On Adaptive Identity Management: The Next Generation of Identity Management Technologies

Marco Casassa Mont, Pete Bramhall, Joe Pato
Trusted Systems Laboratory
HP Laboratories Bristol

HPL-2003-149
July 23rd , 2003*

E-mail: marco_casassa-mont@hp.com, pete_bramhall@hp.com, joe_pato@hp.com

identity management, adaptability, flexibility, integration, policy-driven management, context awareness, collaboration

Identity management plays a key role in enabling personal, business and government activities along with interactions and transactions in the digital world. The "chapter 1" of identity management is about the current paradigm, i.e., multiple, slightly integrated products and solutions for relatively static, closed and well controlled environments. It involves little integration, at the management level, with the management of other aspects such as security, privacy and trust. Current trends suggest that the digital world is going to be more and more flexible, interconnected and open. The boundaries between enterprises, organizations, societies and governments will become increasingly blurry as people play different roles in multiple activities that span across heterogeneous contexts. Identity management needs to evolve. We believe that the "chapter 2" of identity management is about *adaptive identity management* i.e., open, flexible, policy-driven, context-aware identity management that scales across multiple contexts and levels of abstractions and is integrated with the management of security, privacy and trust. The aim of this paper is to illustrate emerging requirements along with our vision of adaptive identity management, describe a possible high-level model for adaptive identity management and explain some of its properties.

* Internal Accession Date Only

Approved for External Publication

On Adaptive Identity Management: The Next Generation of Identity Management Technologies

Marco Casassa Mont, Pete Bramhall, Joe Pato

Hewlett-Packard Laboratories, Trusted Systems Laboratory
BS34 8QZ, Bristol, UK
marco_casassa-mont@hp.com, pete_bramhall@hp.com, joe_pato@hp.com

Keywords: Identity Management, Adaptability, Flexibility, Integration, Policy-driven Management, Context Awareness, Collaboration

Abstract. Identity management plays a key role in enabling personal, business and government activities along with interactions and transactions in the digital world. The “chapter 1” of identity management is about the current paradigm, i.e., multiple, slightly integrated products and solutions for relatively static, closed and well controlled environments. It involves little integration, at the management level, with the management of other aspects such as security, privacy and trust. Current trends suggest that the digital world is going to be more and more flexible, interconnected and open. The boundaries between enterprises, organizations, societies and governments will become increasingly blurry as people play different roles in multiple activities that span across heterogeneous contexts. Identity management needs to evolve. We believe that the “chapter 2” of identity management is about *adaptive identity management* i.e., open, flexible, policy-driven, context-aware identity management that scales across multiple contexts and levels of abstractions and is integrated with the management of security, privacy and trust. The aim of this paper is to illustrate emerging requirements along with our vision of adaptive identity management, describe a possible high-level model for adaptive identity management and explain some of its properties.

1 Introduction

Identity management is important in different contexts, including the enterprise, e-commerce and government, to underpin business processes and services and enable digital interactions and transactions.

There are different competing demands on what identity management should provide, different concerns on what it should focus on and a few conflicting interests: enterprise focus vs. consumer focus, mobility vs. centralisation, legislation vs. self-regulation, subjects’ control vs. organisations’ control, privacy vs. free market, etc. They are dictated by various stakeholders, including identity subjects, enterprises, service providers and government agencies, which have different objectives and priorities when dealing with the management of digital identities.

Many products and solutions are available on the market: they address problems in different areas such as provisioning and accounting, authentication, authorization and data consolidation. Currently, they are evolving to allow a higher level of integration with the IT stack (i.e., networks, platforms, OSs, applications, middleware, services, etc.) and the associated business solutions; nevertheless most of these products and solutions still manage identity aspects in relatively static, closed and well-controlled environments.

Identity management has strong links with the management of security, trust and privacy: all these aspects are directly or indirectly involved when managing identity information. In today’s identity management products, there is little integration and synergy with these aspects. Each product usually provides its own set of management tools. Because of this fragmentation, any request to enforce new requirements or policies on identity information might require a lot of work and take long time to be achieved.

Current trends suggest that the digital world is going to be more and more flexible and dynamic. Barriers and boundaries between enterprises, organizations and government agencies are getting increasingly indistinct as people cover multiple roles and are involved in activities that span across heterogeneous environments. This creates a broad new set of opportunities in the personal, social and business areas. On the other hand this also creates new threats and issues.

Digital identities and identity management need to play a strategic role in enabling this new world and addressing related issues. A new generation of identity management solutions is needed to provide mechanisms to rapidly adapt and cope with changing environments, in personal, business and social contexts. We refer to it as *adaptive identity management.*

The goal of this paper is to create awareness of new requirements and introduce our vision of *adaptive identity management* along with some of its properties. Section 2 describes important aspects of identity. Section 3 provides an overview of the current identity management landscape. Section 4 describes new trends and issues; section 5 illustrates emerging requirements. Section 6 introduces our vision on adaptive identity management and section 7 briefly discusses how to move forwards.

2 Aspects of Identity

Identity and *identity management* are overloaded terms. They are used in different contexts, at different levels of abstractions, with different meanings. This section introduces some terminology and discusses a few identity-related aspects.

Entities in the physical and digital world (i.e., people, devices, systems, services, etc.) can be intrinsically characterised and described by means of *attribute*s and properties. Some of these attributes, including personal details, financial information, social information, etc., can be used for identification and profiling purposes.

In this paper we refer to *identity information* as a set of attributes (along with their values) describing relevant aspects and properties of an entity [6]. This information is dynamic: the set of attributes and their values can change over time.

Different *views* on an entity's identity information can be created, disclosed, accessed and used by multiple parties. A *view* consists of an aggregation of one or more attributes. Each attribute can assume different values, depending on the view it belongs to and the context where it is used.

A *digital identity* (or *identity*) is itself a *view* on the identity information associated to an entity, at a specific point of time. Digital certificates, credentials, etc., are examples of digital identities.

In general, *views* on identity information might include any meaningful aggregations of attributes that can be used for identification and profiling purposes, including e-mail addresses, credit card details, personal information, roles, rights, etc.

Attributes and views can be qualified by *metadata*, i.e., additional attributes such as information about their certifier(s), their provenance and validity, management policies, etc. Metadata might define *relationships*, *references* and *dependencies* among attributes and views.

For simplicity (unless otherwise stated) we will use in an interchangeable way the terms "digital identity" and "view on identity information". We stress the fact that a "digital identity" might consist of any aggregation of attributes and not only classic attributes, such as the ones defined by X.509 identity certificates [1].

Today, digital identities are mainly associated to people. In the future their usage will be increasingly extended to devices, trusted systems, web services and any type of proxies and agents that mediate interactions and transactions in the digital world.

Figure 1 shows the relationships between identity information, attributes, views and usage contexts. In general identity "subjects" are aware of the existence of only a part of their "identity information", they "own" just a portion of it and they can directly control only a subset of it. Broadly speaking, rather than talking of "identity owner" it is more appropriate to talk about "identity subject" as identity information is not necessarily owned by the entity this information refers to. From an identity subject's point of view, there are multiple perceptions of their identity information [2, 43]:

- "**Me Me**": it is the part of identity information that the subject is aware of and directly controls;
- "**Known Me**": it is the part of identity information that the subject is aware of and indirectly controls;
- "**Unknown Me**": it is the part of identity information that the subject is not aware of and has no control on.

Multiple views can exist on an entity's identity information. These views can be used within and across different contexts (personal, social, e-commerce, government, business, etc.) to enable interactions and transactions.

