The European Union's project for ENP South Countries
EUROPEAID/133918/C/SER/MULTI

Enhancement of the Business Environment in the Southern Mediterranean

National Seminar for Israel

« E-Government for Businesses »

Jerusalem, 5 December 2016

This project is financed
By the European Union

A project implemented by
GIZ IS and Eurecna

Disclaimer

This report has been prepared with financial assistance from the European Commission. The opinions expressed herein are those of the authors and may not represent the position of the Commission.

TABLE OF CONTENT

1. Introduction

The '**Efficient e-Government for Competitive Enterprises**' seminar was held in Jerusalem, 5th of December 2016, and was organised in close collaboration between the Small and Medium Business Agency, Ministry of Economy, the Government ICT Authority in Israel and the European Union funded regional project "Enhancement of the Business Environment in the Southern Mediterranean" Project (EBESM).

This was the second seminar held within EBESM project on e-Government (e-Gov) issues and builds on the first seminar that was held in Jerusalem in September 2014.

The seminar highlighted EU level as well as national efforts and resulting e-Gov Services where in particular **e-ID and open data and/or shared data** constitute important elements.

Representatives from various Israeli government agencies introduced each session (five in total) by showing existing solutions and ongoing initiatives in Israel. Examples were presented from Sweden, Norway, Denmark, Belgium, Germany, Austria and the European Union.

Based on the seminar's outcomes, this report presents the main seminar findings. Suggestions, based on the recommendations that were made during the seminar and in the concluding sessions, on potential next steps following the initial two seminars are also presented.

2. Main Findings

Many of the challenges that were captured in the report following the 2014 seminar remain.

Among the general challenges identified in 2014 the following are found:

- Data privacy;
- Information security;
- Lack of /sufficient/ information exchange across Government agencies (and other public sector entities);
- Insufficient use and availability of e-Gov Services;
- Lack of funding and resources; and
- Unclear or insufficiently founded business cases.

One of the most significant obstacles hindering the progress and roll-out of e-Gov services based on commonly used /open/ data was the lack of collaboration between and across agencies.

In the European Union (EU), the disparate national Member States solutions and legal frameworks slowed down progress in terms of creating a single digital market where information flows cross border in a secure and reliable fashion. New challenges have appeared in 2016. The rapid changes in the technology space create huge opportunities, but also emphasise the need for digital transformation in organisations that are not always prepared and equipped to successfully embark on the digital journey. During the seminar, the prerequisites that need to be understood in order to successfully transform an organisation

were discussed. These include both organisational changes, technical efforts as well as new ways of producing and consuming information.

Luckily, however, much progress has been made, both in Israel and within the EU. Legal measures such as the EU's directive on e-Invoicing, the eIDAS[1] regulation and the General Data Protection Regulation (GDPR)[2] will provide sanction and force harmonisation across Europe. Corresponding legislation is now in place in Israel to mandate and encourage sharing data in the public sector.

Overall, the seminar showed that legislation, organisations, technology and ongoing projects/pilots/programs are now slowly but steadily resulting in concrete outputs in terms of providing the necessary e-Gov services.

The seminar also showed that targeted support for SMEs should be improved. Suggestions at the conclusion of the seminar were that a potential follow-up seminar should focus on, and highlight examples of, e-Gov services that have contributed to the development and growth of SMEs. Such a seminar might be orchestrated to present "show cases" of successful e-Gov Services in Europe, based on specific input and guidance from the Israeli SME agency.

General observations

Critical success factors for e-Government, in general, are:

- **Understanding the demand** for relevant e-Gov Services at all public sector levels (national, regional, local);
- **Time-to-market**; velocity and handling and adapting to change;
- **Engaging the private sector**; unless the actual requirements, expected benefits and needs are understood, the risk is obvious that the efforts undertaken might derail and result in not-wanted solutions;
- **Sanction** (regulation, legal framework); a recurring conclusion is that sanction through legislation might in many cases be the decisive success factor;
- **Organisation**; "the right organising" is probably the organisation that is prepared to handle and embrace change and the organisation that not only accept but also use and tap into the power of digitization in order to provide e-Services to citizens, private businesses and collaborating public sector agencies.
- **Simplicity**; this might entail:
  - Supporting mobile solutions;
  - Providing relevant services, specifically services that will make life easier for the individual citizen as well as SMEs. Ensuring a user friendly and task oriented interface;

[1] For more information on the eIDAS regulation, please refer to https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

[2] For more information on the General Data Protection Regulation, please refer to http://ec.europa.eu/justice/data-protection/

– Ensuring that security, privacy and interoperability mechanisms are built-in from start.

