Digital Identity Management based on Digital Credentials

Stefan Brands and Frédéric Légaré
Credentica Inc.
Version 1.0 of June 2002
{brands,legare}@credentica.com

Abstract: Today's commercial Digital Identity Management offerings have fundamental design flaws. This paper provides an overview of a superior solution in the form of Credentica's Credential Management Platform, which holistically addresses the needs of all system participants.

1 Introduction

Virtually every industry relies on the management and transfer of identity-related information stored in databases. In today's corporate and government environments, information sharing is fundamental to cut costs and to manage increasing numbers of customer interactions. Financial institutions, telecommunication organizations, governments, health care providers, and other organizations are transforming their database records and their access methods into electronic forms. Large-scale use of information in electronic form is already encountered in the Internet content provider space, where providers like Yahoo, MSN, and AOL use systems capable of handling millions of users. Information systems are moving from closed environments (such as intranets, extranets, and VPNs) to increasingly open environments, supported by industry efforts such as Web Services, wireless Internet, point-to-point peering devices, and ad-hoc networking (enabled through, for example, WiFi and Bluetooth).

In the brave new world of electronic information sharing, it is much harder to deal with fundamental security issues related to access control and authentication. Traditional trust domains and physical security perimeters are vanishing, and the consequences of fraud can spread almost instantaneously in uncontrollable ways. This renders traditional security techniques, such as simple passwords and firewalls, totally inadequate. Security can only be addressed properly through the use of strong cryptography. Indeed, "Authentication and Authorization" is the fastest growing segment in security software, and Digital Identity Management technologies (which deal with the authentication and management of identity-related information in digital form) are experiencing the fastest usage growth.

Today's Digital Identity Management products, however, have fundamental design flaws. The main problem is that they rely (in the best cases) on a technology that was invented a quarter of a century ago, at the dawn of modern cryptography: digital identity certificates. These were never intended to serve as the basis for access control and information authentication; their design purpose was simply to facilitate the encryption of messages using the public keys of authenticated receipients. As an unfortunate result, commercial Digi-

tal Identity Management offerings today offer no protection against the lending of access rights and other serious attacks, respect virtually none of the privacy principles codified in law, and suffer from performance drawbacks due to their heavy reliance on trusted on-line repositories.

There is a pressing need for Digital Identity Management solutions that holistically address the entire spectrum of needs of all system participants. This paper provides an overview of Credentica's Credential Management Platform (CMP), a superior platform for Digital Identity Management which is suitable for both "physical" and "virtual" environments.

2 Credentica's Credential Management Platform

CMP is based on the strongest and most flexible technology for authentication and access control to have come out of academia in the past decade: Digital Credentials (see `http://www.credentica.com/technology` for details). Figure 1 represents a schematic overview of CMP.

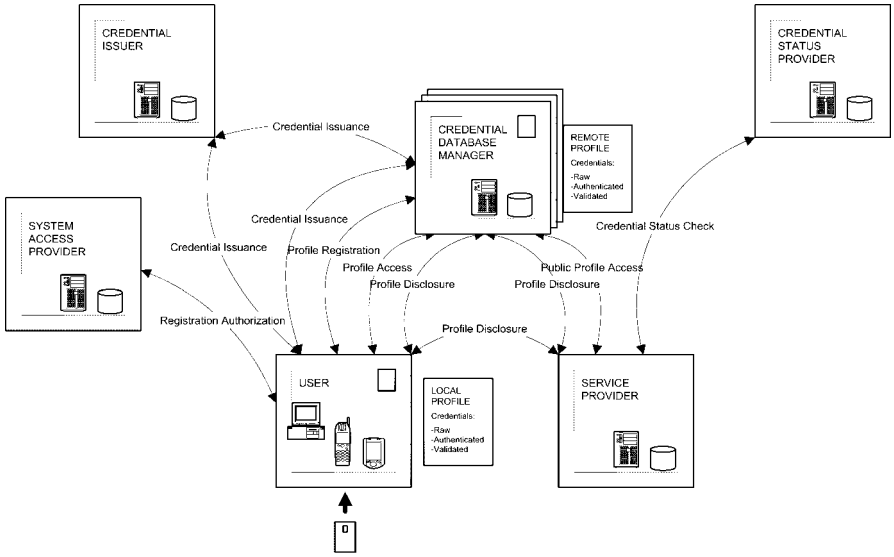

Figure 1: Credentica's Credential Management Platform

CMP is characterized by three central notions: profiles, participants, and protocols.

