimes and puts penalties and additional imprisonment sentences^[8].

However, countries around the world are realising that the legislation in itself cannot prevent or combat identity theft unless they adopt more effective and advanced solutions. One of the approaches pursued by many organisations both in government and private sectors is the employment of advanced technologies such as smart cards biometrics, and PKI. It is widely argued that if properly implemented, such technologies can provide secure and accurate identity verification,

enhance the security of the system and protect the integrity and confidentiality of information. The next few sections will look at these three technologies and explore them in further detail.

2. BIOMETRICS

Biometrics²¹ is defined as the science of using individual's unique physical, behavioural and biological qualities for identification purposes e.g., fingerprint, hand print, facial recognition, iris, voice pattern, etc. The first modern biometric device was introduced commercially over 20 years ago. Apart from being non-transferable among individuals, biometrics do not provide data about the person; but rather, information of the person.

The biometric industry found a global market through smart card technology. Biometric identity cards are being adopted in many countries around the world. Analysts predict biometrics to boom in the next few years, referring to the recently released report from the International Biometric Group (IBG)²², which indicated that the global market sales of biometric technologies will grow from less than \$1bn in 2003 to more than \$4.6bn in 2008, with fingerprint scanning becoming the most dominant technology, as illustrated in Fig. 1 below. Governments and businesses are increasingly adopting biometric technologies in the belief that they will make identity theft and multiple identities impossible.

²¹ The term "biometrics" is derived from the Greek words bio (life) and metric (to measure).

²² is the biometrics industry's leading independent integration and consulting firm, providing a broad range of services to government and private sector clients.

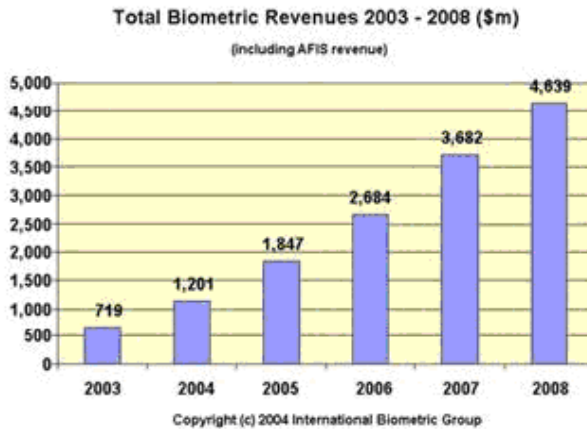


Fig. 1: Biometrics growth ^[9]

The National Physical Laboratory²³ conducted a performance evaluation test of several biometric technologies for a scenario of positive identification involving the following biometrics: face, fingerprint, hand geometry, iris, vein and voice recognition.

²³ The National Physical Laboratory (NPL) is the UK's national standards laboratory, an internationally respected and independent centre of excellence in research, development and knowledge transfer in measurement and materials science.

Iris recognition had the best accuracy, with 1.8 percent false rejections and no false matches in over two million comparisons as illustrated in Fig. 2 [10].

Of the other systems, fingerprint performed best for low false acceptance rates (FAR²⁴), while hand geometry achieved low (below 1 percent) false rejection rates (FRR²⁵). The study demonstrated that there is no one universal 'best' biometric system yet for both identification or authentication, rather a combination of two or more biometrics may enhance the FAR and FRR factors [11].

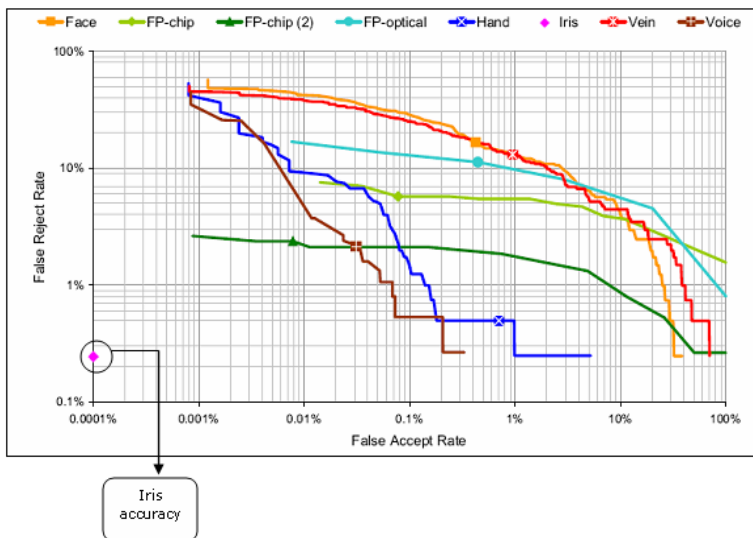


Fig. 2: National physical lab results: FAR vs. FRR [12]

²⁴ False Acceptance Rate (also referred to as **False Match Rate**): incorrect identification or fail to reject an imposter (**Imposter**: is a person trying to submit a biometric in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrollee).

²⁵ False Reject Rate (also referred to as **False Non-Match Rate**): fail to identify or verify a person

In another evaluation, the UK National Physical Laboratory prepared a comprehensive feasibility study into using biometrics as a means of establishing unique identity, to support the proposed entitlement scheme under development by the UK Passport Service and Driver and Vehicle Licensing Agency [12]. The purpose of the study was to assess the feasibility of three main biometrics namely fingerprint, iris, and face recognition technologies as a medium of identification in a national identity scheme and assessing the associated risks, and forwarding recommendations.

The feasibility study concluded once again that biometric methods do not offer 100% certainty of authentication of individuals and that the success of any deployed system using biometric methods depends on many factors such as the degree of the 'uniqueness' of biometric measure, technical and social factors, user interface, etc. However, and in principle, fingerprint and iris recognition were found to provide the identification performance required for unique identification over the entire UK adult population.

In the case of fingerprint recognition, the system required the enrolment of at least four fingers, whereas for iris recognition both iris were required to be registered. However, the practicalities of deploying either iris or fingerprint recognition in such a scheme were found to be far from straightforward in terms of the complexity of implementation, user training, etc. Other studies show that it is the device and the algorithm used that actually determine the effectiveness of the biometric in use. A recent study by the National Institute of Standards and Technology (NIST²⁶) revealed that fingerprint identification systems have approach-

²⁶ NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration, with the mission to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

ed 99 percent accuracy with some enhanced devices and, perhaps more importantly, a slim 0.01 false positive rate i.e., only about one in 10,000 scans resulting in a misidentification [13]. The study tested 34 fingerprint ID systems from 18 companies with about 50,000 sets of fingerprints from 25,000 people. The best systems reached 98.6 percent accuracy for a single-print match, whereas two-finger matches were accurate 99.6 percent of the time.

3. SMART CARDS

1970s	Smart Card Technology invented by one of the Schlumberger companies (i.e., Axalto) to curb fraud
1980s	First commercial applications as a pre-paid memory card in the public telephony sector, followed by the banking industry which incorporated microprocessor capabilities
1990s	telecommunication industry adopted smart cards as SIM cards
Mid 1990s	advent of Open Platform cards e.g., Java cards (invented in 1996) which boosted multi-application cards, Usage of complex cryptography and become a medium to store, carry and transact with digital signatures. Introduction of contact-less technology and the invention of combi cards (contact + contactless) in 1996-97
Late 1990s	Applications based on contact-less technology and the invention of combi cards (contact + contactless) in 1996-97
2002	Invention of .NET technology in 2002 which led to the increase of smart card memory capacity to 512 K byte

Table 1: Smart card developments

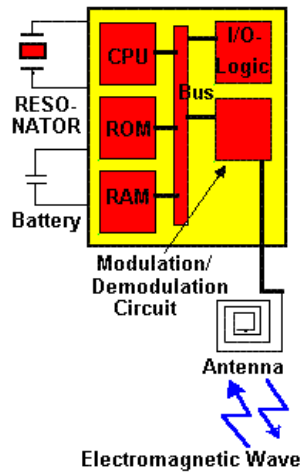
The 'smart card' is a plastic card with an IC (integrated circuit) chip capable of storing and processing data that may come with optional magnetic strips, bar codes, optical strips, holograms, etc, on a variety of card bodies. Developed in 1973 by the Frenchman Roland Marino, the smart card was not introduced commercially until 1981, when the French state telephone system adopted it as an integral part of its

phone card network. This led to widespread use in France and then Germany, where patients have had health records stored on the cards. Table 1 provides a highlight on the developments of the smart card from the 1970s to-date.

Due to their capabilities, they are increasingly popular in many industries around the world most particularly in telecommunications, but also banking, transport-tation (e.g., vehicle registration and driving licences) healthcare, insurance, and e- governance. With the increasing need for security, smart cards are being viewed as the ideal medium for implementing a secure identification and authentication infrastructure [14][15]. Smart Card chips normally look like in the diagram below (Fig. 3), with an integrated circuit built into it. This integrated circuit may consist only of EEPROM²⁷ in the case of a memory card, but may also contain ROM, RAM and a CPU.

As memory capacity, computing power, and data encryption capabilities of the microprocessor increase, many research studies indicate that smart cards are envisioned as replacing commonplace items such as cash, airline and theatre tickets, credit and debit cards, toll tokens, medical records, and keys. Fig. 4 provides further information about the emerging card technologies and their uses.

