Active Digital Credentials: Provision of Up-to-Date Identity and Profile Information

Marco Casassa Mont, Richard Brown
Trusted E-Services Laboratory
HP Laboratories Bristol
HPL-2002-59
March 27th , 2002*

E-mail: marco_casassa-mont@hp.com, richard_brown@hp.com

digital credentials, up-to-date content, identity management, trust, e-commerce

Identities and profiles are important to enable e-commerce transactions both in well-established business relationships and sporadic business interactions. Recent initiatives, like Microsoft MyServices and Liberty Alliance Project, aim at the provision of identity and profile management solutions along with mechanisms to simplify users' experience. To be really successful, these solutions must be trusted and accountable.

Current PKI solutions can be used to deal with certification and trust management: digital credentials are a viable way to certify identities and profiles. Unfortunately the complexity of managing credential lifecycle is one of the obstacles to their adoption. This complexity is accentuated in the case of dynamic environments, where the certified information is subject to frequent changes.

In this paper we address the problem of providing up-to-date certified information in dynamic contexts without the burden of heavy management processes. We introduce and discuss the concept of active digital credential, based on a novel mechanism to provide up-to-date certified identity and profile information along with a fine-grained assessment of their current level of trustworthiness and validity.

* Internal Accession Date Only
Approved for External Publication
© Copyright Hewlett-Packard Company 2002

1. Introduction

E-commerce transactions over the Internet will become more and more relevant in the next years: the current exponential growth of e-commerce sites on the Internet, new B2B initiatives and the rise of web services to underpin enterprise and government activities are going to provide new opportunities for doing business on the Internet to a larger and larger population of customers and users.

Because of the accompanying increase in the number of business interactions where there is a lack of prior knowledge about the participants, the task of establishing, managing and ensuring trust on the Internet [1] is going to be a major issue.

In this context, the problem of dealing with up-to-date identity and profile information is crucial. Personal information, profiles and rights can change quite frequently, sometimes as a direct consequence of business transactions. Each transaction, for example, can have an immediate impact on users' credit limits and their associated credit rating information.

Today people buy and sell goods and services on the Internet by interacting with a multitude of e-commerce sites. Consumers traditionally need to create and manage multiple accounts, one for each web site they want to interact with. This is a problem, because of the need of remembering multiple logins and passwords, the need of supplying many times the same profile information and keeping it up-to-date.

Recent initiatives, including Microsoft .MyServices [2] and Liberty Alliance Project [3], aim at the provision of infrastructure and mechanisms to ease the pain of managing profile information across multiple Internet accounts.

Both initiatives support single-sign-on across multiple service providers by using an underlying network of identity providers. Identity providers are in charge of storing profiles and identity information and providing authentication services.

Identity providers should be accountable for the services they provide and perform due diligence tasks to assess the authenticity and trustworthiness of identity and profile information they provide to relying parties. Moreover identity providers should ensure that the identity and profile information they supply is accurate and up-to-date.

In this paper we address the problem of keeping certified identity and profile information up-to-date without the burden of heavy management processes. We introduce and discuss the concept of active digital credentials, based on a novel mechanism to provide up-to-date certified identity and profile information along with an assessment of their current level of trustworthiness and validity.

2. Background and requirements

The problem of assessing the authenticity of identities and profiles is not trivial as it deals with the analysis of data provenance and implies the cooperation of users and trusted authorities through the process of verification and certification.

The trustworthiness of certification authorities has a direct impact on the trustworthiness of the certified information and it directly influences the way relying parties perceive and make use of this information.

X.509 PKI systems [4], [5] provide mechanisms for dealing with certification of information and underpinning trust management. Certification authorities and registration authorities are in charge of registering, verifying and certifying identities and profiles, according to different degrees of assessment of their authenticity. These controls can range from none to face-to-face meetings.