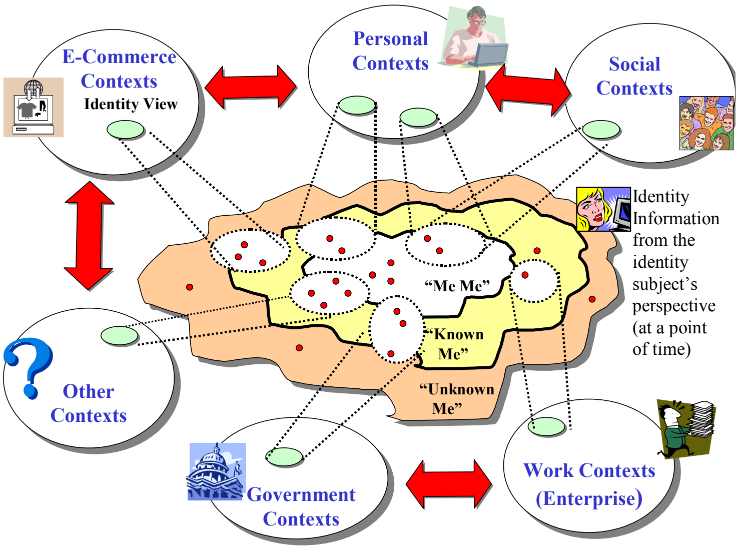


Fig. 1. Identity Information, Views and Contexts

The management of an entity's identity information is constrained and characterised by important aspects, including:

- **Control**: different stakeholders can access, use and manage this identity information and/or related views. These stakeholders include the identity subject, *third parties* that are known by the subject (such as certification authorities, authorised e-commerce sites, TTPs, etc.) and *unknown third parties* (such as credit rating agencies, identity thieves, etc.).
- **Contexts***: identity information* and *identities* can be disclosed, accessed and used by different stakeholders in one or more contexts, including personal, social, e-commerce, enterprise and government ones. This can happen via a variety of means and systems including personal appliances, enterprise systems and web services.
- **Time**: identity information changes over time. New attributes are created, others are updated and others again are subject to expiration. The management of these changes is fundamental as it directly affects identity's integrity and consistency, its trustworthiness and its privacy and, indirectly, it has implications on processes like authentication, authorization, access control, etc.

Figure 2 and 3 are an attempt to graphically represent the above three aspects and highlight their relationships with identity information:

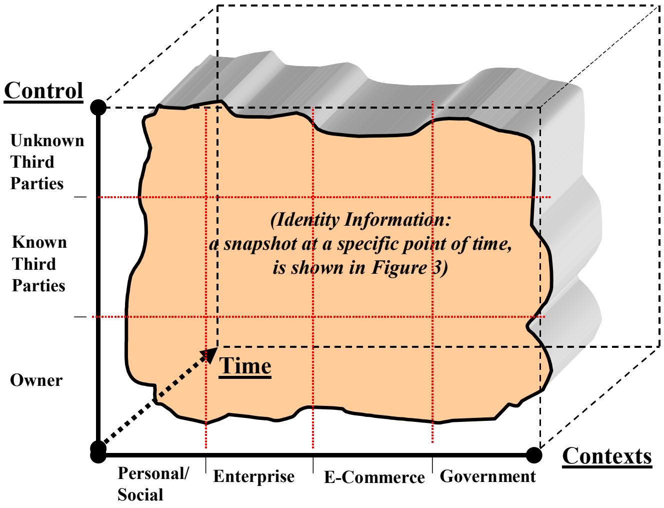


Fig. 2. Multi-dimensional Aspects of Identity Information

Figure 2 conveys a (simplified) multi-dimensional perspective on identity information, i.e., who controls which kind of identity information, at a specific point of time. Not only identity information changes over time but also the contexts where it is used and the stakeholders that control it change too: changes to identity information might happen in different contexts and be driven by different stakeholders.

Figure 3 provides more details about a snapshot of an entity's identity information at a specific point of time:

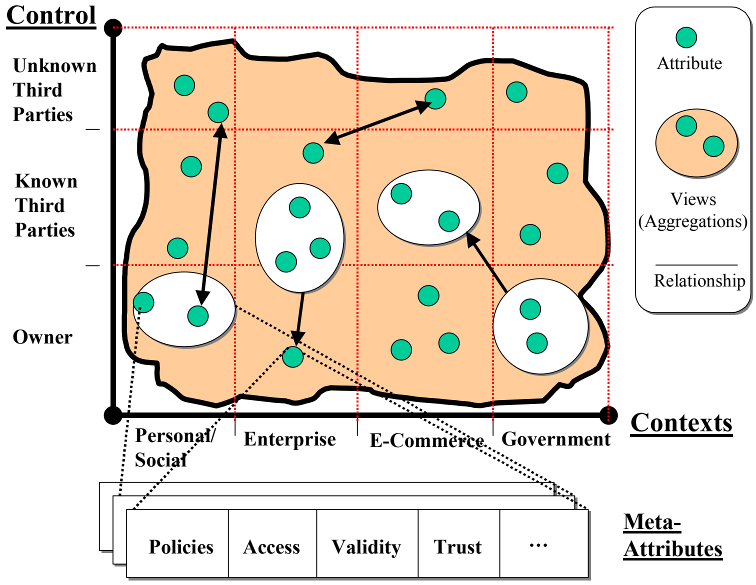


Fig. 3. Attribute Aggregations, Relationships and Meta-attributes

As anticipated, identity information is made of attributes, views and relationships. They are qualified by metadata, including management policies, access constraints, validity, etc. All these aspects can change over time.

Identity management has to deal with the management of this information along with its metadata (meta-attributes), cope with changes and make sure that the associated policies are satisfied.

The next section describes aspects of the current identity management landscape including current solutions and their related issues.

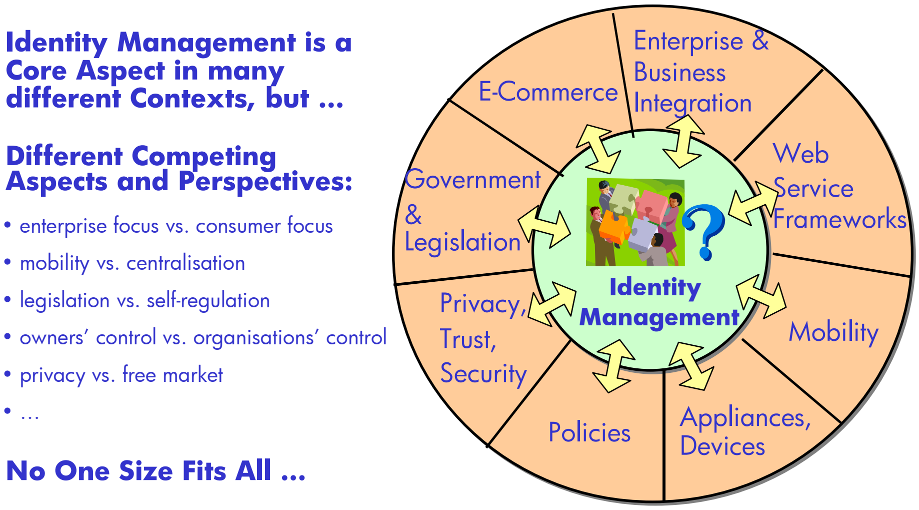
3 Identity Management

In this section we briefly introduce a few aspects of the current identity management landscape: we provide an overview of current identity management solutions and their core functionalities [3] along with related issues and problems.

3.1 Identity Management Landscape

The current identity management landscape is very complex because of the multiple interests, perspectives, concerns and technologies that are involved.

As anticipated in the introduction of this paper, there are different competing aspects on what identity management should provide and concerns on what it should focus on. Conflicting interests include: enterprise focus vs. consumer focus, mobility vs. centralisation, legislation vs. self-regulation, subjects' control vs. organisations' control, privacy vs. free market – see figure 4:



Identity Management is a Core Aspect in many different Contexts, but …

Different Competing Aspects and Perspectives:

- enterprise focus vs. consumer focus
- mobility vs. centralisation
- legislation vs. self-regulation
- owners' control vs. organisations' control
- privacy vs. free market
- …

No One Size Fits All …

Fig. 4. Identity Management Landscape

Priorities, interests and perspectives on identity management differ, depending on the involved stakeholders:

- Enterprises are driven by their business objectives and needs. They aim at the management of large sets of identity data to enable their businesses, rationalize their assets and simplify business interactions with partners and customers, manage the information lifecycle of their workforce and deal with access management to enterprise resources.
- E-commerce sites and service providers manage consumers' identity information with the hope to increase their sales, understand customers' needs, customize the provision of services or just sell this information to third parties.
- Government agencies are concerned with the control and protection of personal information of their citizens, the provision of strong and undeniable authentication mechanisms and the automation/rationalisation of the provision of their services via the web and the Internet.
- People have different concerns and needs depending on the role they play: they are right in the middle (or, depending on the point of view, the source) of most of the above competing aspects. As employees or consumers, they want to access and use services in the simplest and more efficient way, without any hassle. As private citizens they might be concerned about their privacy, they might distrust institutions and demand for more accountability of the involved parties.