²⁷ (**E**lectrically **E**rasable **P**rogrammable **R**OM) A memory chip that holds its content without power. It can be erased, either within the computer or externally and usually requires more voltage for erasure than the common +5 volts used in logic circuits. It functions like non-volatile RAM, but writing to EEPROM is slower than writing to RAM. EEPROMs are used in devices that must keep data up-to-date without power. For example, a price list could be maintained in EEPROM chips in a point of sale terminal that is turned off at night. When prices change, the EEPROMs can be updated from a central computer during the day. EEPROMs have a lifespan of between 10K and 100K write cycles. **Source:** <http://www.gurunet.com>.


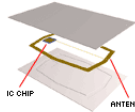
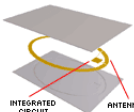
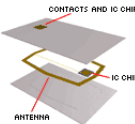
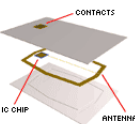


Contact Cards	The most widely used one. They have to be moved past a reader i.e., require insertion into a smart card reader with a direct connection to a conductive micro-module on the surface of the card
Contactless Cards	Require only close proximity (a few inches) of a reader.
Combi Cards	Could be used in both situations. Their main attraction is that one card could fill many purposes, such as credit card, bank card, membership card, ID-card, etc, all in the same card

Fig.3: Types of Smart Card

Smart cards are widely being adopted in many e-government and e-business initiatives as a vital element of a secure identification infrastructure and as a platform to hold both biometrics and PKI [16]. The next section will explain the PKI and its role in providing a higher trusted standard of authentication.

Fig. 4: Emerging card technologies [26]

Contact Cards	Contactless Cards	Proximity Cards	Hybrid Cards	Combi Cards
				
<p>Cards the size of a conventional credit or debit card with a single embedded integrated circuit chip that contains just memory or memory plus a microprocessor.</p> <p>Popular Uses: Network security, vending, meal plans, loyalty, electronic cash, government IDs, campus IDs, e-commerce, health cards</p>	<p>Cards containing an embedded antenna instead of contact pads attached to the chip for reading and writing information contained in the chip's memory.</p> <p>Popular Uses: Student identification, electronic passport, vending, parking, tolls, Ids</p>	<p>"Proximity cards" communicate through an antenna similar to contactless smart cards except that they are read-only.</p> <p>Popular Uses: Security, identification, access control</p>	<p>Cards containing two or more embedded chip technologies such as a proximity chip with its antenna and a contact smart chip with its contact pads.</p> <p>Popular Uses: Accommodates legacy system infrastructure while adding applications that require different e-card technologies</p>	<p>Cards containing one smart chip that can be accessed through either contact pads or an embedded antenna.</p> <p>Popular Uses: Mass transit and access control combined with other applications such as network security, vending, meal plans, loyalty</p>

4. PUBLIC KEY INFRASTRUCTURE

PKI is a framework for creating a secure method for exchanging information based on public key cryptography. It is widely considered to be one of the prime components along with smart card and biometric technologies to enhance the overall security of systems. PKI is known to provide two main features:

(a) security, and (b) encryption, to fulfil four vital requirements and establish what is called a trust environment (see also fig. 5):

- (1) authentication,
- (2) confidentiality,
- (3) integrity, and
- (4) non-repudiation

PKI encompasses a set of complex technologies as illustrated in Table 2 which shows the main PKI components. In a PKI environment, one would require a digital certificate, which usually contains the individual's public key, information about the certificate authority, and additional information about the certificate holder. The certificate is created and signed (digital signature) by a trusted third party; certificate authority (CA). The individual's identity is bound to the public key, where the CA takes liability for the authenticity of that public key, to allow a secure communication environment.

Security Policy	<ul style="list-style-type: none"> Defines requirements and standards for issuance and management of keys and certificates and the obligations of all PKI entities, and used to determine level of trust the certificate affords
Certification Authority (CA)	<ul style="list-style-type: none"> Authenticate subscribers, issue & manage certificates, schedules expiry date for certificates and revokes them when the validity period expires.
Registration Authority - (RA)	<ul style="list-style-type: none"> provides the interface between the user and CA. It verifies the identity of the user and passes the valid requests to the CA.
Certificate Distribution System	<ul style="list-style-type: none"> is usually through a directory service. A directory server may already exist within an organisation or may be supplied as part of the PKI solution.
PKI Enabled applications	<ul style="list-style-type: none"> is a cryptographic toolkit employed to PKI-enable applications e.g., communications between web servers and browsers, email, electronic data interchange (EDI), virtual private networks (VPNs), etc.

Table 2: PKI Architecture
Source: Certicom - www.certicom.com

The registration authority (RA) is where the individual or the organisation requesting the certificate is checked to ensure that they are who they claim they are. Another fundamental component of PKI is the certificate distribution system which publishes the certificates in the form of an electronic directory, database, or through an email to allow users find them. PKI enabled applications usually refer to applications that have had particular CA software supplier's toolkit added to them so that

they are able to use the supplier's CA and certificates to implement PKI functions such as in emails and networks for encrypting messages. The certificate policy, also referred to as certificate management system, is where the certificate procedures are defined including the legal liabilities and responsibilities of the involved parties.

Digital Signature: Based on a range of encryption techniques, digital signature; one of the essential services of PKI allow people and organisations to electronically certify such features as their identity, their ability to pay, or the authenticity of an electronic document. The digital signature also referred to as encrypted hashed text is a digital fingerprint; a value which is calculated from the information in a message through the use of a cryptographic hash function. Any change to the message, even of a single bit typically results in a dramatically different message digest.

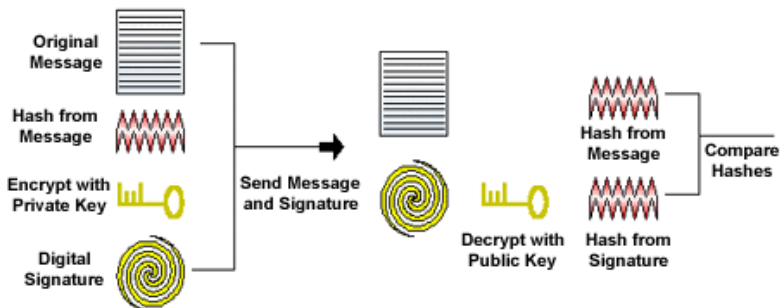


Fig. 7: PKI Trust framework

Figure 7 shows an example of a system generating a hash value from the message and encrypting it with the originator's private key. The message which could also be encrypted is sent along with the digital signature to the recipient who will then decrypt the digital signature with the sender's public key to change it back into a message digest.

If the decryption was successful then it proves that the sender has signed the message, because only him/her has the private key. The recipient then calculates the hash value out of the received message, and compares it with the message digest. If the message digest is the same as the message digest created when the signature was decrypted, then the receiver can be assured that the signed message/data has not been changed or tampered with.

In their study to understand the PKI infrastructure and how it may support electronic authentication and e-governments, [17] adopted an organisational framework to facilitate the understanding and classification of electronic services according to their security requirements (e.g. issuing birth certificates, submitting tax forms, conducting electronic payments, etc.).

PKI services	Security requirements											
	Availability	Performance	Management of privileges	Authentication	Logging	Integrity	Confidentiality	Non-repudiation	Anonymity	Public Trust	Untraceability	Secure storage
Registration			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/> ¹			
Digital Signatures				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>				
Encryption							<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>
Time Stamping					<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Non-repudiation								<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Key Management				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Certificate Management				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Information Repository								<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Directory services				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
Camouflaging Communication							<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> ¹		<input checked="" type="checkbox"/> ¹	
Authorisation			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>								
Audit								<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
TTP to TTP interoperability				<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>		

¹ Not in the context of e voting.

Table-3: Use of PKI services for fulfilling e-government security requirements [17]

The findings of the study demonstrated that the security services offered by the public key infrastructure can be employed for fulfilling most of the identified security requirements for an integrated e-authentication platform and a one-stop e-government portal as illustrated in Table 3. However, other requirements like availability, performance, un-coercibility, un-traceability, and anonymity could not be fulfilled, and additional security measures were found necessary.

In addition, several studies have proved that PKI is the state-of-art technology in the field of digital authentication and overall security infrastructure [17][18][19]. Nonetheless, studies also show that PKI on its own will not provide maximum security for authentication unless it is incorporated with other security technologies such as smart cards, biometrics, virtual private networks, etc. [20][21][22]

5. THE APPLICATION OF THE TECHNOLOGY TRIO

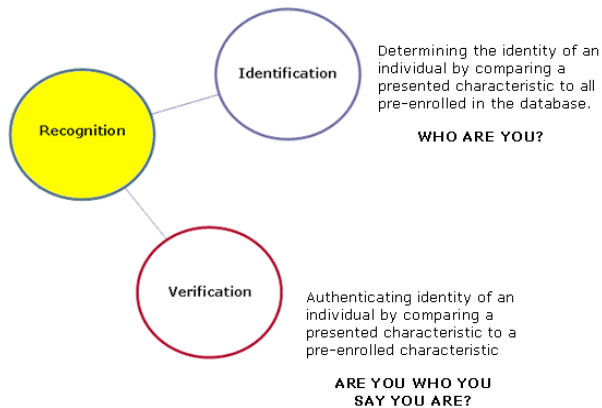


Fig. 8: Accurate identification/verification requirements

As explained earlier, statistical data in the literature provides horrifying data about identity theft and how much it is costing both public and private organisations. In order to combat identity theft, organisations need the means by which they can accurately recognise peoples' identities in two main forms as illustrated in Fig. 8:

- (a) identification (1:N) and
- (b) verification - also referred to as authentication - (1:1).

