



Research Brief

Dec. 2004

Who Are You? I Really Wanna Know: E-Authentication and its Privacy Implications¹

Section I: Privacy & E-Authentication—An Overview

Privacy and Authentication in an Electronic World:

Obtaining a hunting license. Renewing your driver's license. Applying for government benefits. These are all government transactions that are increasingly being provided via electronic means, such as via the Internet. While the placement of these transactions online can reduce staffing and other overhead costs, they present state governments with the challenge of ensuring that individuals are who they claim to be. Within the context of electronic transactions, states have an increased authentication challenge, because the person the state is trying to authenticate is located remotely, as opposed to appearing in-person to transact business with the government. When authenticating individuals via electronic means (which is referred to as E-Authentication), states must be careful to meet citizens' expectation that the state will protect individuals' personal information, keeping it safe from unauthorized disclosure or use and reducing the risk of identity theft.² In fact, the exchange of personal information that accompanies most authentication methods creates a possible tension with privacy concerns.³ While many states provide some protection for personal information via state open records laws that exempt personal information from wide or unwarranted public disclosure, properly implemented E-Authentication mechanisms can lead to enhanced privacy protections.

Key points for states to understand in order to maintain privacy during the E-Authentication process include:

- Properly assessing the risks to privacy that authentication may pose and choosing an authentication method that addresses that risk level
- Raising the awareness of those you authenticate as to potential privacy issues
- When possible, limiting the amount of personal information an individual must divulge for authentication purposes
- Understanding the benefits and privacy risks involved in using a common identifier (such as a Social Security Number) across multiple government applications or linking citizens' information across multiple state systems.

A Note on the Purpose and Organization of this Brief:

This Research Brief is intended to provide state CIOs with an overview of the privacy implications of E-Authentication. Note, though, that authentication is a complex topic, given its placement within the bigger picture of identity management, which involves not only authentication but also the creation of identities and credentials that are used in the

authentication process. Inevitably, when addressing issues of authentication, overlap will occur with other related topics, such as credentialing or security. Where there are instances of overlap within this brief, please note that Appendix B contains an overview of identity management and may be of help in providing clarification. Although this brief does not provide an in-depth treatment of E-Authentication, Appendix A presents additional resources for those who would like to learn about E-Authentication in more detail.

This Research Brief is organized as follows:

- **Section II** provides some perspective on the business drivers that are moving E-Authentication forward.
- **Section III** presents background on the government's unique role in E-Authentication.
- **Section IV** touches upon some key concepts surrounding E-Authentication that are vital to presenting an accurate picture of E-Authentication's privacy implications.
- **Section V** elaborates on the privacy implications of E-Authentication.
- **Section VI** provides information about E-Authentication and privacy at the federal and state government levels.
- **Appendix A** contains additional resources for learning more about authentication.
- **Appendix B** explains more about the identity management life cycle and authentication's role in that life cycle.
- **Appendix C** is a checklist from the National Research Council on ways to lessen the privacy impact when designing or selecting an E-Authentication system.

Why We Should Care about Privacy and E-Authentication: Tuesday, November 2, 2004—Election Day in the U.S. News outlets reported long lines at voting precincts and, the following day, news media outlets reported that an estimated 120 million people had cast votes.⁴ While many focused on the election results, an overlooked aspect of the election was the process by which poll workers made sure that each voter was who he or she claimed to be and only voted once. By presenting a photo ID, probably a driver's license, voters proved who they were to poll workers and signed a register to ensure that they only voted once. *Whether or not they consciously thought about it, voters anticipated that the poll workers would maintain the privacy of the personal information they divulged in order to prove their identities. Voters also cast their votes with privacy protections that included standing behind a curtain when voting.* While authentication is frequently mentioned within the context of online citizen services, citizen confidence in the legitimacy of election results and the protection of our democracy are ensured, at least in part, by proper authentication processes at the election polls. *A vital part of maintaining citizen confidence within this example is ensuring that the personal information that citizens divulge during the authentication process is kept private and not exposed to unauthorized individuals, such as identity thieves.*

Privacy also plays an overall role in maintaining citizens' implicit expectation of the integrity of the voting process. For example, the Help America Vote Act of 2002 (HAVA), a recent piece of legislation intended to modernize federal elections, contains

provisions that attempt to preserve the privacy of voting in federal elections.⁵ Another indicator of privacy's importance to voting integrity is the sometimes fervent outcry of those with concerns regarding e-voting and whether the privacy of votes can be maintained if cast electronically.⁶

Section II: The Business Drivers—Moving E-Authentication Forward

What Is E-Authentication?

