Effectively securing the SOA lifecycle

Effectively securing the SOA lifecycle

Effectively securing the SOA lifecycle

Effectively securing the SOA lifecycle

Executive summary

Although businesses are implementing SOA to improve efficiency and IT management, many are launching initiatives slowly – or not at all – because of security issues.

For positive business outcomes, service-oriented architecture (SOA) is undoubtedly the way to go. But how can organisations fully trust and secure a "loosely coupled architecture" that's intrinsically flexible and reusable?

This white paper introduces an HP identity management solution that solves this conundrum – a unique solution that secures the entire SOA lifecycle by providing strong attribute management capabilities.

Service-oriented architecture

In today's business environment, one of the top CIO priorities is to implement the service-oriented architecture (SOA) within mainstream IT. The strong promise of SOA is to provide IT aligned to business processes. Organisations have discovered that this architecture dramatically improves business flexibility and adaptability by:

- Expediting the time to deploy new applications and processes
- Lowering IT costs by making services reusable
- Enhancing the agility of the enterprise infrastructure to support change

Consequently, businesses can react faster, seize new opportunities and respond more quickly to competitive threats, resulting in more positive business outcomes.

This is especially true for organisations that depend on information sharing and automated transactions with a wide network of suppliers, distributors, partners, employees and customers. Each of these user groups has a growing reliance on connecting quickly and very securely to the IT infrastructure.

> "SOA is not something you chose to do. It will happen to you whether you chose it or not. You only need one service to need governance. You only need one service to destroy your business." Daryl Plummer, Gartner Research

It's essential that security adopts the same principles as SOA – flexibility and reusability – so as not to limit the enterprise. That's the way to secure positive business outcomes.

Security issues

Difficulties arise in a SOA environment when trying to manage and control identity and access across business processes. Traditional security solutions are application-centric and, of course, this doesn't fit with an architecture that's service-centric.

Furthermore, with increasing regulatory pressure, it has become critical to aggressively monitor and consistently control "who's doing what" among all user groups. The hard-coded security within traditional applications is brittle, difficult to maintain and it limits access decision audits. Plus, managing and maintaining multiple security silos is costly.

These difficulties are compounded by the new requirement for collaboration between operations, testing and design people. Once SOA is chosen, these unfamiliar teams must work together to avoid duplicating their efforts to secure services. Together, these teams must test and approve new services, then agree and apply the information and transaction rights of each different user group. Security is something they need to understand and consider from the earliest design stages and at each step of the SOA lifecycle. Only a well-governed SOA will react to allow businesses to promptly manage change and achieve the business benefits it was originally intended to support.

More flexible and dynamic methods are required for propagating, controlling and auditing identity information for SOA applications and services that represent end-to-end business processes.

The secure SOA lifecycle

Security is an integral activity which should be considered at each stage of the SOA lifecycle. It establishes effective control and demonstrates compliance of the SOA enterprise, thus augmenting trust through governance and improving adoption and reuse of the services. The benefit of the lifecycle approach (see Figure 1) is that it captures and manages changes under a common process framework, thus ensuring effective SOA enterprise governance, providing an organisation with a sustainable infrastructure to support their business objectives.

