

Privacy Principles for Authentication Systems

Paula J. Bruening

Alan Davidson

Ari Schwartz

The Center for Democracy and Technology¹

Introduction

New technologies for authentication hold promise to allow individuals, businesses and government to better realize the Internet's potential for commerce and delivery of community and government services. By making online transactions more seamless, linking information on multiple devices, and enabling the development of innovative online services, authentication systems may make it possible for business and government to deliver integrated products and services across domains and across delivery platforms. To perform their function, however, authentication systems often must collect and share personally identifiable information, raising potential risks to privacy.

Indeed, while interest in development and deployment of authentication systems has increased dramatically over the last two years, widespread public adoption of authentication technologies has not yet materialized and will require that individuals trust that the systems incorporate strong privacy protections.

Further compounding these concerns is the potential for authentication systems to function as a *de facto* centralized identification system. Broad deployment of government authentication systems to enhance citizen access to government services, resources and information holds the potential to create a "one-size-fits-all" identifier that may compromise

¹ Paula J. Bruening is Staff Counsel and Alan Davidson and Ari Schwartz are Associate Directors of the Center for Democracy and Technology (CDT) in Washington DC. CDT is an independent, non-profit public interest organization advocating for free expression, user empowerment and privacy on the Internet.

citizens' ability to control the dissemination and use of information about them.

To mitigate the risks authentication systems raise, it is essential that they be designed to offer individuals control over their personal information by supporting traditional principles of fair information practices. While these principles have long formed the basis of federal and state law, industry rules of best practice, and international agreements related to information privacy protection, their application to authentication systems must be carefully considered and articulated so as to take into account the complex and unique questions raised by the technology. In fact, because fair information practices are often ignored in the current use of authentication, the move to new authentication systems offers implementers the ability to offer stronger privacy protections if privacy issues are addressed in the design of the technology.

This paper considers the challenges to privacy raised by authentication systems. It examines the ways in which those risks may be mitigated through deployment of diverse authentication products, by decentralizing their design and limiting the amount of personal information collected. It discusses the importance of applying fair information practices to the management of authentication data. Finally, it proposes guiding principles, developed by the Center for Democracy and Technology in cooperation with industry, government and public interest organizations, for development and deployment of authentication systems.

Definitions

Authentication

Authentication is the process of establishing confidence in the truth of some claim. It is the process of establishing whether or not a real world subject is who or what its identifier says it is. Authentication can be accomplished in three different ways, usually described as “something you know” “something you have,” and “something you are.”

“Something you know” may be a piece of information such as a mother’s birth name, a password, or a personal identification number. “Something you have” may be a physical token or a magnetic stripe or chip card. “Something you are” refers to the use of biometrics to authenticate individual – the automatic identification or identity verification of human individuals on the basis of physiological characteristics such as height, eye color, a retinal scan or fingerprint.

Individuals authenticate themselves often during the course of a day. My library card authenticates that I am resident of a community and authorized to check books out of the library. My health club card authenticates that I have paid my monthly membership and am entitled to use the facility. The EZPass device on my car authenticates that I participate in the system and have authorized billing of my bank account for toll-booth fare.

Credentials and Identifiers

A credential is a token given to prove that an individual or specific device has gone through an authentication process. Credentials that can be used to directly identify an individual or specific device are identifiers. Today, identifiers and credentials are often used interchangeably. Yet, in many cases, authentication should be related to an individual’s identity, in others, authentication requires no personal identification. The report of the National Research Council refers to the amusement park sign that indicates, “You must be at least this tall to ride this ride,” with the appropriate marker on the sign.² All that needs be demonstrated is that the person is as tall as the marker indicates – their personal identity is not necessary to prove their qualification to ride the ride. In another example, my frequent buyer card at a coffee shop indicates that I have bought ten cups of coffee and that I am entitled to a free one. These examples demonstrate the reasons that it is important to better distinguish between authentication and identification since in both identity is not used because it is neither necessary nor even desirable.

² “Who Goes There? Authentication Through the Lens of Privacy,” National Research Council, National Academy Sciences, 2003, prepublication draft, p. 1-3.