The technology trio of PKI, smart cards and biometrics is being widely considered to address the need for precise identification and authentication of individuals. They offer a solid business model that not only addresses high-level security requirements and strong authentication but also protects individual privacy and preserves resources. The adoption of these three technologies will create the two fundamental elements:

- (1) a trustful mechanism to identify and authenticate individuals,
and
- (2) a secure communication and transactional environment.

Smart cards, for instance, can serve as the issuer's agent of trust and deliver unique capabilities to securely and accurately verify the identity of the cardholder, authenticate the ID credential, and serve the credential to the ID system ^[23]. PKI, on the other hand, has emerged as the most reliable framework for ensuring security and trust ^{[24][25]}.

Apart from the main benefit of PKI in enabling secure electronic transactions, PKI can also be used to encrypt the data stored in the chip (e.g., personal information, digital photo, biometrics, etc.), in addition to the data stored in the database, to limit access to only authorised persons and entities.

Biometrics allows the padlocking of the person to the card. In doing so, the card cannot easily be transferred to another individual. In particular, given the current focus on the use of biometrics in ID card systems, it sets out architecture for strongly-authenticated identity cards that deliver (perhaps counter-intuitively) both enhanced security and enhanced privacy.

Through the incorporation of these three technologies in an identity management system, individuals are not locked into one form of authentication, but rather three different forms of authentication (see also Fig. 9):

- (1) *knowledge factor*: a password to ascertain what one knows,
- (2) *possession factor*: a token (smartcard) to ascertain what one has, and
- (3) *biometric factor*: biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is.

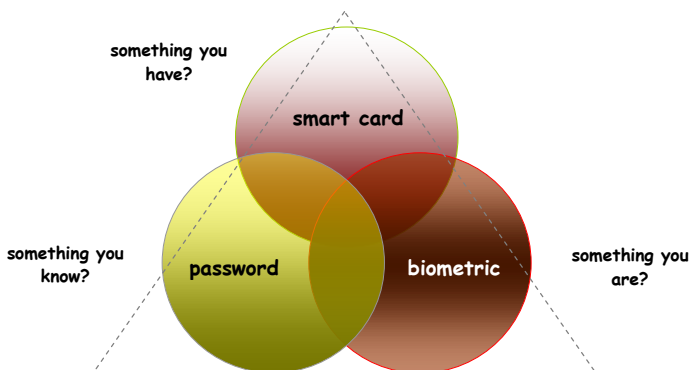


Fig.10: Three factor authentication

As such, if one factor has been compromised, fraudsters need to pass through another two levels of authentication. By requiring three forms of identification to access credentials, organisations will be able to bind card holders' (digital) identities on the card to their physical identities.

From an e-government perspective, the key to G2C e-government is authentication i.e., the ability to positively identifying and proving the authenticity of those with whom the government conduct business with. Without authentication, other security measures put in place for many G2C transactions can be ineffective.

The argument here is that for G2C e-government to progress, governments' need a strong online trusted authentication infrastructure, without which, their efforts is likely to standstill. In other words, governments need varying levels of authentication strength based on the value or sensitivity of their online information or services, balanced against other considerations like usability, deployment, and budget.

It is important to heed that the essence of G2C e-government is that transactions occur between people that are represented by machines. The anonymity of these transactions makes it more difficult to identify the parties involved and to ensure a trusted business relationship. Since all successful business relationships are based on trust, establishing online trust should be one of the primary goals of any e-government initiative^[23].

The focus must be building a trust environment that provides a high level of data privacy, data integrity, and user authorisation. Nonetheless, and as mentioned earlier that the real cornerstone of G2C e-business trust is authentication: that is, knowing with whom the government is doing business with.

PKI, smart cards, and biometrics are the technologies that are believed to be the key components of the trust model to address both electronic transactions security and online identity authentication. Using the power of the presented technologies in this article, government organisations and businesses alike can use varying levels of authentication depending on the level of security required for a particular transaction as depicted in Fig. 10.

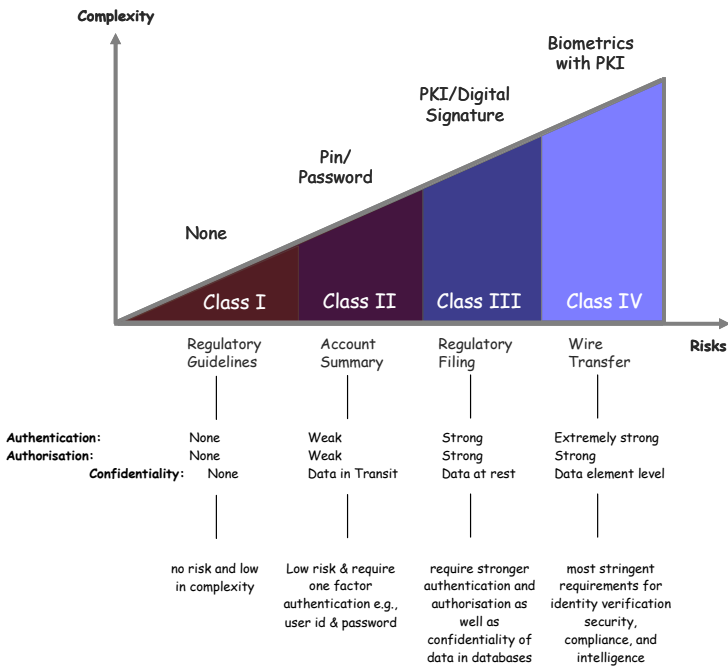


Fig.10: An example of types of authentication for G2C e-gov services

6. CONCLUSION

Organisations will be better able to protect their systems and assets with the application of biometrics, smart cards, and PKI, that provides them with a better verification of both physical and virtual identities. On the plus side, the principal advantage to be gained is more reliable authentication of identities. Without a doubt, strong user authentication must be viewed as the foundation for any e-government and e-commerce initiatives [17]. In fact, apart from improving traditional approaches to identification and authentication, these technologies are seen as the key to e-government, and a secure digital infrastructure.

This utilisation of the three named technologies in this paper should have a profound positive impact not only in terms of the reduction of identity theft and fraud activities, but having such an infrastructure should enable the improvement of current government services and paving the way for more investment in electronic services. In short, the promise of the technology trio is colossal. Hopefully, future applications and developments, implemented in well managed products will prove this right.

REFERENCES

- [1] Briefel, A., 2006. *The Deceivers: Art Forgery and Identity in the Nineteenth Century*. Cornell University Press .
- [2] Shute, J., 2006. *User I.D.: A Novel of Identity Theft*. Mariner Books.
- [3] Adams, J., 2003. E-Fraud Fight Prompts Credit Agencies' Cooperation', *Bank Technology News*, vol. 16. no. 6., p. 14.
- [4] Marcus, R. Hastings, G., 2006. *Identity Theft*, Inc. Disinformation Company.
- [5] Middlemiss, J., 2004. Gone Phishing, *Wall Street & Technology*, August, pp. 38-39.
- [6] McCarthy, C., 2007. Study: Identity theft keeps climbing, *CNET News.com*. http://news.com.com/21001029_3616476-5.html

- [7] Zalud, B., 2003. Real or fake?, *Security*, vol. 40, no. 3, pp. 12-18.
- [8] Anonymous, 2003. ID theft tops fraud list again, *ABA Bank Compliance*, vol. 2, p. 5-6.
- [9] *International Biometric Group*, www.biometricgroup.com
- [10] Mansfield, T., Kelly, G., Chandler, D. and Kane, J., 2001. Biometric Product Testing – Final Report, National Physical Laboratory, UK, <http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf>
- [11] Mansfield, T., 2001. Biometric Authentication in the real world, National Physical Laboratory, UK, http://www.npl.co.uk/scientific_software/publications/biometrics/psrevho.pdf
- [12] Mansfield, T. & Rejman-Greene, M., 2003. Feasibility Study on the Use of Biometrics in an Entitlement Scheme for UKPS, DVLA and the Home Office, National Physical Laboratory, UK: http://uk.sitestat.com/homeoffice/homeoffice/s?docs2.feasibility_study031111_v2&ns_type=pdf
- [13] McCearly, L., 2004. The Fact of Fingerprints, *The Resource for Security Executives*, <http://www.keepmed-ia.com/pubs/CSO>
- [14] George, T.C., 2003. The inside of a smart story: smart cards are increasingly becoming relevant in our everyday life, *Businessline*, Chennai, October 22, p. 1.
- [15] MacGowan, J., 2003. Smart Cards: Enabling e-Government, *Bloor Research*, <http://www.itanalysis.com/article.php?articleid=11151>.
- [16] Gardner, S., 2004. Europe Get Smart, *euro-correspondent.com*, www.eurocorrespondent.com/ed60_110-704.htm
- [17] Lambrinouidakis, C., Gritzalis, S., Dridi, F., & Pernul, G., 2003. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy, *Computer Communications*, vol. 26, pp.1873-1883.
- [18] Conry-Murray, A., 2002. PKI: Coming to an enterprise near you?, *Network Magazine*, vol. 17, no. 8, pp. 34-37.
- [19] Critchlow, D. & Zhang, N., 2004. Security enhanced accountable anonymous PKI certificates for mobile e-commerce, *Computer Networks*, vol. 45, no. 4.
- [20] Ellison, C. & Schneier, B., 2000. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, *Computer Security Journal*, vol. xvi, no. 1, pp.1-8.
- [21] Doan, 2003. Biometrics and PKI based Digital Signatures, *White Paper*, *Daon*, www.daon.com.
- [22] Kolodzinski, O., 2002. PKI: Commentary and observations, *The CPA Journal*, vol. 72, no. 11, p. 10.
- [23] SCA, 2004. Secure Identification Systems: Building a Chain of Trust, *Smart Card Alliance*, Available from: <http://www.smartcardalliance.org>.