Key Findings

Below, key findings, grouped according to the subjects (topics) that were covered at the seminar, are listed. In addition, a short description of the identified enablers is presented.

A - E-ID

- Mobile e-ID solutions are coming of age;
- Achieving cross border interoperability is challenging;
- Simplicity and accessibility is critical for secure and usable e-Gov services;
- Front (user) and Back (provider) side interests must be understood and the differences acknowledged. Recognising and understanding the stakeholders is a given starting point for any effort;
- A holistic viewpoint and understanding the relevance is key;
- Consensus, a supporting legal framework and a connectivity layer are recommended.

Enablers:

- Coordination mechanisms between administrations;
- Enabling legislation such as the right of electronic services for citizens and businesses and/or digital by default measures;
- Basic businesses blocks to assist administrations in deploying eGov.

B - Sharing data - Open Data

Data only once[3] saves time and contributes to the value chain - reducing administrative burden and costs by streamlining processes and dramatically cutting the processing time of workflows. “Only once” can be applied on different scenarios and takes on a slightly different meaning depending on where and how it is applied. In this context, “Only once” means that data is gathered only once and from a single source (i.e. virtually single source, not necessarily physically single source). The common “Only once” principle can also be applied to the scenario where a citizen only need to contact a single authority, even though multiple authorities might be involved in the process / workflow involved in order to provide the requested service for the citizen.

[3] See also: https://joinup.ec.europa.eu/event/egovernment-and-reduction-administrative-burden-applying-%C3%A2%E2%82%AC%CB%9Conce-only%C3%A2%E2%82%AC%E2%84%A2-principle

A basic principle is to base the data only once solutions on open, known and interoperable standards. Sharing data and providing Open Data support the digital single market.[4] To get the trust needed, the existing rules such as laws, regulations or practices need to be catered for and, if needed, amended to accommodate for the use and reuse of data. To extend Once-Only across borders, increased collaboration with existing open source and market solutions is needed. Reuse and avoiding duplication are key success elements.

Enablers

- As with e-ID, coordination and collaboration between administrations is important;
- Exposing shared data in a commonly available repository. In particular, a "common repository" doesn't necessary require a common, single persistence mechanism; the commonality might be achieved by a data storage that is set up as a single source virtually, even though it physically is dispersed and persisted in multiple physical sources;
- Legislation to support and encourage authorities to share and expose data.

3. Seminar content

1 – Welcome and Opening Remarks

Mr Ran Kiviti - Director at Small and Medium Business Agency
Heavy regulation and bureaucracy are preventing the support for SME's in Israel. Thanks to the European Commission for enabling the seminar through EBESM.

Mr Yair Frank - Government CIO and Head of ICT Authority
The Digital transformation is ongoing. Israel is a "startup" country. Heavy investments are made in Venture Capital & Innovation (a leader globally). Examples of successful efforts were presented, where the process time have been greatly reduced.
Moving from "ministry cantered" to "citizen cantered" is key. With a complex population as well as more than 30% Arabic speaking citizens it is needed that Israel can overcome the digital innovation and barriers by being lead on new digital implementations.

Mr Aljoscha Gütermann - GIZ, Project Manager, EBESM
Thanking the Israeli host for the opportunity to do this seminar. And provided some background information regarding the EBESM project, where digitization is of course key. This seminar will focus on e-ID and sharing data and open data, key cornerstones in the provisioning of e-Gov services.

Session 1: Setting the Scene, Introduction and Background

Mr Anders Kingstedt - Expert, EBESM:
Anders introduced the team of experts - mentioning in detail some of its core competences. He made reference to the 2014 seminar on *inter alia* privacy, GDPR, and the conclusion that sharing information across agencies is key. This conclusion bridges to this seminar.