2.1 Profiles

A profile is a logical collection of information pertaining to a User. A profile contains two kinds of information: Credentials and administrative data. A Credential is any information about the User that is asserted either by the User himself or by another party or process;

examples are the User's name, privileges, preferences, access rights, entitlements, transaction history, contacts, habits, and movements. The administrative data defines the access rights for the Credentials in the profile. More specifically, it describes rules that specify for each Credential in the profile who can read, write, modify, or otherwise access and manipulate that Credential. Administrative data includes information such as audit trails (possibly digitally signed) for profile access events.

CMP distinguishes between three types of Credentials in a User's profile:

1. **Raw Credentials**: Credentials specified by either the User himself or by any other party without any guarantee as to their validity. Raw Credentials are typically suited only for Inconsequentially Positive Credentials (i.e., the User has no personal incentive to discard these Credentials or to pretend they do not exist, and modification or discarding would not adversely affect the security of any other participant); personalized display or content preferences for a Web site are an example.

2. **Authenticated Credentials**: Credentials that are digitally authenticated, either by the User himself or by a Credential Issuer, without prior verification of their validity. This prevents the User and other parties with access to the profile from modifying the Credential. Authenticated Credentials are suited primarily for Consequentially Positive Credentials (i.e., the User has no personal incentive to discard these Credentials or to pretend they do not exist, but the User's ability to modify or lend the Credential would adversely affect the security of another participant) that have minimal negative consequences if they would be untrue. In an on-line chat system, for example, a User could make up his own gender but will be stuck with it in future sessions.

3. **Validated Credentials**: Credentials that are digitally authenticated by a Credential Issuer only after the validity of the Credential has been verified. Validated Credentials are suited for Consequentially Positive Credentials as well as for most Negative Credentials (i.e., the User has a personal incentive to discard Negative Credentials or to pretend they do not exist); examples are the description of the insurance coverage of a healthcare insurance beneficiary and a criminal record, respectively.

For Authenticated and Validated Credentials, CMP uses methods taken from the Digital Credentials technology to offer unique security, privacy, and useability benefits. CMP also supports Kerberos authentication and X.509 certificates, in concert with simple password techniques. Note that a Credential can be Negative, Inconsequentally Positive, or Consequentially Positive, depending on the context in which it is used. That context may vary across applications, as well as within an application depending on authorization rules applied by Service Providers.

2.2 Participants

A participant is an individual or an organization (more precisely, one or more devices or applications acting on their behalf) playing a basic role in CMP. A participant may also be an autonomous device that does not act on behalf of a person or a group of persons. In a real-world application, there may be many instantiations of each participant, and the functionalities of multiple participants from either the same or from different systems may all be performed by the same party.

CMP distinguishes between six participants:

1. **User**: The data subject to whom the Credentials in a profile pertain. The User may be represented by a PC, a hand-held, a mobile phone, a smart card, or any other device (or combination of devices) capable of computing and communicating. CMP supports three physical storage locations for a User's profile: in a central database not under the User's control; distributed across multiple databases not all under the User's control; and, in a device operated by, and under the control of, the User. In the first two cases the profile is called a Remote Profile, in the latter case it is called a Local Profile. In general, a Local Profile offers greater security and privacy to the User, but may be less convenient. Examples of Users are: a patient in an e-health system; a citizen in an e-government Web site application; an employee or a client wanting to gain access to physical premises; an immigrant holding an entitlement chipcard; a voter in an Internet election system; and, a subscriber to digital content delivered through a 3G mobile phone.

2. **Credential Database Manager**: A party, or a collaboration of multiple parties, that physically controls and manages Remote Profiles, not necessarily on behalf of the Users to whom the profiles pertain. Examples of Credential Database Managers are: an identity broker providing personal information to Web site operators enabling them to target their offerings and negotiation processes; a financial institution managing bank accounts and monetary transactions; hospitals storing electronic patient records; key escrow organizations that hold key shares for decrypting encrypted traffic when presented with a court order; an Internet music service delivering mp3 files to registered visitors of its Web sites; and, police departments maintaining criminal records.