To increase the perception of trust and transparency, certification authorities state their responsibilities and their degree of accountability by publishing Certification Practice Statements (CPS). They also use chains of certifications and cross-certifications mechanisms to underpin their trustworthiness. However, this approach has negative side effects due to the lack of scalability of certification and cross-certification chains and the complexity of managing and verifying certificates.

In the last few years alternative approaches have been introduced, for example, those based on PGP [6], SPKI [7], [8] (both based on web of trust) and recently Identifier-based Encryption [9] (IBE) techniques. They address part of the X.509 PKI problems for specific realms and contexts by improving their overall usability and changing the dynamics of trust assessment. In addition, trust services [10] are emerging as a viable solution to underpin trust in e-commerce and e-business areas: the management of the information that forms the basis of trust is outsourced to professional and accountable third parties. These third parties include notarisation service providers, recommendation service providers, credit rating service providers and trusted storage service providers.

In all the above approaches, digital credentials are a viable mechanism to represent, certify and convey identity and profile information along with means of verifying their trustworthiness. Digital credentials are particularly important in contexts where there is no prior knowledge of the involved parties and no web of trust is in place.

Traditional X.509 and SPKI digital credentials are usually valid for a predefined period of time, ranging from a few seconds to years: their content can be used for authentication and authorization purposes. They must be revoked whenever their content is out-of-date or it has been compromised.

Unfortunately the revocation process is a burden both for relying parties and for credential issuers. Relying parties need to check credentials against certificate revocation lists (CRLs) to verify their validity or delegate this activity to third parties. Credential issuers must deal with the complexity of the overall credential lifecycle management and they are accountable for maintaining up-to-date CRLs.

The limitation of X.509 digital credentials is evident in contexts where the certified information is dynamic: in such contexts credentials are short-lived and they must be revoked whenever their content changes. This causes the proliferation of digital credentials with consequent implications in term of verification of their validity, correctness of their content, management of their disposal and prevention of their misuse.

X.509 and SPKI digital credentials are either valid or not valid: there is no middle ground even if the degree of trust a certification authority has in their content may vary over time or if there is a wish to vary their content. For example, in traditional X.509 certificates any variation of their attributes implies that the whole certificate must be revoked. Important attributes including credit limits and rating levels may change very often, depending on the occurrence of business transactions and owner's reputation.

To deal with dynamic information, e-commerce service providers currently use back channel communications with trusted information. Emerging mark-up languages, like SAML [11], are used to underpin the exchange of information by means of secure assertions. The disadvantage of this approach is that it requires the set-up of ad-hoc point-to-point communication channels and the exchanged assertions are meaningful in these very specific contexts.

This paper focuses on mechanisms to enable the provision of trustworthy and up-to-date information in dynamic contexts. The objective is to create a coherent and sustainable way to certify identity and profile information and reduce the burden of their lifecycle management.

We introduce a new approach based on the extension of the current model of digital credentials. This approach is meant to satisfy the following requirements:

- Provide up-to-date content of digital credentials;
- Support up-to-date assessment of the trustworthiness and validity of digital credentials;
- Reduce the management of digital credentials, especially in term of issuance and revocation of digital credentials.

3. Proposed approach

This section introduces and describes the concept and principles underpinning *active digital credentials*. Active digital credentials are a mechanism to extend traditional static credentials by providing means for dynamically updating their content along with an assessment of their trustworthiness.