[4] The Digital Single Market strategy is made up of three policy areas or 'pillars'
- Improving access to digital goods and services
  Helping to make the EU's digital world a seamless and level marketplace to buy and sell.
- An environment where digital networks and services can prosper
  Designing rules which match the pace of technology and support infrastructure development.
- Digital as a driver for growth
  Ensuring that Europe's economy, industry and employment take full advantage of what digitalisation offers.
  (ref https://ec.europa.eu/priorities/digital-single-market_en)

Nowadays pressure is on the public sector with drivers like cloud first, mobile first, digital first, etc. creating both opportunities as well as requiring change. Anders refers to IDC studies that the 3rd platform consists of the technology drivers Cloud Computing, Big Data, Social Business & Mobility, and that the 4th wave may be on the horizon like with ambient ICT, biometrics and augmented and virtual reality coming of age.
Given these, three principles to act on are:
(1) every organisation is a software organisation;
(2) innovation equals code and data;
(3) industry cloud will be the main market route.

Some of the many enablers seen are sharing data and open data, business intelligence, integration and interoperability, cloud, device- and technology agnostic solutions, standards, and eID.

Anders referred to EU initiatives, in particular eSENS, regulation like GDPR and eIDAS. There however still is a dependency on big non-European global players. A Swedish case study is presented where processing of economical support decisions could be cut from days or weeks to seconds through sharing information amongst agencies.

Session 2: Digital Renewal of the Public Sector - Challenge to realise the potential of open data

Ms Ilina Pinshaw - Director of Special Projects, Government ICT Authority
Databases open by default is now a government decision in Israel. Agencies increasingly go for open data. The links across data sets is critical to make open data meaningful. Examples of successful projects are the Pension agency, Ministry of Transport, Ministry of Education, etc. Ministries consult with the public to prioritise which databases shall be made public next. Data driven innovation is seen as a driver. Ilina called for all ministries present in the seminar to engage with the ICT Authority to identify further open data project opportunities. Adding data from other sources than government data sources is also necessary. In addition, the data needs to be shared at all levels of the public sector from municipalities to the national level.

Mr Carsten Schmidt: Expert, EBESM - Project Coordinator for the large scale pilot eSENS.eu project:
Carsten provided an overview of the eSENS project, its specific goals and potential outcomes. Carsten referred to the three pillars of Digital Public Services: “Digitize and Enable”, “Connect” and “Engage”.
Policy priorities seen are modernising public services, enabling mobility of citizens, and facilitating digital interactions. Generic transport standards to transfer information is key.
Policy measures in Germany are the e-Government law, the e-Justice law, a national IT security law, and the National Digital Agenda. The Only once principle is seen as rooted already in data protection regulation. Standards are seen important. A question is whether federal public clouds are needed. International impact is evident, as economic relations are there - like if e.g. Estonia introduces a new transport mechanism it may as well influence Germany.

A “reality check” is also necessary - unless you *understand what is actually of interest for the citizen / SME, you might fail* (even though the actual solution is correct).

ePayment and eStorage (short & long term) are two critical and prioritized e-Gov services. “Accessibility” is an important aspect - making sure that uneducated users and disabled users have access is very important.

German goal: eProcurement to become fully transparent, exposed in the eJustice portal.

Discussions in this session revolved around the following:

a) What would be the steps to be taken to make SME access practical?
Carsten referred to the eIDAS Regulation that is an enabler on eID, eSignatures, etc.

b) What is the German approach on data privacy, such as on data location, cross-border transfer, etc.?
Carsten responded that Germany follows decentralised approaches in keeping the data where it has been created. The national law (and in future GDPR) limits the possibility to share personal data.
Christian Rasmussen extended that privacy is also on the policies on the data sets.

c) Mr Yair Frank referred to Israel having two levels (federal and municipality), whereas Germany has three levels (federal, regional and local), what it's the approach to coordinate?
Carsten referred to the IT Councils to coordinate among levels, which indeed can be a challenge.

d) How is the sharing implemented, is it policy principles, is it coding principles?
Carsten saw that as a challenge with ongoing discussions, as Germany does not yet have that many services that share.