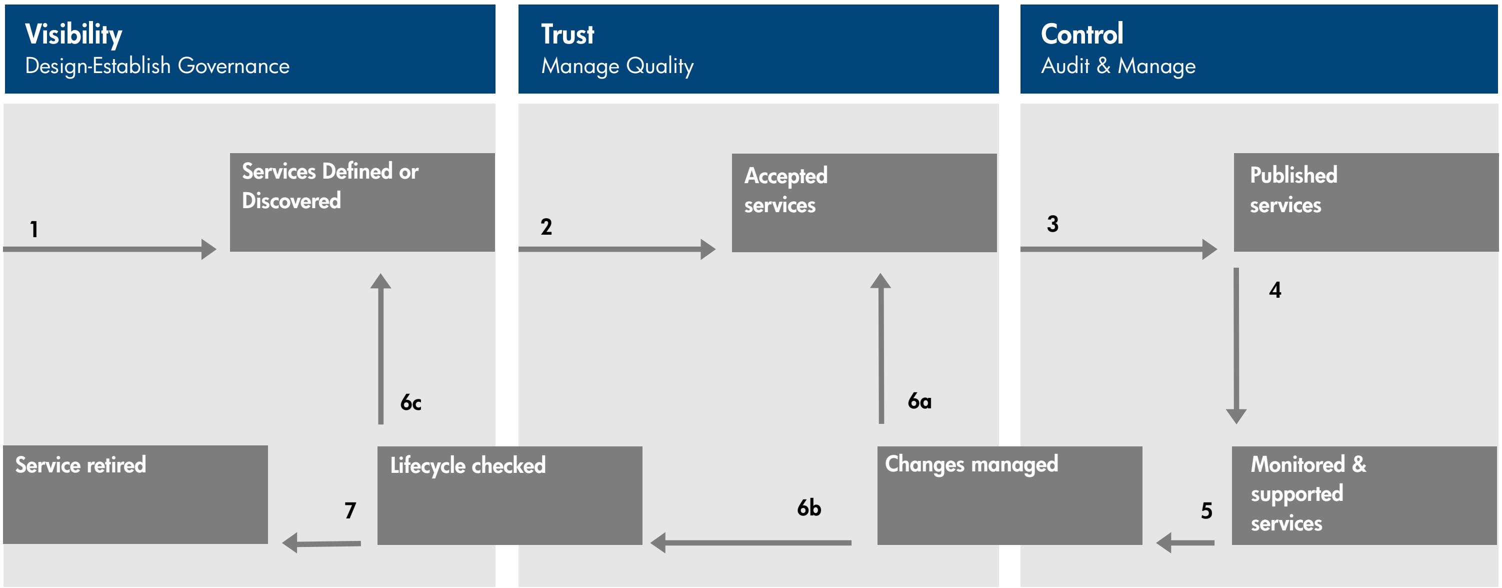
The secure SOA lifecycle (see Figure 1) – or SSLiC – describes a framework for the development, deployment and management of the SOA enterprise by defining a process through which governance is established. SSLiC is divided into three key steps, each with specific security activities:

Visibility – Establishes security policies such as on boarding identities, the approval process and enforcement (authentication and authorisation)

Trust – Tests policies to establish trust such as control of segregation of duty and workflows

Control – Enforces and monitors operational effectiveness of control process

Figure 1: The secure SOA lifecycle



The secure SOA lifecycle reduces implementation and maintenance costs with automated security management and reusable security services for SOA.

In order to secure the SOA lifecycle, operations, testing and design teams should implement the following steps:

1. Define or discover new services or artefact designs and define security policies.
2. Design, implement and execute access testing on the new services or artefacts, and accept these services.
3. Implement services' or artefacts' identity and security policies and deploy the published services.
4. Measure, audit and report service consumption on those monitored and supported services.
5. Audit any change impacts on compliance, and manage those changes.
6. Perform corrective security maintenance on the services or artefacts by modifying and retesting if necessary. If unnecessary, perform service lifecycle checks. Refine or redesign the service or artefact if needed, and repeat the above steps.
7. Invalidate access and decommission the service if no longer required.operations

The key step in securing the SOA lifecycle is embedding security management mechanisms into SOA governance policies. Operations, testing and design teams should consider the following questions:

- How do we integrate security management into the governance policies?
- How do we register a user to access a SOA application/service?
- How and by which business group(s) is an identity approved?
- What are the authentication and authorisation requirements of a SOA application/service?
- How are identities deregistered from SOA services?
- How do we audit the entire SSLiC process?
- How do we deploy reusable security management processes that can serve the entire SOA lifecycle?

Reusing security services
In SOA transformation, organisations are exposing their services to the outside world, that is, their network of suppliers, distributors, partners, employees and customers. As a result, organisations are facing these key security challenges:

- Enabling identities to the right services
- Managing identities' access by policies in real time
- Auditing and governing the entire identity lifecycle management process for proof of regulatory-compliant operations