3.1 Active Credential Model

Figure 1 shows the high level model of active digital credentials:

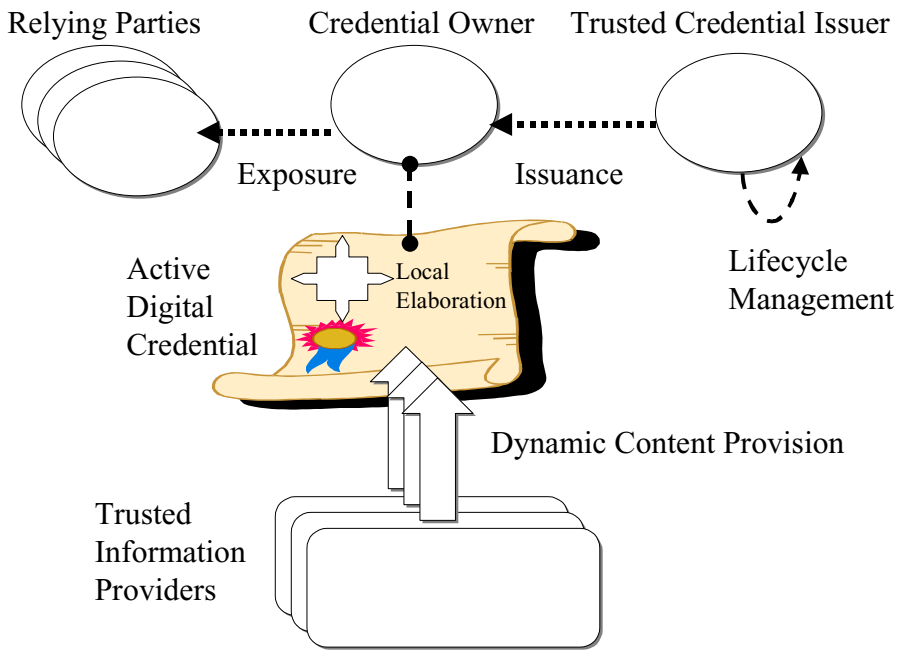

Figure 1: High level model

In contrast with traditional digital certificates - which have static content and a predefined period of validity - active credentials provide certified mechanisms to dynamically retrieve, calculate and update their content and state their current level of trustworthiness and validity. This includes dynamic evaluations of:

- Values of credential attributes;
- Validity and trustworthiness of these attributes;
- Validity and trustworthiness of the whole digital credential.

The proposed method is based on *late binding* of values to credential attributes.

A key aspect of active digital credentials is that not only do 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 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) ensures that specific security and privacy requirements are fulfilled and that the interactions between the involved parties happen in a predefined and controlled way.

The basic model of an active digital credential is showed in Figure 2:

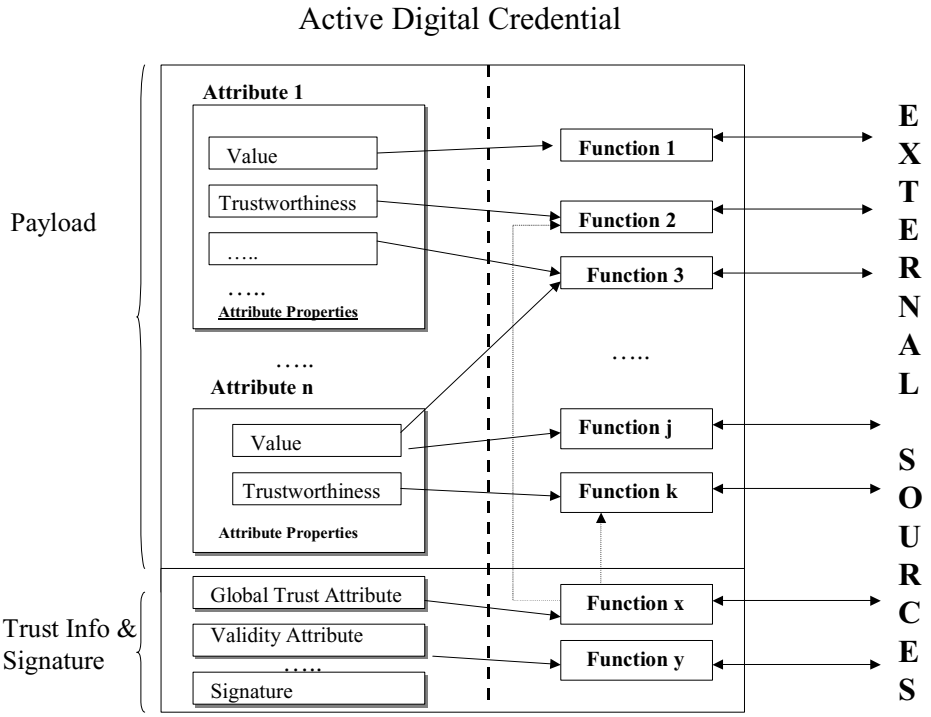

Figure 2: Active Digital Credential - Model

An active digital credential is a certified collection of *attributes* along with embedded *functions*. Its purpose is to represent identity and profile data, along with tools to assess their validity and trustworthiness.

In general, a credential attribute is characterised by a set of *properties* whose values can be determined dynamically by executing embedded functions. Attributes can represent any identity and profile information: name, address, public key, credit card information, credit rating, driving license information, etc.

The properties of an attribute include the value of the attribute, its default value and its level of validity and trustworthiness.

The functions embedded in an active digital credential are certified by digital credential issuer(s) as trusted methods to compute property values. This computation might involve information contained within the credential and dynamic external information, retrieved from local systems or the Internet.

Active credential functions are agreed between the involved parties, including the owner, issuers and the information providers.

An example of active digital credential is a digital credit card credential. The list of associated attributes might include a credit card number, an expiration date, a credit limit and a credit rate along with references to the legitimate bearer. For example, the credit limit attribute might have a default value of $10000 but the current value is determined by an embedded function, which retrieves this information directly from the credential owner's bank account.

Pursuing the example of the credit rating attribute, an associated function can dynamically determine the level of risk and trustworthiness associated to the credential owner, for instance by interacting with a certified credit rating agency.

In another example, an active digital credential can be used for authorization purposes. It contains an access attribute whose value (PERMIT, DO NOT PERMIT) is determined by a function based on the employee's role within an enterprise and the current date and time.

This mechanism is appropriate not only for the attributes contained in the credential "payload" but also for "management" attributes stating the validity and trustworthiness of the whole digital credential. Trust functions can be used to calculate the validity of a credential and its expiration date, along with the current level of trust. Levels of trust and validity could have any value in a numeric range, like [0,1] or values from a predefined set of values (for example, "High Trust", "Medium Trust", "Low Trust", "No Trust").

A simple application of this property is the definition of "decaying" certificates whose levels of trustworthiness and validity depend on the time elapsed since their issuance. Any type of function can be used to calculate this information at different levels of granularity. As a consequence, a digital credential may still be valid and trustworthy even if some of its attributes are not.

In general the level of trust and validity of credentials can be determined in a fine-grained way, ranging from the whole credential to specific attribute properties.

The next sections describe two scenarios involving active credentials along with the infrastructure necessary to properly use them.

3.2 Scenarios

Figure 3 shows a scenario where active digital credentials are exchanged between a credential issuer, a credential owner and a relying party:

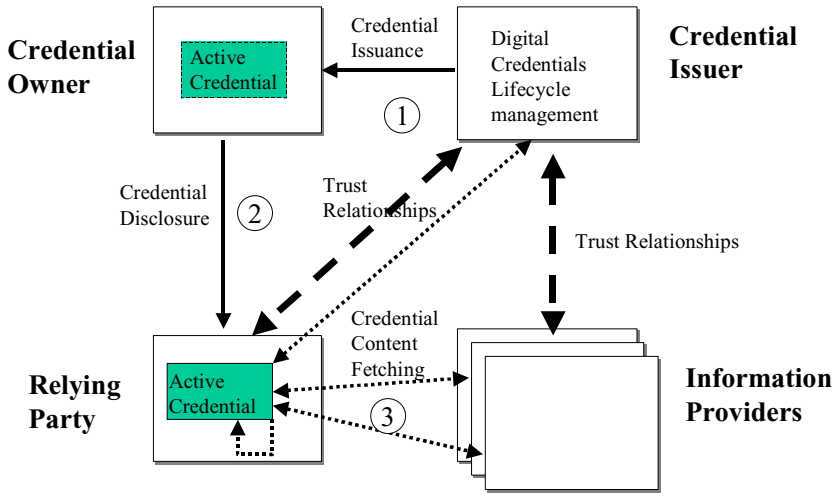

Figure 3: Active credential scenario 1

This scenario involves the following players:

- Active credential issuer: it is a trusted certification authority that issues active digital credentials and manages their lifecycle. This entity has multiple trusted relationships with third parties (including banks, credit rating services, recommendation services, etc.) whom provide up-to-date content for active digital credentials. The credential issuer certifies the functions which dynamically retrieve this content.

- Trusted information provider: it is an information provider that supplies up-to-date information about identity and profiles, under well-defined constraints and agreements. A trusted identity provider has a trust relationship with active credential issuers.

- Credential owner: it is the owner of the active digital credential. At the issuance time, the credential owner may specify which information provider must be used to retrieve identity and profile information. The credential issuer must have trust relationships with those information providers.

- Relying party: it is the entity that supplies products and services on the Internet. It receives active credentials from purchasers. Access might be granted to a user depending on the dynamic evaluation of the content of these active digital credentials.

Users either directly supply their identity and profile information to the certification authority or point to trusted information providers, which must be contacted to collect this information. Active credential issuers might also play the role of trusted information providers.

A certification authority (credential issuer) issues an active digital credential to a user after a due diligence process involving the verification of user's information (Figure 3 – step 1).
Credential owners supply their active credentials to service providers to access services (Figure 3 - step 2). Service providers accept credentials issued by the credential issuers they trust. They evaluate these credentials to retrieve up-to-date content and determine their current level of trustworthiness and validity, based on principles either defined or certified by those credential issuers (Figure 3 – step 3).

Figure 4 shows a variant of the above scenario where identity providers act as trusted authentication services and store identity and profile information. They supply this information to relying parties, on behalf of their owners.

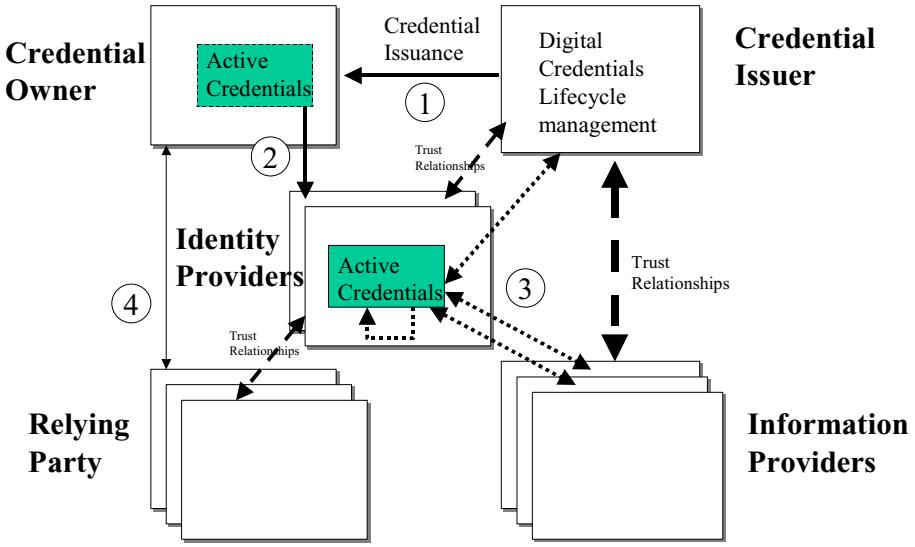

Figure 4: Active credential scenario 2

The parties and relationships in this scenario are conceptually similar to those in scenarios painted by Microsoft MyServices and Liberty Alliance initiatives. We analyse the interactions between the involved parties from the perspective of providing certified and up-to-date information.

