Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Public Sector | the way we see it

Securing Healthcare Information Services

Contents

1 Executive Summary

Information Services in Healthcare

Current IT estates mostly support the needs for a single institution like a hospital or collection of care facilities (e.g., campus, Trusts, etc.). Healthcare services however are no longer just needed on the basis of geographic or institutional boundaries; services such as cancer care and care catered to the individual such as personal care records, remote biometrics for chronic conditions, etc are being offered outside the physical estate and without regard to location. These and many other healthcare services will be offered on a regional, national and, perhaps in the future, on an international basis.

The fluidity of the healthcare delivery processes makes the provision of healthcare and patient information a very complex venture. This complexity has led many healthcare programmes both on regional or national level to follow an approach based on multiple information services working together, rather than a 'single system' that does everything for everybody everywhere. This is embodied in a so called Service-Oriented Architecture (SOA). In this approach the emphasis is on information services rather than information systems. The services concept separates what the information technology does (service) from how it is put together (system).

SOA is a method of linking together a number of "business services" into a complete business support system. Each service is a stand-alone unit of business functionality which is interoperable but loosely-coupled. It provides the orchestration of software and data as granular and re-usable services for users and applications within or outside the boundaries of an organisation.

Once a service has been commissioned it can be used by other business processes without the need for any new development or testing. Together, the services can be viewed as a kit of parts that can be combined and recombined to suit the changing healthcare needs. Essentially SOA offers the benefits of encapsulation and separation of concerns in bringing IT to bear on business problems, but avoids the risk of functional gridlock that can occur in closely coupled, highly inter-reliant systems.

Security in Healthcare

The drive for a services based approach causes a difficult dilemma. On the one hand healthcare institutions want to be agile and patient centric, meaning open to their environment, their patients, suppliers, partners and employees. On the other, they want to be safe and secure in the way they respect the patients' interests, in particular the patient data confidentiality and that of their staff. Moreover the healthcare organisation needs to be compliant with national and international laws to be able to operate.

Since architecture is the key for a service oriented environment, security architecture is essential to provide the necessary assurance that acceptable levels of availability, integrity and confidentiality are maintained. A Services Oriented Security Architecture (SOSA) is needed. In relation to the future direction of

information security in healthcare, Capgemini sees that SOSA will form the core focus for security in Healthcare in the next few years. This paper sets out:

- How Capgemini sees the future regarding SOSA in healthcare and what response is required;
- What architectural elements and services will be essential to give shape to this future; and
- What the challenges are that healthcare organisations face with implementing SOSA.

2 Healthcare Security Vision

The three SOSA components:
PROTECT—Information Protection

ELECT—User Identity & Privilege Management

DETECT —Threat and Vulnerability Management

Services Oriented Security Architecture

The business drivers that encourage services oriented thinking and underpin the need for information services and supporting SOA, force changes in the way security is conceptualised. For this Capgemini has developed the SOSA model, which combines the three major components shown in Figure 1: Protect, Elect and Detect. SOSA represents a fundamental shift from protecting the content, to personalising the security system to the user. Moreover, for the security technology to do its job reliably in support of this trend it must be deployed and managed as an integrated whole, not as a series of separately considered solutions.

Deperimeterisation Principles:
- devices protect themselves
- protected data centres
- security automation
- keep network security, but do not rely on it

Used in the healthcare environment, the following principles apply to three SOSA components:

Protect

Security in this component is focused around the information itself, and provides different kinds of information protection. Principles are:

- Protection requirements are no longer simply about perimeters, the old model is no longer suitable—protection should be provided based on the deperimeterisation principles;
- SOSA requires protection near the services and applications, instead of on the network boundary—build a security abstraction layer that abstracts security from services and applications.
- Application level security has become relatively more important to secure healthcare transactions—provide protection around the information itself, not the medium on which it is stored or transported; this allows protection and control of the information, even when it has left the trusted domain.

Elect

Here security is focused on the user. Elect type controls are designed to manage identities and privileges—access and authorisation. Principles are:

- 'Identity' is now centre stage, replacing 'fortress mentality';
- Separate federated authentication from service or application driven authorisation, allowing re-use of authentication credentials and granular access privileges;
- Define permissive access policies, allowing access to information in emergency situations—'allow access when urgent, ask questions later'.
- Integrate Identity and Access Management with Context Management wherever possible.

