# Identity Management: a Key e-Business Enabler

Marco Casassa Mont, Pete Bramhall, Mickey Gittler,
Joe Pato, Owen Rees
Trusted E-Services Laboratory
HP Laboratories Bristol

HPL-2002-164
June 12th , 2002*

E-mail: {marco_casassa-mont, pete_bramhall, mickey_gittler, joe_pato, owen_rees} @hp.com

identity management, trust, security, privacy, e-business, e-commerce, e-government

Digital identities, profiles and their management are increasingly required to enable interactions and transactions on the Internet among people, enterprises, service providers and government institutions.

Recent initiatives, including Microsoft .MyServices and Liberty Alliance Project, are eager to supply mechanisms to enable identity management and simplify the overall consumer experience. Enterprises and government institutions are exploring the usage of meta-directories, PKI and electronic identity cards.

This paper describes the state of the art of identity management, looks at trends, requirements and hard problems that need to be addressed - including trust, privacy and security - and presents some HP research activities in this area.

* Internal Accession Date Only

Approved for External Publication

# Identity Management: a Key e-Business Enabler

M. Casassa Mont, P. Bramhall, M. Gittler, J. Pato, O. Rees
*Hewlett-Packard Laboratories, UK*
*{marco_casassa-mont, pete_bramhall, mickey_gittler, joe_pato, owen_rees}@ hp.com*

## Abstract

*Digital identities, profiles and their management are increasingly required to enable interactions and transactions on the Internet among people, enterprises, service providers and government institutions.*

*Recent initiatives, including Microsoft .MyServices and Liberty Alliance Project, are eager to supply mechanisms to enable identity management and simplify the overall consumer experience. Enterprises and government institutions are exploring the usage of meta-directories, PKI and electronic identity cards.*

*This paper describes the state of the art of identity management, looks at trends, requirements and hard problems that need to be addressed - including trust, privacy and security - and presents some HP research activities in this area.*

## 1. Introduction

Identity management is today's topic: it is gaining more and more interest in the industry thanks to new initiatives, standards and products in the e-commerce and e-business areas.

Dealing with digital identities and their management is a complex task as it involves not only technical aspects but also social and legislative aspects. It reflects the complexity of dealing with these matters in the physical world.

In the physical world, the word "identity" has many connotations depending on the specific context [1]. For people, identity mean names, addresses, driver licences, passports, etc. It extends to financial assets, deeds, insurance policies and credit reports. It also includes personal preferences, associations and attitudes. For enterprises and businesses, identity includes roles, privileges, rights and responsibilities. For governments, identity has strong implications in term of certificates, residence, citizenship, social security, pension, taxation, etc.

"Digital identity" is, at the core, an effort to recreate, organise, automate and integrate all those aspects in the online electronic world and (increasingly) link them to existing "offline" identities.

Identity management is about the management of digital identities for people and, more general, for systems and services.

Identity management has been around for a while, focused mainly on enterprise and government aspects, it includes digital certificates, smart cards, PKI, roles and privileges, authentication and authorization processes. In a broader sense identity management also involves aspects related to the definition, certification and lifecycle management of digital identities and profiles, infrastructures for the exchange and validation of this information, along with legal and legislative aspects.

The current Internet "renaissance", based on the provision of more and more services online, is defining and creating a broad new set of opportunities not only for enterprises and governments but also for people, including the availability of new web services and means of communication, the provision of on-demand information and the deployment of infrastructures to enable electronic interactions and businesses.

In this new e-world identity management becomes essential. E-business and e-commerce players need to identify the involved entities in a way that fosters trust and respect for privacy and data protection. How the management of identity is achieved has implications on personal, business, social, and government matters.

In this context, identity management is also a key e-business enabler: being able to recognize the digital identity of people and web services, to understand, manage and validate their profiles and rights is fundamental in order to underpin accountability in business relationships and enable commercial transactions. On one hand, the knowledge of profiles, preferences and identity information can provide customised offers and tailored added-value services, which people or businesses might be willing to pay for. On the other hand any misuse could degenerate in violation of people's rights and laws, including data protection and privacy laws.

An objective of this paper is to describe current and foreseeable trends related to identity management in the consumer, enterprise and government areas and highlight business implications and important issues that need to be properly addressed.

Another objective is to present related research topics that are currently under investigations at HP Labs, Bristol, along with some results achieved in this area.

## 2. Current Trends

Identity management affects consumers, enterprises and governments: concerns and issues might be different, depending on the specific context.

This section provides an overview of current trends and a description of how identity management is perceived by the involved parties. It also provides a brief analysis of the possible business benefits and issues deriving from the adoption of identity management solutions.

### 2.1. Consumer and E-Commerce Space

The consumer space [2] is one of the most active in term of identity management. The objective of recent initiatives, such as Microsoft .MyServices [3] and Liberty Alliance Project [4], is to enable smooth and simple interactions between consumers and service providers, on the Internet, to facilitate their navigation across web sites and enable e-commerce transactions without the hassle of multiple users' authentications.

Under the umbrella of so-called "federated identity management" lies a set of techniques and solutions provided by online *identity providers* and integrated with e-commerce sites run by service providers. Ideally the role of identity providers is to act as trusted third parties; provide a point of authentication of customers; store and manage customers' identity and profile information.