This variety of interests and concerns, along with new emerging technologies, contributes to increase the complexity of identity management. All these aspects influence each other, via a spiral of potentially conflicting requirements. For example, new legislations are addressing citizens' needs for privacy but, on the other hand, they are constraining the way enterprises, e-commerce sites and service providers deal with the processing of personal information. The mobility of employees creates on one hand security and trust management problems to enterprises and organisations, on the other hand new business opportunities. Last but not least, emerging appliances and web service frameworks create new issues such as dealing with the identities of devices and web services and coping with delegation aspects and trust matters.

From a technological and IT perspective, identity management is just one of the aspects that are involved in the management of business solutions and the overall IT stack (i.e., networks, platforms, OSs, applications, middleware, services, etc.). Figure 5 shows some of the elements that influence it.

Identity management must be considered in a holistic way by including (among other things) the management of security, trust and privacy along with the management of policies, requirements and changes. All these aspects are very inter-related and affect business solutions and the IT stack at different levels of abstraction. Of course, the context dictates which IT elements and which identity management aspects are meaningful.

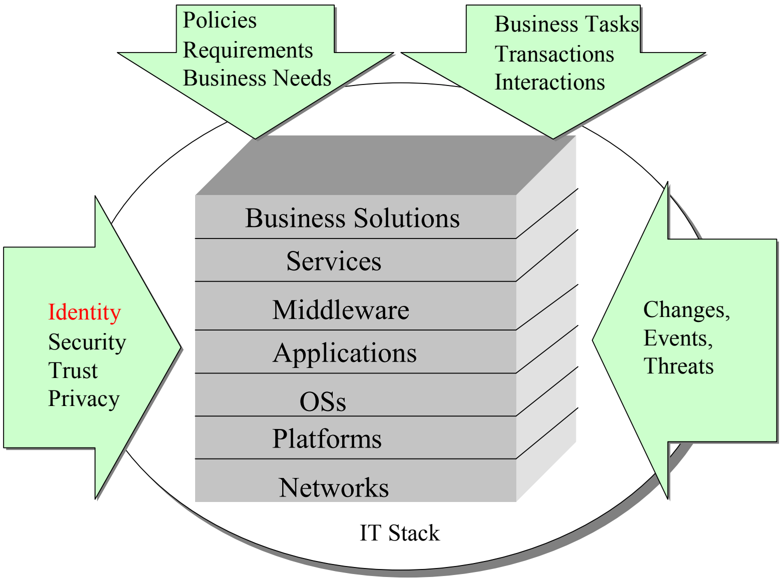


Fig. 5. Context where identity management operates

Further complexity derives from the fact that the execution of business tasks or the management of digital interactions and transactions can span among multiple domains. For example, in an e-commerce context, a digital transaction might require the involvement of identity e-commerce sites and the exchange of identity information among these sites: this has strong implications in terms of management of trust, privacy, authentication, authorization and accountability. Similarly this is true for B2B interactions or transactions within supply-chain communities.

The effectiveness and validity of identity management products and solutions depends, among other things, on how good they are at keeping identity information in a consistent and up-to-date state, satisfy related management policies and legal requirements, preserve privacy and trust and ensure that security requirements are fulfilled.

New requirements, new policies, changes or threats might affect the configuration of elements in the IT infrastructure and business solutions. As a consequence, complex reconfiguration activities might need to be done on multiple components, at different levels of abstraction.

Identity management plays a key role in this space: identity aspects need to be managed rapidly and orchestrated with security, trust and privacy aspects. In environments where business and customers' needs change frequently, identity management solutions have to be flexible and adaptable.

3.2 Current Identity Management Solutions

This section provides a brief overview of the state of the art of identity management products and solutions and discusses a few related issues. A more detailed analysis can be found in [4, 5, 7].

Today, many identity management products and solutions are available on the market. They supply functionalities such as authentication, SSO, authorization, auditing, provisioning, data storage, links to legacy systems and data consolidation. They target different types of users and contexts including e-commerce, service providers, enterprises and government institutions.

Figure 6 shows the main components and functionalities provided by current identity management products and solutions:

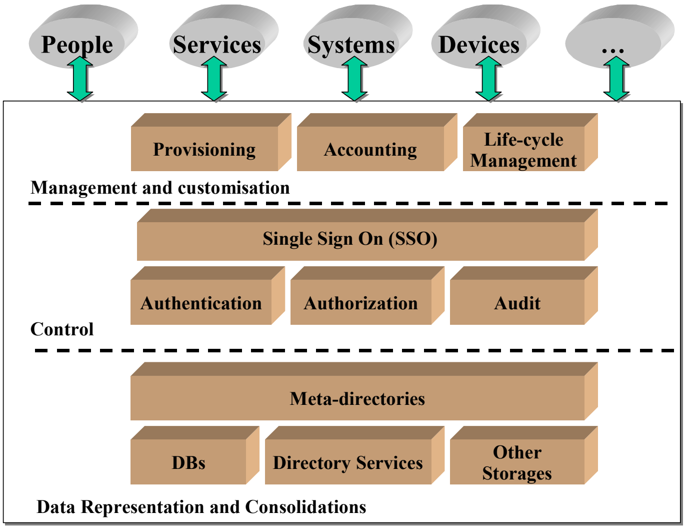


Fig. 6. Current Identity Management Solution Stack

Directory services and meta-directories deal with the representation, storage and management of identity and profiling information and provide standard APIs and protocols for their access [8, 9]. In particular, meta-directories address the important problem (especially for large organizations and enterprises) of consolidating, integrating and preserving the consistency of data, disseminated in a variety of heterogeneous systems, geographically spread across organization sites.

Authentication, authorization and auditing are core identity management functionalities. Authentication, in particular, is provided in a variety of ways ranging from local authentication on a system to complex distributed authentication [10,16], including single-sign-on (SSO) within and across organizational boundaries [11,12]. Recent initiatives, including Liberty Alliance Project [13,14], aim at the provision of SSO for a federated environment [15], by leveraging identity providers acting as trusted third parties. Similarly, authorization functionalities are provided in a variety of forms, usually coupled with auditing capabilities. Authorization can include simple access control management at the OS level, more sophisticated role-based access control - RBAC [44] - up to flexible, distributed, policy-driven authorization, at the application and service levels.

Provisioning and accounting solutions [17] are used by enterprises, organizations and e-commerce sites to deal with the enrollment, customization, modification and destruction of accounts associated to users, employees and customers along with associated identity information (including rights, permissions and access control information).

Life-cycle management solutions deal with the issuance, certification, management and revocation of digital entitlements and credentials in a secure and trusted way. In particular PKI-based solutions [1] are available for this purpose but their adoption is not so widespread, especially in inter-organisational contexts, because of the intrinsic trust management problems, the complexity of CA hierarchies and related costs.

Web-services and the forthcoming web-services standards are also having an impact on identity management [18, 19], especially for aspects concerning the management of identities for web services, single-sign on and federated identity management.

The above components and solutions have been described from an enterprise and organisational perspective: this is where identity management solution providers are concentrating most of their efforts and where, currently, most of the money is.

Nevertheless, as we anticipated, identity management is much more that this and involves other stakeholders. Identity management technologies include, among many other things, authentication devices (smartcards, biometric devices, authentication tokens, etc.), anonymity services, cryptography schemas alternative to RSA - such as IBE [40,41,42], trusted platforms [30,32] and emerging standards [15] including signed and encrypted XML [45,46], XACML [47], XKMS [48], SAML [49] and SOAP [50].