- [24] Hutchison, R., 2000. E-Government: Walk before you run, *Canadian Business*, Toronto, vol. 73, no. 16, p. 36.
- [25] Russell, S., Dawson, Ed., Okamoto, E., & Lopez, J., 2003. Virtual certificates and synthetic certificates: new paradigms for improving public key validation, *Computer Communications*, vol. 26, pp. 1826-1838.
- [26] <http://www.idedge.com>
- [27] Al-Khoury, A.M. & Bal. J., 2007. Electronic Government in the GCC countries, *International Journal Of Social Sciences*, vol. 1, no. 2, pp.83-98.

IRIS RECOGNITION

and the Challenge of Homeland and Border Control Security in UAE ²⁸

.... *An innovative Technology Implementation*

Ahmad N. Al-Raisi, Ali M. Al-Khour

COPYRIGHT © 2008 ELSEVIER LTD.

ABSTRACT: This article discusses the implementation of iris recognition in improving the security of border control systems in the United Arab Emirates. The article explains the significance of the implemented solution and the advantages the government has gained to-date. The UAE deployment of iris recognition technology is currently the largest in the world, both in terms of number of Iris records enrolled (more than 840,751) and number of iris comparisons performed daily 6,225,761,155 (6.2 billion) in 'all-against-all' search mode.

Key words *border control, homeland security, biometrics, iris recognition.*

²⁸ Al-Raisi, A.N. & Al-Khour, A.M. (2008) "**Iris recognition and the challenge of homeland and border control security in UAE,**" *Telematics and Informatics*, Vol. 25, pp.117-132.

1. INTRODUCTION

TODAY security has become a top priority subject on many countries' agendas, as governments find themselves faced with continuous radical strategic challenges related to identity management and verification. Despite the fact that they will not be a panacea in every case, biometric technologies are at the forefront of these agenda discussions since they provide a highly accurate identity confirmation which makes it to be seen as a very effective answer to many security and identity management impediment issues. Recent advances in technology coupled with a significant price drop, and fuelled by the legislative requirements for positive identification and verifications, biometric industry is tremendously growing with an ever increasing market share as a viable alternative to upgrade security levels in local, regional and national security checkpoints.

The term *biometrics* refers to a wide range of technologies available in the market to identify and verify a person's identity by means of measuring and analysing various human physiological and behavioural characteristics. In order to make a decision of which biometric product or combination of products would satisfy stated requirements, different factors need to be assessed. Factors for consideration would typically include accuracy of a specific technology, user acceptance, and the costs of implementation and operation.

Table 1 summarises some of the important biometric features that need to be taken into account when comparing different biometric technologies. The iris is seen as a highly reliable biometric technology because of its stability, and the high degree of variation in irises between individuals. The discussion here in this article is limited to iris as the next sections will explore it in more detail.

Technology characteristic	Fingerprint	Iris	Facial	Hand
How it works	Captures and compares fingertip patterns	Captures and compares iris patterns	Captures and compares facial patterns	Measures and compares dimensions of hand and fingers
Cost of device	Low	High	Moderate	Moderate
Enrollment time	About 3 minutes, 30 seconds	2 minutes, 15 seconds	About 3 minutes	About 1 minute
Transaction time ^a	9 to 19 seconds	12 seconds	10 seconds	6 to 10 seconds
False nonmatch rate ^b	.2%–36%	1.9%–6%	3.3%–70%	0%–5%
False match rate (FMR) ^c	0%–8%	Less than 1%	0.3%–5%	0%–2.1%
User acceptance issues	Associated with law enforcement, hygiene concerns	User resistance, usage difficulty	Potential for privacy misuse	Hygiene concerns
Factors affecting performance ^d	Dirty, dry, or worn fingertips	Poor eyesight, glare, or reflections	Lighting, orientation of face, and sunglasses	Hand injuries, arthritis, swelling
Demonstrated vulnerability ^e	Artificial fingers; reactivated latent prints	High-resolution picture of iris	Notebook computer with digital photographs	None
Variability with ages ^f	Stable	Stable	Affected by aging	Stable
Commercial availability since	1970s	1997	1990s	1970s

Table-1: Important features of biometric technologies –
Source: Dillingham (2002)

This paper is structured as follows. First, some introductory background information is provided about iris and its characteristics. Then some accuracy and performance evaluation tests carried to date to measure its accuracy are put forward to highlight the reported findings. The following sections mainly deal with the iris implementation in the UAE from pilot to mass rollout phase. Some high level information is also presented about the system architecture and the recent statistics from the UAE iris system. The paper and prior to conclusion presents some lessons learned and a number of provisioned applications of iris in the future.

2. BACKGROUND TO IRIS RECOGNITION

Identifying a person from his/her iris record is a concept first thought of by Drs. Safir and Flom, American ophthalmologists (Flom & Safir, 1987). The algorithm underlying the iris recognition to read and map the data in a person's iris was developed by Dr. John Daugman, a Harvard PhD

graduate and a noted computer scientist at Cambridge University in England.

The US Patent 5,291,560 issued in the name of Daugman (Daugman, 1994) has been assigned to Iridian Technologies, Inc., one of the world's principal vendors of iris-based systems, to hold the exclusive worldwide patents on iris recognition (Heath, 2001). The iris pattern variability among different persons is enormous. No two irises are alike. Unlike DNA or even fingerprints, iris recognition works by performing exhaustive searches to identify individuals in real time.

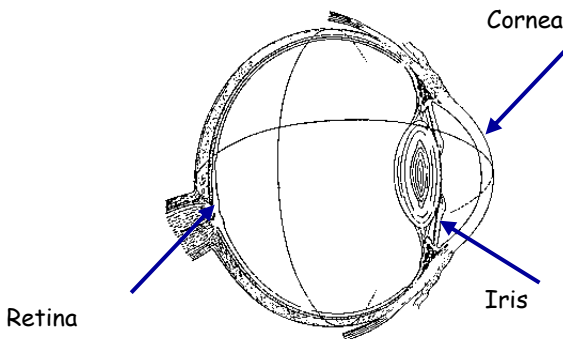


Figure-1: What is iris?

The iris (the coloured ring surrounding the pupil) has in excess of 266 mathematically unique characteristics. The retina on the other hand, is the hemispherical organ behind the cornea, lens, iris, pupil, and is not readily visible (see Figure-1). With no genetic influence on its development, the iris is permanently formed by the eighth month of gestation, a process known as "chaotic morphogenesis" (Daugman, 1993).

Contrasting other biometrics such as fingerprints, iris is seen as a highly reliable biometric technology because of its stability, and the high degree of variation in irises between individuals. Figure-2 demonstrates the variations found in irises.



Figure-2: college of irises

The likelihood of iris damage and/or abrasion is minimal since it is protected by the body's own mechanisms i.e., it is behind the eyelid, cornea and aqueous humour. Extensive research has determined that the human iris is not subject to the effects of aging and it remains unchanged in structure and appearance from the time it is developed and until a few minutes after death.

3. ACCURACY AND PERFORMANCE MEASUREMENT

The accuracy of a biometric system is commonly measured by two factors; false acceptance rate (FAR) and false rejection rate (FRR). Also referred to as a *type II error*, FAR is considered the most serious biometric

security error, as it represents the system instance of incorrectly accepting an access attempt by an unauthorised user. On the other hand, FRR, also referred to as a *type 1* error, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorised user.

A false rejection does not necessarily indicate a flaw in the biometric system. In a fingerprint-based system, for instance, an incorrectly aligned finger on the scanner or dirt on the scanner can result in the scanner misreading the fingerprint, causing a false rejection of the authorised user.

In general, there is typically a direct correlation between FAR and FRR. The lower the FRR percentage the higher the FAR percentage and vice-versa. Finding a medium that keeps both FAR and FRR to a minimum can be difficult. The degree of difficulty depends on the biometric method chosen and the vendor implementation.

For the reason that FAR and FRR are interdependent, it is important to determine the threshold values for these two factors (Liu & Silverman, 2001). Figure-3 plots the two factors against each other, where each point on the plot represents a hypothetical system's performance at various sensitivity settings. With such a plot, we can compare these rates to determine crossover error rate also known as equal error rate (EER) (Liu & Silverman, 2001).

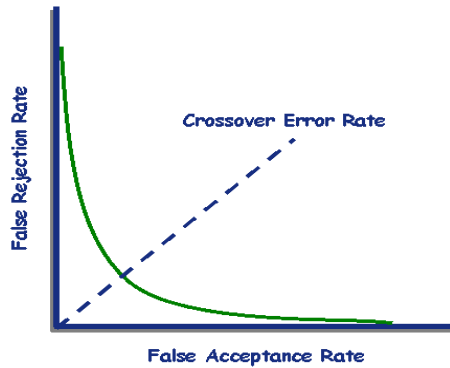


Figure-3: Crossover error rate attempts to combine two measures of biometric accuracy - Source: Liu & Silverman (2001)

This value indicates the error rate at which proportion of FAR equals the proportion of FRR. The lower the equal error rate value, the higher the accuracy of the biometric system. Another factor that needs to be considered with regards to accuracy measurement is the score known as the *hamming distance* that is discussed next.

