EXECUTIVE OVERVIEW

Worldwide, citizens are demanding from government greater efficiency, shared services, and a single way to view personal identification information. Yet, such demand is offset by the need for privacy and the need for appropriate access rights to personal data. This white paper examines the challenges and solutions for governments implementing electronic identification (e-ID) technology. It highlights the importance of incorporating governance, business processes, and a service-oriented architecture (SOA) into this technology—transforming second-generation e-ID–based government approaches into the next generation of Oracle government solutions.

INTRODUCTION

The topic of identity management and the feasibility of an online electronic identity have been highly debated for some time now. So why is there a renewed focus on government now?

Government transformation is riding the proverbial crest of a wave—the third wave, to be precise. The first wave began more than 10 years ago, as central and local governments began to deploy existing public services online, such as useful local civic information and static central government statistics. The second wave—often termed e-government—involved the more-useful deployment of interactive transactional portals, with services ranging from enabling a basic online local council inquiry to the more-sophisticated service of allowing citizens to submit tax returns online. Although this second wave might have represented a revolutionary transformation at the start of the millennium, today it looks antiquated. The services and data managed by disparate government and citizen agencies remained locked apart from one another, making it difficult or impossible for information to be shared. This dilemma has resulted in entrenched service gaps, duplication across multiple programs, reduced efficiency, and reduced transparency.

1 Presently, many of the services reside in fragmented data silos, where transactions are available through only a single government entity responsible for each service.
Now, the third wave has arrived. Driven by citizens’ rising expectations and the fluid movement of goods, services, and citizens across regional and even global borders, governments are being challenged to boost efficiency, share services, and provide a single view across government departments via “joined-up”, or shared, portals. Where consolidated core services exist within and across government departments, there remains the need for an information-sharing and management framework. This framework must allow everyone to access services to the maximum extent appropriately yet dynamically set—and it’s here that the identity issue arises.

If government is serious about offering shared services to its citizens, businesses, and employees, each participant needs to have an identity to access the services they are entitled to. Government must begin to think about sharing citizen information between departments while also ensuring that only the right information is combined in the right way at the right time. Furthermore, the perspective on how to model this sharing must be from the citizen’s point of view and not from that of multiple government silos. Consequently, the drive for shared services also becomes a need to authenticate and authorize users for specific services. These services must be knitted together from existing applications and systems using new integration technologies.

**INFORMATION ASSURANCE SERVICES**

This drive for new technology places information assurance services at the center of the third wave of transformational government. Information assurance is a service-oriented approach to identity assurance that provides fine-grained authorization and entitlement services. With information assurance, shared services across previously siloed government agencies can be designed to preserve privacy and divulge only agreed-upon trusted services, such as application services based on citizen and government data. In such a scenario, the more-common view of identity management is just a starting point. Information assurance requires a collection of processes, procedures, policies, and technology, which together provide a host of services and features:

- Registration
- Enrollment
- Enterprisewide single sign-on
- Federated directory services
- Authentication
- Authorization and entitlements
- Policy-based provisioning
- Identity propagation
- Audit and governance
Information assurance services break down technical and business process silos, a major limitation of current e-government deployments. By combining identity assurance with fine-grained entitlements, information assurance can then propagate those entitlements as specific authorizations to services across government silos. Information assurance services collect the necessary policy information about how authorizations relate to specific processes and data from multiple repositories that might be scattered across multiple agencies. A composite identity and role is then built, federated, and propagated across the various agencies involved in the delivery of services to individuals. This effort is facilitated by the up-front inspection and customization of the business process during service construction and by the establishment of a governance model that ensures policy adherence. Once the service is deployed, embedding security and governance into the runtime, identity-driven service delivery supports identity federation.

**ADOPTING ELECTRONIC IDENTITY-DRIVEN SERVICES**

The combination of identity management suites and SOA platforms—together with an up-front analysis of the cross-organizational workflow to support integrated services delivery—will support the government adoption of identity-driven services. E-ID is simply the precursor, or an “on-ramp,” for accessing identity-driven services. Up until now, citizens have identified themselves with an official paper document entitling them to government services. With e-ID, users are identified and authenticated using a digital document. Depending on the application, e-ID can be used for identification; authentication; electronic signature; and data storage, retrieval, and transfer.