E-Authentication allows the government (or a private sector entity) to verify with a certain level of confidence that the users are who they claim to be within the context of electronic, self-service transactions.

E-Authentication methods can be relatively simple in nature. An example of a less complicated method is the use of passwords. More complicated methods involve encryption and other technologies, including the use of digital certificates, digital signatures, hardware tokens, smart cards, USB fobs, and biometrics, such as fingerprints or retina recognition technologies.

The benefits of E-Authentication include:

- Increasing the speed of transactions
- Increasing partner participation and customer satisfaction
- Improving record-keeping efficiency and data analysis opportunities
- Increasing employee productivity and improving the quality of the final product
- Reducing fraud through up-front authentication checks
- Increasing the ability to authenticate an individual once for access to multiple transactions
- Moving more information to the public
- Supporting citizen trust in e-government
- Improving security and the confidentiality of sensitive information.

The costs of an E-Authentication system include its design, procurement, testing, deployment and long-term maintenance.⁷

Overview of the Business Drivers:

The business drivers that are moving E-Authentication forward include:

- A sense of urgency arising out of the 9/11 terrorist attacks to improve security against the threat of terrorism
- Increased instances of identity theft and fraud
- Budget deficits requiring improved operational efficiencies
- Increased emphasis on improved service and electronic delivery
- Marketplace expectations driven by citizens' experience in the private sector
- Fraud reduction in government entitlement programs.

The Security-Related Drivers:

With respect to security efforts arising out of the 9/11 terrorist attacks—"The 9/11 Commission Report" detailed how the terrorists collectively presented questionable identity documentation in the form of passports and visa applications and how the airport gate personnel authenticated those individuals based upon the identity documentation they presented in order to board the planes.⁸ Concerns with the integrity of identity documents were reiterated by provisions to secure identity documents, including birth certificates, driver's licenses and Social Security Cards, in the bills that were recently passed by both houses of Congress to implement the 9/11 Commission's recommendations.⁹ While these problems focus on the issuance of identity credentials, which involves the first phases of the broader identity management life cycle, facets of these business problems that states must address include questions revolving around policy, technology, and available funding.¹⁰

The Streamlining-Related Drivers:

Tight budgetary times and increasing calls for improved state government services have led to states' moving more citizen services online. While online services offer citizens 24x7 access to government services, they also facilitate the streamlining of those services by reducing staffing and other overhead costs incurred when providing citizens in-person services. Within the context of electronic transactions, E-Authentication provides a way for states to have sufficient confidence in those transactions. More specifically, it allows states to have confidence that they are issuing licenses to the right individuals; to properly manage citizen benefit applications and case files as well as employee benefits and pensions; and, to conduct business and contractual transactions with an increased level of ease.

Moreover, included in the need for improved service and electronic delivery is the need for better cooperation across jurisdictional boundaries. In order for one state to authenticate an individual based upon an identity document issued by another state, the authenticating state needs to be sure the issuing state's business processes are adequate to ensure the reliability and validity of the identity document. This is just one challenge associated with cross-boundary authentication efforts.