Authorization

Authentication and authorization are two other terms are often used interchangeably, but these terms are distinctly different further confusing the role of authentication. *Authorization is the process of deciding what an individual or device ought to be allowed to do.* It is accomplished asking an appropriate authority for an authorization decision every time an individual submits a request to the system to access resources or to act in a certain way. If the authority grants the request, the individual is allowed access; if the request is denied, the individual is not allowed access. Authentication is usually established to further some other goal, most commonly to authorize requests to perform some action. Often the credentials used for the authentication and authorization processes are the same token, but they do not need to be. Looking back to the amusement park example, the height and funds to pay for the ride are authenticated for each individual to get on a ride, but it is the ticket that is offered at the time of payment that provides the authorization. Because authentication and authorization are so closely intertwined in today's daily operations, it can be difficult to distinguish the two when looking at a particular process, however, an understanding of the differences is essential to proscribing the most effective policies for authentication projects.³

Authentication Today

The advent of new communications technologies has understandably made authentication more complex. As different devices proliferate, a wider range of authentication is needed. Also, more authentication processes are automated removing an element of human discretion.

Authentication in Cyberspace

As commercial activity and access to government services increasingly migrate online, consumers engaged in electronic transactions are frequently required to provide some form of authentication. Authentication in cyberspace most often takes the form of a password (“something you know”) combined with a user identification.

³ Id. at 2-2 – 2-3.

Consumers enter their user ID and are prompted for their password. When the correct combination of user ID and password are entered, the user gains access.

The user ID/password combination currently in common use often raise challenges, among them:

- Users tend to forget passwords, leading to an increased number of helpdesk calls or emails concerning forgotten passwords.
- The Internet is increasingly accessible through a variety of devices – from a personal computer, wireless phone or PDA. In such cases, Internet access methods may vary based on technology. Users may also access the Internet from different personal computers, at public libraries or at Internet cafes. Users are, as a result, required to remember multiple log-in names and passwords.
- Finally, some users view providing user ID/password combinations as an interruption of their online experience and would prefer a seamless experience.⁴

Many businesses have begun to believe that providing authentication that will deliver the benefit of simplified sign-on to users, as well as logins that persist across domains and enterprises addressing many concerns. In addition authentication would make it possible to implement applications that could share transactional information while running on different platforms and technologies. Businesses could then integrate multiple transactions to create an innovative, multifaceted service.

Benefits to users have become particularly clear in the back office setting of a business where human resources departments can more easily coordinate employee data, such as employees benefit information, with easy internal access for both the department and employee. Similarly, many government agencies are exploring benefits of better coordinating authentication between related projects where

⁴ Working Document on on-line authentication services, Article 29 Data Protection Working party, 10054/03/EN WP 68, p 2.

bureaucracies have created walls in the past. For example, CDT is working with the US Park Service and US Forest Service on a plan to integrate federal campsite registration services. Today, these services are done by different contractors with different collections of information and no way for an individual to track them seamlessly. In the future, integrated authentication could make sure that the right government agencies and contractors have access to the information they need while providing better service to citizens.

In the business to consumer context, user benefits are not yet as clear. A frequent example suggests that authentication would make it possible to coordinate transactions among several web sites so that a consumer buying airline tickets could also book a hotel, rent a car and buy theater tickets from one location. However, many online travel services already provide this convenience. It is still uncertain, if the simplicity of a single sign-on in new contexts will provide enough incentive to build a user base.

Kinds of authentication

As suggested earlier, authentication, authorization and identification are often used interchangeably. To add another level of complexity there are also at least two kinds of authentication:

Identity Authentication. In some cases authentication establishes a level of confidence that an identifier refers to an identity. In some cases, that authenticated identity is not linked to an individual. For example, a user of a website journal may adopt the user identity “robin.” The correlating password “goodfellow” may link only to that user ID and not to any specific individual. This kind of “pseudonymous” authentication requires two steps: (1) selection of an identifier that will be authenticated and (2) authentication, when the required level of confidence is established.

In some cases, identity authentication is linked to a specific individual. The individual claims the selected identifier, and the authentication involves challenging the individual to produce sufficient credentials supporting the claim that the identifier is linked to the individual. Many identifiers are today often used as authorization credential because it is easy to simply take a number tied to an individual instead of creating a new means of authorization.