e) Which are the bodies that govern data sharing?
The receiving side needs to justify why data is needed and with involving the data subject consent is to be thought.

f) Where is data kept, at the municipality level or shared through the cloud?
Carsten responded that currently data is kept at the level where it is created (e.g. municipality)

g) How do you encourage authorities to share (non-personal) data?
Carsten referred to GDPR on information that should be made available by public administration - for personal data just with consent of the data subject.
Christian extended that Denmark started a strategy in 2007 where the number of municipalities has been reduced. These need to share data as it will be further explained in a following presentation on what the benefits are such as cost reduction.

h) What about digital divide, how are left behinds handled?
Germany considers both internal staff and the general public. For staff training programs are established. For the general public until at least 2025 the paper option remains.

Session 3: e-ID Solutions

Mr Yakov Gutkin - Manager at Identity Digital Unit, ICT Authority
Presentied the projects currently in the pipeline - where are we now and where are we headed. An e-ID smartcard is mandatory for citizens above 16, 800 k; such e-IDs have been issued. For government employees about 100 k certificates or cards are active. First working services was change of address (2016), about 500 k citizens are moving house. A major project is also SSO. SSO is meant as a username-password + SMS one-time password for all public services. A comprehensive identity management system with federation and authorisation capabilities is scheduled for end of 2017.

Mr Ofer Yarom Ishai - Project Manager at Identity Digital Unit, ICT Authority
The e-ID card was explained, it holds a signature certificate and an authentication certificate (validation). Biometrics are supported (two fingerprints and face).
A classical IDM triangle consisting of an Identity Provider, a Service Provider and the User is implemented in the e-ID card. But with "mobile first" mobile e-ID is needed. A software based approach is aimed in order to remain device-neutral. Hardware-based solutions are seen too challenging.
Yakov extended that e-IDAS is seen important by Israel, as interoperability with the EU is sought.

Frank Leyman Expert, EBESM - FEDICT, Belgium
Belgium organised early to cater for IT (The Belgium IT ministry was established in 2001).
Issuing e-ID cards for all citizens is an important part of the strategy. At the beginning expectations were different: What the government wants isn't necessarily what the citizen wants or what companies want. Starting points in the overall e-Government strategy were databases of citizens, companies, and the territory. The infrastructure is based on authentic sources, i.e. the organisation in charge of certain data maintains this, other organisations needing such data refer to that authentic source. The back-office infrastructure is based on a federal service bus. The eID card is seen just as a key to access services - like in Israel two certificates are stored (authentication and signature), the address is added electronically (to avoid replacing cards when moving house).

Future developments are considering adding a third certificate to link to the Population Register. Synergies with driving licenses and passports are sought with contactless chips for Cthe ICAO part (travel document).

An Identity and Access Management (IAM) tool has been implemented, it augments the identity information with roles under which the person acts. Attribute providers and a recently created roles database are consulted. The roles data uses authoritative sources like the company register.

Belgium is now moving towards Mobile Id, but got off to a slow start (2014). There's a "Royal Decree" in place to support Mobile Id solutions. As a citizen, *you can check your own data and who is using it.* To market the available e-Gov Services is key - building momentum is key as well.

Discussions in this session revolved around the following:

a) How is the private sector being engaged, as IdP, as Relying Party?
A strong relation is needed to know what technologies are developed. A further important aspect was getting card readers being installed in PCs by default, which was successful for laptops.

b) What is the process of changing PINs, as about 4k are changed per week?
The PIN can be changed by the citizen through the middleware.

c) What are the concrete mobile e-ID plans?
Initially it was discussed with one mobile network operator, later the project was opened up to further operators.

d) Can the private sector be a relying party? Are private sector interactions being logged?
The relation with the industry depends on what services are provided. Back-office services such as the federated service BUS are provided by private companies, but personal data cannot be accessed by these. For being a relying party the company needs to apply for with

the privacy commission. Only if an agreement is reached, FEDICT can be approached for getting access to the infrastructure.

e) Are there arguments pro and con with regard to having data in only in one database?
It depends, of course the databases need to be secured. If decentralised and stored on the card still the access needs to be considered, i.e. what is private data and what is accessible. The same holds for data in databases.

f) There are special e-ID cards for kids, are there also services for kids?
The primary reason for the kid cards was the need for a travel document. Later the card got used in schools for lectures within certain age groups. It can be used broadly for Secure Internet applications.