The interaction among identity providers is meant to enable single-sign-on [5] across multiple e-commerce sites, driven by customers' interests and provide a transparent exchange of identity and profile information among e-commerce sites. Most of the work currently done in this area is in terms of infrastructure including authentication and authorization mechanisms.

Microsoft's Passport authentication service was announced as a key part of the Windows XP operating system and the Microsoft's .NET software-as-a-service strategy. Currently, Passport has millions of registered users. Much of this information provides the bare minimum of information to support the Hotmail service. However, with the release of Microsoft .MyServices, the amount of information stored about these users will grow significantly. Although Microsoft was initially keen in running identity management services based on .MyServices solutions, it has now reviewed its strategy: it stated that it would concentrate its efforts on the provision of consumer solutions to third parties willing to run those services.

There is no shortage of competition. The Liberty Alliance Project was formed in September 2001 by Sun Microsystems to create open, federated, single sign-on identity standards for the digital economy via any device connected to the Internet. It involves collaboration on standards. The primary goals of the Liberty Alliance Project are to allow individual consumers and businesses to maintain personal information securely; provide a universal open standard for single sign-on with decentralized authentication and open authorization from multiple providers; provide an open standard for network identity spanning all network devices.

At moment most of the initiatives in the "federated identity management" area are still work-in-progress and it will take a few months before the first commercial solutions are deployed on the Internet.

Internet service providers might be motivated to adopt such solutions in order to boost commercial e-transactions, driven by the simplification of the customer experience and the increase of commercial opportunities. Identity providers' interests might be to provide identity management services in return of a percentage of the e-transactions they enable or to use consumers' identity and profile information for other commercial purposes. Currently, the separation of roles between service providers and identity providers is not so clear and it might happen that some service providers will also act as identity providers.

It is not yet clear how much the consumers are willing to embrace these new initiatives and trust a "federated identity management" paradigm. On one hand a simpler and more efficient interaction with e-commerce sites is potentially an adoption accelerator. On the other hand fears for privacy and reluctance to provide authentic and verifiable identity information might be a serious inhibitor [6].

### 2.2. Enterprise Space

For many years, enterprise identity and access management have been a major problem for IT departments with a considerable portion of their time spent creating and removing large numbers of user accounts, administering profile information and dealing with forgotten passwords.

Many solutions and products have been built to address these management problems, including IBM/Tivoli's, Netegrity's, Novell's and Computer Associates' solutions: those solutions help administrators to define authentication criteria for users, set and manage access control lists and administer the access to enterprise resources.

The introduction of PKI solutions [7], on one hand has provided more secure and trustworthy way to authenticate users, by certifying and managing digital identities and profiles (attributes) by means of digital certificates. On the other hand it further complicates the situation where administrators have to manage the process of issuance and revocation of digital certificates as well as manage single sign on infrastructure based on that information.

Removing user accounts and revoking certificates can prove particularly problematic, often leading to errors and security holes.

The overall management of employees' identities and profiles has become more complicated for large and spread enterprises where identity information is often fragmented, distributed and managed by a variety of administrators belonging to different enterprise organisations.

This problem worsens when companies collaborate in B2B contexts, requiring some form of joint user administration. This includes private and public e-marketplaces, supply-chains and Internet business communities. It could become even more challenging if companies were required to be liable to other participating parties for the actions of erroneous identities. Tracking changes in users' identities, roles and job titles is time consuming and somewhat problematic. Again, the issue increases considerably if an enterprise needs to manage identities for each collaborative application.

"User Account Provisioning" [8] is emerging as the next big thing in enterprise and inter-enterprise space. Fast growing technologies, including meta-directories [9] along with new authentication tokens, smart cards and Virtual Private Networks (VPN) are specifically targeting the new need to cope with dynamic and cross-boundary identities and access controls for employees and partners.

Specifically, meta-directories are important in term of identity management [10], as their aim is to associate and synchronise identity and profile data across various sites, applications and storages that use it. The goal is to separate the management of identity and profile information (and more in general enterprise data) from the applications that work on it.

In the enterprise and inter-enterprise space, identity management is clearly a business enabler. It encompasses not only security but also business efficiency and business agility. "Business flexibility" is going to be very important in a world where enterprises more and more frequently will collaborate with external partners, merge with other organisations or split. In this new world being able to properly identify people, manage their access control rights and dynamically integrate this knowledge within inter-organizational business processes is going to become a key differentiator.

### 2.3. Government Space

Identities and identity management are of primary importance for governments as they encompass the identification of citizens and their interactions with public services and government institutions. Identity-related aspects permeate the day-by-day lives of ordinary citizens, as they involve social security, pensions, driving licences, identity cards and passports.

The management of identities for government institutions is similar to those described for enterprises, as it has to deal with fragmented and distributed identity data associated to citizens. Citizens are known and identified by government institutions, including hospitals, tax offices, foreign offices, etc., by means of different identifiers and credentials, depending on the specific context and purpose: they include social security numbers, driver licences, pension numbers, tax numbers, etc.

Many e-government strategies, including [11], [12] aim at rationalising the public sector, by exposing government services on the Internet and requiring proper mechanisms to identify citizens. It is also becoming more and more evident the need to overcome local or national barriers and address transactional aspects of e-government. For example, in Europe there are action plans to provide integrated e-government initiatives and electronic access to public services [13].