3.3 Related Issues

Identity management products and solutions are deployed at different level of abstractions of the IT stack. They provide some degree of interoperability and integration, especially in the area of authentication, provisioning and data consolidation. Their integration with products in the IT stack and business solutions is driven by consolidation and rationalisation of resources within enterprises, government organizations and collaborative environments. For the time being the main efforts are concentrated in the context of Application Integration Software (AIS) [20] and Enterprise Application Integration (EAI) [21].

Despite this, most of the current identity management products and solutions still rely on their own self-contained and stand-alone management and control tools. Little integration or interoperability is available with other management tools, for example to deal with the management of security, trust and privacy in an orchestrated way.

It can happen that, in order to carry on a management task (dictated by business requirements or new policies), administrators need to use different tools at different level of abstraction and rely on different enforcement mechanisms. This is aggravated by the fact that other products and solutions, such as middleware components, workflows, business solutions, etc., might implement and provide their own specific and ad-hoc identity management components. Unfortunately in most cases they are not interoperable or compatible among each other.

Management tasks are becoming more and more complex, very labor and skill intensive and prone to generate vulnerabilities if not performed in an appropriated way.

The process of addressing the above aspects has been very slow so far, partially because of the involved complexity and partially because of the interest of solution providers to lock their solutions and keep their control over their customers.

At the moment, there is no availability on the market of interoperable, flexible, policy-driven management solutions that fully integrate the management of identity with security, trust and privacy aspects at different levels of abstraction and that can scale across multiple contexts to enforce policies, correlate events, quickly identify problems (such as misuses of identity information, attacks, policy violations) and react.

This landscape is going to change. An emerging priority of commercial organizations, enterprises and government agencies is to deal with *changes* that affect their businesses in a flexible, fast and simple way. These changes can be dictated by market needs, dynamic workforces, new security threats, changing legislations and by people that are more aware of their rights.

Identity management products and solutions need to evolve towards higher levels of interoperability, flexibility and capability to react to changes: their functionalities need to be orchestrated with other management aspects, including trust, privacy and security management. The next section describes a few trends and issues which will provide further evidence about new emerging requirements.

4 Emerging Trends and Issues

The aim of this section is to describe a few emerging trends and issues that will affect identity management and identify related needs and requirements. Additional trends and issues are described in [43].

4.1 Trends

On-demand, adaptive infrastructures. The major IT vendors, including HP and IBM, recognise that there is a growing need for enterprises and large organizations to rationalise their IT infrastructure, reduce management costs and have more flexibility and adaptability in the provision of computing resources. Instead of having to configure and manage thousands of self-standing computing devices (PCs, Servers, etc.) and cope with related changes (due to faults, new machines, workload peaks, etc.), management tools for adaptive infrastructures allocate, on demand, the required computing resources depending on needs of users, applications and services.

A few initiatives, including adaptive infrastructures and enterprises [22,23] and on-demand business [24], have been launched to build products and solutions in this area, focusing initially on aspects concerning the lower levels of the IT stacks (platforms, systems, etc.) and then raising the abstraction level towards applications, services, web-services, and business solutions. Identity, security, trust and privacy are important aspects involved in all these initiatives. From an identity management perspective, it is fundamental to be able to manage, in a flexible way, who can access which resource and under which conditions. IT resources are allocated and de-allocated dynamically, depending on needs: they have to be configured with the right access control and managed in a way to avoid leakages or persistency of confidential data, preserve its privacy, deal with trust aspects.

At the moment, most of the available solutions deal with computing environments of enterprises or large organizations. They are deployed within their boundaries so they can simplify some of the requirements in terms of security and trust. In the future computing farms (or even grids) powered by adaptive IT infrastructures could be provided by third parties to a multitude of customers (people, enterprises, other organizations) to satisfy their IT and computational needs. Their adaptability needs will target platforms, applications and services in very heterogeneous contexts. Identity information and profiling permeates all these elements. This will introduce further issues and requirements in terms of identity, security, privacy and trust management.

These adaptive systems will be configurable and manageable (at the platform, application and service levels) via high-level policies dictating constraints and conditions on multiple aspects. These policies will involve identity management aspects such as authentication, authorization, provisioning and data consolidation along with related trust, security and privacy aspects.

Ubiquitous and pervasive computing [25,26,27]. People's lifestyle is getting more mobile and flexible. People play multiple roles in different contexts, sometimes concurrently. They change roles, activities, duties and responsibilities more and more frequently due to the evolution of the marketplace, dynamic working environments and modern societies.

People are increasingly using a variety of devices, such as mobile phones, laptops and PDAs in different contexts to deal with personal, social and work related matters [28]. In a few cases these devices are used in interchangeable ways. For example, it is already a common habit to use enterprise resources, such as laptops and PDAs to store personal and work related documents, run applications and access services for different purposes.

Devices are going to be used at home, during business trips, at the workplace. They are going to sense and acquire information from the surrounding environment [29]. During travels and business trips, they will be increasingly used in conjunction with third parties IT elements such as Internet access points, printing, storage and visualization devices, etc. to perform the required tasks.

On one hand this brings great advantages, on the other hand it creates problems in terms of security, privacy and trust. As devices are used in multiple contexts it will be necessary to enforce pertinent sets of identity management, security, trust and privacy policies depending on the context where they are used. When devices rely on third party systems to perform tasks, it must be possible for them to have degrees of assurance about the integrity and trustworthiness of these appliances and make inferences on top this information, before disclosing any personal information.

Identity management solutions might need to be directly deployed in these devices to cope with local and remote authentication, authorization, trust measurement and privacy enforcement and deal with the local protection of data, driven by the current context. Context awareness, adaptability to changes and contextual policy enforcement are going to be important requirements.

Within enterprises or organizations, identity management solutions will need not only to deal with the management of policies to be deployed within mobile devices but also be able to authenticate these devices and check for their identity, integrity and trustworthiness depending on where they are used, the task they performing and the information they are going to access within the enterprise boundaries.

Trusted platforms. Trusted platform solutions are becoming available on the market. Despite criticisms and fears, which are mostly misplaced and promoted out of ignorance or vested interest, it is likely that they are going to be adopted and used in the industry, driven by initiatives such as Trusted Computing Group (a.k.a. TCPA) [30,31] and Microsoft Palladium/NGSCB [32].

They consist of trusted hardware components, such as trusted platform modules (TPMs) whose integrity and identity are certified by the producers. At the start-up phase of a system, a TPM module can check for the integrity of the hardware and the software installed on this system. Protocols are under development to check similar aspects for remote systems and platforms. For the time being trusted platforms are mainly used to store keys in tamper-resistant hardware and execute secure cryptography operations. In the future, their capability to check for local and remote platform integrity will be increasingly used for trust and privacy purposes.

It is likely that identity management is going to be affected by the adoption of trusted platforms. New products and solutions will be able to exploit this emerging technology for authentication, single sign-on, trust measurement and privacy enforcement.

4.2 Issues

Privacy is an important issue that has to be addressed directly by identity management products and solutions. There are increasing concerns about the fact that enterprises, e-commerce sites, governments and third parties can access and correlate people's identity information, sell this information or misuse it. Laws and legislation only partially address the problem. Despite the fact that many efforts have been made at the legislation level, there are still a lot of problems to be addressed. Privacy laws can differ quite substantially depending on national and geographical aspects.

The enforcement of privacy policies is a key requirement [33]. It has strong implications and repercussions on identity management, especially in contexts where identity information is disclosed during interactions and transactions involving multiple third parties. This includes multiparty B2B communities (such as supply-chains) and federated e-commerce sites. Current works on privacy management, such as P3P [34] and EPAL [35], are moving towards more expressive privacy policies and their enforcement, but more work need to be done.

From an enterprise and organisational's perspective, this creates the problem of how to defend their reputation and brand when things go wrong. Mechanisms and solutions are required to help them to demonstrate that they acted honestly and with due diligence whilst dealing with personal data.

Identity management solutions need to provide accountable mechanisms to interpret and enforce privacy policies customized by the identity subjects, delegate the management to third parties trusted by the identity subjects, adapt to changes in privacy legislation and quickly deal with threats that could compromise the confidentiality of personal data.