Attribute Authentication. Authentication sometimes establishes a level of confidence that an individual or device possesses an attribute that meets some criteria. In these cases, the attribute to be authenticated is selected, and during authentication, the required level of confidence is established. Going back to our amusement park example, the individual's height is an attribute, which determines that they are tall enough to ride. Usually, there is no need to store transactional records of attribute transactions, because any individual or device that raises concern can simply be checked again.

The Relationship Between Authentication and Identification

Different levels of authentication are necessary to assure the levels of security required by different transactions.

In some cases, it is necessary to identify an individual's name in order to meet a required security goal. For example, if one wishes to access their credit report, it is important to know that the person is who he says he is and that he, therefore, has a right to see that report. If, however, one wants to purchase a copy of a magazine at a newsstand, knowing their identity is unnecessary. So long as the person produces the right amount of money to pay for the paper, there is really no need to identify the purchaser. In some instances, it is necessary to know that a person is of the appropriate age to purchase certain goods or services, but it is not necessary to know who that person is.

The relationship between authentication and identity – i.e., the extent to which authentication automatically involves the identity of the person involved in the transaction is an issue key to building privacy protection into authentication systems. An essential requirement for preserving privacy in authentication systems is allowing an individual to choose an authentication tool that meets the needs of the transaction in which they are engaged. CDT agrees with the common sense, but often unheeded, recommendation of the National Research Council that “[t]he strength of the authentication system employed in any system should be commensurate with the value of the resources being protected.”

While convenience may prompt authentication systems to identify individuals' personal names even when it is not necessary to do so, ideally individuals need only provide identity authentication when necessary. To the extent that an individual may wish to use a system that provides identity even when not necessary to complete the transaction, one may do so. However, to the extent that privacy involves the ability of users to "control the extent to which information about them is used and shared," users must be given the option to use a system that does not involve identification when it is not warranted.

Privacy Risks Raised by Authentication

Ideally, and when properly deployed, authentication systems can enhance privacy. Currently, authentication is too often tied to individual identity. Individual names and identifying numbers, such as the Social Security Number, tie individuals to critical information about them, including credit, medical and tax information. Automating the current authentication systems will simply embed this practice in technology, and continue to create opportunities for fraud and identity theft.

Development of authentication technologies presents an important opportunity to build systems that enhance privacy protections for data and the individual's control over uses of data. New technologies can be developed in such a way as to separate identity from authenticating information, so that identity authentication is only used when needed. They can also be designed to support principles of fair information practices. However, without building in proper protections, authentication systems can result in the requirement that identity be authenticated for all interactions and transactions, raising new privacy concerns. Such concerns include:

Aggregation of extensive, dossiers of information – Information for authentication purposes will be collected and compiled from a wide and varied range of sources. In addition to personal information about who a person is, authentication processes include data about the transactions in which individuals have engaged, places they have traveled, where they have shopped and publications they have read. Whether this information is collected and stored centrally or maintained by a federation of record

keepers across the public and private sectors, this intensive aggregation of information can yield a rich picture of an individual, his preferences, purchases, habits and activities. Such dossiers and their uses can create significant privacy risks.

Excessive use of identification authentication – As discussed above, in some cases, identification of the individual is a critical part of authentication. The person accessing a credit report or tax return, for example, must authenticate that they are who they say they are, as their identity is fundamental to their authority to access the information. However, the growing need for authentication for a range of purposes and of different levels of certitude raises concerns that individuals will be forced to use a “one-size-fits-all” authenticator, and that identity will be demanded in situations where it is not necessary.

For example, when purchasing a book, it is not necessary that the merchant know that you are who you claim to be. The merchant only need have sufficient information to assure that you can make payment and that he can effectuate delivery. As the need for authentication services and their deployment increase, concerns arise that individuals will be denied the choice to use a method of authentication that does not involve identity, even when it is not necessary.

Sharing of information for marketing and other unwanted purposes – The databases created and used by authentication systems will store great quantities of data, and be able to retrieve it quickly and easily. Databases will select, match and link data about individuals. Thus, in addition to facilitating authentication, databases can be mined to market to consumers with precision and specificity. Privacy is compromised when this information is used such secondary purposes without the knowledge and consent of the individual.