Recent laws and legislations, including [14] and [15], aim at speeding up the process of adoption of digital identities by recognising the legal validity of digital signatures both on electronic documents and e-transactions.

Identity management play a key role in enabling those e-government strategies. Current trends involve the implementation and deployment of PKI infrastructures, the issuance of electronic identity cards to citizens, the usage of smart cards and embedded digital identity certificates along with the integration of this information with on-line services.

The overall objective is to rationalise government and public sector services, introduce more efficiency and simplify the interaction and dialog with citizens, enterprises and other institutions. On the other hand, those initiatives are reasons of concern among citizens and organisations because of the risk of losing their privacy and possible threats to freedom.

When dealing with identity management, it is important to understand that not only technical issues are involved but also social and legislative aspects.

Next sections discuss possible future trends and highlight important issues that need to be addressed in order to make digital identities and identity management trustworthy and acceptable by the various stakeholders.

## 3. Future Trends

An important future trend is linked to the coming next-generation of ***personal mobile devices***.

The growing popularity of mobile devices, including mobile phones, and the current convergence of the telecom world with the computing world is going to provide people with a broad new range of mobile appliances. These appliances, including new mobile phones, PDA devices and lightweight laptops are going to offer integrated voice and video communications, connections to the Internet and reasonable storage and processing capabilities. They will reflect, in terms of content, usage and access, the multiple attitudes that people have in their lives and the multiple roles they play: they are going to be used for personal, social and business purposes. They will store business and personal data, including identities and profiles.

As those appliances are going to be used, as a matter of convenience, in many contexts, including personal, social and business environments, it is extremely important that their content and their functionalities are properly secured and managed depending on the specific context. That is particularly true for identity and profile information. For example, business related information should be protected when the mobile device is used for personal or social activities and the other way around.

It is likely that the current ***proliferation of digital identities*** on the Internet (due to multiple web accounts with ISP providers, online bank accounts, registrations to web services and remote access to the workplace) will not come to an end but actually it will increase thanks to the availability of more opportunities. This is likely to generate a demand for simple and easy to use tools to manage those identities and profiles, not only in a federated way (as highlighted by Microsoft .MyServices and Liberty Alliance Project) but also locally, directly on people's devices and appliances.

Unfortunately the exposure of digital identities and profiles on the Internet will accentuate a negative trend: ***identity thefts*** and ***identity-based frauds***.

Internet identity thefts and related frauds [16], [17] are fast growing crimes that take advantage of poor security and privacy practices and the underestimation of the involved risks. In the future, if 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 quite seriously our lives and businesses. Identity management solutions can play a key role in protecting identities and profiles, enforcing good management practices and, in case of thefts and frauds, help to detect the criminals or support forensic analysis.

As a consequence of these dangers, people, businesses and governments will be increasingly more aware of the involved risks and recognise the need to define and be compliant with good practices and due diligence whilst dealing with identities and profiles.

This may lead to a trend where more ***control*** on digital identities and profiles is given back to their owners. Nevertheless, people will not be necessarily willing to be involved in the protection and management of their digital assets: it is more likely that trusted third parties will do this on their behalf and provide people with easy-to-use tools to monitor and keep the situation under control. This is another opportunity for identity management solutions to inject accountability, confidence and trust in the system.

## 4. Identity Management Issues

As we highlighted in the previous sections, the management of identities involves issues at the technical, social and legislative level. This section describes a few important related issues and introduces high-level requirements for identity management solutions.

First of all, it is important for identity management solutions to deal with the ***authenticity*** of identity and profile data. The provenance and credibility of this data has a direct impact on the overall perception of trust and the consequent willingness of people or enterprises to engage in business relationships and commercial transactions. This has strong implications on the mechanisms and solutions that are put in place to assess and certify identity and profile information. The importance and impact of the authenticity of this information is directly proportional to the involved risks and the overall value of the transaction. In low-value e-commerce transactions the process of checking the authenticity of identity-related information, like credit card numbers, might be relaxed, because of other mechanisms underpinning the business model, for example based on credit card insurances. In case of more important and valuable e-business transactions, obsolete or compromised identity information may have huge implications for a party engaged in these transactions, possible provoking financial and social losses.

***Trust*** and ***trust management*** play a key role in this space. A common way to address authenticity and provenance issues is to rely on trusted third parties to assess, certify, verify and potentially revoke identity and profile information. Trusted third parties commonly include entities such as certification authorities, consumer organisations, business associations, etc. For example, Identrus [18] has been created in the banking environment to provide a B2B and e-commerce trust framework, which includes mechanisms based on PKI to deal with authentication, confidentiality, non-repudiation and integrity of identity information. The current trend is toward the provision on the Internet of ***trust services*** [19], which deal with various aspects of trust and are accountable for the services they provide. Those services provide not only certification and management of identity information but also their verification, recommendation, credit rating, notarisation, trusted auditing, and trusted storage.

One of the hard problems when dealing with information on the Internet is coping with their ***dynamic*** and ***volatile*** nature. This aspect is even more relevant for digital identity and profile information when it is used online, in real-time, to access enterprise resources or public sector services, to enable business relationships or to identify entities during e-commerce transactions. For example credit limits, privileges, digital rights, etc. are example of information that is subject to quick changes as they are affected by interactions and transactions. It is important that this information is kept up-to-date and trustworthy. Achieving this objective is clearly of vital importance for the credibility and effectiveness of identity management solutions.