Session 4: Sharing data across government agencies

Ms Ravid Been-Zeev, Gov't ICT authority
New regulation (1933) taken in August 2016 is now in place in Israel to support transfer and sharing of data between and across agencies.
Its main goals are:

- Increased usage
- Lowering the thresholds and red tape

Example from day care management - the current situation imposes a heavy administrative burden on the administrator of the processes that handle day care aspects.

The starting point in terms of support its citizens which will be followed by private companies. Transition plans reach out up to 2022 (technical infrastructures by 2018, only once in the public sector in 2021, only once for citizens by 2022).

A pilot project constitutes the first step, in order to identify where information is located and how the data should / can be transferred.

Mr Christian Rasmussen – EBESM Expert - DTI Denmark
Creating value for citizens is key, whatever the project is – e-ID, data sharing, etc. Data only once saves time and contributes to the value chain - reducing administrative burden and costs. A basic principle is open, known and interoperable standards. This shall support the digital single market with its free movement of citizens, businesses and services. To get the trust needed, the existing rules like laws or practices need to be catered for.

To extend **Once-Only** across borders, increased collaboration with existing open source and market solutions is needed - reuse is key.

Denmark started in 2010 with an Open Data Innovation Strategy. Open standards are essential so that users can create value by analysing structured data. Joining forces like for example when multiple municipalities or several countries come together and form projects is more cost effective, this is particularly important for smaller countries. Regarding using the data, a snowball effect was seen with a few businesses in the beginning and more and more businesses joining over time.

The Danish project "Grunddata" (meaning "basic data") was born with the Open Data initiative. It entails and covers all the basic registrations of businesses and citizens. It has resulted in standardised ways to present data, as well as in increased data quality. Clear rules exist on who can access the data.

Reference to the TOOP project is made that aims at cross-border aspects of Once-Only Principle.

Discussions in this session revolved around the following:

a) What is needed in addition of once-only is also the availability of the data, so any participant should see himself as part of a production line, as unavailability may stop a process?

Christian referred to an ongoing effort on decentralising data to avoid single points of failure.

b) On data distribution, is that seen between federal and local services?

The approach followed was through data replicators, detailed descriptions exist.

c) How are privacy fears being approached to establish trust?

Citizens should get aware that there is value in sharing data. This needs trust in the actors, as citizens need to realize that data sharing does not lead to data leakage.

d) What are the geographical limits of sharing information?

Christian does not think that there is an actual limit, it is more mental barriers. Digital natives may have a more relaxed approach.

e) What is the significance of information structure, categorization and ontologies? Would you agree that the actual structure of data must be understood and controlled? The point being - unless you understand the very nature of information / data, it is difficult to assess which data to share.

Yes, structuring and classification of information is important – it is a matter of "information control" to a certain degree.

Session 5: Different e-ID solutions

Mr Herbert Leitold, EBESM expert - Secretary-General A-SIT

Key topics discussed: - Background - leading up to the present and the future eIDAS.

The first e-ID efforts started in the late 90s. The early solutions led to national "island's" - non-interoperable cross-border. E.g., STORK has operated on 100 different "systems" for e-ID. Different solutions exist - based on the national situation.

Whether e-ID is mandatory or voluntary varies throughout Europe, many times because of legal concerns or the national situation. The choice of e-ID is based on national situation and "preference".

Estonia and Belgium are examples of countries that require the use of e-ID cards. The mobile phone solution now outperforms smartcard eID in Austria by far.

Examples from Austria, Germany, Estonia and Norway are shown.

Herbert concluded by mentioning that the landscape in Europe is heterogeneous:

Creating interoperability - the Stork e-ID pilot. The experiences from Stork are a basis for the e-IDAS regulation.

Lessons learned from Stork: "Technology is not problem". Operational aspects such as change management are important. But legal issues are essential. That led to eIDAS.

eIDAS harmonises “trust services”. The e-ID solutions remain national level responsibilities. Notification of eID can be done at “different levels of assurance” (3), where the requirements related issuance and security are defined different for each level.