The Fraud-Reduction Drivers:

In order to protect taxpayer dollars from fraud and waste, state governments are looking to E-Authentication methods in order to reduce the amount of government benefits paid to individuals who are ineligible to receive them. E-Authentication can provide a way to increase the government's confidence that it is providing benefits to the right individuals. For example, Connecticut uses a combination of digitally-scanned fingerprints, photos, and signatures to identify and also deter instances of welfare fraud. Although the state acknowledges that estimating the savings from the use of this authentication method is difficult, it did save the state \$9 million in the first few years after implementation.¹¹

Section III: The Eye of the Storm--The Challenging Role of State Government

Multiple Roles in Authentication:¹²

State governments have a unique role in authentication, whether conducted manually or online—they frequently create identities (for example, through issuing birth certificates), change identities (changing a name on a driver's license), and end identities (ensuring that a deceased person's birth certificate and driver's license cannot be used by anyone else). In other instances, states play the role of a party relying upon an identification document or other means of authentication offered by an individual within the context of a transaction.

Complicating Factors:

The following factors that are unique to state governments can complicate states' E-Authentication initiatives:

- The typically mandatory nature of citizens' transactions with government (whereas individuals' interactions with the private sector are normally discretionary in nature)
- The heterogeneous citizen marketplace, which can make it difficult for states to serve various market sectors electronically
- The cradle-to-grave relationship governments tend to have with citizens that can be intermittent yet span a long period of years
- Higher citizen expectations of government's ability to protect the privacy and security of their personal information¹³
- Citizens' generalized distrust of government's ability to protect the privacy of their personal information¹⁴
- The lack of a strong identifier that can be used by multiple governmental organizations
- The expense and complicated nature of implementing strong E-Authentication systems.

While the task of E-Authentication may appear daunting for states, not all transactions require high levels of authentication. For example, if a user self-registers a user ID and password on a government webpage in order to customize that webpage, correctly identifying the individual is of little or no value. However, other transactions require higher levels of confidence because of the inherent risk or value of the transaction. An example would be if a beneficiary changes his or her address of record through a government website or if an agency employee uses a remote system that gives him or her access to potentially sensitive client information where the transaction occurs via the Internet.¹⁵

Section IV: Key Concepts to Understand Before Addressing the Privacy of Authentication Processes

Understand What You Are Trying To Authenticate: When considering an authentication method, states must understand which type of authentication they need. The three main types are:

- **Individual Authentication:** With an understood level of confidence, linking an identifier to a specific individual (using a driver's license to authenticate that an individual is the exact person he or she claims to be).
- **Identity Authentication:** With an understood level of confidence, linking an identifier to an identity (verifying that a password is linked to an email address). It may not be possible to link the identity to a specific person.
- **Attribute Authentication:** With an understood level of confidence, ensuring that an attribute applies to an individual (verifying that a person is an employee).¹⁶

Note that a stronger authentication method may be needed to authenticate an individual, as opposed to authenticating an attribute or an identity.

Know Whether You Are Authenticating and/or Authorizing:

States must distinguish the act of authentication (establishing a level of confidence in a claim made by an individual) and the act of authorization (establishing what an individual is permitted or restricted from doing).¹⁷ These concepts are often confused when policy is being debated.

Understand the Risks:

In assessing whether and what type of authentication methods may be needed, a state must examine the types of harm that are possible. Potential types of harm include:

- Citizen inconvenience or distress or damage to a citizen's standing or reputation
- Financial loss for a citizen or agency liability
- Harm to an agency's programs or public interests
- Unauthorized release of sensitive information (such as centrally-stored personal information that is used to authenticate individuals)
- Personal safety
- Civil or criminal violations.

This risk analysis also includes considering the likelihood of whether a risk will occur.¹⁸ While the quantification of both the impact and the probability of risk for such analyses is ideal, a qualitative analysis may also be very informative for decision makers. Through examining both the impact and probability of a risk, state officials can make informed decisions about risk mitigation. The risks involved will play a vital role in determining the strength of the authentication that is needed.

Understand the Range of Available Solutions:¹⁹

Authentication solutions and their enabling technologies can be categorized as authenticating upon the basis of (1) something you know, (2) something you have or (3) something you are.