The ***longevity*** of identity and profile information is another important issue. In general, any e-transaction is susceptible to disputes, especially for high value ones. When a dispute occurs several years after the transaction has been initiated, the ability to prove the authenticity of logged events becomes crucial. During that time, however, the identities and credentials of the parties involved will have changed. This need to retain provable authenticity long after the action takes place implies that changes in identity have to be traceable – that is where longevity issues arise. It is especially important within an enterprise (or government) context: the roles of people in the organisation change, together with people themselves. At the same time, other entities want to know who occupied a role previously, as well as the role history for a specific person. Identity management solutions therefore have to include mechanisms for keeping information about expired identities and for specifying relations between the new identities/credentials and the old ones. Such information would allow tracking down the responsible entity even years after its identity was first registered and verified.

***Privacy*** is another important issue that has strong implication on the management of identity information. There have been many cases in e-commerce where personal identity profiles have been misused, sold and disclosed to third parties without the authorisation of their owners' or they have been compromised because of a lack of security. There is a common fear among people that organisations and governments will misuse personal data for purposes that can directly or indirectly limit their freedom and damage their interests.

The information handled by identity management solutions is often perceived as highly confidential and it is therefore essential to achieve a high level of privacy conforming to strict privacy and data protection policies. The underlying privacy framework has to interoperate between various jurisdictions and trust domains. Identity owners should be allowed to decide when and where they want to disclose their identity, implying that in some cases pseudo-anonymity must be available. Whilst enforcing it the solution must have means to associate pseudo-identities to the real ones and keep track of those associations over long periods of time. All those aspects have strong accountability implications.

***Accountability*** is fundamental for identity management solutions and currently it is a major issue. It is important that the entities that deal with identities and their management are responsible and accountable and that the practices and policies are transparent. For example in the e-commerce space, service providers should clearly state their privacy and data protection policies, and mechanisms should be put in place to check and enforce their compliance to those policies. This is necessary in order to underpin trust and credibility on the Internet, to clearly set expectations, responsibilities and liabilities.

The objective of achieving privacy and accountability is quite hard, because of many different business practices and the inconsistent juridical approaches between nations. In addition there is a relative lack of legislations related to Internet matters. Nevertheless, there is more and more awareness that steps need to be done, as soon as possible, to overcome those barriers and harmonise principles and legislations.

The last note is on the importance of ***simplicity*** and ***integration*** for identity management solutions. This is currently an important issue. For example the complexity and lack of usability of large-scale PKI solutions, along with their intrusive approach, have been one of the barriers for their adoptions in the consumer, business and government space. All the entities that are exposed to identity management tasks should be able to achieve their objectives by using easy-to-use systems. This is particularly true for customers, in the e-commerce world, where complex authentication or identity management mechanisms are perceived as a barrier and obstacle to access the desired web services.

It is also true that identity management administrators need more intuitive tools to cope with complex and laborious administrative tasks, access information through simple visualization tools and automate tasks.

Finally, easy-of-integration is important for the success of identity management solutions. These solutions must be easy to integrate with enterprise or governmental processes and services without disrupting them or requiring expensive changes.

## 5. Identity Management Model

According to current and foreseeable trends, people will have multiple digital identities (and related profiles), for convenience and practicality or because of business, e-commerce or government constraints. In addition, the overall identity and profile information of a person is likely to spread across various boundaries including private, social, and work areas. Multiple "views" on that identity are going to be available, some of them directly under control of the owner, others managed by third parties, as illustrated in figure 1:

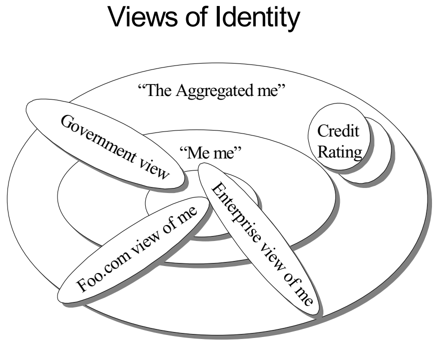

Figure 1. Multiple Views of Identity

Identity management solutions must cope with this "distributed" nature of identities and profiles and address the issues described in the previous section. The emerging solutions are likely to be pervasive, in the sense that they are going to involve all the stakeholders: identity owners, identity providers, enterprises, relying parties, governments and other third parties.

In our vision identity management solutions are modular and composed of multiple service and system components, to address the new administrative and operational challenges. Components include *infrastructure* components, *identity management lifecycle* components, and *added value* tools. Figure 2 shows our high level model for identity management solutions, as an attempt to capture the relationships among relevant identity management components:

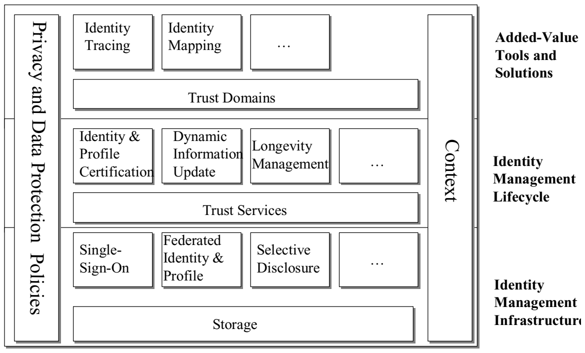
Privacy and Data Protection Policies
Identity Tracing
Identity Mapping
...
Trust Domains
Identity & Profile Certification
Dynamic Information Update
Longevity Management
...
Trust Services
Single-Sign-On
Federated Identity & Profile
Selective Disclosure
...
Storage
Context
Added-Value Tools and Solutions
Identity Management Lifecycle
Identity Management Infrastructure

Figure 2. Identity Management Model

***Infrastructure components*** underpin operational aspects of identity management. These components include mechanisms for authentication, authorization and single-sign-on. Authentication and authorization components are in charge of authenticating entities and granting rights depending on policies and involved risks. Those modules are critical as they check the validity of identities, their trustworthiness and allow entities to access resources and services accordingly. They have a direct effect on the perception that users have of the reliability and trustworthiness of providers of services.