Misuse of Credentialing and Identity Information – Personal information is stored and retained during the process of creating reliable authenticators. When proper controls and security procedures are not placed on the resulting databases of the information identity theft and fraud can be common. For example, state Departments of Motor

Vehicles have become targets of bribery and theft because of the value of the personal information maintained at the agency.⁵

Proliferation of use of authentication credentials – Use of authenticators for multiple purposes erodes their ability to secure systems and transactions. To serve as a strong authenticator, a credential must act as a shared secret (“something you know,” “something you have” or “something you are”) between the individual seeking authentication and the authentication system. Widespread use of the credential throughout society necessarily means that it is no longer a secret and is available to too many people who may misuse it. The credential is weakened as an authenticator and, when placed in the wrong hands, becomes a tool to commit identity theft and fraud.

The widespread use of the Social Security Number (SSN) provides a good example. When the SSN was originally created, it was intended only for use to authenticate the identity of individuals for to participate in the Social Security system. Over time, the number was adopted for a myriad of uses including identification for credit reporting, tax payment, medical insurance and the driver’s license, to name only a few. As a result of these multiple uses, the number is available to countless people, and so severely compromised as an identifier that it is an increasingly weak form of authentication and has become instead a key cause of identity theft.⁶

The General Accounting Office discussed the problems raised by widespread use of the SSN in a recent report:

The uniqueness and broad applicability of the SSN have made it the identifier of choice for government agencies and private businesses, both for compliance with federal requirements and for the agencies' and businesses' own purposes. In addition, the boom in computer technology over the past decades has prompted private businesses and government agencies to rely on SSNs as a way to accumulate and

⁵ CDT has been monitoring security at motor vehicle agencies. See <http://www.cdt.org/privacy/030131motorvehicle.shtml> for an updated list.

⁶ States have responded to this over-use of the SSN and the identity theft problems such over-use causes by passing legislation limiting its use in commercial settings and as a driver’s license ID.

identify information for their databases. As such, SSNs are often the identifier of choice among individuals seeking to create false identities.⁷

Consumers have consistently pointed to privacy concerns as a key deterrent to their Internet use.⁸ To derive the maximum benefit from new online services and to encourage robust use by consumers, it is essential that authentication systems recognize these concerns and address them at the outset.

Addressing Privacy Concerns

Late in the 19th century, Justice Louis Brandeis articulated the American right to privacy as “the right to be let alone.”⁹ Entering the 21st century, networked computing and powerful databases make it difficult, if not impossible, to be “let alone” in an absolute sense. In the environment of the electronic marketplace, a more contemporary concept of privacy is often characterized as the ability of people to control the disclosure and subsequent uses of their information.¹⁰

Assuring user privacy in authentication systems entails building into the systems themselves the capability of users to control the flow of their information. This can be accomplished in at least two key ways: building systems that foster compliance with principles of fair information practices, and assuring consumers have a diverse range of authentication services from which to choose.

⁷ "Social Security Numbers: Ensuring the Integrity of the SSN"
<http://www.gao.gov/new.items/d03941t.pdf> GAO-03-941T July 10, 2003

⁸ Pew Internet and American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* 4(Aug.20, 2000). Available online at http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf, National Consumers League, E-Consumer Confidence Study (2000), Forrester Research, Personalization v. Privacy 6 (2000).

⁹ Warren & Brandeis, *The Right to Privacy*, 4 Harvard Law Review, 193 (1890).

¹⁰ Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated personal Data Systems* (July 1973). Available online at <http://www.aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

Providing for a Diversity of Services

Assuring that consumers have the ability to choose among authentication services is key to providing for user control and trust. As discussed previously, different transactions require different levels and kinds of authentication, and users should have the ability to avail themselves of services that provide only the level of authentication necessary to the transaction. A marketplace that provides a diverse range of authentication services mitigates the risk that consumers will be required to adopt a “one-size-fit-all” authentication tool that provides more information about the individual than necessary.

Current methods of online authentication that involve *use of a user ID and correlating password* provide one example of the use of diverse services in the marketplace. The current system requires that for each transaction, the consumer establish authenticating credentials. In doing so, the individual shares only the information necessary for the transaction in question.