Among the plethora of documents that e-ID can encompass, a few examples are listed here:

- Health record and prescription
- Passport
- National ID
- Vehicle registration
- Driver’s license
- Resident card
- Visa
- Citizen ID

**Benefits of E-ID to Citizens**

The benefits that e-ID delivers to citizens are as follows:

With e-ID, users are identified and authenticated using digital documents. Depending on the application, e-ID can be used for identification; authentication; electronic signature; and data storage, retrieval, and transfer.
• The smart chip technology within an e-ID card acts as a secure vault that prevents the unauthorized hijacking of an e-ID card when lost or stolen, thereby protecting the personal information of the citizen.

• In a transaction environment, e-ID quickly verifies and authenticates a citizen so that traveling is easier and safer and citizens can securely access government services online.

• E-ID enhances citizens’ privacy by enabling access only to specific authorized information.

• Simplified processes and procedures—citizen verification and identity authentication—can be done offline.

• Information residing on the e-ID card can be kept to a minimum. Requirements can also be put in place for this on-ramp information to be used in tandem with other information prior to divulging additional information or delivering services. This limits the damage from a stolen or hacked e-ID card.

**Benefits of E-ID to Governments**

The benefits of e-ID to governments include the following:

• E-ID smart chip technology protects the individual’s privacy while securely ensuring their identity with personal identification numbers or biometrics—further strengthening authentication.

• E-ID—proven security increases confidence in any national credentialing system.

• E-ID enables citizen verification and identity authentication to be performed offline: online access to a central database is not required.

• E-ID cards are extremely difficult to counterfeit, thereby providing a strong countermeasure against identity theft.

• E-ID digital signatures contribute to the accountability of government officials and employees.

• E-ID enables citizen authentication and accountability.

• E-ID reduces government expenses by eliminating multiclaim benefit fraud.

• E-ID in combination with digital signatures streamlines and speeds up service delivery.

Historically, the problem with these examples has been that they have only elevated identity management from the first wave (the official paper document) to the second wave (electronic access to the silo services associated with the e-ID card). For example, not much is gained with an e-ID card that acts solely as an e-health card—only providing access to insurance details. Instead of carrying an e-ID card for each service, you would want to access a variety of services, from both the
public and commercial sectors, with a single e-ID card. After all, how many e-ID cards would you want in your wallet?

**INFORMATION ASSURANCE FOR TRANSFORMATIONAL SERVICES IN GOVERNMENT**

Today's technology enables much more than just an e-ID on-ramp. It supports tighter border security, protection for the vulnerable, and enhanced crime detection. Moreover, e-ID helps combat financial and benefit fraud and offers citizens access to additional public services. Belgium—a country at the cutting edge of e-ID—provides a barometer for the demand for e-ID in government. The Belgian government estimates that by the end of 2009, about 8.2 million citizens age 12 and older will have Belgian e-ID cards. But, for e-ID to become a key part of twenty-first century government transformation, it must support joining up services as an on-ramp for the third wave scenarios previously discussed.

**Public Safety and Emergency Response**

The U.S. Homeland Presidential Directive 12 (HSPD-12), for example, is a policy to develop a common identification standard for federal employees and contractors. Its primary objective is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. Not only will the directive allow users to instantly access the physical identity of federal employees and contractors, but it will also cater to emergency situations in which an individual might need access to services that would not normally be available to them. However, the impact of the directive extends beyond the 1.8 million federal government employees or the millions of military personnel and contractors it directly affects: the directive has converged government demand for e-ID with the commercial sector’s demand for physical and logical security. There is a need for the card to act as the entry point for multiple services.

**Commercial Sector**

For e-ID to succeed, there needs to be buy-in from the commercial sector. In essence, the delivery of government-led e-ID services needs to act as a lever for commercial services integration. Citizens and businesses will balk at being charged for the provision of their e-ID cards if it only provides access to public services. However, if commercial incentives were provided for citizens to use their cards—for example, if citizens were allowed to use their driver’s license to identify themselves in a bank or a video store or as a replacement for their ATM or membership cards—there might be more-widespread acceptance of the system.

**Shared Services**

The notion of shared services is not new. The commercial enterprise market has been sharing services for almost two decades, consolidating IT, human resources, finance, and other horizontal functions across business units. Driven by the need for efficiency and modernization, government agencies are extending the shared
services concept: instead of merely consolidating services on the back end, they are seeking to join front-end services across multiple organizations to create new and improved services for users.

With shared services, they can address issues such as how to share information among law enforcement, public safety, and intelligence communities; how to affordably deliver new government services; and how to deliver employment, welfare, and other citizen services. Governments are now becoming federated digital communities that share information and offer 24/7 self-service. They have to support applications, directories, and data repositories for services that are delivered across multiple government and private enterprise boundaries. Clearly, all of these require full information assurance services, including the correct identification of the user; centralized, policy-based authorization and propagation of authorization across disparate enterprise services; and administration and lifecycle management of user identities.