Identity thefts and identity-based frauds. Internet identity thefts and related frauds [36,37] are fast growing crimes, because of poor security and privacy practices and the underestimation of the involved risks. In the future, when digital identities and profiles are going to be more pervasive and used for day-by-day life tasks, the consequences of those crimes could affect very seriously people's lives and businesses. Identity management solutions need to play a key role in protecting identities and profiles, help organisations to enforce good management practices and, in case of thefts and frauds, help to detect the criminals or support forensic analysis.

Lack of control on identity information. Identity subjects have little control over the management of their identity information. It is very hard (if not impossible) for the subjects of identity information to define their own privacy policies (or delegate this task to trusted third parties), check for their enforcement, track in real-time the dissemination and usage of their personal information, be alerted when there are attempts to use or misuse it, etc.

Because of emerging data protection laws, new legislations and the need of service providers to simplify the overall management, there is a tendency towards the delegation to users of the authoring of their identity profiles.

Despite this, identity management solutions mainly address the needs and requirements of the "consumers" of identity information, not their subjects. Identity management solutions need to evolve and include mechanisms that allow people to author their management policies and monitor their enforcement [38] (or delegate these activities to trusted third parties). Identity management solutions will have to quickly adapt to changes dictated by people's requirements and needs.

Accountability is an important issue for identity management. There is currently a lack of mechanisms and solutions to ensure accountability when dealing with the management of identity information. Today, when people disclose their identity information to third parties, they rely on them to protect and manage this information, as agreed. It is a matter of trust. Unfortunately, the number of cases where identity information is leaked or misused is increasing, due to lack of security, incompetence or fraudulent behaviours.

On the other hand, solutions are required to help organisations to demonstrate that they acted honestly and with due-diligence whilst dealing with personal data.

Identity management solutions need to provide strong, undeniable auditing and logging mechanisms and solutions that can be flexibly configured based on policies [38, 39]. In doing this they might need to leverage trusted platforms and rely on trusted third parties.

Complexity of identity management solutions: it is a barrier for common people and, increasingly, also for administrators, given the broad set of skills and knowledge that are required to have to make them work. New privacy and data protection laws, the increasing awareness of people about their rights, the need of organisations and service providers to adapt to customers' requirements and the consequent workload for organisations, might be important factors to move towards delegation and the provision of simpler to use identity management solutions.

5 Requirements

The previous sections highlighted important problems that affect current identity management solutions and described new trends and issues that could affect identity management in the future. We can derive a (non-exhaustive) list of high-level requirements that need to be addressed:

- **Integration**: functionalities provided by identity management solutions need to be integrated and be interoperable with products and solutions in the IT stack, at different levels of abstractions (including business, service, application, middleware, OS, platform and network levels). Identity management tasks must also be coordinated and integrated with other management tasks, including policy management, security management, privacy management and trust management. Integration must be possible within and across organisational boundaries.
- **Rationalisation**: the duplications of identity management functionalities and competences across products and solutions need to be eliminated or reduced drastically. Specifically, this is necessary for tasks involving management activities, such as administration, configuration and monitoring.
- **Flexibility**: the behavior of identity management products and solutions needs to be re-configurable in real time to cope with changes, rapidly address security threats, adapt to the context, support users' needs and satisfy their requirements.
- **Context awareness:** identity management products and solutions need to take in account contextual information, such as measures of the trustworthiness of the IT platforms currently in use, the identities of the involved entities, the integrity of the applications and services to be used, the current location, etc., whilst dealing with management tasks, such as authentication, authorization, trust and privacy management.
- **Privacy management**: the management of privacy has to be tightly coupled with identity management and be a core functionality provided by products and solutions in this area. The enforceability of privacy has to be provided and ensured with a negotiable degree of assurance and accountability.
- **Control over identity flow:** it is necessary to increase the control over the flow of identity information (including access, usage and exchange) at different levels of abstraction of the IT stack. This control needs to be active, programmable and adaptable to contextual requirements. Management tools are required to monitor and track disclosures of identity information and check for their compliance to agreed policies.
- **Delegation of control**: mechanisms are required to support a flexible delegation of the management of identity information to their subjects or trusted third parties acting on their behalf. This includes not only the possibility to author identity information but also the authoring of associated policies (such as privacy policies) and checking for their enforcement.
- **Accountability:** it is necessary to increase the accountability of all the parties involved in the management of identity information.
- **Simplicity:** identity management solutions need to be simple to use for all the involved parties, including identity subjects, identity owners and data administrators.

6 Adaptive Identity Management

The requirements described in the previous section have in common a key element: the *need for flexibility* and *adaptability* of identity management to changes.

Changes can be dictated by new policies and requirements: their enforcement can impact business solutions and different elements of the IT stack, at different levels of abstraction. For example a new privacy policy might define constraints and conditions that need to be enforced at the application, platform and network levels. Or a change in a business policy might allow identity and profiling information to be shared with third parties, under well-defined constraints and after checking the trust policy compliance of the remote systems. Any delay in enforcing new policies can have serious repercussions in terms of competitiveness, security or compliance to laws.

Changes can also be dictated by the surrounding environment or by events. For example, by discovering that a system is under attack, actions can be taken in real-time to further protect stored identity information or move it in safer positions. In case of mobile devices or adaptive infrastructures spanning across organisational boundaries, decisions about the level of security of the stored identity profiles and running applications can be based on the analysis of contextual information, including measures of the trustworthiness of the surrounding systems, location and identities of other parties.

As identity management is becoming more and more entangled with other management aspects the overall complexity is dramatically increasing. This introduces a challenge and, more interestingly, an opportunity for identity management to evolve towards a new generation of products and solutions.

We refer to this new generation of identity management as ***adaptive identity management,*** to stress its capability to quickly adapt and react to changes, both from an operational and a management perspective.

We believe that adaptive identity management is characterised by the following core properties:

- Integrated and collaborative management;
- Policy-driven management;
- Context awareness.

Figure 7 shows the high level model underpinning adaptive identity management. Adaptive identity management solutions and products are going to be deployed in heterogeneous environments, at different level of abstractions, and in a variety of contexts, ranging from enterprise back-ends to people's personal appliances. Their management will be integrated: this does not mean it will be centralised. It will consist of a set of management tools deployed at the right level of abstractions that cooperate to provide the requested functionalities. It will be possible to monitor and supervise the whole set of management activities, from different perspectives and levels of abstraction.

The integration of management functionalities across identity management solutions and other involved components constitutes the ***nervous system*** of adaptive identity management. Policies are the "stimuli" sent through this nervous system to make sure that requirements dictated by high level needs are fulfilled or contingent situations are handled, from a variety of perspectives, including security, trust and privacy. Depending on the circumstances:

- Policies could be immediately deployed at the right level of abstraction of the IT stack and enforced by the identity management components;
- Policies might need to be refined and deployed by means of intermediate management proxies.

Similarly, management data and contextual information provided by the involved components constitute the foundation for sensing the surrounding environment and reacting to it.

Management proxies contain integrated management tools: they are competent at specific levels of abstraction of the IT stack. They cooperate with each other to achieve common management objectives.