- **Something You Know:** Passwords and PINs are within this category. While cheap and relatively easy to implement, they pose inherent risks, because they can

- be forgotten or compromised through social engineering (for example, an individual being coaxed to reveal his or her password) or spyware applications. The NRC Report recommends the education of password users and that system designers take “great care” to ensure the proper balance between usability and security.²⁰ Password management should be addressed within a state’s security architecture.
- Something You Have: Magnetic Stripe Cards, Secure Tokens, PKI (Public Key Infrastructure), Digital Certificates, RFID (Radio Frequency Identification) Chips, and Smart Cards are examples. More complex than the “something you know” technologies, these technologies generally contain information that can be used to authenticate a person. While these technologies vary in their resistance to alteration and forgery, they still can be compromised if lost or stolen or if the information they contain is accessed. “Something you know” authentication (a PIN) is often combined with “something you have” authentication (an ATM card) to provide multi-factor authentication.
 - Something You Are: These types of technologies authenticate a person based on behavioral or physiological characteristics. Examples are voice prints, fingerprints, facial recognition, iris scanning, keystroke dynamics, and even handwriting. False negatives and positives pose potential problems along with the fact that, once compromised, a biometric cannot readily be changed.²¹ Hand geometry or fingerprint authentication is often combined with “something you have” authentication, through a Smart Card, to authenticate users regarding physical access control.

Section V: Privacy Implications of E-Authentication

The Key to Achieving Authentication Success:

When a state is evaluating whether and what kind of authentication system is needed, it is imperative for states to remember that privacy can be enhanced with *the proper level of authentication*. However, privacy can be compromised if a state implements authentication when it is not needed to achieve an appropriate level of security.²² The discussion below highlights some of the general privacy implications of E-Authentication. States are encouraged to perform a detailed risk analysis that takes into account privacy risks when considering an E-Authentication implementation.²³ See Appendix C for a NRC Report checklist on lessening authentication privacy concerns.

Notice:

Ideally, citizens need to be aware that they are being authenticated and informed of any privacy implications that are associated with the authentication. Related to this is the difficulty or ease with which the citizen can proceed through the authentication system. The NRC Report cautions that citizens need a clear understanding of the security and privacy threats to an authentication system. Otherwise, they may behave in ways that undermine existing privacy protections.²⁴ An overly burdensome authentication system also may lower citizens’ participation in the system, which, in turn, could lower the system’s anticipated benefits.²⁵ Many citizens may not read or understand the implications of authentication schemes.

Information Collection Limitation:

To protect the privacy of personal information, many experts recommend that entities should not use individual authentication when attribute authentication will suffice. This recommendation minimizes the personal information collected from individuals. For example, individuals who want to go on a ride at the state fair may have to show that they satisfy the height requirement by standing against a measure of their height (attribute authentication), but do not need to present a photo ID as authentication to go on the ride (individual authentication).

Secondary Uses and Linkages:

The reliance on common identifiers, such as Social Security Numbers, across multiple state authentication systems and the linking of user information across systems can create privacy concerns, because, with each new use or linkage, there are more associated risks that could compromise the information's privacy.²⁶ The minimization of secondary uses and linkages of personal information collected via authentication is consistent with the Fair Information Practices. However, states must be careful to weigh those risks with the opportunities for operational efficiencies that are created through a shared identity management infrastructure that supports the common identity needs of government and private sector transactions. For example, an enterprise identity and access management service could provide self-registration, digital identity creation, password management and synchronization, and improved service delivery 24x7 for a wide-range of users who desire access to government information and/or systems. A thorough risk analysis can be of great assistance to states in balancing the privacy risks with the operational efficiencies that can be created by the aggregation and sharing of authentication information.

Identity Credentials--A Word About Foundational Documents:

Foundational documents, such as birth certificates and driver's licenses, are created during the early phases of the identity management life cycle and are used to authenticate individuals in the later stages of that life cycle.²⁷ However, foundational documents pose general concerns regarding their validity and reliability. This is particularly true when one state is relying upon another state's foundational document (such as a birth certificate) in order to issue another identity document (for example, a driver's license). The NRC Report recognizes this concern, because these types of documents, including passports and Social Security Cards, are issued "by a diverse set of entities that lack ongoing interest in the documents' validity and reliability." Hence, the NRC Report recommends that "birth certificates should not be relied upon as the sole base identity document. Supplemented with supporting evidence, birth certificates can be used when proof of citizenship is a requirement."²⁸ States should consider the validity and reliability of any foundational documents used to authenticate an individual.