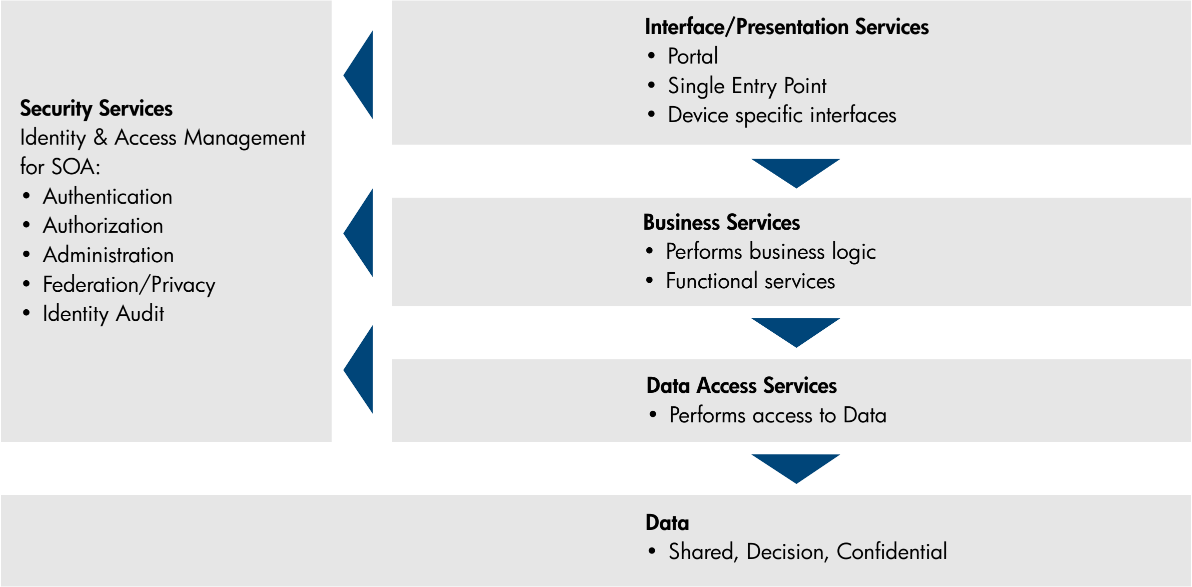
In a dynamic SOA environment, the automation of these key identity and access management processes is critical in enabling business growth.

Today, most SOA deployments simply focus on access management by policy enforcement since the authentication and authorisation components can be easily centralised and offered as a reusable service. But this is only one part of the SOA security management picture. Other important security requirements are essentially left untouched, such as:

- Enabling entities to access SOA services by obtaining approvals from different business organisations and units
- Managing identities accessing to SOA services and applications
- Deregistration and termination of identities

The end-to-end security for the entire SOA lifecycle – incorporating administration, access and audit aspects of security – is crucial for SOA governance. However, it's essential that security is also bound by the same guiding principles of SOA's reusable, loosely-coupled services (see Figure 2).