Discussions in this session revolved around the following:

In Israel - the signature act stems from 2001 and other legal frameworks are in place. Israel is now ready to move on. “*Everyone is eventually going to have e-ID cards*”.

Anders presented an example on Mobile Id used in Sweden, “**Swish**”, an application that is used to transfer money based single sign on solutions using the Swedish BankID solution for identification. The Swish application is very popular and now SMEs are starting to accept and use Swish as a means to make payment transactions. The simplicity and support for smart phone and the integration with Mobile ID are success elements. Another prerequisite is of course a reliable telecommunication infrastructure.

Session 6: Roundtable discussion

The discussions during the round table revolved around the following:

Sessions summary and highlighting some critical success factors and trends within the e-Gov space:

- Understanding the demand
- Time to market
- Private sector engagement
- The importance of “sanctions” through legislation / legal frameworks
- Simplicity
- Mobile eID emerging
- Simplicity and accessibility
- Differences between user and service provider views
- The difference between sharing data and open data must be understood

Potential next steps:

- Continue and accelerate collaborations (as done in the EBESM project)
- Benchmark and map existing solutions to the requirements in Israel
- Small scale project as pilots might create opportunities for concrete actions

Questions/comments from the audience:

- Leadership is critical
- There’s a “chicken and hen” problem
- ISO standards are important in Israel
- Cooperation with legal advisors is important

Frank added that the life cycle aspect /in e-ID/ needs to be understood - as well as the “business case”. *Can you skip smart cards and go to mobile solutions directly? Yes - maybe*.

Fraud - a concern? Yes, but not more so than with manual routines.

4. Recommendations

Interestingly, but perhaps not surprisingly, many of the recommendations from the 2014 seminar are still valid. The recommendations formulated during this seminar are summarised below.

a) Putting the User First

This recommendation remains unaltered. Unless the user perspective is understood and acknowledged, the obvious risk is that the outcome of any effort will be disappointing.

b) The "Once Only" Principle

This topic constituted one of the main "themes" of the seminar. The "Once Only" principle is key to streamlining processes and an important fundamental cornerstone for e-Gov Services. In particular, when sharing data, the underlying architecture and IT infrastructure should support the end user – citizens, government institutions, private companies, civil servants at municipalities etc. – to only have to enter and retrieve information once. The overarching key principle is – "citizen centric" not "government centric" (as illustrated in more than one of the presented slide decks).

In terms of IT architecture, setting up data transport services is one possibility discussed during the seminar.

The services are preferably grouped according to "domain" and/or "main purpose". For instance – one data transport service facilitating the exchange of necessary data for tax related services is set up and another for social welfare etc. Now, each data transport will manage and cater for the exchange of data with ALL agencies, at all public sector, that need to provide data for the task at hand. During the seminar, an existing service used by managers at municipalities in Sweden provide data from sources that persist at five (5) different agencies was described. The "base service" acts as the middle-man and acts on request from the municipality managers financial aid application. The process time was reduced from weeks to seconds when the base service was launched.
Elements that might need to be considered to support the once-only principle in summary include:

- Sanction (possibly changes in the existing legislation)
- Collaboration contracts (signed by all parties involved in the data exchange in only-once and data sharing scenarios)
- A service oriented architecture
- A clearly defined "business case", where the expected outcomes, needs and requirements are defined and successively validated

c) Accommodating the User

This recommendation is still valid. The need to accommodate the user include many different aspects and has many different implications. For example, the use of mobile smart devices (smartphones and tablets) accentuate the need to provide device agnostic solutions that provide equal functionality irrespective of the device employed by the user. However, this requires full support for development strategies that ultimately support the "Mobile First" paradigm without requiring separate development efforts based for individual devices. Such tools now exist and should be considered in order to support the provisioning of device-independent solutions. Another aspect is understanding what, on a practical level, creates value to the user, which might entail querying the end-user through surveys or similar activities.

d) Simplification

This recommendation is still valid. For Small and Medium Enterprises, simplicity is especially critical as the resources set aside for anything besides the core business typically are scarce. Streamlining and simplifying the life of the SME actor is key.