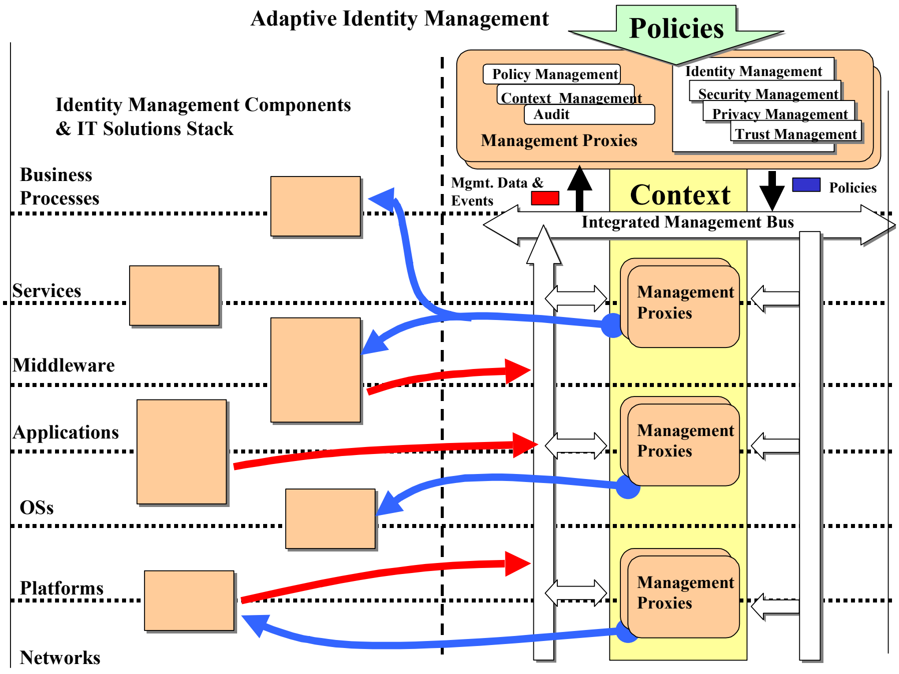


Fig. 7. Model of Adaptive Identity Management

Figure 8 shows this collaborative aspect when multiple environments are involved:

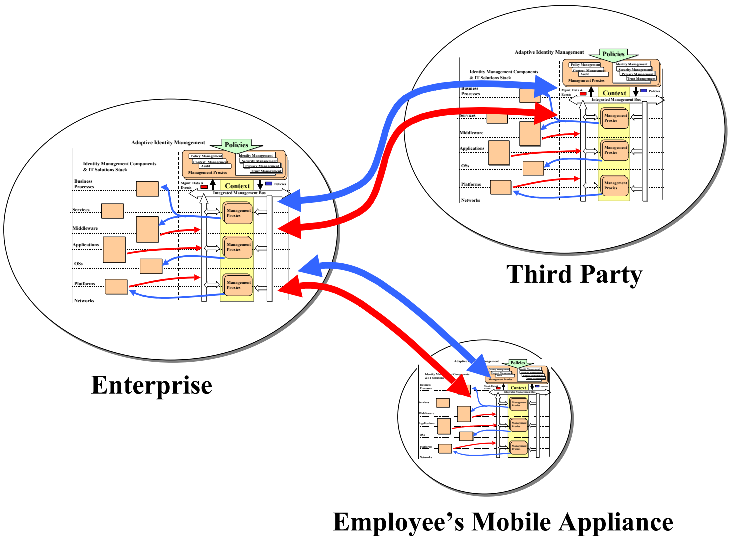


Fig. 8. Adaptive Identity Management across Boundaries

The same mechanisms described before apply in a distributed scenario, both regarding policy refinement and deployment and context sensing ad reacting. Of course each involved environment (for example, enterprise back-end, supplier's environment, mobile appliance, etc.) will run a suitable subset of identity management tools and components to achieve the requested identity management tasks.

The migration and evolution towards adaptive identity management is going to be gradual and incremental, because of the involved complexity; contingent needs and priorities will drive the process.

Within enterprises, this is going to be part of a larger evolutionary process that involves the whole IT ecosystem, towards higher degrees of integration, interoperability, adaptability and simplicity. This process will be driven by various initiatives, such as HP's adaptive infrastructures and enterprises and IBM's on-demand business solutions.

It will affect the *IT management* industry by forcing it to move from today's situation consisting of fragmented and stand-alone management tools (which address different issues at different level of abstraction) to more integrated, multi-purpose and cross-level management solutions.

The following sections provide more details about the core properties of adaptive identity management and some of their implications. Further reports will follow providing more technical details on implementation matters.

6.1 Integrated and Collaborative Management

The integration of identity management products and solutions within the IT stack is a prerequisite to move towards adaptive identity management. Within an integrated ecosystem, new requirements, changes and upcoming events can be quickly addressed, processed and managed by the competent elements, at the right levels of abstraction.

The integration process needs to involve **openness** and **standardization** of the identity management components. This requires the definition of **open APIs** both for management and operational functionalities. It also requires the standardization of the formats used to represent and exchange identity information along with mechanisms to protect this data.

Multiple players in the identity management space will continue to build and supply products targeting different identity management aspects at different levels of abstraction.

From an operational perspective, these components are going to be accessed and integrated within the IT solution stack via open APIs. Adaptors will be used to allow the integration in the short and medium term.

It is likely that most of the identity management components will preserve (at least in the short and medium term) their capabilities to provide local configuration, enforcement and monitoring because of the specificity of the tasks that each of them targets. As part of a broader process involving the evolution of the whole IT solution stack, adaptive identity management will integrate these management capabilities, across multiple components, and handle them from different perspectives, including security, privacy and trust.

This implies that adaptive identity management has to:

- Provide an integrated and collaborative *management of identity management tasks*, including the specification of management policies, monitoring and correlation, at convenient levels of abstraction;
- Delegate the refinement and enforcement of these tasks to the competent components, via the management proxies, at the right levels of abstraction.

A simplified representation of the integrated management model is shown in figure 9:

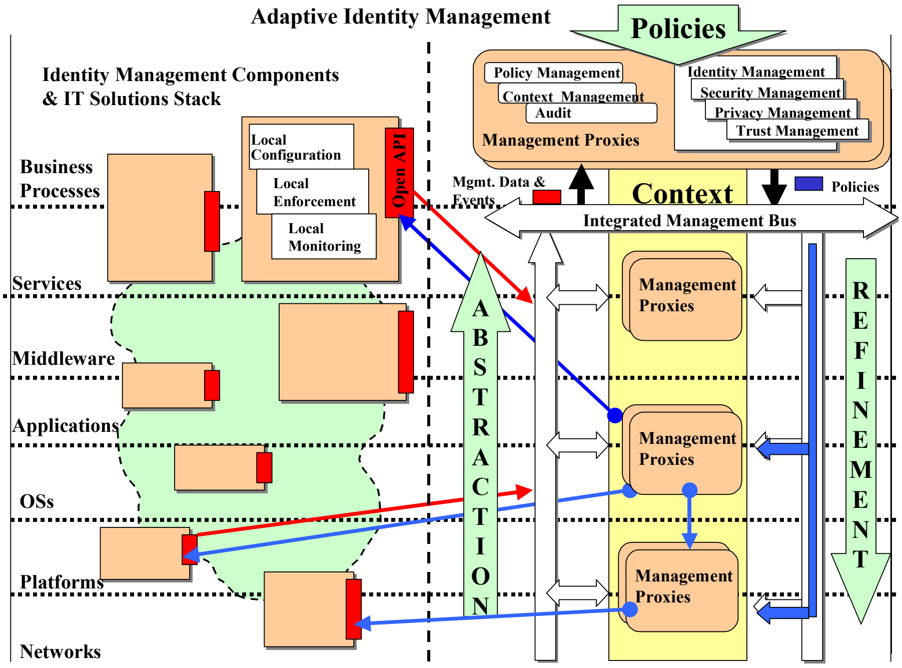


Fig. 9. Integrated Management Model

The integration of management activities enable administrators to rapidly configure components, monitor their behaviour and react to changes at different level of abstraction.

It is likely that this integration process will happen first within enterprise and organisational boundaries and then it will be extended across boundaries and management domains: the core mechanisms and philosophy are the same. Gateways among boundaries will enable the exchange of policies and management data to allow federated coordination of the management activities. For example in B2B or supply chain contexts, adaptive identity management solutions will span across enterprises' boundaries to enforce identity management constraints/rules and react in a coordinated way according to global and local policies. Similarly, in federated e-commerce sites, adaptive identity management will enable a variety of federated functionalities, beyond the current SSO initiatives. An active enforcement and monitoring of privacy policies will allow identity subjects to be directly involved in multi-party disclosures of their confidential data (or delegate the control to trusted third parties) with the consequence that organizations will be more accountable. Another example is about the deployment of adaptive identity management solutions within mobile appliances (PDAs, laptops, phones, etc.) used by people for a variety of tasks, including personal and work related ones. These solutions will be driven by a variety of policies (which will include constraints and conditions on identity, trust, privacy and security aspects) to be activated and enforced depending on the context and surrounding environment.