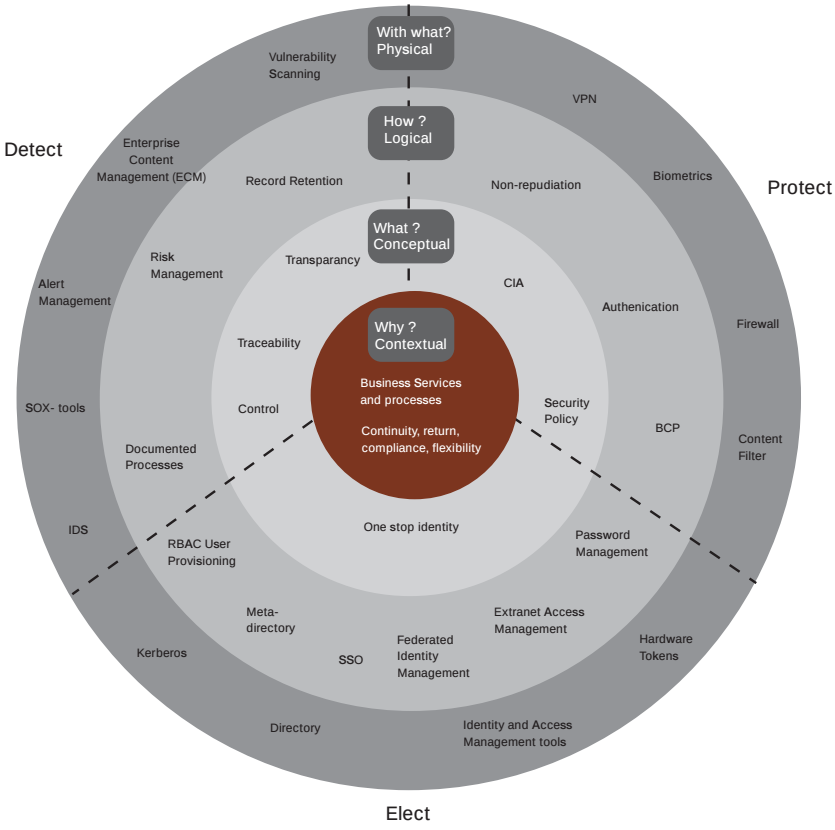
Detect

Technology in this space provides the capability to monitor, analyse, and respond to threats and incidents and relates to the audit and analysis capability needed to support the third principle in the elect space. Principles are:

- Less emphasis on prevention and more on reaction with real-time monitoring and response;

- Thorough logging and audit is required to ensure users that perform unauthorised actions can be held accountable;
- Real-time monitoring and response capabilities are becoming essential to ensure a timely response can be given to incidents that threaten the availability of services;
- Align access and audit policies to ensure a high level of scrutiny in case of emergency or in case of unpredicted but valid access requirements.

Figure 1: Services Oriented Security Model



Although Web Services security is a major building block of SOA security, it only addresses the technical capability to create, exchange, and interpret security information, which is an essential but relatively small part of SOA. SOA security is predominantly concerned with information and process, rather than technology.

SOSA does not necessarily require the implementation of available 'per message security' standards if the business does not require it. The implementation o of SOSA with conventional Internet security protocols (e.g., TLS/ SSL), good record keeping and tight business agreements can be a solid basis.

Deperimeterisation

Capgemini view is that SOSA and SOA security goes hand-in-hand with deperimeterisation. The increasing emphasis on application level security and the increasing inadequacy of the network perimeter based security model, encourage the adoption of a new model also called the deperimeterisation model. The following principles concerning deperimeterisation apply:

Re-perimeterisation requires a good balance between manageability, security and cost

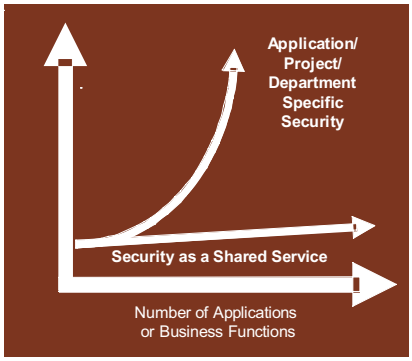
- All devices should protect themselves.
- All devices should authenticate themselves.
- The data centre should be.
- Automation is the key to success.
- Keep network perimeter security such as conventional firewalls, but do not rely on them.

Based on the last principle, a better term for deperimeterisation would be reperimeterisation. In the new model perimeter security will still be used, but at different locations, with the protection of corporate networks becoming more focused on maintaining service availability than protecting the data itself.

