Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

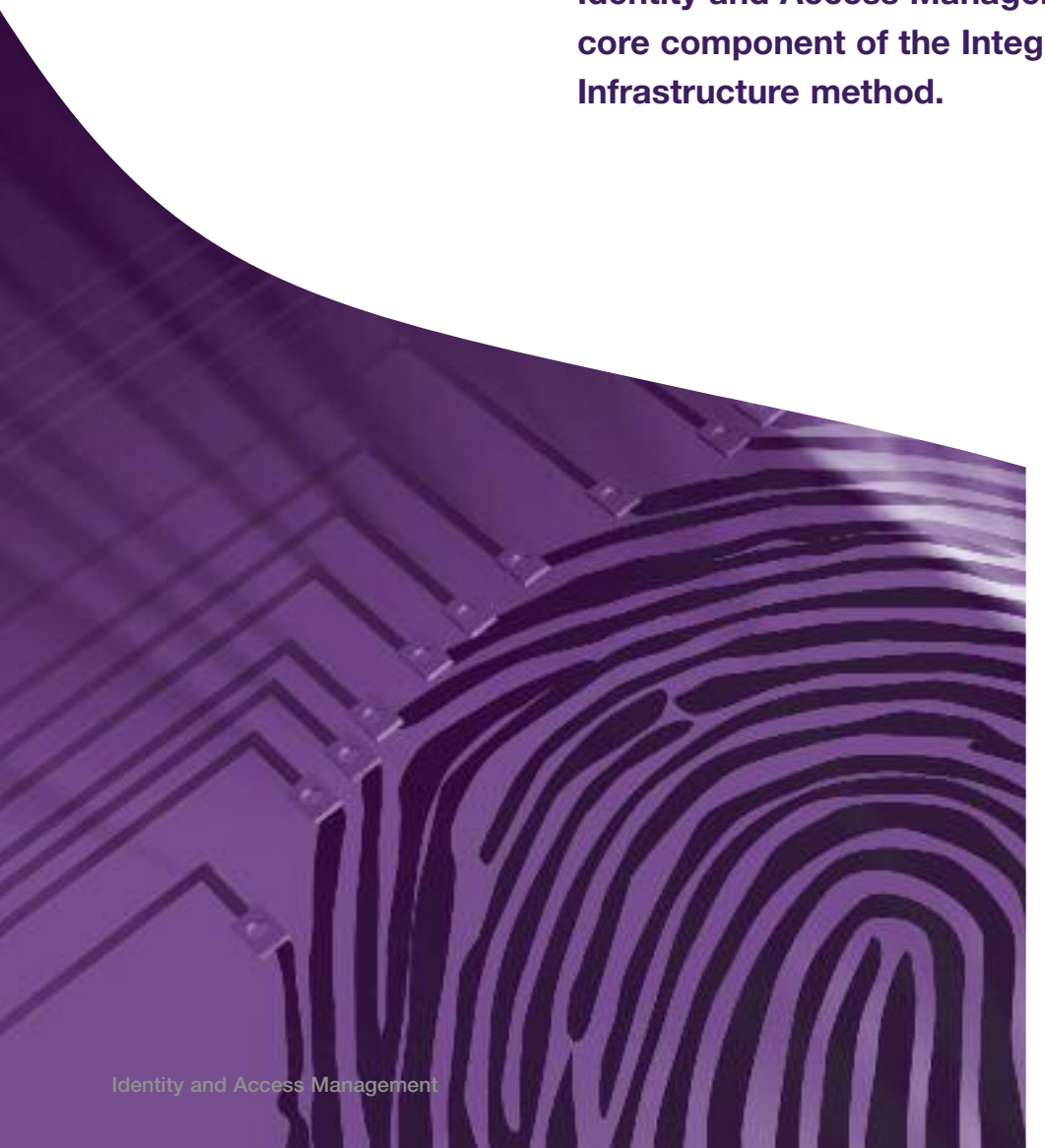
the way we do it

Identity and Access Management

Contents

Identity and Access Management is a central asset in today's enterprise landscape. It comprises processes and information technologies that are interrelated and mutually dependent on all business areas. If planned and implemented well, it ultimately helps strengthen regulatory compliance, secure operations and improve operational agility.