Regulatory Compliance

Government agencies are required to comply with evolving regulatory and privacy directives—particularly those that monitor cross-agency or interborder processes and service agreements. As a result, e-ID—backed by an SOA approach to information assurance services—is key to government agencies’ ability to track and audit all user and administrative activity across multiple organizations. Such a solution allows agencies to satisfy regulatory and legal mandates, thereby increasing the public’s trust in online citizen services.

Fraud

Fraud costs governments worldwide millions. For example, benefit fraud alone, as a result of identity fraud, costs the U.K. government between £20–£50 million per year, according to the Department for Work and Pensions (DWP). The U.K. government estimates that the use of false identity information currently costs more than £1.7 billion per year. Like the DWP, Medicaid and Medicare in the United States have seen their share of fraud as well. The U.S. Government Accountability Office estimates that as much as 3 percent of all Medicare and Medicaid payouts are fraudulent, and the National Center for Policy Analysis believes the cost of fraud is US$33 billion per year. Although these are just estimates, real examples point to their validity. From October 2007 to October 2008, New York State auditors recovered US$269 million in Medicaid fraud.

Much is debated regarding the costs and benefits of introducing e-ID cards, or even whether e-ID cards would solve the identity fraud issue, but there is no escaping the fact that identity fraud is a significant national cost. More than likely, the resolution to this problem would need a service-oriented approach as well, starting with coupling information assurance services with business intelligence software. Such a solution could analyze anomalies and pinpoint fraudulent transactions. By
managing business processes and closely monitoring activities, governments could gain visibility into process orchestration and implement fixes to avoid future fraud.

**TECHNOLOGY CHALLENGES OF INFORMATION ASSURANCE AND SHARED SERVICES**

There are many challenges surrounding the technology requirements for trusted online services based on a shared e-ID on-ramp and information assurance across multiple government silos. For a government to transform the way it delivers services, the challenges outlined in Figure 1 and discussed in the following sections need to be taken into account.

---

**Figure 1:** There are many challenges to building out services based on e-ID and information assurance.

**Securing Identity**

First, there is the issue of authenticating and authorizing users for access to shared services. The security and reliability of authentication mechanisms might vary, depending upon the desired authentication level. Further, the stronger the authentication, the greater a government’s confidence will be that an entity corresponds with the claimed set of attributes.

Authentication is typically subdivided into two separate classes. *Data authentication* is the e-ID technical process of verifying that a claimed attribute corresponds to the actual attribute held by an entity. *Entity authentication* can be identified by factors, including knowledge (password), possession (token), a personal characteristic
Some governments and citizens are cautious about using biometrics, although opinions are likely to change and opposition will weaken as the benefits become evident.

The use of personal identification numbers (PINs) is the most common means of securing identity, although biometrics is increasingly used as an additional security feature to the PIN. Some governments and citizens are cautious about using biometrics, although opinions are likely to change and opposition will weaken as the benefits become evident. Where biometrics are not available or insufficient, using software like Oracle Adaptive Access Manager provides real-time risk scoring that helps identify potential fraud and prevent identity theft.

**Securing Services**

The challenges in securing services are related to ensuring compliance with laws and deploying travel and border control tools for improving national security. A further challenge concerns how to maintain up-to-date secure e-IDs in a climate of potential theft and fraud.

The difficulty of securing services is compounded by applications within government agencies that are frequently built using distributed architectures. This makes it hard to manage security consistently across multiple government agencies. Governments need to manage security in many different places, where data is often stored in multiple independent silos. To foster reuse of existing information and encourage transactional resources as services, they must resolve the issue that most existing services are built in a different application environment and therefore might use different security technologies.

In addition, security is frequently embedded in critical business applications. Often, the oldest data silos that are tightly coupled to legacy mainframes are most likely to hold the important information that requires federated identity association. Significant manual effort is needed to change the security policy across each application. Financing the recoding of the application to update the (hard-coded) security policies inside the application depletes capital and resources.

**Data Privacy**

Who should get access and across which services? Citizens and businesses require full control of their data with select access to specific data. They also need to be educated regarding their personal data. For example, citizens should know who is using their data as well as how, when, and to what extent it is being used.

Government agencies—as stewards of their citizens’ personal data—would then need to build policy and automate processes to support the granular sharing of citizens’ personal data for government shared services across organizations and even across borders.
More specifically, e-ID requires role-based access control—connecting users to resources while controlling access to those resources—determining who can access what. However, it gets more complicated when the system must also control who can access what from where (when they are in a different country) or with which e-ID (when they are requesting information with an e-ID card for a siloed government service). For example, could an electronic driver’s license be used to access electronic health records when a citizen is abroad—either for routine healthcare or in an emergency such as a vehicle accident with a critically injured driver?