Figure 2: Security as a service



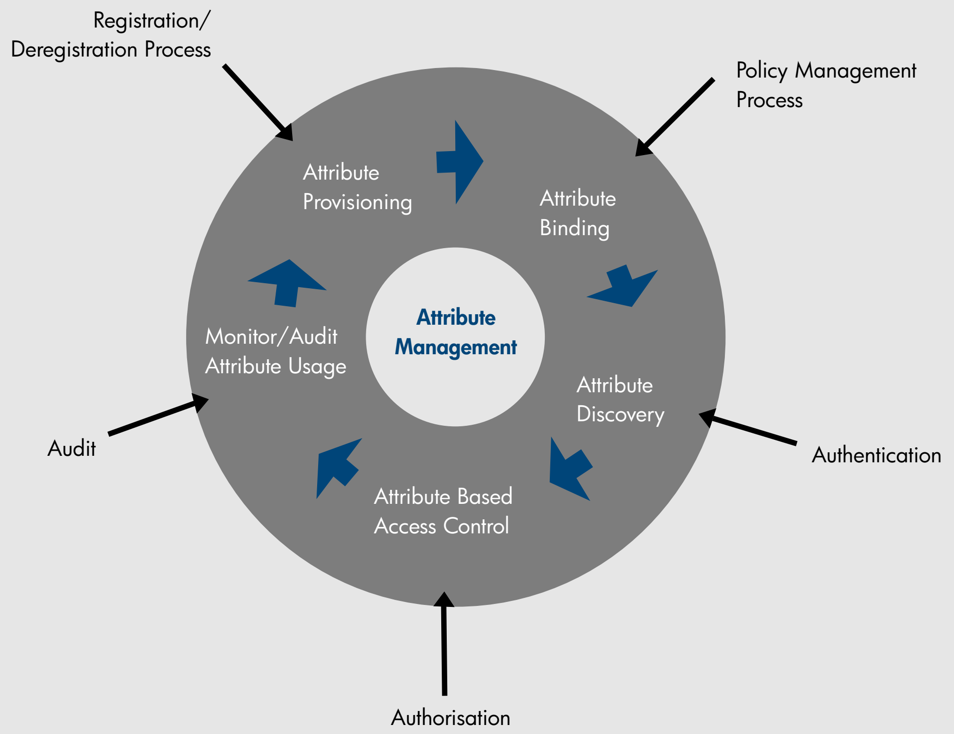
Managing Attributes in SOA

Implementing a flexible and reusable security service for identity and access management is crucial for security in the SOA lifecycle. This service must incorporate authentication, authorisation, administration, federation/privacy and audit.

Authentication is based on user credentials like user name, password and token. Authorisation is based on user profile attributes such as location, department and job function. These in turn are checked and enforced by access policies. The missing part of this picture is the actual administration of users: their registration, enabling, binding with access policies, managing changes and deregistering.

Given the complexity of today's business environments, especially with the number of employees, suppliers, customers, distributors and other users – along with the growing amount of IT services – increasing volumes of information are required to manage each account. This makes it virtually impossible to effectively manage an identity through manual means. Automation is the key.

Figure 3: Attribute management


Registration/ Deregistration Process
Policy Management Process
Attribute Provisioning
Attribute Binding
Attribute Management
Monitor/Audit Attribute Usage
Attribute Discovery
Attribute Based Access Control
Audit
Authentication
Authorisation

Attribute provisioning and binding: Creation and synchronisation of identity attributes on various identity repositories by user provisioning solutions.

Attribute discovery and access control: Find relationships between services, discover ungoverned "rogue" services and bring them under management control. Access control policy enforcement by web access management solutions.

Monitor and audit attribute usage: Audit and monitor the authorisation (attributes) assignment and usage for providing the proof point for regulatory compliance.

Identity and access management for SOA
An identity management (IdM) system is the only practical solution for automating the process of identity provisioning and the management of all associated changes. Collectively, this is known as identity lifecycle management.

Today, most IdM systems are based on the concept of roles. The idea is simple: group employees and other users in hierarchical structures that represent the different job or relationship types (e.g., suppliers, distributors and partners) within an organisation and how they relate to each other.

For automated provisioning of new users, simply assign the user a specific role and the system will:

- Check the definition of that role
- Find the defined IT applications and privileges
- Create an account and assign privileges

This allows the user to access the IT services they need to perform their specific tasks.

However, in the SOA world, it is difficult to get a single organisation to agree on the roles, titles and definitions . . . and nearly impossible to achieve role-based automation across multiple organisations.

In SOA, the services have a loosely coupled design, and interaction is mainly peer-to-peer. To access SOA services (see Figure 4), an identity – a specific user – logs onto a session at an enterprise level using a device (i.e., PC, laptop, PDA), and within the session automatically signs on to various SOA services, usually through the aid of centralised access management solutions. The authorisation decision for accessing the service is made by assessing the identity, resource and environmental attributes.

Limitations of the role-based access control mechanism for SOA

Instead of roles, the agreement on user attributes for authorisations – either within a single organisation or across organisations – is far more likely to be successful across SOA services. And furthermore, the dynamic and peer-to-peer nature of the SOA environment requires more fine-grained access control systems. This can be achieved by including more information such as attributes of identities, resources and environment for the authorisation decision process. Today, role-based access control-based (RBAC) identity management models have the limitation of role explosion: as the number attributes increases, the number of roles dramatically increases and the identity management operation becomes difficult to manage. The result? Additional cost and time overheads for securing SOA services.

Securing SOA services is heavily dependent on access control decisions based on identity attributes. Thus, they require the implementation of attribute-based access control (ABAC). Although ABAC policy and architecture models are very powerful, they only focus on authorisation of requests from information consumers to information providers. The end-to-end security architecture requires more than just the access control model, but a systematic methodology around how these attributes are managed in their lifecycle. (see Figure 3).