Although deperimeterisation has many advantages, such as network cost reductions, it has several drawbacks:

- Costs for security operations are increased, because device protection requires more effort than perimeter protection. Patch management for 150,000 workstations and 4,000 servers is more difficult and time consuming than for one firewall, even if this process is fully automated.
- Protecting the networks using VLANs and VPNs requires very intricate configuration if the network must perform well and be secure at the same time. Managing a single firewall is far simpler. This means that managing deperimeterisation does involve a certain amount of additional risk.
- Lots of legacy machines exist that cannot be protected or many applications that will not work if you harden the platform, which means that deperimeterisation cannot be implemented in one fell sweep and requires careful and long-term planning.

3 SOSA services for Healthcare



Security Abstraction

The main SOSA principle dictates that security should be abstracted from the core functional services. The main advantages of security abstraction are:

- Reduced application development costs;
- Reduced security, identity and access management effort and cost through centralisation;
- Homogeneous and consistent security policies through centralised specialist security services managed by Information Governance services.

For SOA environments, this implies the implementation of separate and dedicated security services. It depends on the type of service whether it will be a shared services invoked by other services (such as authentication and authorisation services) or whether they are reverse proxy or mandatory gateway services (such as filtering and anti-virus).

The characteristics of the most important SOSA services for healthcare are described below.

Federated Authentication

In the new reperimeterised security model, the enforcement elements (the so-called policy enforcement points) must be distributed across the various data centres and implemented either in the applications or close to them. The components that make the security decision (the so-called policy decision points) could be implemented in a more centralised fashion, possibly as published services. The implementation decisions regarding the policy decision points are mostly based on requirements such as security, performance and resilience. The main examples of a published security services would be the authentication service to enable federated authentication.

Federation allows the registration of users in a local environment (a hospital or otherwise) and the re-use of the authentication credentials elsewhere. This avoids the user having to re-register in every other locality. The main requirement for federation is that the various environments have to agree common policies and standards and must trust each other's ability to register users properly and manage the associated IT professionally according to these standards. Not a trivial requirement.

Federation if implemented properly supports single sign on (or reduced sign on where relevant). Many healthcare organisations grapple with SSO to reduce user frustration and increase user effectiveness.

Granular Authorisation

Authorisation services determine whether access or data manipulation requests are appropriate. In healthcare this decision can be based on various pre-established pieces of information, such as the specific access request, the assigned user role(s), information related to the patient such as patient preferences, patient stated permissions or refusals and relationships between patient and care professionals.

This pre-established information however would not cater for emergencies or unforeseen circumstances. Therefore for certain roles also the notion of legitimate purpose might be used to in effect override the authorisations based on pre-established information.

Within the limits of that particular role, a certain level of confidence of the legitimacy of purpose of the request should be established based on several pieces of information, such as professional registration, employment status, user statement of legitimate purpose, etc. and, if required, physical user location, end-system identity (e.g., PC number or address), etc. A relatively low confidence due to the suspect nature of the request does not necessarily imply the request is denied. It does mean however that such as access event will be subject to increased scrutiny. That is why the Audit and Logging services are very important for healthcare SOSA.

The Authorisation Policy that governs the access could be seen as the sliding bars on a music mixer, which is the tool to control the risk levels associated with access control. The ideal mixer position is where the security risk related to illegitimate access is acceptable and balanced with the risk of false refusal of legitimate requests (i.e. the clinical and other business processes can function without restriction from the access controls).

Authorisation services are policy decision points that can be implemented in shared services that can be called by various other healthcare information services, but also as dedicated functionality. Note that in SOSA, the authentication and authorisation services are distinctly separate, particularly in a federated environment.

Context Management

Particularly important for healthcare is the integration of the authorisation service with context management services. Context Management allows a user to gain access to all relevant information for a single specific patient at the same time, even though this information resides in various different systems or information services. This significantly reduces the risk of selecting the wrong patient, increases user effectiveness and supports single sign-on.

Logging and Audit

A cornerstone of SOSA in healthcare is the ability to investigate user behaviour and hold users accountable for their actions. This requires gathering a comprehensive and aligned set of infrastructure and application logs to form an end-to-end audit trail. This trail might cover user actions across various services and systems owned and managed by different organisations.

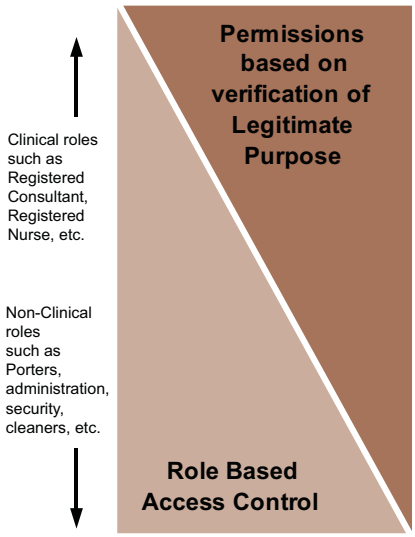
With the limited budgets in healthcare and the importance of harmonised logging and audit policies (see below), this facility seems best to be provided in a central or shared fashion.