3.1 Hamming Distance

In order to measure the difference or 'variation' between two given IrisCodes™, the hamming distance (HD) is normally calculated. The way it works is that when compared against each other (bit by bit), if the two bits are identical, the system assigns a value of zero to that pair comparison, and one if they are different as illustrated in Figure-4. If the distance between the two compared iris codes is below a certain threshold, they are called a match. In other words, if two patterns are derived from the same iris, the hamming distance between them, in theory, will be close to 0.0 due to high correlation.

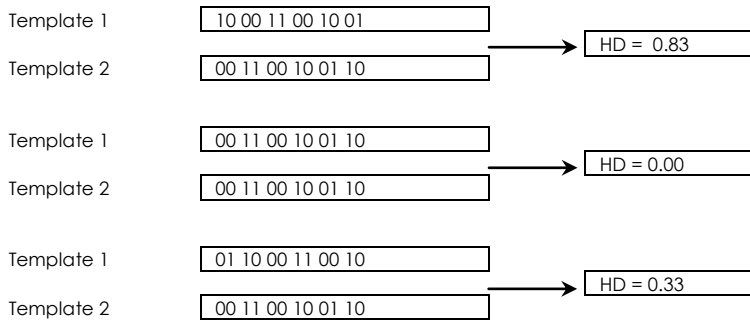


Figure-4: Iris matching and HD calculation - Source: (Daugman, 2005)

The smallest hamming distance corresponds to the best match between two templates e.g., a hamming distance 0.10 means that two IrisCodes™ are different by 10%. Furthermore, as it is the case with any biometric, as one may force the threshold lower, the likelihood of a false reject increases. In a comprehensive 200 billion cross comparisons carried out on the UAE Database by Prof. John Daugman of Cambridge University (discussed in section 10), not a single false match was found lower than the hamming distance of 0.262.

3.2 Performance Tests

Several performance and evaluation tests over the last nine years have identified iris recognition technology as the most accurate biometric. Table-2 depicts a summary of the different independent performance tests performed since 1996 to measure the accuracy of iris. The largest sample performed was by Prof. John Daugman in 2002, endured around 9 million comparisons and showed a surprising zero false match rate.

Testing Body	Year	Comparisons	False Match
Sandia Labs, USA	1996	19,701	None
British Telecom Labs, UK	1997	222,743	None
Sensar Corp., USA	1999	499,500	None
Joh. Enschede, NL	2000	19,900	None
Prof. John Daugman, UK	2000	2,300,000	None
Eye Ticket, UK	2001	300,00	None
National Physical Labs, UK	2001	2,735,529	None
Prof. John Daugman, UK	2002	9,200,000	None
Iridian Technologies, USA	2003	984,000,000	None

Table-2: Iris performance tests

Another evaluation was reported by the National Physical Laboratory²⁹ in April 2001. The performance test included evaluation of several biometric technologies for a scenario of positive identification involving the following biometrics: face, fingerprint, hand geometry, iris, vein and voice recognition as illustrated in Figure-5.

Iris recognition had the best accuracy, with 0.1 percent false rejections, no false matches in over two million comparisons and a 0.0% failure-to-acquire rate (Mansfield et al., 2001).

Of the other systems, fingerprint performed best for low false acceptance rates (FAR), while hand geometry achieved low (below 1 percent) false rejection rates (FRR). The study illustrated that there is no one universal 'best' biometric system yet, rather a combination of two or more biometrics may enhance the FAR and FRR factors (Mansfield, 2001).

²⁹ The National Physical Laboratory (NPL) is the UK's national standards laboratory, an internationally respected and independent centre of excellence in research, development and knowledge transfer in measurement and materials science.

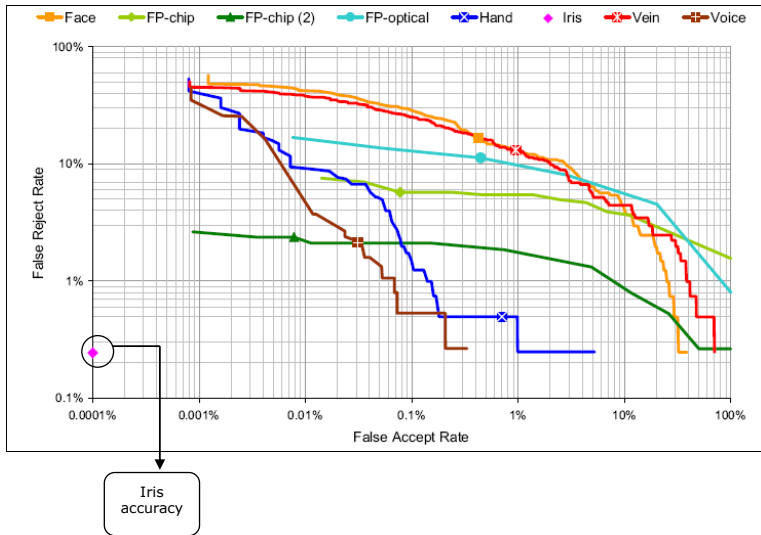


Figure-5: National physical lab results: FAR vs. FRR
 Source: Mansfield & Rejman-Greene (2003)

4. THE CHALLENGE AT UAE BORDERS

The border control system in the United Arab Emirates is comprehensively managed in accordance with strict pre-qualification and visa issuing processes. Border control forms a key aspect of controlling the various ports of entry and exit throughout the UAE.

The physical processes although not fully integrated, are functioning adequately at the various ports of entry. One of the greatest challenges the country is faced with is the repeated attempts of former expellees to re-enter the country (foreign nationals expelled for various violations). Various control measures were implemented to detect such cases. However, these measures appeared to be inadequate to control and detect the return of deportees back in the country. The analysis of the *status quo* revealed that despite the huge investment in information

technology systems at the Ministry of Interior, there was a clear gap in the accurate identification of a deported person who is back in the country either using fraudulent or genuine travel documents.

Officials at the border used to rely on computer systems to check the validity of the presented documents and run a parallel *data* check against the blacklist database to check for a hit. This showed a complete reliance on biographical data. The problem was that deported people were coming back to the country by changing their personal information such as name and date of birth and obtaining new passports that reflect these new details, which makes the task of identifying him or her unachievable.

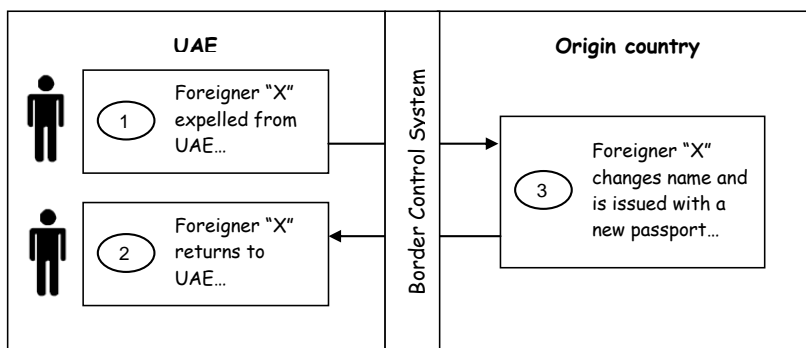


Figure-6: The challenge of returning expellees

Figure-6 shows a graphical illustration of such situations where a person is expelled from the country to his origin country. He changes his details and issues a new passport and returns back into the country, where the single point of failure is represented in the employed computer systems at borders making the existing control systems completely fail to detect such cases.

5. THE TECHNICAL SOLUTION

With extensive research and looking at the different lab results mentioned in section 3.2 above, the Information Technology Department at Abu Dhabi Police GHQ that was tasked to prepare a technical report on this matter, found out that biometrics would be a very effectual method to prevent illegal immigrants and former expellees from entering the country.

The desired biometric system was specified to be capable of scanning all incoming arrivals and provide positive or negative hit feedback. The department then prepared a list of requirements that were later translated into specifications for the desired biometrics solution. Following are some criteria cited in the specification document and was used for evaluating the different biometric options:

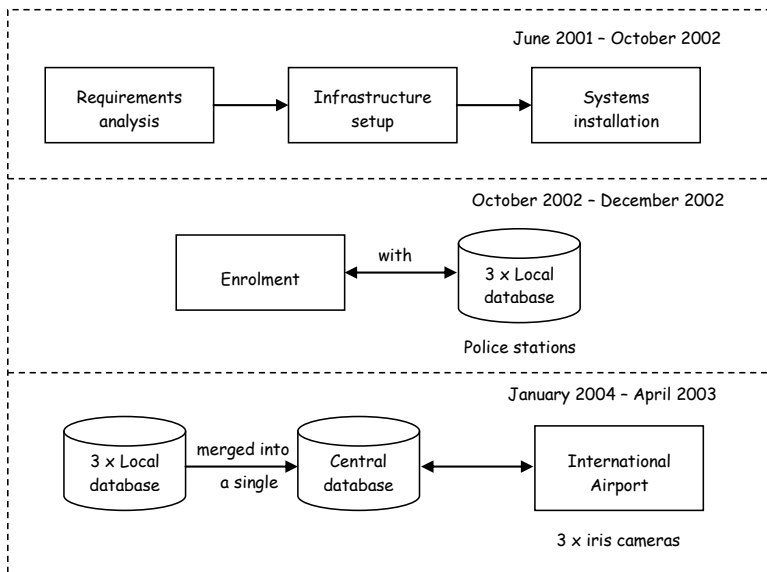
- can identify a single person from a large population of people.
- does not change over time.
- fast to acquire and easy to use.
- can respond in real-time needed for mass transit locations (e.g., airports.)
- safe and non-invasive (disease control)
- can scale in millions and maintain top performance.
- is affordable.