Section VI: Federal and State E-Authentication Efforts

The Federal Level:

At the federal level, the U.S. Office of Management and Budget (OMB) has issued guidance for federal agencies on E-Authentication. The guidance is technology-neutral and requires agencies to perform risk assessments regarding new or existing E-

Authentication systems. Agencies then map the risks to assurance levels established in the guidance. The assurance levels provide agencies with guidance as to the confidence level provided by the authentication.²⁹ Guidance from NIST (the National Institute of Standards and Technology) provides more specific technical guidance as to what types of processes and authentication methods must be in place at each assurance level.³⁰ NASCIO will monitor any state impact that might devolve from these federal efforts.

The U.S. General Services Administration (GSA) is the managing partner of the federal E-Authentication Initiative, which focuses on building the necessary infrastructure to support common, unified E-Authentication processes and systems for government-wide use.³¹ Currently, the initiative is focusing on E-Authentication within the context of the banking sector in order to provide banks with access to select federal information systems. GSA will work with other sectors, including states, in the future as it advances a federated model for E-Authentication.

Other federal authentication-related efforts include the Federal Bridge Certification Authority (FBCA), which helps to support interoperability among various federal PKI efforts.³² Moreover, OMB has an effort underway via the Federal Identity Credentialing Committee to make policy recommendations on identity credentialing as a component of the broader federal Enterprise IT Architecture effort.³³

The State Level:

At the state level, government agencies generally opt for technology based on “what you know,” and typically use some form of password protection for low-risk authentication. Higher-end E-Authentication methods, such as PKI, are less frequently used, due to their complexity and expense to implement. One example is Washington State’s PKI infrastructure, which allows citizens and businesses to conduct online transactions.³⁴ Some states also use a form of electronic signatures that allows users to digitally sign and transfer documents and gives them the same legal effect as written documents. However, even rarer at the state level is the use of biometric identifiers, such as facial recognition and iris scans. In part, concerns with false negatives and positives and the public perception of privacy encroachments with the use of biometrics appear to have slowed their adoption in the state government sector.

While E-Authentication is critical to the expanded application and broader adoption of online government transactions, states must proceed with E-Authentication in a way that properly assesses and addresses the risks, including potential compromises to citizen privacy. In that way, states will ensure that they are providing the proper level of authentication, which will enhance individuals’ privacy protections.

What CIOs Need to Know

- E-Authentication is critical to the availability of secure and privacy-protecting online transactions.
- Key concepts in addressing the privacy risks of authentication include the following:
 - Choosing the right level of authentication can enhance privacy.
 - Authentication methods must be tailored to address privacy and other risks. A method that provides greater protection than what is needed can encroach on privacy, because personal information is involved in most authentication transactions.
 - CIOs must be proactive in conducting a thorough risk assessment (including privacy risks) and choose a technology that addresses the identified risks.
- CIOs need to understand the policy issues that are critical in cross-boundary initiatives. Jurisdictions must agree to treat privacy concerns in a consistent manner.
- E-Authentication is but one part of an overall identity management life cycle that deals with the creation and management of identities (see Appendix B for more on the identity management life cycle).
- In addressing the privacy implications of E-Authentication, CIOs should involve not only individuals who deal with IT privacy policy issues but also those individuals who understand the technical aspects of E-Authentication. CIOs also should include business or program officials, who can understand the risk and reward trade-offs for their programs and particular group of users, as part of the risk analysis process.

Appendix A: Need More Information on E-Authentication? References and Resources

NASCIO Publications:

For more information about NASCIO's other privacy publications, including "Information Privacy: A Spotlight on Key Issues," and "Think Before You Dig: The Privacy Implications of Data Mining and Aggregation," please see our Privacy Committee Webpage at, <<https://www.nascio.org/nascioCommittees/privacy/>>.

NASCIO's Enterprise Architecture Development Toolkit, v 3.0,
<<http://www.nascio.org/publications/index.cfm#architecture>>.