The current trend towards federation of identities for distributed services, both on the Internet and across enterprises and organisations, on one hand provides new business opportunities to users and service providers but on the other hand it introduces new threats. Single-sign-on components, including those proposed by Microsoft .MyServices and Liberty Alliance Project, allow entities to authenticate once and access services supplied by multiple providers. Hackers or third parties can take advantage and misuse this process. These components have a direct impact on the liability that organisations have with their customers and other parties that rely on the supplied identity information. They need to be secure and compliant with privacy laws and data protection legislation.

In this context, it is important that identity management solutions provide mechanisms that allow identity owners (or trusted third parties acting on their behalf) to express their preferences and policies in term of privacy management. These mechanisms should allow a selective disclosure of identity information according to the policies expressed by their owners.

In general, infrastructure components rely on judgements and decisions made both at the time of the assessment and certification of identity information and during their overall lifecycle management.

***Identity management lifecycle components*** are necessary to provide mechanisms for the assessment, creation, certification and evolution of identity information over short, medium and long periods of time.

Specifically, certification components include processes to assess and certify identities, depending on their authenticity, nature, purpose and provenance. Auditing tools need to be deployed to collect data about actions and decisions made during the execution of these processes and provide evidence about due diligence.

Lifecycle management components also must deal with the dynamic evolution of information associated to identities and their trustworthiness. Identity providers (or certification authorities) are accountable and responsible for the identity information they provide to third parties: this information needs to be up-to-date and trustworthy. Obsolete or compromised information might provoke financial and social losses and cause identity providers to be legally and financially responsible.

In the short term, specific lifecycle-management components are in charge of retrieving up-to-date identity information from trusted sources, periodically evaluate their validity and trustworthiness (as dictated by policies) and revoke compromised data. In the medium and long-term, those components are responsible for longevity maintenance of digital identities: this can be achieved by tracking the evolution of identities and associated profiles overtime. Evidence is created and collated each time identity information are modified or renewed. This information need to be stored in distributed and fault tolerant systems to preserve its survivability and integrity over long periods of time.

In general, the overall management of identities is quite complex because of the fragmented and increasingly distributed nature of identity information.

***Added-value identity management components*** are required to simplify the operational usage and management of identities and to make sense of laws and legislation.

Specifically, in our vision, organisations will use tools to cope with the administration of distributed and heterogeneous identities in increasingly more and more dynamic and boundary-less environments. These tools manage aggregations of multiple identities owned by the same entities, according to privacy and data protection policies (dictated by identity owners, trusted third parties or organizations) and help administrators to visualise this information along with the associated policies. By better understanding identities, their inter-relationships and the implications of their usage, organisations will have more visibility of the requirements and constraints they need to be compliant with and the effects that those requirements have on their businesses.

Along the same line, identity-tracing tools are added-value components that help organisations to administer and keep under control chains of disclosures of identity information that they manage on behalf of their owners. This applies, for example, to identity providers or enterprises involved in B2B context, during single-sign-on processes or inter-organizational interactions. Tracing tools help administrators to keep track of which information has been disclosed to whom and the compliance of those disclosures to privacy requirements and business policies. In case of a federated identity framework, these tools may rely on trusted platforms, messaging mechanisms for the notification of the requests to disclose identity information and the communication of authorization decisions. Evidence collected during those interactions is used for auditing and forensic investigations, in case of identity thefts or frauds.

The understanding and monitoring of the compliance of identity management solutions to requirements, policies, privacy and data protection laws make organisations more accountable and trustworthy.

Some of the components described above (including identity mapping, tracing, mechanisms for selective disclosure of information) might be installed and run locally, within users', employees' or consumers' resources (PCs, PDA devices, next generation mobile phones, etc.) to help them to manage and monitor their identities (and profiles) and actively control their usage.

Privacy, data protection and business policies must drive the behaviour of identity management components. As the accountability of the identity managers is dictated by the fulfilment of identity owners' requirements and the evaluation of involved risks and laws, these components need to adapt their behaviours accordingly, depending on the context where identities are used and the purpose by which they are used.

Policy-driven engines and rule-driven authorization systems are mechanisms that can be used to enforce contextual privacy and data protection policies. They are at the very core of many of the components described above.

## 6. Research

The vision and the model described in the previous section helped us to create an identity management framework and formulate our current research topics. In this section we describe a few related research activities that were carried out at the Trust, Security and Privacy Laboratory - HP Laboratories, Bristol, UK. We also briefly introduce some new research topics that we are currently investigating.