Authentication systems that employ *smart cards* are examples of systems that rely on “something you have” as the authenticating credential. The smart card could be set up to be the sole storehouse of necessary authenticating information. When designed in this way — with no information stored in a database — control over the information remains, literally, in the hands of the individual. Passwords that allow access by certain entities to some but not all data on the card enables card holders to limit sharing of data to that necessary to the transaction.

Federated authentication systems may be able to provide simplified sign on to users but without storing users’ personal information centrally. It makes it possible for an authenticated identity to be recognized and take part in personalized services across multiple domains.

Federated systems can allow users to link identity information between accounts without centrally storing personal information. The user also controls when and how their accounts and attributes are linked and shared between domains and service providers, giving them greater control over their personal data.

Many of the federated authentication systems envision utilizing a *circle of trust* – a group of service providers that share linked identities and have established business agreements in place that determine how to do business and interact with respect to identities. The members of the circle of trust share credentials based on the defined business agreements. Users are notified of the information being collected and grant consent for the kinds of information shared with others. Ideally, within the circle of trust only information necessary to the specific transaction authenticated is shared. Once a user has been authenticated by a circle of trust that individual can be easily recognized and take part in targeted services from other service providers within that circle of trust. Then, a user can have several main trust providers to help build a Web of relationships and a diverse marketplace of services.

Principles of Fair Information Practices

Principles of fair information practices provide guidelines for managing information in record-keeping systems in a manner respectful of privacy. These principles form the basis of the Privacy Act of 1974,¹¹ legislation that gives individuals the right to access much of the personal information about them kept by federal agencies, and similar laws enacted at the state level. They also serve as the foundation of laws enacted at the federal level to address privacy in various industry sectors, such as the Cable Communications Act of 1984,¹² the Children’s Online Privacy Protection Act,¹³ and the Driver’s Privacy Protection Act.¹⁴ Principles of fair information practices are incorporated into industry codes of best practices and form the underpinnings of international agreements on data protection.¹⁵

¹¹ Pub. L. No. 93-579, 5U.S.C. Sec. 552.

¹² The Cable Communications Policy Act of 1984 establishes a comprehensive framework for cable regulation and sets forth strong protections for subscriber privacy by restricting the collection, maintenance and dissemination of subscriber data. Pub. L. No. 102-385, 47 U.S.C. Sec. 551.

¹³ The Children’s Online Privacy Protection Act was intended to protect children’s personal information from collection and misuse by commercial websites. Pub. L. No. 105-277, 15 U.S.C. Secs. 6501-6505.

¹⁴ The Driver’s Privacy Protection act restricts public disclosure of personal information contained in state departments of motor vehicles. Pub. L. No. 103-322, 18 U.S.C. Sec. 2721.

¹⁵ The most widely accepted version of fair information practices are the Organization for Economic Cooperation and Development *Guidelines governing the protection of privacy*

Explaining how privacy principles work for authentication would be the next logical step to help developers and implementers understand how to build systems that protect privacy.

CDT Authentication Principles

CDT has worked on digital authentication and digital signature policy

and transborder flows of personal data. OECD Doc. No. C(80)58 final. They read as follows:

1. *Collection Limitation Principle* - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. *Data Quality Principle* - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. *Purpose Specification Principle* - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. *Use Limitation Principle* - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: a) with the consent of the data subject; or b) by the authority of law.
5. *Security Safeguards Principle* - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. *Openness Principle* - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. *Individual Participation Principle* - An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time, and at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. *Accountability Principle* - A data controller should be accountable for complying with measures that give effect to the principles stated above.

The full text of the OECD Guidelines is available at http://europa.eu.int/comm./internal_market/privacy/instruments/ocdeguideline_en.htm and <http://www.privacy.gov.au/publications/oecdgl.doc>.

and systems for several years. In 1998, for example, CDT participated in discussions with the US General Services Administration on its Access Certificates for Electronic Services (ACES) project. This dialog led to an ongoing exchange of letters resulting in a set of three principles for how GSA could assure privacy in ACES. They were: 1) Promotion of Security and Privacy through a Decentralized Infrastructure 2) Multiple Certificates for Multiple Purposes and 3) Fair Information Practices.¹⁶ The ACES project largely incorporated these principles.