Government Resources:

"E-Authentication Guidance for Federal Agencies," Executive Office of the President, Office of Management and Budget (OMB), M-04-04, December 16, 2003,
<<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>.

"Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology," National Institute of Standards and Technology (NIST), June 2004, <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf>.

"Standards for Security Categorization of Federal Information and Information Systems," NIST Federal Information Processing Standards Publication 199, December 2003,
<<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>>.

NIST Smartcard Research and Development Homepage, <<http://smartcard.nist.gov/>>.

"Policy for a Common Identification Standard for Federal Employees and Contractors," Homeland Security Presidential Directive, August 2004,
<<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>>.

Federal Bridge Certification Authority Website,
<<http://csrc.nist.gov/pki/fbca/welcome.html>>.

Federal Identity Credentialing Committee Website, <<http://www.cio.gov/ficc/>>.

U.S. General Services Administration (GSA) E-Authentication Initiative Homepage,
<<http://www.cio.gov/eauthentication/>>.

Washington State Public Key Infrastructure (PKI),
<http://techmall.dis.wa.gov/master_contracts/e_commerce/digital.asp>.

Other Organizations:

“e-Authentication Risk and Requirements Assessment: e-RA Tool Activity Guide,” Carnegie Mellon, Software Engineering Institute, May 2004 (updated), <<http://www.cio.gov/eauthentication/era.htm>>.

“Identity Management: Are We All On the Same Page?” National Electronic Commerce Coordinating Council (NECCC), 2004 <http://www.ec3.org/Downloads/2004/identity_management.pdf>.

“Enterprise Identity and Access Management: The Rights and Wrongs of Process, Privacy and Technology,” NECCC, 2003 <<http://www.ec3.org/Downloads/2003/EnterpriseIdentity.pdf>>.

“Identity Infrastructure,” NECCC, 2003, <http://www.ec3.org/Downloads/2003/identity_infrastructure.pdf>.

“Identity Management: A White Paper,” NECCC, 2002, <http://www.ec3.org/Downloads/2002/id_management.pdf>.

“Who Goes There? Authentication Through the Lens of Privacy,” Stephen T. Kent and Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2003, <<http://www.nap.edu/catalog/10656.html>>.

“Understanding Electronic Signatures: The Key to E-Government,” Stephen H. Holden, IBM Center for the Business of Government’s E-Government Series, March 2004, <http://www.businessofgovernment.org/pdfs/Holden_report.pdf>.

Appendix B: A Word About Identity Management

While this Research Brief focuses on E-Authentication, that topic is only a part of the broader picture of the identity management life cycle, which embraces the full spectrum of how identities are created and used. The generic phases of the identity management life cycle are:

- **Phase 1:** Identity proofing by a credentialing authority
- **Phase 2:** Creation of an identity credential
- **Phase 3:** Presentation of an identity credential to a relying party
- **Phase 4:** Acceptance of a credential by a relying party.³⁵

E-Authentication processes occur during Phases 3 and 4 of the identity management life cycle. For purposes of this Research Brief, the reader should assume that activities in Phases 1 and 2 of the life cycle have already taken place.

We can use our example of the voting process at the beginning of this Research Brief in order to illustrate the identity management life cycle.

- **Phase 1:** A voter completes a registration card, providing information such as a name and address, and submits the form back to the appropriate state voter registration agency. There may be verification processes that occur during this phase in order to verify the validity of the information that the voter provided to the voter registration agency. Since the voter will be required to present a form of photo identification at the polls on Election Day, Phase 1 also may include a voter's application for a photo ID, most likely a driver's license. In this phase, the state Department of Motor Vehicles (DMV) verifies that the individual is who he or she claims to be through methods that might include the presentation of a birth certificate.
- **Phase 2:** During this phase, the state voter registration agency places the voter's name on the roll of registered voters. This phase also entails the issuance of a photo ID to the individual by the state DMV.
- **Phase 3:** This phase occurs when the voter arrives at the polls on Election Day and presents his or her photo ID to the poll registration worker. The voter's identity must be authenticated before the voter is permitted to proceed into the voting booth.
- **Phase 4:** The poll worker verifies that the name on the photo ID matches the name on the voter registration roll and that the face of the person on the photo ID matches the voter's face.