Capgemini's vision of Adaptive Security(SM) places Identity and Access Management technology as the core component of the Integrated Security Infrastructure method.



Business Rationale

Identity and Access Management fuses technology and process in a way that impacts both the cost base and productivity of an organization.

Business has always been about relationships. Whether they're with customers, employees or partners, relationships are one of the most valuable assets in business. Electronic identities are increasingly used to create and maintain these relationships and therefore are an important enabler for e-business or public services.

There is also a close and vital relationship between business processes, business functions, the organizational structure, the identities and the resources used. As a result, data requires context-driven access management to support the interaction between different identities. IT departments need to be able to adapt access management to the ways in which systems are actually used.

The character of these relationships has changed substantially over the years, making their effective management essential. First, the relationships now span beyond the organizational boundary and form the basis of extended business processes that connect the organization with its suppliers and customers. Second, their nature is becoming more dynamic, reflecting the changing business models. Finally, the number of relationships today is much bigger than at any time in the past. As a result, organizations today must maintain a network of dynamic relationships between customers, employees and partners to continuously adapt to the changing environment. Simultaneously, they must do this in a way that provides a safe and secure platform upon which they can conduct their business.

Organizations have deployed—and continue to do so—a range of (information) systems that are changing rapidly. They also extend beyond organizational boundaries. There is increased and complex exchange of data, and more storage of data in various places and in different formats. Data is increasingly dependent and there is more use of central administration. Today's diverse communities of users all need access to the right information at the right time.

Legislators and regulators are increasing the requirement for organizations to demonstrate that they are adequately managing risks to the value of their information assets. This value can be impacted by threats to information confidentiality, integrity and availability. Breaches to information security can cause direct financial losses, directly impact customers, adversely affect reputation and brand, and even reduce the value of shareholders' equity. In addition, legislative and regulatory pressure is creating increased demand for individual traceability and accountability. For these reasons, organizations need to place Identity and Access Management at the center of their information security strategies.

This paper provides an insight into what Identity and Access Management comprises, what it can deliver, and what Capgemini can offer in this space. We also take a look at the future with our TechnoVision and near-future developments.

Services

An Identity and Access Management system can administer the authentication and entitlement of users to access a resource. It identifies the user and the context and determines what the user can access. It also determines what the user can do, and protects the information by signaling when the security has been compromised. However, an Identity and Access Management system needs to do much more than simply regulate access; it must also manage the lifecycle of the user, the resources and the access. Otherwise, every time a customer, vendor, or employee changes status, the process of updating access privileges would waste precious man hours and drive up costs. To handle these different requirements, an Identity and Access Management system is composed of different services:

Service	Functionality
Authenticate Subject (administrative functions behind identities i.e. Identity Management)	▪ Identity Directory Service ▪ Joiners/Movers/Leavers Services ▪ Management of the user's identifiers ▪ Identity Federation ▪ White pages/Yellow pages ▪ Management of (strong) authentication.
Access Resource (Entitlement i.e. Access Management)	▪ Rule Management, Business Role and Profile Management (what is a subject allowed to do with a resource, under what conditions/in what context) ▪ User Self-Services, Delegated Services and Admin ▪ Workflows (management) ▪ Provisioning of user accounts and access ▪ Management of physical access ▪ Application Policy Enforcement/Management ▪ Single Sign On ▪ Real-time control of access to objects/resources.
Monitoring	▪ Audit and Reporting ▪ Re-Certification (Attestation) ▪ Alarm & Event Management

Benefits of Identity and Access Management

Identity and Access Management fuses technology and process in a way that impacts both the productivity of an organization and its bottom line. This gives an organization three different ways to justify a strong Identity and Access Management strategy: one focuses on the cost of avoidance, while the others describe the benefit of this approach:

1. **Cost of Non-Investment (CONI)**
   - Failure to improve business facilitation and service levels
   - Inability to improve security through lifecycle management of joiners, movers and leavers
   - Regulatory non-compliance
   - Inflexible IT infrastructure that cannot adapt to changing user communities and behavior.
2. **Total Cost of Ownership (TCO) – benefit**
   - Reduced operational costs through automation and streamlining of IT administration processes
   - Reduced lead time and cost of new application development.
3. **Return on Investment (ROI) – benefit**
   - Improved productivity and user experience
   - Enables secure (online) business models
   - Improved ability to cope with organizational and business changes
   - Savings on per-user software licenses.

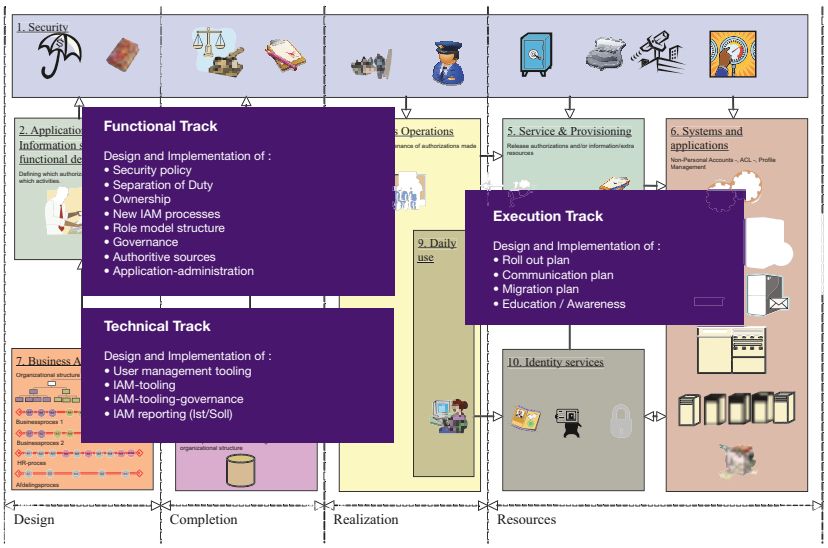
Our Solution

Capgemini's vision for Identity and Access Management sees it working as an Invisible Infostructure[1] connecting and integrating various technology and departmental islands. From a technical perspective, identity infrastructure consists of user security and registration functionality that is underpinned by directory and integration services, and supported by advanced administration services. Related business processes and services then leverage the identity infrastructure. From an organizational perspective, Identity and Access Management elaborates on and extends the security and risk management organization.

It is clear that there is a major dependence between Identity and Access Management and Enterprise Architecture as far as governance, risk management and compliance are concerned. Our Identity and Access Management Framework, which is at the basis of our solution, provides views of technical, organizational and business aspects of Identity and Access Management.

The unique aspect of Capgemini's Identity and Access Management Framework is its flexibility. Partitioning of the Identity and Access Management landscape into distinct process and technology parcels delivers flexibility. This provides a solution that allows for phased implementation and migration to the new infrastructure and business processes.

Figure 1: Identity & Access Framework



1 Invisible Infostructure is the end-state of infrastructure as we currently know it, using virtualization, grid and automated management technologies to deliver infrastructural services as a commoditized—preferably invisible—utility.

Our Approach

We employ a three-stage approach to the development of an Identity and Access Management infrastructure. This begins with careful planning, which then transitions into preparation, followed by the final implementation of the solution.

In the planning stage, we focus on understanding and capturing the high-level business (functional) and technical context. This is achieved by utilizing a combination of focused interviews and facilitated sessions with key stakeholders. From this information, we can identify benefits and concerns and provide the justification for the expenditure.