Major Commercial Authentication Projects

While CDT continued to develop these principles internally, commercial interest in authentication systems also continued to grow. By 2002, Microsoft Passport had developed a widespread user base and was under government scrutiny. Meanwhile a new group of companies, the Liberty Alliance, had formed to create a new set of protocols for online authentication.

Microsoft Passport. Passport is an authentication service providing single sign-in across multiple participating websites in order to help users to save time and avoid repetitive data entries when surfing on the Internet. It is not currently an authorization or identification service, but an authentication service, aimed at securely authenticating a user by verifying the credential presented.

As part of Passport, Microsoft compiles a user's ID, password and other personally identifying information, and this "wallet" follows a customer to enable the customer to participate in a number of online transactions. Among other services, Microsoft has utilized Passport for Hotmail and MSN Messenger email services, Microsoft's .Net Web service, Microsoft Reader e-book purchases and Microsoft Developer Network access.

In the summer of 2001, a number of privacy and consumer groups filed a complaint at the Federal Trade Commission (FTC) challenging Microsoft's marketing and use of the Passport technology. The

¹⁶ The final letter was written to GSA Office of Governmentwide Policy Director G. Martin Wagner from CDT Deputy Director Daniel Weitzner.
<http://www.cdt.org/digsig/gsaletterrep.html>

complaint led to a consent agreement between the Commission and Microsoft, under which Microsoft agreed to build a privacy and security program for Passport to be monitored by the FTC.

The complaint charged that Microsoft failed to comply with its own privacy statements about Passport. Microsoft settled with the FTC, resulting in a consent order that places requirements on Microsoft. In particular, Microsoft is required to :

- establish and maintain a comprehensive information security to protect the security of personally identifiable information.
- obtain reports from independent professionals with respect to the effectiveness of its security program; and
- maintain and make available to the FTC on request its representations to customers regarding its collection, use and security of personally identifiable information.

Microsoft is also expressly prohibited from misrepresenting personal information collected from customers, the extent to which its services will protect the privacy and security of personally identifiable information, the steps to be taken to protect personal information and the extent to which a service allows parents to control information about their children.

The European Union (EU) Working Group on Data Protection also came to an agreement with Microsoft to make changes to Passport to help protect the privacy of users and to assure that the system comports with EU data protection laws. The main changes are intended to give European users more control over how their personal data is shared with partner sites. The agreement included providing users get increased options about the information they want to be shared with partnering sites, additional guidance to help users create secure passwords, and a link to the European Commission's web site on data protection. The agreement also involved the delivery of a white paper by the EU's Article 29 Data Protection Working Party on On-line Authentication Services.¹⁷

¹⁷ Working Document on on-line authentication services, Adopted on 29 January 2003, 10054/03/EN WP 68.

Liberty Alliance Project. A group of companies called the Liberty Alliance has designed its own standard for digital authentication and information exchange. The Liberty Alliance Project is comprised of more than 100 companies, non-profit organizations and governments world-wide. The Liberty Alliance Project is an ad hoc project in which different companies participate pursuant to the terms of an agreement.

The mission of the Liberty Alliance Project is to establish open standards for federated network identity through open technical specifications. Simplified sign-on and federated network identity - binding multiple accounts for a given user - are key elements of the system. The consumer authenticates once in a session and then navigates within a circle of trust without having to re-authenticate. The circles of trust form a federation of companies that have business relationships based on the Liberty Alliance architecture and operational agreement.

Liberty Alliance released the 2.0 version of its specification in April 2003 that includes rules for the sharing of credential information. While the specification itself makes little reference to privacy or security, the Liberty Alliance released a detailed set of privacy and security guidelines.

Recognizing the privacy concerns raised by these systems, and the proven wisdom that privacy protections are best built into the initial design of new technologies and software, CDT engaged the participation of interested companies, experts and advocates to create guidelines to enhance privacy in authentication systems.

The CDT Authentication Working Group Process

To develop authentication privacy principles, CDT has engaged in a process beginning in September 2002 that involves industry, advocates and academics with expertise in the area of authentication. The process initially included a small group of committed companies, experts and public interest groups.