After extensive research and analysis of the different biometric products available in the market, iris recognition was found to satisfy most of the set requirements. Despite the newness of the technology at the time, the government decided to pilot iris and have a pioneering global seat in the implementation of such innovative technologies.

6. PILOT APPROACH

The pilot implementation took around a year and a half in total. The first stage of the pilot operation involved requirements analysis, infrastructure setup, and system installation as well as the enrolment of expellees at three police stations with local databases. The build up of the iris database i.e., the acquisition process continued for around 3 months.

The three databases were then merged into a central database hosted at Abu Dhabi police GHQ data centre as depicted in Figure-7. With only three iris cameras installed at Abu Dhabi international airport, the system was put to a real test.



Result = 50 people caught in less than 3 months

Figure-7: Iris pilot in the UAE

Surprisingly, the system was successfully able to catch more than 50 people in less than 4 months of operation with the small number of registered expellees, indicating a serious threat in the existing border control system at the time. The result of the pilot was enough to get the buy-in from the higher management and trigger a large scale implementation of the system across the country.

7. MASS ROLLOUT

The mass rollout of the system started in January 2003 and in less than five months, a total of 63 iris cameras were installed at 36 deportation (acquisition) centres and border control (recognition) points throughout the seven Emirates. The enrolment process involved the registration of inmates and expellees' irises from geographically distributed prisons and deportation centres throughout the UAE into a central iris database.

Today, the UAE is considered to be the largest national deployment site of iris recognition in the world. More than 100 iris cameras are installed in all 17 air, land, and sea ports including the deportation centres with a total number of 20 enrolment centres and 27 border centres.

Via secure national network infrastructure, each of the daily estimated 7,000 travellers³⁰ entering the country is compared against each of expellees, whose IrisCodes™ were registered in a central database upon expulsion. The real-time, one to all, iris-check of all arriving passengers at any UAE border point will reveal if the person had been expelled from the country.

³⁰ Travellers required to go through iris check are those who enter the country for the first time with a work permit entry visa, and those with visit visas from certain non-visa waiver countries.

It was again surprising sometimes how organised some criminal activities are. For instance, some of the encountered cases showed that people after being deported come back to the country in less than 24 hours with genuine identity and travel documents with modified personal information such as name and date of birth. The latest statistics from the system shows some absolutely amazing figures, indicating iris recognition effectiveness and the continuous attempts of those expelled to re-enter the country and challenge the system. The most recent statistics are presented in a later section in this paper.

8. SYSTEM ARCHITECTURE: HOW IT WORKS?

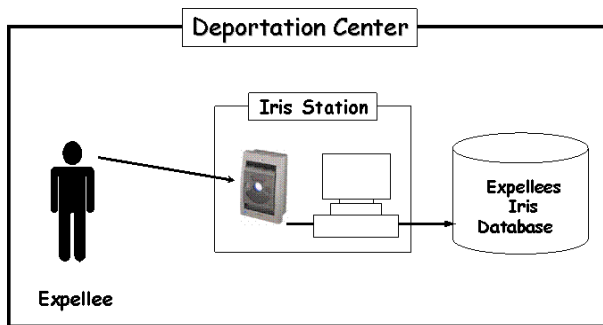


Figure-8: Expellees enrolment process

The enrolment process which usually takes place in prisons or deportation centres distributed around the country, takes less than 2 minutes. The process involves the scanning of the person's both eyes' irises, and storing them in the local database as shown in Figure-8.

IrisCodes™ collected at enrolment centres around the country are deposited into a central iris repository database, which performs database management such linking with geographical and time base

data, as well as update and maintenance. The local databases are synchronised with the central database with a user-set refresh call every 2 minutes (see also Figure-9).

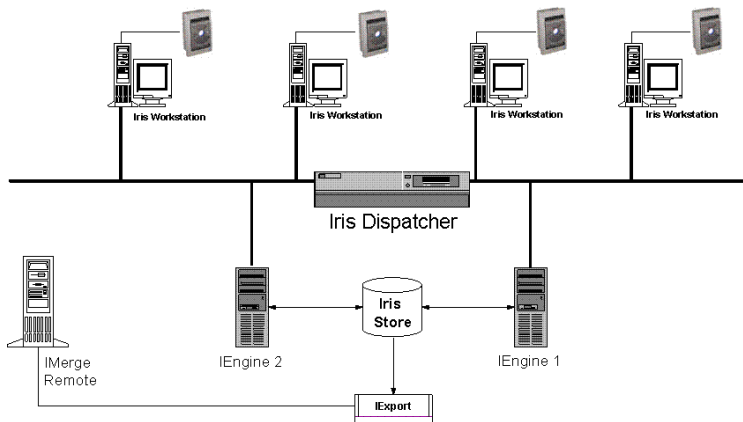


Figure-9: Typical deportation structure

8.1 System Platform and Components

The UAE system is constructed from a variety of Commercially Off The Shelf (COTS) components integrated with special Iris Technology cameras, interfaces and software. The databases of irises are all memory resident, offering unparalleled search speeds reaching more than 650,000 Iris comparisons per second. The operating system upon which the system resides is Microsoft Windows 2000 platform. All communications between the central repository and the geographically detached locations are encrypted TCP/IP communications (see also section 8.6).

8.2 System Performance and Scalability

A full enrolment process of a person does not take more than 30-45 seconds by a trained operator. This includes the enrolment of both irises and the typing of the associated biographical information. The overall search turn-around time does not exceed a few seconds.

It can perform over 650,000 Iris searches per second. The system architecture is designed to sustain scalability without any loss of performance. The central iris repository can be served by an unlimited number of search engines each capable of searching with speeds exceeding 650,000 irises per second.

8.3 System Threshold

All finds are reported at all border point as they are found. To assist the officer in interpreting the quality of the match, the following scale is used:

1. If score is within 0.03 of the reported HD, the score is a *MATCH*.
2. If score is within 0.03 to 0.04 of the reported HD, the score is a *HIGH MATCH*.
3. If score is greater than 0.04 of the reported HD, the score is a *VERY HIGH MATCH*.

8.4 Synchronisation of Central Database

As the enrolment process takes place in various geographically detached enrolment centres, the central database makes routing polls to each enrolment centre and reads in the latest set of information that may have been acquired by that centre since the last time the poll was

made. This user-set, regular and fully automatic procedure ensures that the central database is always maintained in an up-to-date state. The synchronisation process is designed to be performed without any interruption of service or slowing down the performance of any of the enrolment or acquisition centres.

8.5 Application Security

The system maintains a comprehensive audit trail that provides verification of all system related activities e.g., records creation and modification, sessions logs, found records by each workstation, number of searches performed, etc. Iris workstations are controlled by the central iris repository, which can disconnect remote workstations and redefine their search scope as well. Standard security and performance reports can be produced from the main site to monitor remote workstations at any time.

8.6 Data Security

All IrisCodes™ in the system are encrypted using TripleDES encryption system to provide maximum protection with a 192-bit key. All transmissions to and from the central database are also encrypted.

8.7 Fault Tolerance

The system is designed to handle an unlimited number of enrolment centres and remote iris workstations working simultaneously. Each enrolment centre can lose the connection with the central iris repository without loss of functionalities as each centre locally stores the IrisCode™ it enrolls and, if a communication link is open, the balance of the recently enrolled irises will be transferred without user intervention.

Therefore, the enrolment centre can continue to enrol people independent of the availability of a communications link. For obvious reasons, the recognition sites need online connectivity to the central iris repository to perform the search operations. Although not yet available, the authorities are studying to set up a disaster recovery site as a secondary backup central iris repository that will be synchronised with the main site. The enrolment sites will be configured to automatically switch over to the secondary site in case of failure of the primary.

8.8 Backup Procedures

Backups are performed automatically at enrolment centres as well as the main site on backup tapes and hard disks. The total time for each backup session does not exceed few minutes. The system during this process will become temporarily not available, and the end-users are informed automatically through the status displayed on the iris workstations.

No user intervention is required in any location for the backup to be carried out. The backup procedure can be configured to occur multiple times depending on the requirement. The system supports a frequency setting of 0 (no backup) up to 24 (once every hour).

9. CURRENT UAE IRIS SYSTEM STATISTICS

Item	Value
Database Size (IrisCode™):	840,751
Database size in bytes	2.8 Gbytes
New enrolments per day (rate of database growth per day)	700
Searches carried out between 2001 & 2005:	6,471,722
Average Searches Per Day:	7,405
Daily cross comparisons (billion):	6.23 (6.23 x 10 ⁹)
Expected next 12 months (trillion):	2.20 (2.2 x 10 ¹²)
Total Comparisons to date (trillion):	2.5 (2.5 x 10 ¹²)
Persons Caught:	56,484
Persons Caught/day:	90-100
Search Turn-around (including image acquisition):	3-4 Sec.

Date generated: 26 11 2005

Table-3: UAE iris system statistics

As illustrated in Table-3, the UAE owns to date the largest iris database in the world with more than 840,751 iris records representing more than 153 different nationalities. The time required for an exhaustive search through the database is about 3 seconds.

So far around 6.5 million exhaustive searches against that database have been performed. The iris system in the UAE has performed more than 2.5 trillion comparisons³¹ to date with a zero false match rate³² under the 0.262 Hamming Distance.