### 6.1. Past Research Activities

Research has been done at HP Labs to explore the implications of identity and profile management on trust, to boost business in a dynamic B2B environment, test the feasibility of representing this information by means of digital credentials and understand business and personal implications. We briefly describe the lessons we learnt.

#### 6.1.1. PASTELS project

The PASTELS project [20] is about research in the space of trust management and authorization in a dynamic B2B environment.

The main research problem is related to the establishment and the preservation of dynamic B2B relationships among organisations, on the Internet. Enterprises might be willing to do businesses on the Internet with other enterprises, expose their services and make them accessible to these third parties during business relationships. An inhibitor of this process is the lack of knowledge about the other parties, due to the presence of new Internet companies or the lack of previous relationships. Negotiation and contracts play a key role in establishing business relationships but at the very base, identities, profiles, digital credentials and their overall management are of vital importance to boost trust, enable business relationships and business transactions.

We explored the usage of digital credentials (including X.509 digital certificates and attribute-based, digital signed, XML credentials) and X.509 PKI infrastructure to represent identity and profile information and underpin the assessment of their authenticity and their certification.

We investigated mechanisms and solutions to deal with the dynamic and up-to-date evaluation of trust associated to digital credentials both at the user site and at the enterprise, the automation and simplification of the process of exchanging credentials and the usage of those credentials to drive authorization processes. Users, in this context, are employees with specific roles (including e-procurement roles) and willing to do businesses with remote (and potentially unknown) enterprises by accessing their services. In doing so both parties try to establish or evaluate the trustworthiness and reliability of the remote party – figure 3.

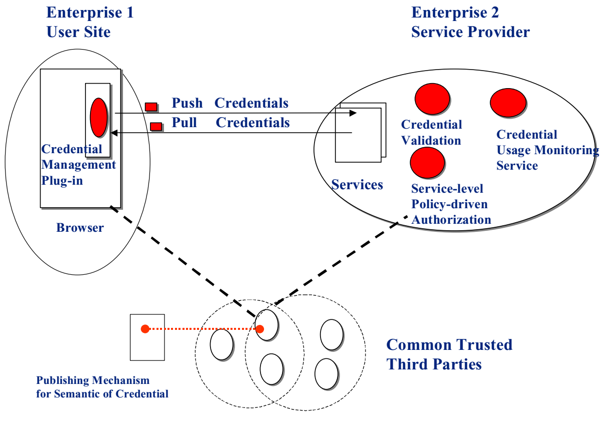
Enterprise 1
User Site
Enterprise 2
Service Provider
Push Credentials
Pull Credentials
Credential Validation
Credential Usage Monitoring Service
Credential Management Plug-in
Services
Service-level Policy-driven Authorization
Browser
Common Trusted Third Parties
Publishing Mechanism for Semantic of Credential

Figure 3. PASTELS - Trust and Authorization Framework

At the user site a browser plug-in solution has been developed and integrated with standard browsers to allow a simple assessment and trust evaluation of digital credentials and automate the exchange of personal or enterprise credentials to establish trust or access resources and services of the remote enterprise.

At the enterprise site a policy-driven credential verification service has been built along with a monitoring system to evaluate on-the-fly the validity and trustworthiness of digital credentials used during active Internet sessions with remote partners. Those evaluations involve trust policies defined by the enterprise and the interaction with trusted third parties, including certification authorities and other trust services: the result is used to recognise dangerous situations and block any misuse of digital credentials. A flexible authorisation framework has also been implemented and integrated at the service and business process level. Authorisation is driven by the content of digital credentials and fine-grained enterprise policies containing business level conditions on trust and service provision aspects.

A fully working prototype was developed and a few experiments carried out in a B2B e-marketplace environment.

The lesson learnt by this research activity is that simplicity and easy of use are important for solutions involving identity management, especially when end-users are involved.

We definitely understood that flexible and policy driven solutions are necessary to cope with dynamic business requirements and that it is important that their interfaces are simple and well defined in order to allow their integration with business processes and services.

We recognised that the usage of X.509 PKI infrastructure and their integration with business applications is hard because of the current technology-focus approach, the complexity of dealing with proper certificate validation tasks and the difficulty of dealing with hierarchical Certificate Authorities(CA). The management of identity and profile information by means of static digital credentials is hard too, because of the volatility of their content (especially if related to profile information) and the complexity introduced in the management of their lifecycle.

This last problem directed us to think of new ways of representing digital credentials and dealing with their dynamic content. This was the foundation of the work we did in the area of active digital credentials.

### 6.1.2. Active Digital Credentials

The concept of active digital credentials [21] has been investigated as a mechanism to extend traditional static digital credentials by providing means for dynamically updating their content along with the assessment of their trustworthiness.

The main goal is to provide enterprises and people with certified and up-to-date data, specifically identities and profiles information to boost trust during Internet relationships and transactions, provide accurate data to be used for access control and decision-making purposes and simplify the overall lifecycle management of digital credentials.

Figure 4 shows our high level model of active digital credentials.

In contrast with traditional digital certificates - which have static content and a predefined period of validity - active credentials embed certified mechanisms and algorithmic procedures to dynamically retrieve, calculate and update their content and check their current level of trustworthiness and validity. This includes dynamic evaluations of: values of credential attributes (including credit card numbers, credit limits, expiration dates, references, etc.); validity and trustworthiness of these attributes; validity and trustworthiness of the whole digital credential.