As the process continued, however, CDT broadened its outreach to establish a critical mass of interest and input into the project and to enlist backing for the final product. Participants included software and hardware developers, telecommunications and wireless communications providers, content providers, e-commerce companies, financial institutions, trade groups, research services and companies involved in Internet security. Consumer and privacy advocates represented the consumer and public interest. CDT convened approximately six meetings to develop its Interim Report.¹⁸

The Center for Democracy and Technology's Authentication Principles

The Authentication Privacy Principles are intended to serve as guidance for companies now developing authentication systems. The goal is to encourage developers to build privacy and security protections into authentication technologies to use in consumer-initiated transactions and in online interaction with government.¹⁹ It is also expected that the principles will serve as a marketplace guide for companies and individuals deciding which authentication systems to implement or adopt.

To build trust in consumer initiated transactions and government services and consistent with applicable law, authentication systems should:

1) Provide User Control - *The informed consent of the individual should be obtained before information is used for enrollment, authentication and any subsequent uses.*

Consent controls are vital to building trust in authentication systems. Authentication systems should offer individuals meaningful control over

¹⁸ While the document has been presented at the Federal Trade Commission and has been discussed with federal and state agencies, the principles remain in draft form. Comments on the principles are being accepted as of this writing.

¹⁹ CDT is also developing principles for data mining and pattern analysis that are used for fraud and security checks. This kind of authentication is complicated by the fact that the individual is not involved and perhaps unaware that the authentication is taking place. CDT expects progress on this project in 2004. Please contact us for more information.

disclosure of their information. Under this principle, individuals may choose to use a single form of authentication that always discloses the same information or credential for all interactions, or choose to employ a variety of authentication tools for different transactions. This principle is particularly important in systems designed to share attributes and/or also serve as authorization systems, which will likely be successful only if they balance added convenience with trust in the system. Individuals should not be forced to accept the sharing of information for secondary uses as a condition of utilizing the authentication or data transfer system.

2) Support a Diversity of Services - *Individuals should have a choice of authentication tools and providers in the marketplace. While convenient authentication mechanisms should be available, privacy is put at risk if individuals are forced to use one single identifier for various purposes.*

Concerns persist that one or a very few implementations will be used for multiple purposes, coercing individuals and diminishing the ability of authentication systems to enhance privacy. This need not be the case. Authentication systems should be designed to support development of a marketplace offering multiple services that deliver varying degrees and kinds of authentication. A marketplace with a diversity of services also helps to support the principle of user control. Rather than attempt to serve as the perfect single key, authentication services for individuals should function like keys on a key ring, allowing individuals to choose the appropriate key to satisfy a specific authentication need. Different government agencies, companies and organizations will likely need different types of authentication.

3) Use Individual Authentication Only When Appropriate - *Authentication systems should be designed to authenticate individuals by use of identity only when such information is needed to complete the transaction. Individual identity need not and should not be a part of all forms of authentication.*

Not all transactions need be tied to identity. In fact, different kinds of authentication happen all of the time. For example, a store may need only to verify that an individual can pay for a service without collecting personal information, as we do today with cash transactions. Or, in another example, a membership organization may need to verify that an

individual is authorized to partake in an activity without gaining access to detailed personal information. Different types of transactions require different levels of confirmation.

Authentication systems that use identity create greater privacy concerns as they can become ripe for abuse and targets for identity fraud and theft. Identity based authentication should only be used when necessary. To enable user control, support a diversity of services and protect privacy, it will be important to use both identity authentication systems relying on pseudonymous identifiers and attribute authentication relying on anonymous attributes whenever possible.

Credentials created in individual authentication systems are particularly sensitive information. Secondary use and sharing of these credentials for purposes such as authorization or marketing often compromise privacy and security. In particular, entities should be aware that Identification numbers become open to greater privacy misuses if they are often used for secondary purposes. Therefore, multiple uses of these numbers should be discouraged.

4) Provide Notice -*Individuals should be provided with a clear statement about the collection and use of information upon which to make informed decisions.*

Notice should be given in a manner consistent with the technology and be provided before information is used for enrollment, authentication and any subsequent use. Notice should not occur several links removed from the enrollment and authentication processes. The notice should in no way be a burden to read or understand.