³¹ Each system search involves one eye being searched and found or not found in the database. A cross comparison involves comparing one eye to the whole database of 840,751. So one search will represent 840,751 cross comparisons. The formula used to calculate the cross comparisons is to multiply the number of searches by the size of the database. So if we do 7,405 searches per day against a database of 840,751, the total daily cross comparisons performed becomes: 6,225,761,155 or 6.23 billion per day.

On the average day, some 7,000 arriving passengers (peak of 12,142) are compared against the entire watch list of 840,751 in the database; this is about 6.5 billion comparisons per day with a sustained real-time response reported by all sites on a 24x7 basis. A total of 56,484 persons have so far been found on the watch list and seeking re-entry.

The number of searches is expected to rise considerably in the next few months as the government is currently studying to include more traveller categories to submit for an iris recognition at all UAE border entry points. The amazing results of the system lie in the fact that more than 56,484 people were caught at borders attempting to re-enter the country after being deported using both forged and genuine travel documents. To the stakeholders, this means a great return on investment.

10. THE UAE STUDY

The UAE study was based on 632,500 IrisCodes™ acquired from the UAE system, representing more than 152 nationalities, where they were compared against each other generating over 200 billion comparisons in total as shown in Figure-10. This task that was performed by Prof. John Daugman took more than four weeks of computing and human power effort in Cambridge University Labs.

The study showed extreme accuracy of iris and re-affirmed the management observations of the very high level of confidence in the collected IrisCodes™ and in all the subsequent matches that have taken place over the years in the UAE.

³² If a match is found say during the scanning of irises of incoming travellers at airports, the person is directed to another station connected to the immigration and black list system, capable of pulling the matching record which will typically show the person's particulars e.g., photo, name, expulsion data, crime, etc. The authorities would take action as appropriate.

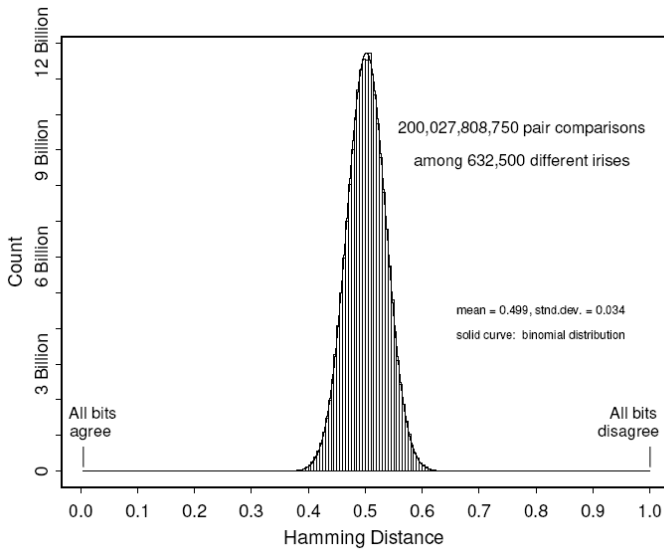


Figure-10: UAE study cross comparison results - Source: Daugman (2005)

From a technical perspective, the study examined the distribution of similarity scores obtained from comparing different irises, and likewise the scores obtained from comparing different images of same irises (see also Figure-10). These two distributions showed all cross-comparison similarity scores obtained from making all possible pair comparisons amongst 632,500 different irises. The cumulative scores of the distribution, up to various Hamming Distance thresholds, revealed the false match rates among the 200 billion iris comparisons if the identification decision policy used those thresholds.

HD Criterion	Observed False Match Rate
0.220	0 (theor: 1 in 5×10^{15})
0.225	0 (theor: 1 in 1×10^{15})
0.230	0 (theor: 1 in 3×10^{14})
0.235	0 (theor: 1 in 9×10^{13})
0.240	0 (theor: 1 in 3×10^{13})
0.245	0 (theor: 1 in 8×10^{12})
0.250	0 (theor: 1 in 2×10^{12})
0.255	0 (theor: 1 in 7×10^{11})
0.262	1 in 200 billion
0.267	1 in 50 billion
0.272	1 in 13 billion
0.277	1 in 2.7 billion
0.282	1 in 284 million
0.287	1 in 96 million
0.292	1 in 40 million
0.297	1 in 18 million
0.302	1 in 8 million
0.307	1 in 4 million
0.312	1 in 2 million
0.317	1 in 1 million

Source: Daugman (2005)

Table-4: observed false match rates

As shown in Table-4, no such matches were found with Hamming Distances below about 0.260. The table has been extended down to 0.220 using equation (7) for extreme value samples of the binomial (plotted as the solid curve in the above figure) to extrapolate the theoretically expected false match rates for such decision policies.

The performance test of the Daugman algorithms allowed conclusions to be drawn about the *numerical decision policies that should be implemented in large-scale identity searches to ensure the absence of false matches and to calculate confidence levels.*

The report stated the rule to be followed for decision policy threshold selection is to multiply the size of the enrolled database by the number of searches to be conducted against it in a given interval of time, and then to determine from the above table what Hamming Distance threshold will correspond to the risk level that is deemed to be acceptable. It is worth to mention at this point that the study was carried out by the inventor of the algorithm himself, and is deemed important that further studies need to be carried out to validate the results of this study.

11. LESSONS LEARNED

Following are some learned lessons that were captured during the implementation of the system.

As it might be the case with any system implementation, lack of operator awareness and training may lead to resistance due to incapability of understanding how the system works.

Periodic re-education and re-training programs were found effective to address this concern. Training programs played a significant role in promoting the appreciation of employee expectations and their willingness to accept the system as it eased the smooth implementation and operation of the system.

The system tested enrolment and recognition with people wearing eye glasses and contact lenses, and did not affect the accuracy or the speed of the system in almost all the times. However, dirty or scratched glasses in certain cases caused the inability of the system to capture the iris.

In general, enrollees and travellers were asked to remove their glasses at the time of image acquisition. Some tests were carried also with fun contact lenses. The system was able to successfully detect such cases; captured image was not recognised to carry a human pattern, and hence rejected.

As indicated earlier, the UAE database represents more than 153 different nationalities. The system did not encounter any incident where it was unable to enrol people because of their gender, age, or racial differences, as was the case in other deployments in other countries³³.

There were also those cases where some people used eye-drops to bypass the system. The eye-drops³⁴ were found to cause a temporary dilation of the Pupil, meaning that the use of this substance will lead to a false reject; the person is not found in the database when he is supposed to be found.

In abnormal cases of dilation using some of the identified eye-drops, the ratio of the pupil radius to the iris radius exceeded 60 per cent. (see also Figure-11).

³³ Other trial deployments in some countries faced problems such as enrolling Asian people and people with dark skin (black iris). The problem is most probably believed to be because of the type of utilised cameras which was not able to detect the irises of those people. With 6.5 million travellers who used the system in the UAE to-date, there is no single incident where the system failed to acquire an iris regardless of the gender, age, or racial differences.

³⁴ The most common use of this type of drops comes from ophthalmologists wishing to examine a patient's retina; the dilated Pupil helps the physician better see the inside of the eye through the pupil's large opening. The effect of the eye-drops is temporary and the eye is back to normal in a day or two.

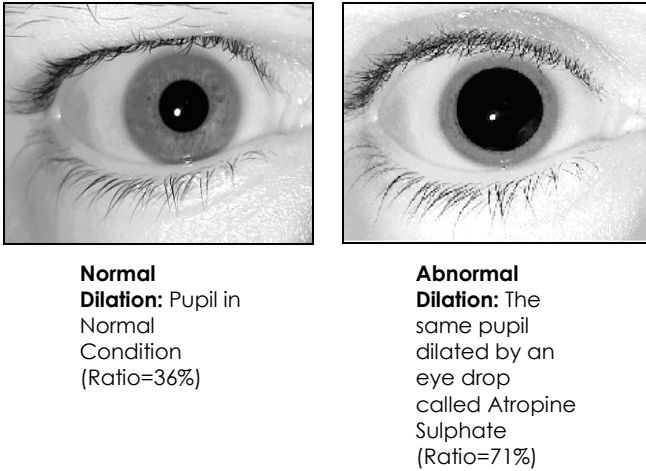


Figure-11: Pupil dilation

The UAE was a pioneer in solving this problem in iris. The system was enhanced to reject any acquisition of irises where the ratio of pupil to iris is greater than 60 per cent and show the ratio percentage on the screen for the operator.

In such cases a simple test was carried out using a pocket flashlight onto the eye. If no movement of the pupil is observed, then this person is most likely using an eye drop. A second check was required in a two-day timeframe after the effects had worn out.

Lighting and other environmental conditions were found to affect the acquisition process and therefore the functioning of the system. In many cases, calls received by the help desk reporting that '*the system is not working*', were caused by insufficient lighting at those sites. This required the authorities to improve the enrolment and acquisition centres to ensure that the sources of bright white light (windows) are closed and that no sources of light reflect off the cornea from the light sources and obscure the iris.

The accuracy of the iris system since its implementation was very much astonishing to the authorities. When it comes to enrolment, the system up to the time of writing this paper had zero cases of FTE (failure to enrol), meaning that it was never unable to enrol a person for whatever reason.

As for False Rejects, meaning how many times the system failed to find an expelled person thus allowing him into the country, the only measure to determine this factor was through the biographical information stored in the immigration system.

However, if the person changes this information, there will be no other way to determine this factor. This lies in the fact that the system is a negative application and should this happen, then it would not be reported for obvious reasons (i.e., a former expellee will be happy that the system has failed to recognise him).