Infomation Governance

The proper governance of IT security within a federated healthcare environment is essential. Federation requires trust. Trust that the partner healthcare organisations comply with IT and security related service level agreements, trust that they manage their information and security services accurately and trust that the IT security mechanisms behave predictably. Information governance is needed to provide this trust.

In the commercial on-line world trust is mostly established on a peer-to-peer basis. In healthcare however it is much more efficient and effective to jointly agree governance standards to which compliance will monitored centrally and enforced locally. Service oriented environment lend itself well to this governance approach.

Figure 2: Sliding scale authorisation



Services publish what they do, not how they do it. Similarly with the information governance standards, they prescribe the results of the process and not exactly how they must be achieved. This approach allows freedom to organise information governance processes according to local requirements but which ensures mutual trust in the quality of these processes.

Specific information governance aspects that need to be covered are:

- Joint policies and standards on user registration and authentication.
- Joint policies and standards on logging and audit.
- Facilities to allow security officer (in UK the Caldicott Guardian) to control (access to) their data even though this data does not reside on the IT system directly in control of their organisation.

Web services security

SOA security is more information and process oriented rather than technology oriented. Web services security (WS-security), however, addresses the technical capability to create, exchange and interpret security information. This provides a motivation to view Web services and services based architecture separate. They are not synonym for each other: Web services provide the technical capability whereas SOA concerns information, application and process.

SOA and Web services security are typically associated with 'per message security' and in, say five years' time this is probably applicable. At the moment however standards are still not mature enough, therefore more conventional measures are required. Experience with SOA security architectures shows us that it is possible to implement SOA security with the current more traditional approach and technologies. Transport level security, good record keeping and procedurally built trust relationships would still do the trick.

4 Main implementation challenges

Service Oriented Security Architecture is not simple. It must be adequate to accommodate various business relationships, but it must also provide sufficient flexibility to support the ever changing business environment, which is particularly important in a healthcare environment. The following challenges exist.

Achieving and maintaining trust

The trust between the various participants in transactions is paramount to the success of SOSA. Currently international activities have started to provide technical support for the establishment of trust between participants. Examples of standards that are currently being developed are WS-Trust and WS-Policy that enable the secure exchange of tokens and credentials between participants. However a major challenge still remains in establishing trust at the business level.

How do you know whether a participant achieves and maintains an appropriate level of security to underpin the trust required for a business transaction to take place?

Joint Information Governance and Security Accreditation is required to continuously audit the partner's security processes and infrastructure. The major challenge now is to create Information Governance hierarchies in which regional, national and international policies and standards are agreed and enforced. This is the only way in which service orientation can be implemented on a national or even international level.

Interoperability

Interoperability and compliance should be part of the strategy but depends heavily on the maturity and convergence of the technical standards that are developed and the products that become available that implement them. These standards should not only be applied for external interoperability only, they are also essential for internal communications on a SOSA basis as well.

Policy management

Each service requires a security policy which mandates the required security services that should be incorporated into the overall service policy. For instance patient preferences, security officer requirements, data sensitivity, etc. Currently standards exist to support policies, such as WS-Policy, however it is still a major challenge to define the required policies that suit a particular business best.

Legacy system inclusion

In healthcare many large and monolithic systems still exist and will not be phased out any time soon. Any SOA environment must take this into account and cater for this type of legacy systems, for instance by service enabling them by implementing a service oriented front-end. For SOSA this means that legacy system security mechanisms must be designed into the overall design and not be discarded as unimportant or irrelevant.

About the global Capgemini Security Consulting Community…

Comprehensive logging and audit

As mentioned before, the system of audit trails is one of the most important security controls, because in healthcare environments information access controls can be overridden, e.g. in emergency situations—excellent system of audit trails are therefore essential to provide the required level of traceability and accountability. The effort required to get this right should not be underestimated, the provision of an end-to-end audit trail is still a major challenge. Consolidation and analysis of both infrastructure and application logs covering many system and services across various organisations proofs very difficult in most environments and in particular healthcare; No single product on the market today can do all of this.