3. **Service Provider**: A party that relies on some or all of the Credential information in a User's profile in order to make an appropriate authorization decision pertaining to that User. A User's Credentials, or more generally properties about the Credentials that are stored in one or more profiles, are presented to the Service Provider either by the User (for a Local Profile) or by the Credential Database Manager. In the latter case, the User's involvement and/or explicit consent may be needed. Credential entries in a Remote Profile may be encrypted by a key known only to the User, the Service Provider may need to provide a digital authorization provided by the User in order to access the Credential, or the User may need to cooperate with the Credential Database Manager to authenticate the disclosure of the Credential to the Service Provider. The Service Provider may use the help of a Credential Status Provider to complete the verification of Authenticated and Validated Credentials. Examples of Service Providers are: medical practitioners who want to view and update information in electronic health records; companies that deliver pay-for-content services to mobile phones; and, organizations that want to restrict external access to their LAN in accordance with varying authorization levels.

4. **Credential Issuer**: An authority that issues Authenticated or Validated Credentials. The Credential Issuer can issue Credentials that are valid a limited number of times or for a limited time period. Credential information may be supplied to the Credential Issuer by one or more Registration Authorities; in the case of a Validated Credential, the Registration Authorities will verify the validity of the Credential information. Examples of Credential Issuers are: medical professionals who add digitally signed health and prescription information statements to the electronic health records of their patients; merchants issuing

digital receipts in e-commerce transactions (e.g., to enable their customers to electronically claim tax credits); issuers of electronic gift certificates and electronic cash; and, Web sites that issue anonymous attribute certificates instead of persistent cookies to provide personalized services.

5. **System Access Provider**: An authority similar to a Credential Issuer, but serving only the role of granting a User the right to register a Remote Profile and to transact on the basis of Local or Remote Profiles. It issues Registration Tokens to Users, either one per User until the token expires or a new one at regular time intervals or when requested by the User. Examples of System Access Providers are: a government issuing proofs of citizenship for on-line elections; an on-line gambling or news service selling electronic subscriptions that allow Web site visitors to view items on-line during a restricted period of time; a credit bureau issuing a statement showing that a person applying for a bank account has a good credit status; and, a state department issuing digital declarations that a person is over 18 years of age, or lives in a certain jurisdiction, to allow that person to participate in on-line gambling.

6. **Credential Status Provider**: A party that verifies the validity status of a Credential presented to it by a Service Provider. It's primary role is to verify the revocation status of Validated Credentials, to manage and issue updates of Credential Revocation Lists, and to keep track of the number of times a limited-show Credential has been shown. The Credential Status Provider may also perform application-dependent verification outside of the Service Provider's scope. Examples of Credential Status Providers are: a commercial organization providing on-line revocation for X.509 certificates using OCSP; and, a financial institution in an electronic cash system verifying deposited electronic coins against a double-spending list.

2.3 Protocols

Participants interact with each other by means of various protocols. CMP distinguishes between seven protocols:

1. **Registration Authorization**: A protocol between a System Access Provider and a User whereby the User obtains a Registration Token. In the case of a Remote Profile, the User needs the Registration Token to have the Central Database Manager initiate the profile. The Registration Token may be issued to a standard 8-bit smartcard of the User. CMP offers protection against fake-terminal attacks and smartcard data leakage by routing communications from and to the smartcard through a device trusted by the User. Furthermore, computationally expensive operations for the card can be off-loaded from the card to another User device; virtually no card storage space is required, so that sufficient room is left for a software solution to protect against card attacks such as differential power analysis.

2. **Profile Registration**: A protocol between a User and a Credential Database Manager whereby the User presents a Registration Token and opens a Remote Profile. The Registration Token can be presented in a manner that does not enable identification of the User. As part of the protocol, the User and the Credential Database Manager will specify the appropriate administrative data for the profile.

3. **Profile Access**: A protocol between a User and a Central Database Manager whereby

the User accesses a Remote Profile pertaining to him. This enables the User to inspect the information in the profile, and to modify any information that is outdated, erroneous, or false (assuming the settings in the administrative data permit the User to do so). The User must show an Credential to demonstrate proper access rights, but can choose to be identified or to remain pseudonymous (that is, persistently anonymous). The ability to pseudonymously hold a Remote Profile reduces the risk of identity fraud, and minimizes the damage that can be done by malicious insiders and outside attackers. In the case of a dispute a pseudonymous User will not be able to deny having accessed the profile; only pseudonymous Users who did not access the profile can prove they did not do so. CMP also provides a software-only method for the Central Database Manager and other parties to strongly discourage the User from lending or cloning his access rights, even for pseudonymous access. Furthermore, CMP facilitates the sharing and synchronization of Credentials between Local and Remote Profiles in accordance with application-specific administrative data, and supports roaming.