Achieving a security services architecture

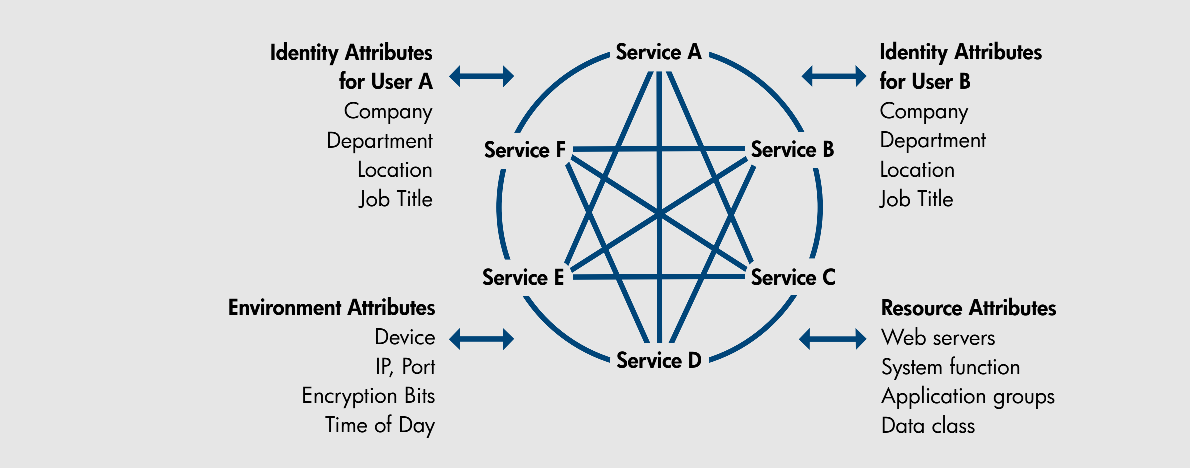
With complete control over the identity attributes, SOA and security enterprise architects are empowered to develop a flexible – and reusable – security services architecture that can:

- Automate the process of enabling identities to appropriate services via strong attribute management and control
- Centralise and enforce access control and policy management based on fine grained attribute-based authorisation
- Federate identities and manage privacy while building trust-based access control mechanisms required across organisations
- Audit and monitor identity- and access-related operations at the SOA services level

This can be achieved by implementing integrated identity and access management components with strong attribute management capabilities like user provisioning, Web-access management, federation and audit.

When these IdM solution components are integrated with SOA management and governance solutions, the change management process can also now be automated.

Figure 4: Attributes in identity and access management for SOA



Governing and auditing the SOA lifecycle

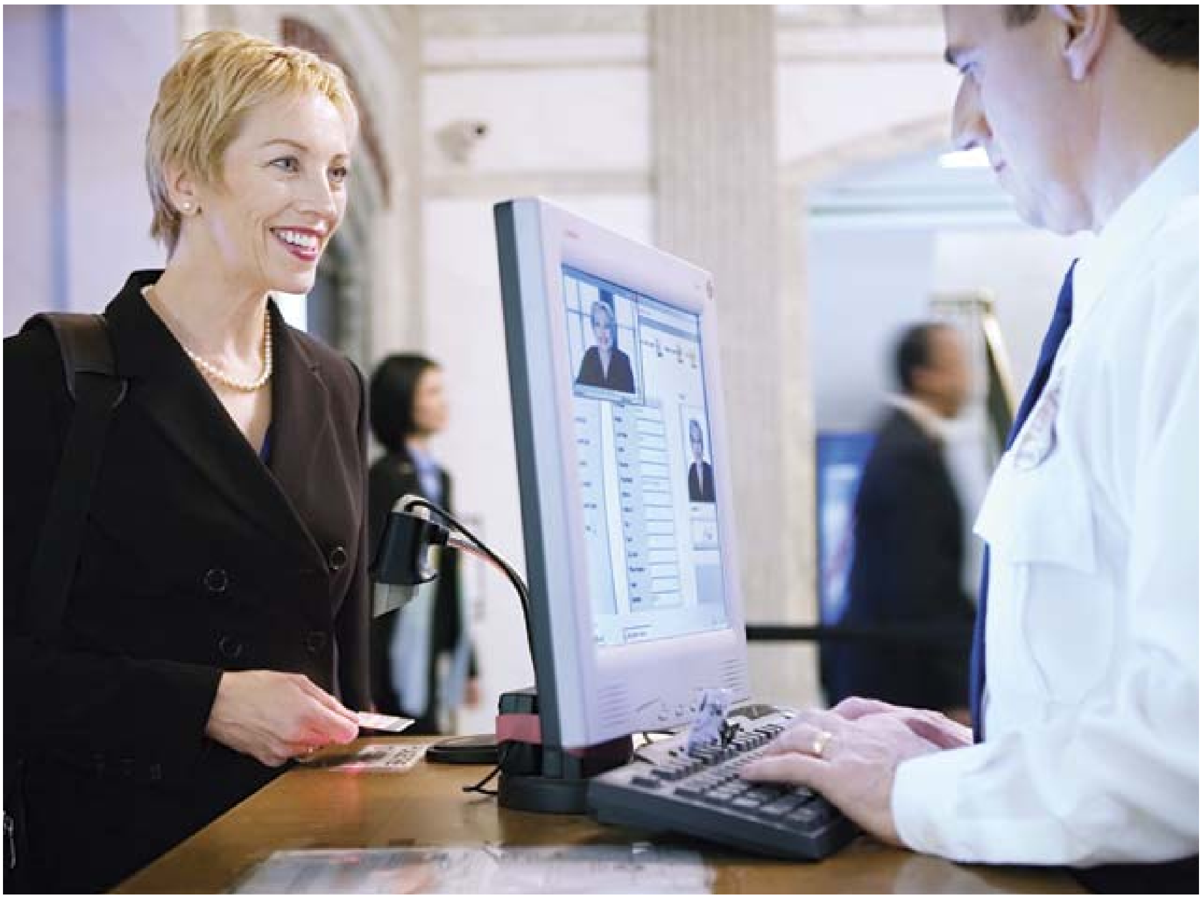
The secure SOA lifecycle reduces risks from a security perspective and lowers costs associated with assuring regulatory compliance.