Although e-ID might remove some of the technical challenges in accessing disparate sets of data, government policies will still determine how securely and efficiently information will flow across governmental data silos. Data-sharing challenges across silos have always existed; however, e-ID combined with SOA will enable joined-up service scenarios that force policy decisions in the near term. Examples of these policy decisions include the following:

- **Organizational perspective.** Governments need to decide which authorizations are required in the system, who can give and hold them, and what they mean—based on how and when they are propagated to additional government and commercial entities.

- **Technical perspective.** Governments need to decide how to model and share a composite view of citizen’s personal data. Do they create a central authorization database? Or do they send referrals to related trusted systems? Who can manage the authorizations? How should their validity be checked before an authorization is exercised?

- **Governance perspective.** Governments need to be aware of the legal requirements for authorization: Does it require a written contract, signature, or acceptance of the receiver? What are the legal issues for cross-border activity? Is the authorization valid in the country where it is given, where it is received, or where it is exercised?

**Shared Service Interoperability**

The fact that governments across the globe are striving to have a single sign-on for their online services for each citizen and business demonstrates how e-ID needs to be a shared, integrated cross-government service. Although software components for single sign-on provide unified single sign-on and authentication across multiple government agencies and departments, they are the tip of the integration iceberg. Several other components necessary for e-ID–driven shared services interoperability are required. These components must also take an SOA approach to identity because SOA is currently the underlying infrastructure.

- **Federated directory services.** Oracle Internet Directory and Oracle Virtual Directory provide an SOA approach to handling disparate, siloed, and third-party heterogeneous identity repositories. Oracle Internet Directory offers
metadirectory and cross-directory data synchronization features, and Oracle Virtual Directory ensures the identities within those directories can be associated with applications and databases without changing the underlying infrastructure or applications.

- **Centralized identity administration.** Oracle Identity Manager and Oracle Role Manager can be used to centrally control the lifecycle of user accounts and access privileges. They can also be used for the authorization of resources and entitlements across a disparate set of directories. (These directories are managed by Oracle Virtual Directory.)

- **SOA access management.** Access management to SOA services is provided by a combination of Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Federation, and Oracle Web Services Manager. Working in tandem, these products create an identity access management platform to link e-ID to a shared services, SOA-based platform by providing
  - Standards-based integration for cross-domain Web services including modern and proprietary legacy platforms
  - Centralized, standards-based policies across these platforms
  - Web services security and service-level agreement (SLA) implementation and management across the same heterogeneous set of platforms

### Building a Services Portfolio

Within the brave new world of shared services, government IT has increased its value as well as its profile. IT is now in charge of providing a scalable, adaptable architecture for the delivery of government services that meets the ultimate demand of having to do more with less.

Doing more with less isn’t just about less-expensive new infrastructure; it is about securely reusing and aggregating legacy data and leveraging the existing infrastructure. Just as there is a need to build composite applications that reuse an existing application infrastructure as a cost-effective means of building shared services, e-ID and its associated single sign-on will require composite records that are dynamically created and altered based on the specific set of services delivered to an individual citizen or private business.

The challenge here is that a significant portion of the necessary data associated with current IDs from silo services, such as driving records, business permits, and electronic health records, resides in legacy databases that have point-to-point connections only to the legacy application platforms within those silos. Furthermore, the security mechanisms that act as the gatekeepers to these data records through these legacy applications are embedded directly into these applications as proprietary APIs and implemented as part of each point-to-point connection. To build a dynamic composite record, both security and data must be
offered as fine-grained services that are decoupled from the upper-layer service delivery platform. So, analogous to the practice of encapsulating legacy applications with Web services and extracting point-to-point connections into reusable, loosely coupled application and data services, security services will need to capture functions with a more-flexible architecture.

**Service Control and Management**

As mentioned above, the key to the successful sharing of services based on e-ID will be agreement and coordination among several government agencies. Again, the technology will provide the basis for a minimum set of information about an individual to be stored in electronic format and dynamically aggregated and filtered for various data records—ultimately determining how and what services to deliver to that individual. However, this cannot be done without strictly adhering to existing regulations that each organization must follow or without complying with the guidelines of their respective data stewards. In some cases, laws will need to be rewritten to allow the information to be shared and for new auditing routines to ensure compliance.