e) Digital by Default

Looking back at 2016, it's not unlikely that the "digital transformation" will be listed as one of the top three recurring themes of the ICT topics of the year. If not THE top topic. For public authorities, transforming the organisation to cater digital solutions is one of the priorities. Other activities to consider include automating previously manually executed services. Access to /shared/ data and secure /e-/identification of the users are obviously critical elements and enabler of digital transformation.

f) A Platform for Discussion and Consultation between Stakeholders

During this seminar, several participants shared information/experiences on the importance of understanding the end user and end user needs. Unless the actual value creation and requested support of the target group are understood, the risk is obvious that the solution (e.g. e-Government Service) developed and made available works find, but is of no or little use. To ensure full disclosure on the drivers and requested functionality expected by the stakeholders, a "platform" for discussions and consultations should be considered as part of any effort. "Platform" implies a "technical platform", which - many times - will be natural part of the platform concept. But providing a "platform" obviously also entails setting up an organisation that will cater for the ongoing discussion and consultation, finding the right forum and engaging with the relevant target audience. As pointed out by Frank Leyman: "*To market the available e-Gov Services is key - building momentum is key*".

g) Standardisation and Harmonisation of Components

Using standards and open source might accelerate the provisioning of solutions and the components that form the solutions. The trend towards /open/ API can both force stakeholders to provide well documented interfaces and can also be regarded as fundamental principle on which to build and provide solutions in the public sector. The EU project "e-SENS" was showcased during the seminar as an example of an effort running with the overarching objective to simplify and make use of "building blocks" that provide functionality that span many different domains and usage areas.

h) Risk Management for Data Security

Risk management is a key to understand the implications of data security.

Additional recommendations and elaborations made during this seminar include:

a) Public procurement

Ensuring that the barriers that prevents SMEs from doing business with public entities is one of many measures that might be considered. To achieve this, legislation and/or policies might have to be rewritten to accommodate for small businesses. Initiatives such as UK's "G-Cloud" marketplace were realised in part thanks to changes made to the regulation in place for procurement. Lowering thresholds, encouraging "service based" IT (as opposed to using large and monolithic oriented systems to provide IT support) could also enable SMEs to establish business relationships in the public domain.

b) Mobile solutions

As users today are primarily and predominantly using mobile devices (i.e. “smartphones”) to consume IT services, secure access to e-Gov service using mobile e-ID solutions should also be provided. During the seminar, several examples of successful software based e-ID solutions for mobile devices were presented. Mobile solutions are particularly useful for SMEs as they allow business in temporary environments, such as market places. Providing secure payment services through mobile devices, such as the Swedish “Swish” service (a collaboration project between Swedish banks based on the mobile version of the software based e-ID solution “BankID”), can help SMEs grow their businesses using cost effective and lightweight solutions.

c) Information aspects:

Sharing data across agencies, moving information to the cloud as well as publishing data as “open data” requires a certain of control. Control in this respect might entail:

- Security and physical aspects; location, integrity, privacy, access control (authentication and authorisation mechanisms), contingency and more;
- Classification; structure, categorisation and ontologies. “Not all information is created equal”. The difference, e.g., between transactional data and data that stores company information or personally identifiable information (PII) is in this respect significant. The case in point is that understanding the nature of information is critical in order to process and move information in a secure and reliable fashion.

5. Potential next steps

Potential next steps include but are not limited to the following:

a) Changing policies
b) Setting up a collaboration between the EU EBESM project and targeted Israeli authorities with the goal to conduct Proof-of-Concept / Proof-of-Technology in relevant areas.
c) Potential actions (to be elaborated and complemented by additional actions with EBESM technical support):
    - Feasibility study - Defining the right architecture for sharing data
    - Feasibility study - Open Data; based on EU experiences and past efforts - what constitutes “the low hanging fruit”? How can Open Data benefit SMEs?
    - Feasibility study - mobile e-ID vs. other e-ID solutions; pros and cons
    - Workshop - the e-SENS building blocks; applicability and use for Israel

The above suggestions are just ideas based on the main seminar themes, following the discussions during the seminar. Other and complementing actions might exist.