Device protection

A major element of deperimeterisation is the protection of end-devices, such as PCs, laptops, PDAs, USB memory devices, etc. To protect an end-device adequately is currently still a challenge because the technology is not yet matured and integrated sufficiently. Device protection products however, will evolve over time which will be more integrated and manageable centrally.

With more than 500 people delivering security services globally, Capgemini provides one of the largest security centres of excellence in the world. The global security community provides end-to-end information security services and solutions including:

- Security Management and Governance
- Infrastructure Security
- Identity and Access Management
- Architecture and Application Security
- Security Operations

Capgemini has an extensive track record of successfully delivering security services across the public and commercial sectors, enabling its clients to proceed with confidence—mitigating the threats, leveraging the opportunities and maintaining trust, and realising enhanced value.

Our experience has taught us that security technologies are not 'point' solutions; they require careful planning and should be considered as a strategic component of an Integrated Security Infrastructure. There is no 'one size fits all' solution as the needs and characteristics of each organisation vary widely.

Our consultants and engineers with experience in this area are networked globally via our security community of practice, actively sharing knowledge & experience. To maintain our advantage, we conduct regular market scans and internal product research studies. We closely follow the development of relevant emerging standards such as those developed by OASIS and our experts have access to research by analysts such as Gartner, META & IDC.

We have established formal alliances with leading security technology vendors. Our ability to deliver security solutions is further strengthened by these relationships; the scope and nature of our alliance activities ensure that we maintain our impartiality in consulting assignments while providing us with advantage on systems integration assignments.

For over 25 years, Capgemini Health has been a leading provider of consulting, technology, and outsourcing services to the healthcare industry. We deliver a broad spectrum of results driven solutions to make the vision of patient/citizen centric care a reality while maintaining a constant focus on improvements to the core care and operational services for our clients.

With a team of more than 700 dedicated professionals ranging from clinicians to care administration to industry consultants, to IT professional, Capgemini is able to cover the full scope of strategic, operational and financial issues including: business and IT strategy, solution architectures, business transformation, customer relationship management, revenue and supply chain management, cost reduction, ERP, health information system and outsourcing.

Capgemini's Healthcare Practice has been working with private and public health care organizations in countries around the world including Australia, Austria, Bulgaria, Canada, Denmark, France, Netherlands, Norway, Spain, Sweden, United Arab Emirates, United Kingdom, and the United States. We have worked with individual hospitals, national health services, public sector health agencies, academic health centers, post acute care facilities, physician groups, health insurers (payers), life sciences companies and health-related technology companies. Each has their own unique set of strategic, operational and business opportunities that are critical to the ongoing success of the organization. In addition, they all offer a set of specific information and care services required in the end-to-end patient/citizen centric care delivery model.

About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of Consulting, Technology and Outsourcing services, has a unique way of working with its clients, called the Collaborative Business Experience.

Backed by over three decades of industry and service experience, the Collaborative Business Experience is designed to help our clients achieve better, faster, more sustainable results through seamless access to our network of world-leading technology partners and collaboration-focused methods and tools. Through commitment to mutual success and the achievement of tangible value, we help businesses implement growth strategies, leverage technology, and thrive through the power of collaboration.

Capgemini employs approximately 75,000 people worldwide and reported 2006 global revenues of 7.7 billion euros.

More information about our services, offices and research is available at **www.capgemini.com**

PS456_12012006

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

www.capgemini.com

John Sluiter
Managing Security Architect
Tel: +44 (0) 870 238 2369
john.a.sluiter@capgemini.com

Austria
Thomas Fuschl
+43 1 211 63 8678
thomas.fuschl@capgemini.com

Benelux
Marlene Gigase
+31 (30) 689 6200
marlene.gigase@capgemini.com

Central & Eastern Europe
Alex Lagas
+31 (30) 68 92200
alex.lagas@capgemini.com

Denmark
Erik Kragelund Helms
+45 87 38 70 15
erik.helms@capgemini.dk

European Commission
Celine Charpiot
+33 6 83 66 12 73
celine.charpiot@capgemini.com

France
Antoine Georges-Picot
+ 33 1 49 675305
antoine.georges-picot@capgemini.com

Portugal
Jorge Martins
+351 93 783 31 38
jorge.martins@capgemini.com

Spain
Julio Gómez Medina
+34916377847
jgomezme@capgemini.es

Sweden/Nordic
Håkan Petersson
+46 853684843
hakan.petersson@capgemini.se

United Kingdom
Andrew Jaminson
+44 (0)870 904 3723
andrew.jaminson@capgemini.com

United States & Global Lead
Gerry Yantis
+1 571 336 1614
gerald.yantis@capgemini.com