In this Research Brief, we examine the privacy implications that are associated with E-Authentication during Phases 3 and 4.

Appendix C: NRC Checklist to Lessen Privacy Impact When Designing or Selecting an E-Authentication System

The checklist below was formulated by the National Research Council (NRC) in its publication “Who Goes There? Authentication Through the Lens of Privacy.” You can find more about this publication at: <<http://www.nap.edu/catalog/10656.html>>.

- Authenticate only for necessary, well-defined purposes
- Minimize the scope of data collected
- Minimize the retention intervals for data collected
- Articulate what entities will have access to the collected data
- Articulate what kinds of access to and use of the data will be allowed
- Minimize the intrusiveness of the process
- Overtly involve the individual to be authenticated in the process
- Minimize the intimacy of the data collected
- Ensure that the use of the system is audited and that the audit record is protected against modification and destruction
- Provide means for individuals to check on and correct the information held about them that is used for authentication.³⁶

Notes

- ¹ The title of this Research Brief was inspired by The Who's 1978 single "Who Are You?"
- ² For more information about identity theft and the role of authentication as a solution, please see testimony from a hearing on identity theft by the House of Representatives, Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, entitled "Identity Theft: The Cause, Costs, Consequences, and Potential Solutions?" September 2004, <<http://reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=1365>>.
- ³ "Who Goes There? Authentication Through the Lens of Privacy," Stephen T. Kent and Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2003, <<http://www.nap.edu/catalog/10656.html>>.
- ⁴ "2004 Election Results," CNN, November 3, 2004, <<http://www.cnn.com/ELECTION/2004/pages/results/president/>>.
- ⁵ For more information on HAVA, please see NASCIO's April 2004 Briefing Paper on HAVA at: <<https://www.nascio.org/nascioCommittees/privacy/HAVA04.pdf>>.
- ⁶ Examples of voting privacy concerns are available on the website of the National Committee for Voting Integrity at: <<http://www.votingintegrity.org/issues/Privacy.html>>.
- ⁷ "E-Authentication Guidance for Federal Agencies," Executive Office of the President, Office of Management and Budget (OMB), M-04-04, December 16, 2003, <<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>.
- ⁸ "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States," 2004, <<http://www.gpoaccess.gov/911/>>. Note that these and other similar concerns raised by the 9/11 Commission involve issues of identity management that are broader than the E-Authentication privacy issues that we discuss in this Research Brief. Please see Appendix A for additional resources, including white papers by NECCC (National Electronic Commerce Coordinating Council), on the wide array of issues associated with identity management.
- ⁹ "The Intelligence Reform and Terrorism Prevention Act of 2004," §§7211-7214 (identity management provisions), <<http://govt-aff.senate.gov/files/IntelligenceReformconferencereportlegislativelanguage12704.pdf>>.
- ¹⁰ For more about the identity management life cycle and authentication's role in it, please see Appendix B.
- ¹¹ "Digital Imaging Program Fact Sheet," State of Connecticut, Department of Social Services, January 2004, <<http://www.dss.state.ct.us/pubs/difacts.pdf>>.
- ¹² E-Authentication is a mere step within the broader context of the identity management life cycle that encompasses the creation and management of the various identities we use in transacting business with multiple entities on a daily basis. See Appendix B for a more detailed explanation of the identity management life cycle and E-Authentication's role in it.
- ¹³ "Who Goes There? Authentication Through the Lens of Privacy," Stephen T. Kent and Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2003, <<http://www.nap.edu/catalog/10656.html>>.
- ¹⁴ Note that, according to a 2004 survey sponsored by Carnegie Mellon's CIO Institute and the Ponemon Institute, 83% of the responding public said that data privacy was important or very important to them. However, many respondents had a high level of uncertainty about the government's ability to use and collect personal information. For more information, please see, <<http://cioi.web.cmu.edu/newsroom/press/20040209.jsp>>.
- ¹⁵ "E-Authentication Guidance for Federal Agencies," Executive Office of the President, Office of Management and Budget (OMB), M-04-04, December 16, 2003, <<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>.
- ¹⁶ "Who Goes There? Authentication Through the Lens of Privacy," Stephen T. Kent and Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2003, <<http://www.nap.edu/catalog/10656.html>>.
- ¹⁷ "E-Authentication Guidance for Federal Agencies," Executive Office of the President, Office of Management and Budget (OMB), M-04-04, December 16, 2003, <<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>.
- ¹⁸ Ibid.