Although using e-ID as the single entry point to joined-up services could generate cultural, organizational, and political issues, there are still elements of business process management (BPM) and SOA that can facilitate efforts to build trusted identity-driven services and mitigate risks associated with these services. These technologies can align stakeholders within each government’s line-of-business operations and IT organizations, and across multiple organizations. In addition, they can help build SLAs across organizations that define how identity is used, how policies are implemented, and how agreements are enforced.

From the line-of-business side, BPM suites (for example, Oracle Business Process Management Suite) can provide a means for operations and business analysts to model, simulate, and orchestrate workflows for delivering services based on e-ID. Oracle Business Process Management Suite can be used at each stage of developing and testing to determine how identity is safeguarded for a given routine process. It can also help determine when and how exceptions must be handled based on a set of policies—for example, the vehicle crash scenario previously mentioned. For both the routine process and its exceptions, Oracle Business Process Management Suite can pinpoint where and how IT systems will need to be involved, and the extent to which automation and efficiency are necessary.

Once a process has been defined and is ready for high-bandwidth, transaction-oriented, identity-driven services, Oracle BPEL Process Manager can provide process orchestration services using the industry standard Business Process Execution Language. Where Web security services and messaging between disparate applications and their associated data repositories are required, Oracle Service Bus can be used.

For these points of IT use (or potential use where the current process is not automated), other tools, including enterprise repositories such as Oracle Enterprise
Repository, can be used to assess and document all resources available—from components of IT systems to sets of policies and compliance regulations. Guidelines can be set for determining what the routine and exception use policies will be for specific applications and their associated data components. Security mechanisms can be put in place within the enterprise repository to ensure that only organizations that own the specific data sets with which they are entrusted can set the rules of governance for their use by other organizations. This assessment at design time can help determine which reusable components are best of breed and can be integrated, prior to loading them into a set of deployed, shared services.

In a deployed phase, the set of shared services delivered to e-ID would also require a level of governance that is supported throughout the SOA architecture. Governance of the SOA lifecycle of the e-ID would be handled using the same tools that publish and subscribe to applications and data as services. An enterprise registry, such as Oracle Service Registry, would be used as a runtime directory of available services and guidelines. Just as with the repository, the registry would provide security mechanisms to ensure that only those with authorization to publish or subscribe can do so.

SOA—THE HEART OF SERVICE DELIVERY

The fundamental issue for government agencies considering e-ID is to look at it as the on-ramp to delivering shared services. So what does on-ramp mean? In essence, once role-based access control has been achieved, e-ID can act as the secure gateway to providing citizens, businesses, and other communities with a wealth of online services. Unlock the authorization and access issue and online communities have a ramp onto federated portals and services.

So how can government agencies bridge the gap and make e-ID this type of on-ramp to next-generation services? The answer is SOA. It represents an IT strategy that encourages the creation of loosely coupled government services that are interoperable and technology agnostic. These can be combined and reused quickly to flexibly meet the needs of citizens and businesses. The “service” part of the SOA acronym relates to government services, such as authenticating the identity of an individual, making a tax payment online, or updating a record in a database.

SOA isn’t a new strategy, but the advent of emerging standard technologies—such as Web services—makes it significantly easier to implement. An SOA solution consists of a composite set of services that encompass an end-to-end business process. Each service provides an interface-based service description to support flexible and dynamically reconfigurable processes. SOA provides general, reusable interfaces at the business level rather than at the component level. Within this scenario, the public sector IT manager becomes less like a plumber racing to fix a leaky pipe and more like an orchestra conductor, composing freestanding services into smooth flowing workflows that model business processes.
The secure and appropriate exchange of identity-related information among users, applications, and service providers (both internal and external) is the basis for providing deeper and richer SOA functionality.

SOA enables e-ID to deliver the next generation of government services because it

- Provides a single, shared view of services
- Allows communities access to legacy and multiple heterogeneous platforms across different government departments
- Provides service mediation and process orchestration among a set of heterogeneous applications and systems
- Allows government to build secure, host-based e-ID services
- Moves security embedded in the applications to the services infrastructure level as open standard reusable modules
- Applies governance to services

Figure 2: SOA makes e-ID the on-ramp to next-generation government services.
Citizen Online Services

SOA requires a new set of technical standards and design patterns as well as new strategies for design, implementation, testing, operation, and governance. In fact, the definition of what comprises an application changes too. It requires a shift from a standard programming model based on application-specific APIs developed within the application infrastructure to a compositional, higher-level integration model implemented at the services infrastructure level. Specific processes would be decoupled from the application infrastructure based on process analysis by government management.