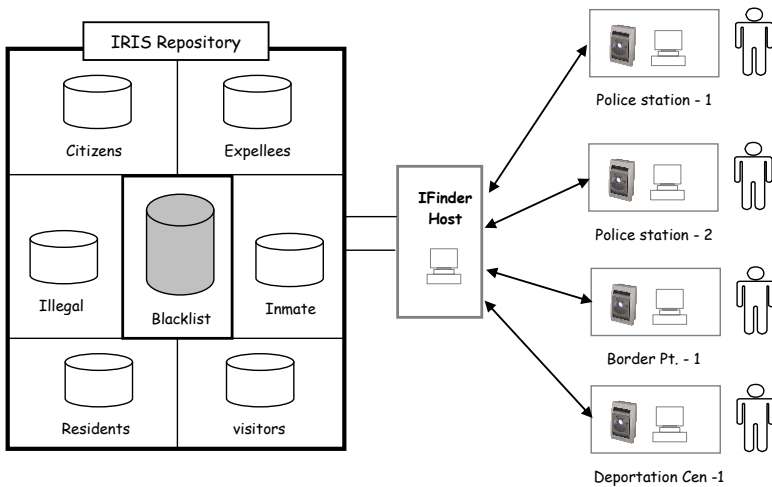


Figure-12: Proposed structure for a national iris repository

The local authorities invested in acquiring the most accurate cameras in the market and improving the acquisition environment as explained above. With this, the false reject rate in the UAE system is indicated to be no more than 0.01% according to the claim of the vendor. However, the system is designed to enrol both eyes of the person, where they both are checked at recognition sites (e.g., airports and border points), so if one eye experiences a false reject, the chance of the other experiencing the same is $0.01\% \times 0.01\% = 0.0001\%$ or 1 in a million.

12. FUTURE APPLICATIONS

With staggering results in the expellee project, the government is currently studying a proposed structure for building an integrated national iris repository for identification and verification purposes as depicted in Figure-12. Following are some key projects where iris is considered to play a complementary role to support other biometrics for identification and authentication purposes specially when rapid and real-time live detection is desired.

12.1 National ID project

This project is considered to be one of the most sophisticated technical projects in the Middle East, aiming to develop a modern identity management system that provides a secure and safe environment for the five million citizens and residents in the UAE. The government has plans to include iris as a supporting biometric in the national ID project besides its current fingerprint technology based card.

12.2 e-Passports

In a step towards enhancing its border security control, the UAE government is in the process to launch a project to issue RFID chip with biometric enabled passports (e-passport). Iris recognition is being considered for inclusion in the pilot program that is planned for execution towards the end of next year.

12.3 Electronically operated gates (e-Gate)

In 2002, an electronic gate (e-Gate) project was launched at Dubai International Airport to allow frequent flyers fast access through immigration via electronically controlled gates. This fully automated passport control system replaces manual checks with proximity smart card and fingerprint technology to identify and clear registered passengers.

The government have recently launched a larger scale of e-Gate project to cover all international airports in the UAE. Iris is considered as a viable option to support its current scheme and complement the currently used fingerprint biometric technology. The UAE and the UK Government (Immigration and Naturalisation Department – IND) are considering cooperating to use the same Iris technology to enter the UK and UAE.

13. CONCLUSION

Technology is evolving at a very rapid speed. As technological advances in terms of security, there are other groups of people who are always trying to penetrate such developments and exploit its weaknesses. Iris as other biometric technologies has been criticised for

inefficiency and ineffectiveness. The UAE accepted the risk and pushed itself to the pioneering seat and tested the system to become the world's largest iris database holder.

In its application in the UAE, iris has proved a quick, reliable means of checking identity. In fact, the results presented in this study clearly show some very interesting facts about the system performance. With 2.5 trillion comparisons performed to date on the system there was a zero false match rate under the 0.262 Hamming Distance.

The full database search (1:N) is performed in less than 3 seconds. Having the largest iris database in the world with more than 840,751 iris records, the UAE government is satisfied with the results gained to date and is committed to take part of the development of this technology as it is studying the incorporation of iris recognition in other high-tech projects such as electronic passport and national ID schemes.

ACKNOWLEDGMENT

The authors would like to thank Mr. Imad Malhas from IrisGuard Inc. for his feedback on this paper. They also would like to extend their gratitude to the editor and the reviewers of this article who provided feedback that improved the overall structure and quality of this paper.

REFERENCES

- [1] Daugman, J.G. (1994) 'Biometric Personal Identification System Based on Iris Analysis,' US patent 5,291,560, Patent and Trademark Office, Washington, D.C.

- [2] Daugman J.G. (2003) The importance of being random: Statistical principles of iris recognition. *Pattern Recognition*, 36, 279-291.
- [3] Daugman, J.G. (2005) The United Arab Emirates iris study: Results from 200 billion iris cross-comparisons. University of Cambridge, UK.
- [4] Dillingham, G.L. (2002) Aviation Security. Registered Traveller Programme Policy and Implementation Issues. General Accounting Office, USA [Online]. Available at: <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.88&file-name=d03253.pdf&directory=/diskb/wais/-data/gao> [Last Accessed 12 August 2005].
- [5] Flom, L., Safir, A. (1987) Iris recognition system. U.S. Patent No. 4,641,349, Patent and Trademark Office, Washington, D.C.
- [6] Heath, D. (2001) 'An Overview of Biometrics Support in NetWare Through NMAAS,' Novel, USA [Online]. Available at: <http://support.novell.com/tech-center/articles/ana20010701.h-tml> [Last Accessed 12 September 2005].
- [7] Liu S. & Silverman, M. (2001) 'A practical guide to biometric security technology,' *IT Professional*, 3(1), pp. 27--32.
- [8] Mansfield, T. (2001) Biometric Authentication in the real world. National Physical Laboratory, UK [Online]. Available at: http://www.npl.co.uk/scientific_software/publications/biometrics/ps-revho.pdf [Last Accessed 12 August 2005].
- [9] Mansfield, T. & Rejman-Greene, M. (2003) 'Feasibility Study on the Use of Biometrics in an Entitlement Scheme for UKPS, DVLA and the Home Office', National Physical Laboratory, UK, [Online]. Available: http://uk.sites-tat.com/homeoffice/homeoffice/s?docs2.feasibility_study031111_v2&ns_type=pdf

ABOUT THE AUTHOR



Dr. Ali M. Al-Khouri

Dr. Ali M. Al-Khouri is a senior UAE government official and is currently working with Emirates Identity Authority. He received his Engineering Doctorate degree from Warwick University where his research focused on the management of strategic and large scale projects in the government sector. He is a Certified Project Management Professional and a Chartered Fellow of the British Computer Society. He has been involved in many strategic government development projects, and lately the UAE national ID project as an executive steering board member and the chairman of the technical committee. His main research interests include the application of modern and sophisticated technologies in large contexts, projects management, organisational change and knowledge management

Email: ali.alkhouri@emiratesid.ae

ABOUT THE CONTRIBUTING AUTHORS

H.E. General Ahmad N. Al-Raisi

H.E. General Ahmad N. Al-Raisi is the Director-General for Central Operations at Abu Dhabi Police GHQ,, and Chairman of the Executive Board Committee at Emirates Identity Authority. He received his degree from Otterbein, Ohio State University in the United States, and is currently doing his doctorate research in London in the field of risk and disasters management. With projects ranging from force automation, administration and security systems, and fingerprint/PKI-based smart card systems to iris recognition, H.E. Al Raisi has championed many successful innovative and complex projects on both the local and federal levels. His research interests include strategic management and innovation.

Email: alraisi@adpolice.gov.ae.

Professor Jay Bal

Dr. Jay Bal is an Associate Professor, University of Warwick, UK. He joined the Rover Advanced Technology Centre at the University as "IT and Organisational Strategy" Program Manager in 1986 as a founder staff and set up a program of research and consultancy for the Centre. Concurrently he helped to develop Rover IT strategy and managed a number of key IT projects. Since joining the University Dr. Bal has devised and taught courses in Information Technology, Artificial Intelligence and on Design and Manufacturing systems in the Electronics Industry to senior managers in Hong Kong, Malaysia, India, China and South Africa as well as the UK. In the last five years he has published over 10 papers in International Journals, and spoken at many international conferences on aspects of EBusiness.

Email: jaybal@warwick.ac.uk.



Author Biography:

Dr. Al-Khoury is the Director General (Under Secretary) of Emirates Identity Authority; a federal government organisation established in 2004 to rollout and manage the national identity management infrastructure program in the United Arab Emirates. He has been involved in the UAE national identity card program since its early conceptual phases during his work with the Ministry of Interior. He has also been involved in many other strategic government initiatives in the past 22 years of his experience in the government sector.

He holds an engineering doctorate degree in strategic and large scale programs management from Warwick University, UK; Masters Degree (M.Sc.) in Information Management from Lancaster University, UK; and a Bachelors Degree (B.Sc., Hons.) from Manchester University, UK. He is also a member in several academic and professional institutions.

He is an active researcher in the field of advanced technologies implementation in government sector, and the approaches to reinventing governments and revolutionising public sector services and electronic business. He has published more than 50 research articles in various areas of applications in the past 10 years.

Papers Included:

Project Management

Projects Management in Reality: Lessons from Government IT Projects

An Innovative Project Management Methodology

Projects Evaluation

UAE National ID Programme Case Study

Using Quality Models to Evaluate Large IT Systems

Electronic Services

Electronic Government in the GCC Countries

Technology Implementations

Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics

IRIS recognition and the challenge of homeland and border control security in UAE

ISBN978-9948-16-736-5