¹⁹ While the technologies used in E-Authentication may be complex in some instances, there are many resources available that treat in detail the privacy and security features of E-Authentication technologies such as PKI (Public Key Infrastructure), Digital Certificates, Digital Signatures, LDAP (Lightweight Directory Access Protocol), and RFID (Radio Frequency Identification). NASCIO recommends starting with the resources in Appendix A of this Research Brief.

²⁰ “Who Goes There? Authentication Through the Lens of Privacy,” Stephen T. Kent and Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2003, <<http://www.nap.edu/catalog/10656.html>>.

²¹ Ibid.

²² Ibid.

²³ When considering the risks to privacy, it is helpful to examine the risks to privacy in light of the widely-used Fair Information Practices (FIPS). The FIPS include considering privacy as it relates to: (1) the collection of information (2) data quality (3) the purpose of information collection (4) uses (including secondary uses) of the information (5) notice to individuals of the collection of information (6) individual participation in the collection, use, assurance of accuracy, and correction of the information, and (7) enforcement and redress for individuals. For more about the FIPS, please see NASCIO’s “Information Privacy: A Spotlight on Key Issues.” It is available for free download to NASCIO members and for purchase by non-members at, <www.nascio.org>.

²⁴ “Who Goes There? Authentication Through the Lens of Privacy,” Stephen T. Kent and Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2003, <<http://www.nap.edu/catalog/10656.html>>.

²⁵ “E-Authentication Guidance for Federal Agencies,” Executive Office of the President, Office of Management and Budget (OMB), M-04-04, December 16, 2003, <<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>.

²⁶ Ibid.

²⁷ For more about the identity management life cycle, please see Appendix B.

²⁸ “Who Goes There? Authentication Through the Lens of Privacy,” Stephen T. Kent and Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2003, <<http://www.nap.edu/catalog/10656.html>>.

²⁹ “E-Authentication Guidance for Federal Agencies,” Executive Office of the President, Office of Management and Budget (OMB), M-04-04, December 16, 2003, <<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>.

³⁰ “Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology,” William E. Burr, Donna R. Dodson, and W. Timothy Polk, June 2004, <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf>.

³¹ For more information, please see GSA’s E-Authentication website at, <<http://www.cio.gov/eauthentication/>>.

³² View the FBCA’s webpage at <<http://csrc.nist.gov/pki/fbca/welcome.html>>.

³³ View the Federal Identity Credentialing Committee’s webpage at <<http://www.cio.gov/ficc/>>.

³⁴ Unique to Washington State’s PKI is its ability to create “digital signatures” which can be applied to electronic forms. These digital signatures have the same force and effect under Washington law as a handwritten signature, and agencies are beginning to look to digitally-signed transactions as a way to minimize the use of paper and reduce transaction cycle time. For more information about Washington State’s PKI program, please contact Scott Bream, Washington State Department of Information Services, at scott@dis.wa.gov.

³⁵ “The Identification Process Deconstructed,” J. Scott Lowry, Caradas, Inc., PowerPoint Presentation at NIST Smart Card Workshop, June 8-9, 2003, <<http://csrc.nist.gov/card-technology/presentations/security-privacy/Lowry-Caradas-Identification-Process.pdf>>.

³⁶ “Who Goes There? Authentication Through the Lens of Privacy,” Stephen T. Kent and Lynette I. Millett, Editors, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, 2003, <<http://www.nap.edu/catalog/10656.html>>.