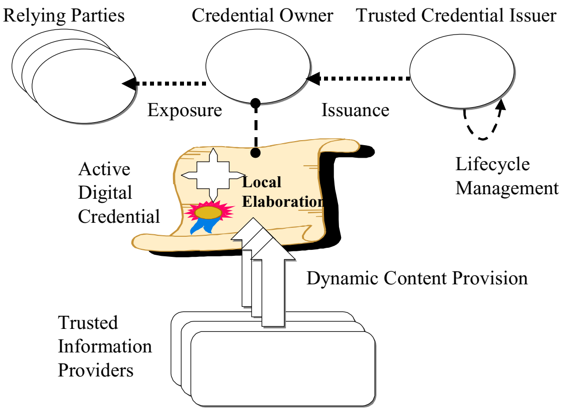
Relying Parties
Credential Owner
Trusted Credential Issuer
Exposure
Issuance
Lifecycle Management
Active Digital Credential
Local Elaboration
Dynamic Content Provision
Trusted Information Providers

Figure 4. High Level Active Digital Credential Model

This method is based on a *late binding* of values associated to credential attributes. A key aspect of active digital credentials is that not only they provide certified mechanisms to retrieve their up-to-date content, but they also contain mechanisms to perform local elaboration of this information. Credential issuers certify the trustworthiness of these *mechanisms*: the relying party uses them to obtain up-to-date information from trusted sources and evaluate their trustworthiness and validity.

This contrasts with traditional approaches, in which the credential issuers only certify the trustworthiness of *data*. A local interpretation of active digital credentials (at the relying party site), by using an execution framework [21], ensures that specific security and privacy requirements are satisfied and that the interactions between the involved parties happen in a predefined and controlled way.

The work on active digital credential is ongoing. A prototype is under construction including mechanisms to represent credentials (including attributes and procedures), issue and evaluate them. Further research needs to be done to understand the complete set of requirements for the underlying infrastructure and the implications in term of life-cycle management. We are planning for real life experiments in order to judge the benefits brought by this approach and compare them to traditional PKI systems.

## 6.2. Current Research Areas

This section briefly describes three topics we are currently investigating in the area of identity management to address part of the identity management issues illustrated in the initial part of this paper.

### 6.2.1. Accountable Management of Identity Information

This research topic is about managing identity information in an accountable way by people and enterprises. The aim is to address the identity management issues related to privacy and accountability highlighted in the initial part of this paper.

It involves the definition of enterprise and personal policies for handling personal data, their representation and enforcement. It is an attempt to address the basic question: “how can you be sure that entities holding your personal data are keeping their promises about how they handle it?”

This research activity involves the investigation and design of solutions for tracing disclosure of personal data among multiple parties along with the possibility to analyse and visualise the result. Those solutions aim at answering questions like "who knows what about me?” or "who broke their promise and gave away identity and profile data?” both in a personal and business environments. It has implications in term of forensic analysis and detection of frauds and identity thefts.

Being able to address these identity management issues has business relevance. For an enterprise, an identity provider (populating the solutions offered by Microsoft .MyServices or the Liberty Alliance Project) or a government service it is a way to show its due diligence whilst handling personal data.

Accountability offers a way for enterprises to be better citizens and show that they are. We believe that accountability makes the enterprise trustworthier. It is also a way to move towards the delegation of control. In this sense, research needs to be done to verify that moving confidential data and the intelligence to handle it to the people (at the edges of the organisations) makes enterprises more dynamic and adaptable to changing situations, without compromising their businesses and preserve responsibilities.

### 6.2.2. Virtual Private Identity Network

This research topic is about the management of personal identity and profile information according to personal interests and polices. The objective is to understand the needs dictated by a broader adoption of digital identities in social and personal contexts and provide proper technologies and solutions to address them.

People are gregarious, but concerned about privacy. They want to form groups of interests or interact with other people but care about privacy and do not necessarily want to give away personal information to outsiders.

Specifically we are investigating mechanisms and solutions to allow people to recognise or contact colleagues, friends or family members in mobile and dynamic environments (such as working environments, large commercial centres, malls, areas in towns covered by wireless services, etc.) but reveal minimum to anyone that they do not already know. This implies prior knowledge of each other, but only those with that prior knowledge see anything coherent. We are also investigating mechanisms for the management of dynamic common interest groups based on selective disclosure of identity and profile information. In this context people will reveal a little about themselves in order to find others with a common interest. Negotiation is a key aspect to balance what you reveal with what it is revealed to you.

We believe that people will spend money on appliances that help them communicate and provide added value functionalities.

### 6.2.3. Personal Identity Assistant

This research topic focuses on the management of identity and profile information made by people that make use of mobile appliances in their day-by-day lives, for work, personal and social matters.

We are currently researching on the concept of a *personal identity assistant* that looks after its owners' interests, during transactions and interactions carried out in a mobile and dynamic environment.

This assistant understands a person's preferences and matches them to the environment surrounding that person, to enhance their experience without giving away their secrets or personal information.

People like to have a personal experience, but they are wary about revealing enough to let someone else create it. Ideally the system will adapts to both the culture of the owner and the surrounding environment and helps its owner to fit in.

A personal identity assistant can be fitted on the next generation of mobile appliances. We believe that a personal and customisable device will be more desirable and fashionable that traditional standard ones.

## 7. Discussion

Security is important for identity management and has to be kept in account whilst designing identity management systems and solutions.