The preparation stage identifies the particulars of the technical solution and relevant user processes. We refine the understanding of the current technical landscape and develop a technical solution blueprint. Products are considered based on the requirements. Finally, a roadmap comprising the initiatives required to implement the blueprint is developed.

In parallel, we model the relevant user and business processes to ensure cohesion with the technical solution. This allows us to streamline the administration processes to gain operational efficiencies. Finally, we develop user training and communication modules to ensure a smooth rollout.

The implementation stage realizes the components of the technical solution, such as directory integration and consolidation, provisioning, authorization, authentication services and application integration. This stage also puts in place the operational processes for the governance of Identity and Access Management.

Our experience has taught us that security technologies are not 'point' solutions. They require careful planning and should be considered as the strategic component of an Integrated Security Infrastructure. There is no 'one size fits all' solution as the needs and characteristics of each organization vary widely. The chosen model must fit with the characteristics of the organization. Identification and authentication have more focus in the educational sector. Think about e-exams. Is the person taking the exam really the student the exam is intended for? Access is the same for all students. In other sectors it is different. For example, in the health sector logging (audit based access control) is more important. A first aid team needs instant access, but needs to justify their access. In the finance sector, least-privilege, compliance & separation of duties are important factors.

The Capgemini Advantage

The Intelligence Grid©

A recognition of the importance of collaborative behavior in response to this complex environment prompted Capgemini's launch of a new approach to Public Security technology in 2006. We called this concept the Intelligence Grid©—an innovative concept that improves internal efficiencies and opens up enhanced avenues of collaboration. Founded on the sound principles of Service-Oriented Architecture, the Intelligence Grid® approach allows the smooth interoperability of Public Security systems, enabling the active and efficient collaboration needed between different government agencies as well as different governments.

Capgemini Public Security recognizes Identity and Access Management as the core of the Intelligence Grid.©

It is crucial to be able to identity what the current situation is and to have knowledge of the various approaches in use. One must also be able to translate demands into technical, functional and organizational elements in order to develop a consistent, safe, effective and efficient strategy for Identity and Access Management.

Our advantage in the field of Identity and Access Management is built on our experience, our capabilities and strategic alliances.

We have considerable experience with various types of Identity and Access Management engagements ranging from organization strategy, solution architecture and business change consultancy assignments, through to the implementation and integration of technical solutions. These engagements have been carried out in diverse commercial and public environments.

Capgemini's expertise embraces both commercial and public security. We have, for example, proven capabilities in iris identification at borders, mobile digital fingerprinting supporting police departments on the front line, and automatic number plate recognition, video identification and integration of physical and logical access. These are all examples of Identity and Access Management.

Our consultants and engineers with vast expertise in this area are networked globally via our Identity and Access Management Center of Competence, actively sharing knowledge and experience. To maintain our advantage, we conduct regular market surveys and internal product research studies. Capgemini also closely follows the development of relevant emerging standards such as those developed by OASIS and our experts have access to research by analysts such as Gartner, IDC, Burton and the Open Group. We often present aspects of Architecture and Security to and from these groups.

Our ability to deliver Identity and Access Management solutions is further strengthened by our strong alliances with leading Identity and Access Management vendors such as IBM, Microsoft, Sun, CA, SAP, Oracle and BMC. The scope and nature of our alliance activities ensure that we maintain impartiality in consultancy assignments, while leveraging maximum advantage on systems integration assignments.