4. **Public Profile Access**: A protocol between a Service Provider and a Central Database Manager whereby the Service Provider accesses part or all of a User's profile in order to read, write, or modify Credential information. Access can be done in the various manners available for the Profile Access protocol, as well as in additional manners. Specifically, the Service Provider can be either identified, pseudonymous, or anonymous. The latter two cases prevent the Central Database Manager from gaining competitive intelligence on Service Providers or from improperly rejecting valid requests for access on the basis of the identity of the Service Provider. At the same time, the Service Provider can disclose exactly that which is required to enable the Central Database Manager to make an authorization decision: CMP provides for role-based access. Digitally signed audit trails can be kept, which may be identified, anonymous, or role-based; in the case of a dispute only Service Providers who did not access the profile can prove they did not do so. CMP also allows multiple Service Providers to jointly demonstrate possession of sufficient access rights to perform a certain action on the information in the profile, without disclosing more than strictly required.

5. **Credential Issuance**: A protocol between a Credential Issuer and a User, whereby the Credential Issuer issues an Authenticated or Validated Credential for entry into the User's Local or Remote Profile. This protocol provides all the functionality of the Registration Authorization protocol, as well as additional functionalities. Specifically, the User can obtain the Credential on the basis of showing a Registration Token obtained from a System Access Provider, or upon disclosing Credential information obtained from other Credential Issuers. In either case, CMP allows the User to be fully anonymous, and the providers of the other Credentials or the Registration Token can strongly discourage the User from cloning or lending his right to obtain a new Credential. Furthermore, the User can present the Credential Issuer with a previously issued Authenticated or Validated Credential to have it re-authenticated or updated, without enabling the Credential Issuer to learn more than it strictly needs to. Also, the Credential Issuer can be prevented from learning the Credential information it is authenticating; this facilitates data separation when the information resides in the databases of Registration Authorities. In the case of a limited-show Credential, a built-in identifier, value token, or self-signed fraud confession will be ex-

posed if the Credential is used more times than allowed.

6. **Credential Disclosure**: A protocol between a User and a Service Provider whereby the User discloses Credential information that is stored either in a Local Profile or in a Remote Profile. The protocol can be conducted either with or without the assistance of the Credential Database Manager; CMP defines multiple protocol variants with incremental levels of Credential Database Manager involvement. CMP also allows the User to provide the Service Provider with a digitally signed permission specifying the latter's access rights. In all cases, Credential information can be disclosed without enabling identification of the User. More generally, only the minimum Credential information (such as a particular property of multiple Credentials) needed to meet the authorization requirements of the Service Provider are disclosed; in case the Credential is stored in a Remote Profile, this requires the User to have some trust in the Credential Database Manager. Furthermore, the Credential information can be presented to the Service Provider in such a manner that the Service Provider is left with self-authenticating evidence that digitally proves only a part of the Credential information disclosed by the User; this enables the Service Provider to pass on the evidence to third parties (such as the Credential Status Provider), while being able to protect its own privacy, comply with privacy legislation, and avoid leakage of competive data. In the case of on-line validation of an Authenticated or Validated Credential, the Credential Status Provider cannot falsely deny access to targeted Users on the basis of uniquely identifying information.

7. **Credential Status Verification**: A protocol between a Service Provider and a Credential Status Provider whereby the Service Provider requests and obtains information on the validity status of a Credential beyond what it can infer from the Credential itself. Credential revocation may be done either on-line (during the Credential Disclosure protocol) or off-line. The Credential Status Provider can identify Users who show a limited-show Credential more times than allowed, even if it has no prior relation with the Credential Issuer and honest Users are anonymous. CMP also provides for short-lived Authenticated and Validated Credentials, in which case the Credential Status Verification protocol may not be needed. The Service Provider can submit to the Credential Status Provider non-repudiable digital evidence related to Credential information that Users disclosed to it, while hiding any competitive or privacy-sensitive information. CMP enables the Service Provider to prevent the Credential Status Provider from learning with whom it is communicating, and the Service Provider can choose to be anonymous or pseudonymous.

In most real-life application, it is strongly recommended to use Digital Credentials as the basis for at least a subset of the seven core protocols. The choice of the particular subset depends on the needs of each of the Participants regarding security, privacy, and usability.

3 Conclusion

CMP relies on the most powerful authentication and access control techniques to have come out of cryptographic research. In this paper we described the basic architecture of CMP, and its general benefits over Digital Identity Management solutions based on unsophisticated techniques. In the full paper, we will describe various real-world applications to illustrate the full power of CMP, and describe the CMP architecture in greater detail.