People still own active digital credentials, issued by certification authorities (Figure 4 – step 1). These credentials might be directly exposed to trusted identity providers, that act as proxies on behalf of the owners (Figure 4 – step 2).

The fact that active credentials have been assessed and certified and their content is up-to-date increases the overall perception of trust and accountability.

Third party information providers may still retain profiles and information about the credential owners. They can disclose (part of) this information to identity providers

under terms and conditions defined by the owners, through active digital credentials (Figure 4 – step 3).

Identity providers are enabled to supply identity and profile information to service providers according to credential owners' policies, through the evaluation of active digital credentials (Figure 4 – step 4). They retrieve up-to-date certified information, evaluate its current level of trustworthiness and supply it to the relying parties.

In particular circumstances identity providers might also play the role of credential issuers.

3.3 Infrastructure

Because of the nature of active digital credentials, the entities that evaluate these credentials (evaluators, e.g. relying parties, identity providers, etc.) need to use a proper infrastructure. This section describes high-level aspects of an infrastructure for the interpretation and execution of active credentials.

Figure 5 shows its basic components:

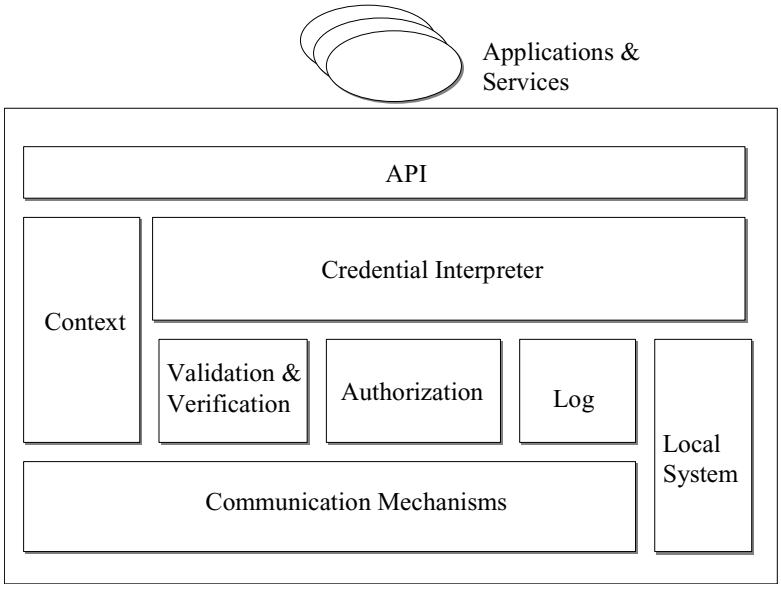

Figure 5: High level infrastructure

This infrastructure includes:

- Credential interpreter: it is an engine that interprets active digital credentials. The interpreter is in charge of coordinating the traditional verification and validation processes (about the trustworthiness of the credential issuer) that are executed by validation and verification sub-components.
  The interpreter creates an internal representation of the credential including its attributes, their properties and related functions. It locally executes credential functions in order to retrieve up-to-date information from remote information providers and it calculates the values of attribute properties

- Context manager: it is the component that aggregates and manages contextual information about the credential owner and the entity that is evaluating the credential (evaluator). Specifically the evaluator context might contain information about the identity and profile of the evaluator, which might be passed (as parameters) to the functions embedded in the credential, during their execution. This could be requested to enable the interaction with remote information providers and fulfil constraints dictated by the credential owner.

- Validation and verification component: it is the component that provides policies and processes necessary to deal with the validation and verification of active digital credentials [16]. The credential interpreter uses this component to make decisions about the validity and trustworthiness of active credentials including the trustworthiness of the issuers and their digital signatures.