With governance and compliance regulations like Sarbanes-Oxley and Basel II, SOA can introduce new levels of complexity that can put a business at risk. One of the key objectives of SOA governance is the ability to establish, control and verify security between SOA components and intermediaries participating in a transaction. This requires an ability to certify and validate SOA consumer identities, even in transactions that span federated departments and partners. It also requires the ability to define, provision and execute policy across SOA consumers and providers in a consistent way.

An identity audit management solution can add great value to an SOA governance framework by:

- Monitoring end-to-end SOA environment identities administration and access time domain actions
- Reporting based on various control objectives, modelled by regulatory compliance institutions or organisations, combined with attestation capabilities
- Alerting or fully automated remediation in case of violations of agreed policies between service providers and service consumers

> "While SOA makes IT-enabled business processes more efficient, it complicates identity and access management. This is an issue for companies that must comply with financial controls and reporting regulations required by the Sarbanes-Oxley Act (SOX) of 2002"
> SoX Compliance Journal



HP Identity Center for automated attribute management

Today, HP is the only vendor that offers a complete solution that can effectively secure the SOA environment, reduce time and cost overheads, and maximise the business outcome of SOA transformations.

The HP Identity Center is a comprehensive identity and access management solution. The centre helps businesses reduce costs, enhance user experience and productivity, and improve compliance by optimising identity and access management processes to meet business needs for SOA transformations.

Combining the HP Identity Center with the HP SOA Center enables organisations to automate their identity and access management for the entire SOA lifecycle The HP Identity Center components – Select Identity, Select Access, Select Federation and Select Audit – can fully automate attribute management. And the HP SOA Systinet delivers SOA governance and lifecycle capabilities, including an SOA repository for storing metadata and managing relationships. A suite of SOA governance and lifecycle management applications, HP SOA Systinet can be deployed independently or as an integrated suite.

Summary

While SOA has a strong promise to provide IT aligned to business processes, security is the greatest concern as a potential inhibitor to organisations seeking the promised positive business value.

HP offers a unique approach through the secure SOA lifecycle (SSLiC), combining the value of their Identity Center and SOA Center to effectively secure and govern an enterprise SOA.