Near-Future Developments

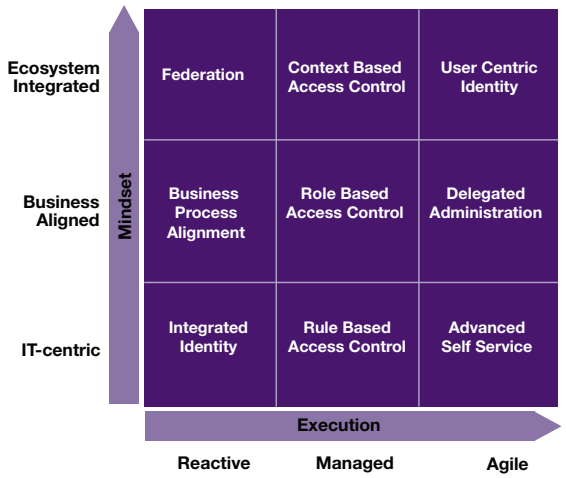
Capgemini is deeply rooted in the fast changing business and IT environment, and is constantly upgrading capabilities to stay current with the latest innovation in the marketplace. In many cases, we have taken a thought leadership role to lead the way. There are various new developments where Identity and Access Management plays an important function:

- Web 2.0
- Mashups
- Federation
- Trust(ed brokers)
- Data classification, Data leakage and Deperimeterization
- Rightshore®
- Shared services, one-authoritative source
- Service Orientation
- Identity fraud/theft and Privacy protection
- User Centricity and Lifelong personal identity
- Lifecycle Management
- Trend analysis and (real-time) monitoring
- Integration of physical & logical identities and access.

With the evolution of Web 2.0, which is focused on the enablement of unstructured collaboration, it will be harder to associate an identity to a predefined role. It will become more critical for enterprises to secure their information through management of application policies. The system needs to be more responsive to autonomous system users in heterogeneous environments. Management of application policies has to be identified in a hierarchy structure that is defined at the enterprise level, while at the same time delegating granular policy definitions at the business unit level. Management of these policies can be addressed through effective Identity and Access Management and its consistent security services and business rules.

Another development around Web 2.0 is user centricity. Service-specific identities are managed transparently. On the one hand, a user can create as many identities as he or she wishes and has full control over his or her privacy (e.g., pseudonyms). Identities and attributes become independent from identity providers, and can be freely moved between providers. On the other hand, life-long personal identities store more personal data about someone, including biometric (non-changeable) aspects. Because of this, identity information (financial, medical, biometric, etc.) needs special attention, and privacy friendly service discovery and search techniques are expected to emerge in the near future.

Figure 2



About Us

The Open Group – Jericho Forum

Capgemini is a founder and member of the Jericho Project Research Group (as part of The Open Group). It focuses on defining new security architectures and a security roadmap for implementing networks without perimeters. In order to design and build a de-perimeterized network solution, a combination of at least the following modules is needed: secure communications, inherently-secure computer protocols, endpoint security, adequate authentication and authorization of all the entities, accounting, trust brokering services, and automatic data classification on multiple security levels. It places Identity and Access Management as a major cluster.

TechnoVision 2012

Our "TechnoVision 2012" provides a clear picture of the information technologies that are the most relevant to users and sheds some light on how these technologies and their evolution will impact business. It places Identity and Access Management in various clusters:

- 'User Management' as part of the YOU Experience
- 'Real-Time Business Process Control' and 'Composite Applications' as part of Process-on-the-Fly
- Identity and Access Management is essential in order to be able to 'Thrive on Data'. This includes 'Mastered' Data Management (Data Governance)
- 'Software-as-a-Service' as part of the Sector-as-a-Service
- 'Deperimeterized Jericho style Security and Identity' as part of the Invisible Infostructure
- And the virtual Service Orientation cluster.

About Capgemini

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies.

Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working - the Collaborative Business Experience® - and through a global delivery model called Rightshore®, which aims to offer the right resources in the right location at competitive cost. Present in 36 countries, Capgemini reported 2007 global revenues of EUR 8.7 billion and employs over 86,000 people worldwide.

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

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

www.capgemini.com

Contact:
Barry Beal (UK), Managing Technical Architect
Coen de Jonge MSc CISSP CISA (NL), Managing Consultant
Jan-Roel Löwenthal MA. BA. CISSP (NL), Managing Consultant
Abdullah Rashid CISSP (USA), Senior Manager

The Netherlands: security.nl@capgemini.com
UK: barry.beal@capgemini.com
USA: abdullah.rashid@capgemini.com