In some cases, these processes might be generic core services, identical to those in the commercial space. Government agencies have the same needs for document management, e-mail, enterprise resource planning, and other more-generic functions. In other cases, public sector IT managers must deal with stricter e-ID security requirements; the need to deliver actionable real-time information; and the need to provide public access to government services to allow citizens to vote, register as a driver, and pay taxes, among other tasks.

Much of this can be accomplished through a federated portal that bridges the applications and data records of multiple back-end systems and their government department owners. Portals, like Oracle WebLogic Portal or Oracle WebCenter Suite, facilitate federation across multiple government organizations. As such, they can provide a first step to integrating existing data silos while also leaving them relatively untouched. With these portals, composite applications and shared services delivery can begin to emerge.

IT must then work closely with the managers responsible for the execution of specific processes to convert them into activities and workflows that can be modeled using BPM tools such as Oracle Business Process Management Suite. This means that business analysts cannot only model business processes, but they can also monitor and analyze them for future refinement.

Centralized Security in an SOA Environment

Organizations can no longer hard code security inside their applications. They need to leverage security as a service and extract security out of their applications. Why is it so critical to manage security as a service?

When implementing an e-ID approach, government needs to enforce a common security policy across a whole community. Therefore, if security remains at the application level, it will not be possible to have a common and consistent approach. Solutions such as Oracle Access Management Suite allow government to centralize security as a service and remove the need for security at the application level.

Oracle Access Management Suite provides centralized administration of security across the infrastructure, including custom applications built in Microsoft .NET and Java environments. Administrators can simplify the building, deploying, and auditing of access control policies that model the business. Oracle Access
Management Suite protects resources based on both software components (such as URLs, Enterprise JavaBeans, and portlets) and business objects (such as case management records and bank accounts).

SOA security should not be based on the software component or Web services level alone, but it should also incorporate business objects into the security logic.

**Governed Service and Managing the Lifecycle of Information Assurance**

The goal of joined-up services is to build and use an array of services based on existing components where possible. These services can be augmented over time by adding new components from new organizations as well as by developing new infrastructure within newly joined and existing organizations. Ideally, user usage patterns and demand for changes and additions to this service portfolio will drive changes in the service lineup. E-ID cards as an on-ramp to that portfolio of services must be adjustable to the service portfolio scenarios available to the end user. In the case of e-ID, a representative set of adaptability issues are as follows:

- **As services are added, how are the policies implemented that set up identity propagation to this new service?** It is not simply a matter of a single sign-on providing access to yet another service, but single sign-on has to granularly set authorization to resources associated with existing services and their underlying IT assets, which should be available for this service.

- **How will legacy cards that provide access to this new service be treated?** Will they allow access to the service that was formerly a silo service at the same level and breadth, or will they be able to use this e-ID as a token in exchange for access to the new portfolio of services available? If so, to what extent?

- **How will the identity propagation change access and use of the portfolio of services as e-ID cards are retired and new ones brought online?** Will the new cards have phase-in periods as a function to meet the SLAs for specific services within the portfolio?

**E-ID IN THE REAL WORLD**

E-ID has been implemented in various forms by governments around the world. Common themes across successful implementations have been the provision of information assurance services on the front end, SOA-based integrations, and the exposition and delivery of services infrastructure on the back end.

**Finland—Katso**

Finland is spearheading work on SOA-driven shared services delivery. The Finnish government was challenged with the need to create a flexible means of issuing and authenticating identities to customers, organizations, and citizens. It also needed to
reduce the cost of supporting customers at the point of service and implement a solution for role-based access control and organizational authentication.

The outcome is Katso—a nationwide identity management, authentication, and authorization system. Katso is already used by the Finnish Tax Administration and the Social Insurance Institution. As part of the development of government services, both of these institutions required a solution for role-based identity management and organizational authentication.

The Katso system resides on Oracle WebLogic Server, an open, service-centric application server infrastructure. Katso uses standards such as Security Assertion Markup Language for Web-based authentication and Liberty Identity Web Services Framework for non–Web-based applications, allowing organizations to implement Katso authentication across the application landscape.

The Katso system will become the de facto authentication and authorization solution for online government services in Finland. New government agencies and services are joining Katso in growing numbers and more than 300,000 organizations will be using Katso when it is fully deployed. It is also estimated that up to 30 large-scale online government services will be using Katso by the end of 2008. Katso will likely be a model of standard adoption for large-scale government infrastructure services around the world.