5) Minimize Collection and Storage- *Institutions deploying or using authentication systems should collect only the information necessary to complete the intended authentication function.*

Authentication systems can collect and share information in several ways. They may collect sensitive information for enrollment, vetting and verification of an individual; they may use a subset of a user profile as the primary purpose of any intended authentication; and they may facilitate the onward transfer of information for secondary purposes. It may be necessary to store some information to provide ongoing services.

Information on retention practices should be available. In every instance, the information collected and stored should be limited to the minimum necessary to provide the intended authentication and service.

6) Provide Accountability - *Authentication providers should be able to verify that they are complying with applicable privacy practices.*

Privacy practices must be the cornerstone to building a trust relationship in authentication.²⁰ Training and regular audits are necessary to ensure that reasonable technical, administrative and physical privacy and security safeguards are in place. New privacy technologies can aid in tracking data flows for these purposes. Individuals, with appropriate authentication, should be able to access their own information used in the ordinary course of business and correct inaccurate information. The Working Group had only a short time to gain endorsement from major companies and organizations. Despite the quick turn around Center for Democracy and Technology, Consumer Action, Corporate Privacy Group, eBay, Hewlett-Packard, Intel, Liberty Alliance, Microsoft, NeuStar, TRUSTe and VeriSign signed on to encourage the consideration of these Authentication Privacy Principles in the development, procurement and use of authentication technologies

Future Work

CDT has sought and received feedback from businesses involved in authentication and government regulators. At a Federal Trade Commission workshop held May 14, 2003, the National Academy of Sciences commented that the recommendations comported well with those set out in their report, “Who Goes There? Authentication Through the Lens of Privacy.”²¹

Going forward, CDT continues to engage stakeholders. CDT is currently looking more deeply at authentication systems used to access

²⁰ All organizations collecting, maintaining or using personally identifiable information should develop internal practices that address applicable regulatory and self-regulatory guidelines, such as, the OECD Fair Information Practices Principles, the EU Directive on Data Protection, the Online Privacy Alliance guidelines, the US Financial Services Modernization Act, the US Health Information Portability and Accountability Act, as appropriate.

²¹ Op. Cit. at fn. 2., National Academy of Sciences,

government services²² and in consumer-initiated transactions. In the coming months, the Working Group will develop its final report, expected to be a more detailed document that will include case studies that illustrate how the Privacy Principles would work in everyday transactions. The process for the development of the case studies will mirror the inclusive, collaborative process used to develop the authentication principles themselves. CDT plans to publish a final draft of the principles and case studies and to consult with US officials and companies and European Union officials.

The Working Group is not considering the question of authorization and security applications that may utilize credentials created in the authentication process. In a separate effort, CDT is creating a working group to develop privacy guidance for the related but distinct questions that arise from the sharing and use of personal information for data mining or pattern analysis.

Tremendous challenges for implementers of authentication systems remain. For example:

Implementation Difficulties. Although CDT is working on case examples, unforeseen challenges in implementing the privacy principles are bound to arise for many new authentication systems. Education of developers and implementer will also be essential.

Bad Actors. Even with completion of and education on privacy principles, there is a risk that companies and agencies will simply not take privacy into account because of the expense or competing business plans. This will lead to misuse and eventual mistrust of all authentication systems.

Tendency Toward Overuse of Authentication. When successful authentication applications emerge in the marketplace, there will undoubtedly be a push to utilize these services for multiple applications

²² The members of the group developing case studies of the use of authentication to access government services include representatives of the Office of Management and Budget, the General Services Administration, the Federal Trade Commission, the National Association of Secretaries of State and the American Association of Motor Vehicles Administration.

in order to save on resources. As mentioned earlier, if proper safeguards are not put in place, multiple uses can compromise both privacy and effectiveness of applications.

Lack of Oversight. Even with the authentication privacy principles in place at the beginning of the process, there must be continual review of the risks of overuse and misuse.

Governance Issues. For diversity to work, competing companies and organizations in different sectors will need to communicate and trust one another. CDT is working on a project led by the Center for Strategic and International Studies to address the many difficult concerns in authentication governance.

Clearly, there is still much work to be done in this complicated and increasingly important technology policy field.