It is common to hear about e-commerce sites that have been hacked and whose content, including identity and profile information has been stolen or publicised on the web. Most of the time this is due not only to software bugs but also to a lack of due diligence in assessing security threats and risks whilst building e-commerce sites and components that deal with identity and profile information.

Identity and profile information need to be stored in secure systems and processed in a way to preserve their confidentiality and integrity. Encryption techniques and strong access control mechanisms need to be put in place in order to protect data and avoid unauthorised disclosures.

Processes and applications must be designed and implemented in a way that they can deal with sensitive data in a secure and protected way, perhaps by using trusted computing platforms to avoid unauthorised exposure of this data to potentially hostile environments.

Communications between systems, applications, services and people should happen by using secure and protected channels (including SSL links or encrypted messages) whenever confidential identity information is transmitted.

In addition, non-repudiation mechanisms (including strong authentication) should be put in place every time sensitive operations are carried on identity information for their management, processing and disclosure.

The combination of secure and accountable systems and audit mechanisms, along with a clear specification and enforcement of privacy laws and data protection policies are at the very base of successful identity management solutions.

The perception of trustworthiness, reliability and simplicity that people have about those solutions is very important to determine their adoption as much as their operational and functional capabilities.

## 8. Conclusions

Identity management is about the management of digital identity and profile information. It encompasses operational aspects such as certification and issuance of identity information, authentication and single-sign-on, aggregation of fragmented identity information across organizations and authorization. Its importance spans across the consumer, e-commerce, enterprise and government worlds.

On one hand, trusted, secure and accountable identity management solutions are key e-business enablers. On the other hand identity management introduces social dilemmas and issues due to the implications on privacy and fears to lose freedom.

We discussed current and foreseeable trends for identity management along with an analysis of important issues and requirements. We introduced a model of an identity management framework and discussed some of our past and current research activities in this area.

More work and research need to be done in this space, especially for open and dynamic contexts. Whilst closed environment (including stand alone enterprises, private Internet business communities, etc.) can define strict criteria to deal with identity management issues and leverage their heavy and centralised control, the real challenge is for open and dynamic environments based on cooperation and collaboration of heterogeneous parties, ranging from people to organizations.

Trends suggest that this is the directions towards which people, organizations, enterprises and governments are moving: being able to understand these new issues and provide solutions that address them is going to be strategic to enable new commercial and social opportunities.

## 9. Acknowledgements

Special thanks to Adrian Baldwin, Yolanta Beres and Simon Shiu – HP Laboratories, Bristol, UK - for their feedback and material used in this paper.

## 10. References

[1] B. Parr, R. Villars - Digital Identity: The Coming Struggle for the Future of the Net – IDC Bulletin #24929 - 2001

[2] J. Gaw - Digital Identity Solutions: A Road Map for Software and Services - IDC Bulletin #26102 - 2001

[3] Microsoft – Microsoft .MyServices: a platform for building user-centric applications - http://www.microsoft.com/myservices/ - 2002

[4] Liberty Alliance Project - http://www.projectliberty.org/ - 2002

[5] A. Volchkov - Revisiting Single Sign-On: A pragmatic Approach in a New Context – IT Pro – IEEE – 2001

[6] J. Wilcox - Study: Customers Wary of Online Ids - http://news.com.com/2100-1001-892808.html?tag=fd_lede - Extract from Gartner Study - 2002

[7] R. Housley, W. Ford, W. Polk, D. Solo – RFC2459: Internet X.509 Public key Infrastructure Certificate and CRL Profile, IETF - 1999

[8] J. Penn - Market Overview: User Account Provisioning - GIGA Report - 2001

[9] M. Neuenschwander - Meta-Directory Services and the Emerging Enterprise Data Network – The Burton Group - 2002

[10] J. Penn - IT Trends 2002: Directories and Directory-Enabled Applications - GIGA Report – 2001

[11] UK - e-Government Strategy Framework Policy and Guidelines - http://www.govtalk.gov.uk - 2001

[12] Italy - Italian e-Government Action Plan - http://www.pianoegov.it/open.asp?cat=276 - 2000

[13] Europe - eEurope Action Plan – e-Governement: Electronic Access to Public Services - http://europa.eu.int/information_society/eeurope/action_plan/ - 2002

[14] S.761 - The Electronic Signature in Global And National Commerce Act -US - S.761 - 2000

[15] 1999/93/EC – Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signature - 1999

[16] T. Arnold –Internet Identity Theft: A Tragedy for Victims - White Paper - SIIA – 2000

[17] D. Coates, J. Adams, G. Dattilo, M. Turner - Identity Theft and the Internet - Colorado University – 2000

[18] Identrus - Identrus Case Studies - http://www.identrus.com/ - 2002

[19] A. Baldwin, Y. Beres, M. Casassa Mont, S. Shiu – *Trust Services: A Trust Infrastructure for E-Commerce.* HPL-2001-198 - 2001

[20] M. Casassa Mont, R. Brown - PASTELS project: Trust Management, Monitoring and Policy-driven Authorization Framework for E-Services in an Internet based B2B environment. HPL-2001-28 - 2001

[21] M. Casassa Mont, R. Brown – Active Digital Credentials: Provision and Up-to-Date Identity and Profile Information - HPL-2002-59 - Hewlett Packard Laboratories, Bristol, UK - 2002