- Authorization component: it is the component that provides authorization and access control policies and an enforcement engine [16]. The credential interpreter uses this component to make decisions about the information that can be disclosed to third parties and which access can be granted to local resources, while interpreting active credentials.

- Communication component: it is the component providing basic communication mechanisms to interact with external systems and services (via common Internet protocols, including HTTP, SSL, etc.). It is in charge of establishing secure connections with remote parties.

- APIs: it is a set of high-level APIs to the infrastructure that allow external applications and services to manipulate active credentials in a way that is transparent to the underlying mechanisms.

- Logging system: It is the component that logs all the activities and events that happen during the evaluation of active credentials. Logged data can be used for auditing purposes and as evidence in case of disputes.

The above infrastructure provides a safe environment to interpret active credentials and execute their functions. The interpreter acts as a virtual machine for these functions and it makes sure that their executions happen in a controlled way, according to predefined policies.

For privacy and confidentiality reasons the communication between the interpreter and the remote information providers might be encrypted. The credential evaluator might be asked to authenticate itself to satisfy credential owner's privacy policies. The interpreter mediates all the interactions during the authentication process by providing support for secure connections, for example including traditional SSL two-way handshakes.

The interpreter verifies the validity and trustworthiness of the credential issuer and provides fine-grained information to the credential evaluator according to local policies, defined by the evaluator. If the active credential issuer is trusted, the execution of trust functions within the active credential allows the retrieval and elaboration of detailed information about the validity and trustworthiness of the

credential and their attributes. In a similar way, other embedded functions allow the retrieval and elaboration of the values of attributes properties.

The above infrastructure can be implemented in many different ways and deployed in multiple contexts, ranging from browser plug-ins to back-end middleware processes.

4. Discussion

Relevant prior work in this area is described by patent [15]. It introduces the concept of static references to external information within a credential. Those references are usually implemented by an identifier (label) to retrieve information stored elsewhere. The solution described in [15] does not provide any certified mechanism to locally elaborate the retrieved information.

We introduce mechanisms to dynamically evaluate the content of credentials by defining and certifying those mechanisms (functions) within the credentials themselves: an active digital credential is a tool for describing, certifying, retrieving, elaborating and assessing dynamic identity and profile information.

An active digital credential can be seen as a "contract" agreed between the credential owner, information providers and the credential issuer(s). As credential owners can dictate the criteria for the disclosure of their data, active credentials enable them to retain control over their data. There is no system-induced requirement for actual data values to be disclosed to relying parties; this privacy characteristic is especially important when the credential owner has no prior trust in the relying parties.

Active digital credentials still need to go through traditional credential lifecycle management processes. Moreover, their active functions need to be assessed and certified by the issuers. Issuers and information providers need to stipulate agreements, along with trust relationships. However these trust relationships are also required in scenarios that do not involve active credentials, in order to underpin trust and accountability.

Active digital credentials improve the lifecycle management of digital credentials by diminishing the dependency of credentials' validities on the unchanged nature of all their contents. This is particularly true for very dynamic environments.

On one hand, the value of attributes can be retrieved dynamically and their validity and trustworthiness assessed on the fly. This allows active credentials to be valid and trustworthy even if part of their attributes are not anymore. The effect is to reduce both the number of revoked credentials and the need for short credential lifetimes, at least in contexts where the objective is to supply identity and profile information instead of authentication or authorization rights.

On the other hand, the content of active credentials depend on the availability of external systems, services and Internet connections. When those entities are not available, active credential content cannot be retrieved. This can be an issue. Risks can be partially mitigated by introducing default values for attribute properties and local elaborations. It must also be said that the content of an active credential does not necessarily depend on external information providers but it might depend on local

elaboration of information like date and time (for example in case of decaying certificates).

Active credentials need a proper infrastructure in order to be evaluated. However, this is also true for traditional digital certificates, to deal with their validation and verification. The advantage of the proposed active credential infrastructure is that it provides certified and agreed mechanisms to assess the validity and trustworthiness of active credentials and up-to-date content. This can be achieved in a safe and secure way thanks to the mediation of the active credential infrastructure.