6.2 Policy-driven management

Policy-driven management is a key property of adaptive identity management. It ensures that the behaviour of adaptive identity management components and the other involved components can be changed on-the-fly to affect control, monitoring and enforcement at the right level of abstraction.

Identity management policies specify rules, conditions, obligations and constraints on the management of identity information. They could require the involvement of third parties, etc.

Policy-driven management involves:

- The definition of rich policy languages, able to describe constraints, conditions and obligations from multiple perspectives;
- The availability of mechanisms to refine, deploy and enforce these policies at the right level of abstraction;
- Context aware mechanisms to enable (disable) set of policies.

These policy languages need to be standardized, in order to enable interoperability and have broad acceptance. They must be flexible enough to allow the representation of conditions, constraints and obligations at different levels of abstraction.

Due to the complexity of these management policies, they might require multiple steps of refinement until they can be deployed and enforced. These refinement steps can be done by management proxies at the right level of abstraction or directly by competent identity management components.

Figure 10 provides a high level overview of the iterative refinement and enforcement process.

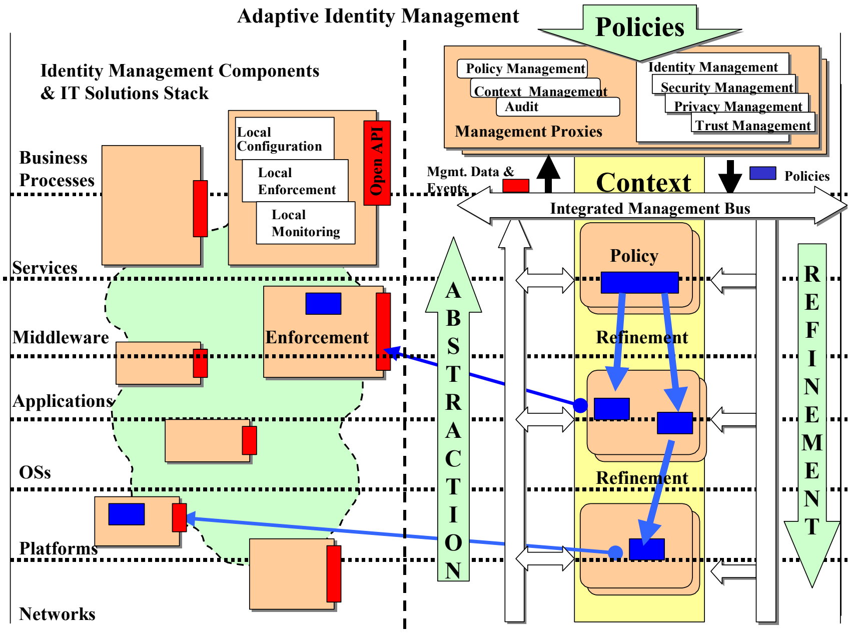


Fig. 10. Policy-driven Management

Each management proxy will have the knowledge about which policies it can directly refine, for example via predefined templates, and which policies it needs to send to other management proxies for further processing.

Identity management components and management proxies are able to access pertinent contextual information at the right level of abstraction in order to sense and react to changes or any contextual needs. This can trigger the activation and deployment of pertinent set of management policies or make issues escalate at the right level of abstraction.

6.3 Context awareness

Context awareness is fundamental to model the surrounding environment and provide information the processing of which allows identity management components to sense and adapt to new situations. The behaviour of adaptive identity management components (and other involved components) is therefore affected by the context in which they operate.

Contextual information can include any sort of data, such as physical data (location, proximity, trust measures, etc.), IT data (configurations, system details, etc.), business data, etc.

This information can be used to:

- Enable and deploy pertinent sets of management policies at the right levels of abstraction: ultimately this means a change of the behaviour of the affected components.

- Affect decisions during the evaluation of management policies, concerning multiple aspects such as security, privacy and trust.

Identity management components and management proxies can aggregate and abstract contextual information to make sure it is meaningful at the right levels of abstraction of the IT stack. Related events can be generated to trigger reactions in other adaptive identity management components, at different levels of abstraction.

7 Addressing the Requirements

Section 5 introduced a few requirements to be addressed by the next generation of identity management products and solutions:

- Integration;
- Rationalisation;
- Flexibility;
- Context awareness;
- Privacy management;
- Control over identity flow;
- Delegation of control;
- Accountability;
- Simplicity.

In section 6 we discussed how integration, rationalization, flexibility and context awareness are key elements and aspects of adaptive identity management. This section provides extra details about how adaptive identity management can address the other requirements.

We anticipate that policies, policy-driven behaviors, integration and cooperation are key elements to address them.

In terms of *privacy management*, policies can define conditions and constraints on multiple aspects, involving not only identity but also related trust and security. For example a privacy policy might require the encryption of identity management data depending on the context where it is manipulated or transmitted, require the satisfaction of high level conditions based on the identity of the receiver, ask for the measurement and evaluation of the trustworthiness of the platforms where personal data is going to be sent, involve external trusted third parties in the enforcement of aspects of this policy.

Adaptive identity management allows for the refinement, interpretation and enforcement of these policies at the right levels of abstraction, in an integrated way: in the above example of privacy policy [38], its enforcement might involve privacy engines at the application and service levels to deal with business related matters, the settings of ACLs at the OS level, involvement of TPMs within trusted platforms, etc.

Privacy management is a specific case involving the *control over identity flows*. In general, thanks to the deployment of management proxies at the right level of abstractions and their integration and cooperation with other components (in addition to the identity management components) it is possible to define, in a fine-grained way, how identity information has to be processed, managed in the IT stack and exchanged (especially across boundaries). Thanks to context awareness, the management behaviour can be modified to react to changes and emerging needs, including the violation of some of the mandated policies.

Delegation of control can be achieved via the collaborative nature of adaptive identity management, by allowing authorized third parties to access specific organisations' management proxies or by allowing the third parties' management proxies to cooperate. Third parties can define their management policies via management proxies. These policies will be checked, refined, deployed and enforced at the right levels of abstractions, in the appropriate domains. This mechanism allows identity subjects to directly control their identity information or delegate it to third parties.

The *accountability* requirement can be addressed via the usage of fine-grained tamper resistant logging systems along with auditing mechanisms to collect and store undeniable evidence at different levels of abstraction. Management proxies and identity management components can use logging systems locally provided or be forced to interact with third parties which provide trusted logging and auditing services [38,39].

Simplicity is actually the hardest requirements to achieve. The philosophy of relying on refinements and delegations of tasks at the right levels of abstraction should reduce the overall complexity and allow administrators and other users to focus on aspects relevant at their current levels of abstraction. Nevertheless, management tools within management proxies and identity management components still need to be designed to provide high level, intuitive, visual or audio interfaces to access and perform management tasks.

8 Discussion

The transition from current identity management solutions to more adaptive and flexible solutions will be incremental, due to technical and practical issues. This is going to happen as part of a broader process towards adaptive IT infrastructure and adaptive enterprises.

Current initiatives driven by companies like HP and IBM, are creating a new set of opportunities for players in the IT solution stack, and in particular for the players in the identity management area, as identity management is going to be a core functionality.

In the short term, solution providers who own or have control over a large set of products and solutions in the "identity management stack" are undoubtedly in a privileged position as they can drive the process towards more integrated and flexible identity management solutions and increase their competitive advantage. This might also imply a phase of consolidation in the identity management market via acquisitions and partnerships.

In the medium and long term, solution providers should move towards open and interoperable solutions, which have a higher chance to get broader acceptance, minimise risks and exposures of the buyers and cope with the complexity of the integration process. This can be achieved via standardisation organisations, open forums and alliances.

A big opportunity for solution providers to diversify themselves and add value is to focus on the production of *integrated policy-driven management tools* to coordinate different identity management products and address different aspects in an integrated way, including security, privacy and trust. A competitive advantage would be integrating these tools with the management of the other components of the IT stack, via a simplified and common set of interfaces. Solution providers should also move towards the provision of identity management solutions that can scale and can be integrated across organisational and domain boundaries.

The buyers of identity management solutions, in particular enterprises and organizations, should start exploring the implications of moving towards more flexible and adaptive identity management solutions and the impacts that this might have on their businesses and IT stack.