Belgium—Belgian Personal Identity Card

The Belgian Personal Identity Card (BELPIC) is a highly secure, easy-to-use, and affordable digital identity system for all citizens to use to file taxes, open bank accounts, and make purchases online. It’s based on Oracle WebLogic Server. Citizens can use their e-ID through the Belgian government’s portal that runs on Oracle WebLogic Portal. Oracle Service Bus provides the underlying services orchestration bus to back-end platforms across the various government agencies.

Belgian citizens can already use the new e-ID card for identification, authentication, and authorization for many public services, including secure online tax form declaration, official document requests, electronic submission of court case conclusions, as well as access to the public library and other community services. The Belgian government estimates that by the end of 2009, about 8.2 million citizens age 12 years and older will have national e-ID cards.

Germany—Eclipse E-Health Card

Germany has begun trialing an electronic healthcare card (the eclipse), which will contain basic patient data such as name, age, next of kin, and insurance details, as well as electronic prescriptions. The concept is based on distributed broker services, which guarantee message switching on the basis of request chains between the telematics infrastructure and connectors, professional services, and other services—including identity verification. Oracle Service Bus (an enterprise service bus) and Oracle WebLogic Server (an application server) are at the core of this SOA.
The solution includes comprehensive functionality to meet the requirements for the broker service. These include the implementation of the broker services as a Web service, intermediate message relaying, and XML-based messaging based on Simple Object Access Protocol. The broker services are composed of several interacting services, one of which is the Smart Document Solutions registry service. Oracle Service Registry is delivering this service and will act as the base technology for the entire service directory. The concept of the broker services is based on an SOA and uses an intermediate communication style. This enables the implementation of flexible and agile components inside the telematics infrastructure.

France—GIE SESAM-Vitale E-Health Insurance Card

The Groupement d’Intérêt Economique (GIE) SESAM-Vitale is a service provider whose mission is to provide the technical expertise to develop and promote the SESAM-Vitale program. The GIE SESAM-Vitale program was created by the partners of the French Health Insurance to develop common solutions to meet the needs of all its members—whether they are part of the compulsory systems or the complementary insurance organizations. SESAM-Vitale currently links more than 223,000 healthcare professionals in France with the health insurance system, for the benefit of millions of insured persons who have the Vitale card. It is an innovative project composed of new technologies to simplify and accelerate exchanges, thereby eliminating any paperwork.

Oracle WebLogic Server is being used within this project to manage the main functionality on the Vitale card. The smart card is the most used in France (circulated to all insured persons and beneficiaries age 16 and older). The application server helps process more than 900 million claim reimbursement forms per year and has reduced the time taken to reimburse insured individuals from three weeks using the paper-based system to five days.

Italy—Ministry of the Interior E-ID Card

The challenge facing the Italian Ministry of the Interior was to develop a national identity card. The solution needed to offer a greater degree of security and availability than the previous methods of identification. Simultaneously, the solution also needed to combine previous identification and social services cards.

The solution—called the Carta d'Identità Elettronica (CIE)—currently supports, integrates, certifies, and tracks more than 70 million national identity cards. To obtain the CIE, Italian residents in the municipalities simply provide identity information that is checked against a central infrastructure at the Ministry of the Interior, which authenticates the information, generates a signature and digital certification, and then the municipality produces the actual e-ID card. Oracle WebLogic Server underpins the CIE infrastructure.
The Italian Ministry of the Interior is able to identify and authenticate all citizens on the Web using digital certificates. Initially delivered by 80 municipalities, the e-ID card can now be requested in any Italian city. Local municipalities will be able to install services on microchips and offer them to all citizens.

**Mexico—National Commission for Social Protection in Health E-Health Card**

In 2001, Comisión Nacional de Protección Social en Salud—or Seguro Popular de Salud (Popular Health Insurance) as it is more commonly known—was created as a joint effort between the federal government and the state governments in Mexico. Its objective is to offer Mexican citizens access to medical attention. Today, the commission has more than 5 million affiliated families and beneficiaries in the country and hopes to reach approximately 50 million affiliates by 2010.

Seguro Popular de Salud has implemented an e-ID card on-ramp to a multichannel health benefit services operation, including online access and in-person branch offices, that is based on Oracle’s Siebel Customer Relationship Management (CRM). The Siebel CRM system connects the operations of 1,500 users in the country’s offices and remote areas with the commission’s main offices and services.

Oracle Database and real-application clustering provide centralized information in one reliable and highly available database for the front-end Siebel CRM system’s Web environment. Oracle Internet Directory and Oracle Identity Management provide controlled access to information and management of the 3.7 million e-health cards currently active. Oracle Application Server and other Oracle Fusion Middleware components consolidate disparate systems for budgetary control over expenses, facilitate database management, and provide access from the front-end Siebel CRM system. This system enables nearly 800,000 transactions per minute.