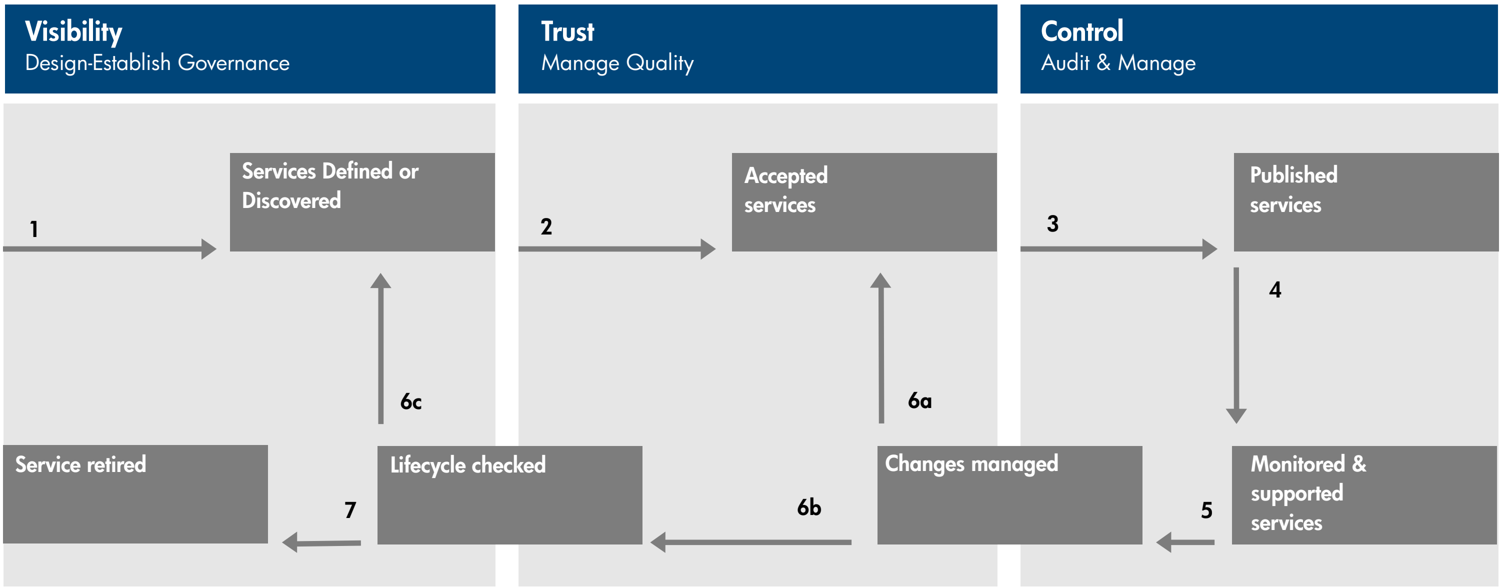
Through SSLiC, HP ensures that SOA adoptions deliver the desired business outcomes. Organisations can now eliminate the constraints of security on the flexibility of SOA, assure complete SOA governance, obtain a flexible IT architecture that can react quickly, and adopt to change and enable business growth.

Resources

HP provides comprehensive SOA and identity management solutions and components that help businesses through the three key SSLiC steps of visibility, trust and control. In securing the SOA lifecycle, organisations can increase their growth and productivity, enhance security, remain compliant and stay competitive.

To learn more about the HP Identity Center, SOA Center, components and the other HP identity management and SOA products and solutions, please visit: **www.hp.com/go/soa** and **www.hp.com/go/identity**

The secure SOA lifecycle with HP solutions



System of Record
- Systinet

Quality
- Service Test Manager

Performance
- Load Runner
- Protocol Bundles

Security
- SPI Dynamics

Runtime Enforcement
- SOA Manager

Provisioning
- Select Identity

Monitoring
- BAC for SOA
- Select Audit

Access Management
- Select Access
- Select Federation

HP also offers a comprehensive set of services for a successful secure SOA implementation. HP BTO Services for SOA help throughout the SOA journey – from getting started, and deploying a full set of processes and organisational structures, to collaboration in designing and building services that meet specific business needs. These services include:

Express consulting services: A set of brief and to-the-point consulting engagements that get organisations started on a specific need for SOA – governance, quality or management

SOA consulting services: Service offerings that can help you at different points in your SOA journey

Education: A comprehensive curriculum to meet the training needs throughout your organisation

SOA delivery approach and methodology: A tested and proven SOA delivery approach and methodology

Competency centres: Centres located in France, India, Singapore, Japan and the United States to demonstrate what is possible and practical with HP BTO solutions for SOA

4AA0-xxxx,Sept. 2007

invent