A first step would involve a rationalization and optimization process in the area of identity management, by eliminating redundancies and duplication of functionalities of existing solutions. This should also include further integration of identity management solutions with the components in the IT stack (including business solutions).

Broadly speaking, when possible, this rationalisation and integration process should try to avoid to embed policies (i.e. conditions, rules, etc.) within business processes, services, applications and systems, especially if they are known to be subject to frequent changes. It is important to start moving towards solutions that allow the management of external, reconfigurable policies or use approaches and solutions that keep this option open.

Identity subjects will ultimately benefit from the availability of adaptive identity management solutions, as they will have more control on their identity assets. They will be able to configure their own policies and preferences for the management of their personal information, delegate to trusted third parties to act on their behalf and have degrees of assurance of the accountability of the involved parties.

In the short and medium term identity subjects should benefit from the integration and consolidation of identity management solutions, as they will reduce duplication of tasks for some of the involved activities, such as authentication, provisioning and profiling management.

9 Conclusions

Current identity management products and solutions show their limitations: they provide little integration of management of identity, security, trust and privacy aspects; they also have little flexibility to quickly react to changes, new requirements or contextual situations. This, along with emerging trends and issues will drive the evolution of products and solutions towards a new generation of identity management.

We argue that this new generation is about *adaptive identity management* i.e. open, flexible, policy driven, context-aware identity management that scales across multiple contexts and level of abstraction and is integrated with other management aspects including security, privacy and trust.

We described a few emerging requirements, presented our vision and a high level model of adaptive identity management and discussed its implications for the various stakeholders.

10 References

1. R. Housley, W. Ford, W. Polk, D. Solo, RFC2459: Internet X.509 Public key Infrastructure Certificate and CRL Profile, IETF - 1999
2. J. Pato, Identity Management: Setting the Context, HPL-2003-72, 2003
3. Meta Group, Identity Management Value Quantification, Executive Summary of Research Findings, 2003
4. R. Gamby, D. Blum, Developing Identity Management and Directory Services Architecture Principles, Technical Positions and Templates, The Burton Group, 2002
5. J. Gaw, Digital Identity Solutions: A Road Map for Software and Services, IDC, 2001
6. B. Parr, R. Villars, Digital Identities: The Coming Struggle for the Future of the net, IDC, 2001
7. D. Senf, Identity Management in the Enterprise: Consolidating eBusiness Interactions, IDC, 2003
8. J. Penn, IT Trend 2002: Directories and Directory-Enabled Applications, IdeaByte, 2002
9. M. Neuenschwander, Meta-directory Services and the Emerging Enterprise Data Network, The Burton Group, 2002
10. R.E. Smith, Authentication: From Passwords to Public keys, Addison-Wesley, 2001
11. A. Volchkov, Revisiting Single Sign-on. A Pragmatic Approach in a New Context, pp. 39-45, IT Pro, IEEE, 2001
12. J. De Clercq, Single Sign-On Architectures, proceedings pp. 40-58, InfraSec 2002, Bristol, UK, 2002
13. Liberty Alliance Project - http://www.projectliberty.org/ - 2002
14. Liberty Alliance Project, Liberty Architecture Overview, v. 1.1, 2003
15. D. Blum, Toward Federated Identity Management, Burton Group, 2002
16. Burton Group, User Authentication, Burton Group, 2002
17. J. Penn, Market overview: user Account Provisioning, GIGA Information Group, 2002
18. Summit Strategies, Identity Management, Bolstered by Web Services, Takes Center Stage, Summit Strategies, 2002
19. Liberty Alliance Project, Liberty Identity Web Services Framework Primer, v. 1.0, 2003
20. S. Rogers, Worldwide Application Integration Software Forecast Summary 2002-2006, IDC, 2002
21. D.S Lintichum, Enterprise Application Integration, Addison-Wesley, 1999
22. HP, HP Adaptive Enterprise Solutions, web site, http://www.hp.com/large/globalsolutions/ae/whitepapers.html, 2003
23. HP, Infrastructure and management solutions for the adaptive enterprise – white paper, http://www.hp.com/large/globalsolutions/ae/whitepapers.html, 2003
24. IBM, on-demand business, web site, http://www-3.ibm.com/e-business/index.html, 2003
25. M. Weiser, Hot Topics: Ubiquitous Computing, IEEE Computer, 1993
26. NIST, Pervasive Computing Program, Information Technology Laboratory, NIST, http://www.itl.nist.gov/pervasivecomputing.html, 2003
27. MIT, MIT Project Oxygen: Pervasive Human-Centered Computing, MIT, http://oxygen.lcs.mit.edu/index.html, 2003
28. S. Riche, G. Brebner, and M. Gittler, Client Side Profile Storage. Presented at the International Workshop on Web Engineering, Pisa, Italy, May 24th 2002.
29. S. S. Yau, F. Karim, Y. Wang, B. Wang, and S.K.S. Gupta, Reconfigurable Context-Sensitive Middleware for Pervasive Computing, IEEE Pervasive Computing, July-September, 2002.
30. Trusted Computing Platform Alliance, TCPA Main Specification, Version 1.1, http://www.trustedcomputing.org, 2001
31. S. Pearson (ed.), Trusted Computing Platforms, Prentice Hall, 2002.
32. Microsoft Corporation, White Paper on Palladium, http://www.microsoft.com/presspass/features/2002/jul02/0724palladiumwp.asp, 2002

33.Y. Beres, P. Bramhall, M. Casassa Mont, M. Gittler, S. Pearson, On the Importance of Accountability and Enforceability of Enterprise Privacy Languages - position paper, W3C Workshop on the long-term future of Enterprise privacy Languages, http://www.w3.org/2003/p3p-ws/pp/hp1.pdf, 2003

34.W3C, The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, September 2001. For updates on P3P and a list of compliant sites, see http://www.w3.org/P3P.

35.P. Ashley , S. Hada , G. Karjoth, C. Powers, M. Schunter, Enterprise Privacy Authorization Language (EPAL), IBM, 2003.

36.T. Arnold, Internet Identity Theft: A Tragedy for Victims, White Paper, SIIA, 2000

37.D. Coates, J. Adams, G. Dattilo, M. Turner, Identity Theft and the Internet, Colorado University, 2000

38.M. Casassa Mont, S. Pearson, P. Bramhall, Towards Accountable management of Identity and privacy: Sticky Policies and Enforceable Tracing Services, TrustBus 2003 workshop, 2003

39.A. Baldwin, A. Ferreira, S. Shiu, Towards Accountability for Electronic Patient Records. 16th IEEE Symposium on Computer-Based Medical Systems - CBMS 2003, June 2003

40. D. Boneh, M. Franklin, Identity-based Encryption from the Weil Pairing. Crypto 2001, 2001

41. C. Cocks, An Identity Based Encryption Scheme based on Quadratic Residues. Communications - Electronics Security Group (CESG), UK. http://www.cesg.gov.uk/technology/id-pkc/media/ciren.pdf, 2001

42. L. Chen, K. Harrison, A. Moss, D. Soldera, N.P. Smart, Certification of Public Keys within an Identity Based System, Proc. 5th Int. Information Security Conference (ISC), 2002. LNCS 2433, Springer-Verlag, 2002

43.M. Casassa Mont, P. Bramhall, M. Gittler, J. Pato, O. Rees, Identity Management: a key e-business enabler, HPL-2002-164, presented at SSGRR2002s, L'Aquila, Italy, 2002

44.D. Ferraiolo, R. Kuhn, *Role-based Access Control*. NIST, 1992

45.W3C, XML Signature WG, http://www.w3.org/Signature/, 2003

46.W3C, XML Encryption WG, http://www.w3.org/Encryption/2001/, 2003

47.OASIS, eXtensible Access Control Markup Language TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, 2003

48.W3C, XML Key Management Specification (XKMS), http://www.w3.org/TR/xkms/, 2003

49.OASIS, OASIS Security Services TC: SAML, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, 2003

50. W3C, Simple Object Access Protocol (SOAP) v.1.1, http://www.w3.org/TR/SOAP/, 2003