As a result of Seguro Popular de Salud, several time-consuming manual processes have been eliminated, and the time required for administrative processes has been reduced from two weeks to two days through automation. To create an environment of continuous improvement, Seguro Popular de Salud has also implemented Oracle Business Intelligence Suite, Enterprise Edition (now Oracle Business Intelligence Suite, Enterprise Edition Plus) and set 20 indicators for efficient credential monitoring and drug and medicine distribution to manufacturers and pharmacies with Oracle’s Siebel CRM applications. This has enabled negotiations with program providers to be carried out with a high degree of automation, from the application process through payment for participation in the program.

**Hong Kong—Propagating Single-Sign-On Identity into Disparate Packaged Applications**

The Hong Kong Housing Society (HKHS), a nonprofit housing provider for more than 60 years, wanted to provide identity-driven, online citizen services to Hong Kong’s citizens in need. HKHS used an SOA approach to link an integrated,
transaction-oriented, single-sign-on portal front end to its back-end enterprise resource planning and human capital management applications that include Oracle’s PeopleSoft applications. This link provides automated, end-to-end execution of business processes. HKHS used Oracle Identity and Access Management Suite, Oracle Internet Directory, Oracle Virtual Directory, Oracle Portal, Oracle Web Services Manager, and Oracle Enterprise Repository to build streamlined, end-to-end business processes for full self-service, identity-driven services delivery.

CONCLUSION

An SOA approach to information assurance services improves how e-ID cards are managed and used, offering the following benefits:

- **Single view of services.** E-ID delivers federated portals and identity services to users.

- **Identity assurance.** Governments provide trusted user authentication as a shared service that, over time, builds citizen confidence in online services.

- **Leveraging existing services.** Using SOA to leverage existing applications and data as reusable building blocks, new business processes and applications can be quickly and easily combined.

- **Centralized policy management.** Compliance can be ensured with regulations for cross-border, cross-organization, and other multiparty agreements around services delivered to e-ID credentialed users.

- **Identity propagation.** E-ID can be used as a federated ID mechanism by threading ID and associated privileges and restrictions used throughout the government agencies participating in shared services delivery.

- **Managed service growth.** Service governance and lifecycle management can optimize identification, collection, publishing, and subscription to a set of public and privately built shared services.

- **Increased return on investment.** Leverage BPM into SOA planning and execution to ensure all policies are properly implemented and the underlying processes to execute these policies are optimized.

In the central and local government spheres, trust will be the necessary foundation for secure interoperability and will be key to the successful realization of what’s possible with online services. From the user perspective as well as that of the deploying organization, it’s an issue of who is trusted with what. Ensuring trust in the system requires the proper organizational culture, policy, business, technology, and infrastructure that can adapt to changing needs and improve the understanding of requirements. Sharing and interoperating among agencies and government departments creates opportunities to simplify processes and unify work, as well as improve the overall transparency and efficiency of government. Secure interoperability, based on identity management solutions, enables substantial cost savings, streamlined processes, and faster communication of vital information to the benefit of governments and citizens.
savings, streamlined processes, and faster communication of vital information to the benefit of governments and citizens.\(^2\)

The danger is when organizations view deployment of an e-ID strategy as a “vertical application” for the citizen. This is confusing the means and the goal. The final goal for joined-up online government projects is to deliver new value-added services to citizens, enterprises, and other government agencies. Very few “customers” of government organizations are impressed by the added value of e-ID deployments in themselves. However, it is clear that reuse of e-ID in other projects is key for success. It is no longer acceptable to a citizen to have to provide other means of authentication when technology exists to avoid the clutter of cards, passwords, and the like. This is another reason to adopt SOA and integrate the e-ID deployment as a foundation service.

As for the future, the e-ID i2010 road map paves the way toward a pan-European recognition of electronic IDs (efforts like HSPD-12 and Real ID are analogous e-ID efforts in the United States). The objective is the implementation of a European Union–wide interoperable system for recognition of e-ID and authentication that will enable business, citizens, and government employees to use their national identities in any member state.\(^3\) The cross-border element re-emphasizes the importance of building national e-ID solutions on SOA. If e-ID is treated as an on-ramp service rather than part of an application, and if identity assurance is seen as a front-end identity component of an overall SOA platform, it will be significantly easier to build interoperability between participating governments.

---


\(^3\) [http://www.eid-stork.eu/](http://www.eid-stork.eu/)