On one hand it is easier to enforce privacy and data protection constraints over credentials' content. The content of an active credential can be disclosed and made available to a relying party only after the authentication of this relying party and the fulfilment of criteria dictated by the credential owner.

On the other hand, functions within active digital credentials need to be carefully built in order not to introduce vulnerabilities within the systems and services they access at the information providers sides. Those risks can be mitigated by constraining the kind of access and activities those functions can perform on the remote sites. Credential issuers must be involved in building those functions, in cooperation with the information providers.

In general active credentials simplify the process of retrieving information, as the mechanisms for doing this are embedded and available within active credentials. This reduces the need for ad-hoc back-channel connections between the involved parties, as predefined and certified communication links are already available. Because credential issuers assess the trustworthiness and suitability of active credential functions, there is also a shift of accountability from the relying parting to the credential issuers.

Current technologies can be used to easily implement active digital credentials. For example digital signed XML [12], [13] can be used to describe such credentials and WSDL [14] to describe embedded functions. Java classes, scripts and Microsoft (.NET) web services can possibly be used to implement those embedded functions.

Although technology is already available, the involved parties must agree on the format of active credential, both in term of semantic of the attributes (and their properties) and definition of the embedded functions.

5. Conclusion

The provision of up-to-date and trustworthy identity and profile information is important to enable e-business transactions.

Digital credentials are a viable way to certify and verify identities and profiles but their limitations are due to their static content and the complexity of the underlying infrastructure to manage them. When dealing with dynamic environments, current digital credentials introduce further complexity at the management and usability level.

We introduced and discussed the concept of active digital credentials, as a way to couple certified attributes with mechanisms to retrieve their up-to-date values. Embedded active credential functions are used to evaluate not only the current content of a credential but also its validity and trustworthiness, in a fine-grained way.

We believe that this approach simplifies the overall management of credentials in dynamic environments, by reducing the need for certification revocation practices and short-lived certificates. We also believe that it boosts accountability and trust because of the definition of clear mechanisms for retrieving information (compliant with privacy and data protection constraints), the assessment and certification of these mechanisms by trusted third parties and the provision of up-to-date content, along with a dynamic assessment of its validity and trustworthiness.

6. Acknowledgements

We would like to thank members of the Trusted E-Services Laboratory, Bristol, UK, for their feedback: in particular Pete Bramhall for his precious comments and suggestions.

7. References

[1] L. J. Camp – Trust and Risk in Internet Commerce – The MIT press – 2000

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

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

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

[5] S. Farrell, R. Housley – An Internet Attribute Certificate Profile for Authorization – IETF - 1999

[6] IETF – An Open Specification for Pretty Good Privacy (PGP) - http://www.ietf.org/html.charters/openpgp-charter.html - 2001

[7] C. Ellison – SPKI Requirements, RFC 2692, IETF – 1999

[8] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T Ylonen – SPKI Certificate Theory, RFC 2693, IETF – 1999

[9] D. Boneh, M. Franklin – Indentity- Based Encryption from the Weil Pairing - Crypto 2001 – 2001

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

[11] OASIS – SAML 1.0 Specification Set - http://www.oasis-open.org/committees/security/#documents - 2002

[12] D. Eastlake, J. Reagle, D. Solo – XML-Signature Syntax and Processing, draft-ietf-xmldsig-core-08, IETF – 2000

[13] T. Bray, J. Paoli, C.M. Sperberg-McQueen – Extensible Markup Language (XML) 1.0 – W3 Recommendation, 10 February 1998

[14] W3C – Web Services Description Language (WSDL) 1.1 – 2001

[15] P. Zubeldia, G. Romney – Digital Certification Systems - EP 0869637 A2 – 1998

[16] 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