Digital Identity: Opportunities for the Postal Service

May 29, 2012

Prepared by U.S. Postal Service Office of Inspector General
Risk Analysis Research Center
Report Number: RARC-WP-12-011

Digital Identity: Opportunities for the Postal Service

Executive Summary

As a highly trusted, venerable government institution with both a legal mandate to protect privacy and the authority to protect users from fraud,[1] the U.S. Postal Service is in a unique position to play a key part in a vital infrastructure for new digital identity creation and authentication services. These new services would make transactions requiring authentication of identity more convenient and secure than is possible with today's technologies. They would provide a foundation for new communications applications with an inherently high level of privacy for users, the digital equivalent of First-Class Mail® privacy protection.

Use of such services would be entirely voluntary, with clear, comprehensible, and concise privacy guidelines. The Postal Service could facilitate and build on existing joint public-private sector initiatives, which are currently hindered by the inability to tie a user's digital identity to a physical identity, such as a verifiable address. Although an in-depth legal examination would be required to pursue such an authentication offering, a previous U.S. Postal Service Office of Inspector General (OIG) Risk Analysis Research Center (RARC) study suggests that current regulations pertaining to the Postal Service are likely to permit such ventures.[2]

Today's digital identities are primarily limited to attributes (descriptions of characteristics) provided by the end-user, which may be fact-based or fictional. This makes them unfit for use with many applications that require authentication between a digital identity and a real person, business, or entity. Further, some identity services may expose sensitive information to identity providers in ways that the users are unaware of and would not agree to if given the choice. This dissuades some potential users; more importantly, weaknesses in digital identity authentication serve to discourage or prohibit the introduction of some Internet services that otherwise could be brought online, including some in the financial, health, and government sectors.

The current standard for digital identity — username and password — is inadequate for providing appropriate security in many contexts. It is often compromised and leaves users vulnerable to fraud. This has led to a fragmented system where users must keep track of numerous password-username combinations and visit different websites to navigate the Internet. This standard, although expedient, is not consumer-friendly and was not designed with consumer ease of use in mind.

[1] Title 39 U.S. Code.
[2] U.S. Postal Service Office of Inspector General, *Bridging the Digital Divide: Overcoming Regulatory and Organizational Challenges*, Report No. RARC-WP-12-004, November 22, 2011, http://www.uspsoig.gov/foia_files/RARC-WP-12-004.pdf.

Single sign-on services, where one username and password combination can be used on different websites through an intermediary (or "trusted third party"), are simpler and growing in popularity but have significant limitations as currently applied. For example, some large intermediaries, such as Google and Facebook, use their position to track users' Internet activities and develop behavioral profiles. Further, while the services may authenticate a user's profile, they may not be able to authenticate other attributes the user ties to that profile — or indeed, prove that any of the attributes are real.

Some single sign-on solutions utilize OpenID, from the OpenID Foundation, a nonprofit organization of individuals and companies committed to fostering OpenID technologies that allow a single password managed by an "identity provider" with strong security. While OpenID may ultimately develop and become a standard authentication tool, at present, its technology leaves many users open to "phishing"[3] — where a user is persuaded to log-in to a malicious website impersonating an official web page — and other Internet fraud. And none of the options currently under consideration for OpenID necessarily tie the user to real and verifiable attributes of identity, such as a physical address.

In May 2012, the Federal Government's Chief Information Officer unveiled a new Digital Strategy emphasizing that government "must ensure confidentiality, integrity, and availability by building security into digital government services."[4] One obvious area for building added security is the need for a trusted and neutral body to identify, authenticate, and certify users in a straightforward manner that reduces sign-up friction and maintains privacy. Currently, there are several formal initiatives outside of OpenID to explore the use of digital identities by government agencies and to encourage an interoperable standard for identity on the Internet. These include the National Strategy for Trusted Identities in Cyberspace (NSTIC), a White House initiative with a mandate "to improve the privacy, security, and convenience of sensitive online transactions."[5] While the Postal Service is participating in some NSTIC discussions, it could play a far more active role.

The Postal Service is in a strong position to help fill an important part of the digital authentication gap. While the lifecycles of many Internet-related companies have been unpredictable, the Postal Service offers an institutional permanence. It has a powerful nationwide presence that is known for respecting and protecting individuals' privacy. The Postal Service's significant tangible and intangible assets include its geographic reach and nationwide addressing system databases, including its Address Management System (AMS) and National Change of Address (NCOA) databases, which cover all residences and businesses. Between its systems and its physical network of retail locations and carrier services, the Postal Service has the right data, reach, and customer relationships to verify the link between citizens and their digital identities, making online transactions more secure. Such services could include in-person

[3] The risk of phishing is a problem shared by all of today's commonly used identity solutions.
[4] Digital Government: Building a 21st Century Platform to Better Serve the American People, Office of Management and Budget, http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html.
[5] National Strategy for Trusted Identities in Cyberspace, "About NSTIC," http://www.nist.gov/nstic/about-nstic.html.

authentication at Post Offices or by carriers, an extension of the current U.S. Passport Service offering.

Authentication is foundational: as noted in previous work by the OIG, it is a needed service and could provide the base of a digital platform with many applications. These applications could be developed and offered either by the Postal Service alone or in conjunction with other government agencies, nonprofit organizations, private businesses, or a combination of these. Partnerships could provide an expedient way for the Postal Service to become more involved in digital identity services, although care must be taken to assure that any such offerings meet rigorous postal privacy guidelines.

The Postal Service is in a position to enhance an important part of the infrastructure for online commerce by authenticating digital and physical identities. This will allow more consumer-friendly applications involving sensitive information, thus facilitating new eGovernment and eCommerce opportunities while securing important privacy protections for all users.

Table of Contents

Table

Figures

Appendices

Digital Identity: Opportunities for the Postal Service

Introduction

How much certainty do we have about the identity of those we deal with on the Internet? Shopping online, participating in an online discussion, or filing tax returns all require different levels of certainty about the identity of the other parties involved. Many "identity-centric services" (services that are heavily dependent on accurate and precise identities) either are not offered or underutilized for two main reasons: (1) the difficulty in verifying that a particular Internet user is who she claims she is; and (2) users' fears of identity theft or other fraud — whether factual or perceived — hinder adoption. In short, today's approaches to identity on the Internet leave much to be desired. Their limitations are holding back potential business applications and may jeopardize users' privacy.

In some industries such as banking and mobile phone service, the customer and the organization have agreed upon pre-existing measures that can be used to verify that an Internet user is legitimate. Examples are personal identification numbers (PINs) and account numbers, which have weaknesses.[6] Without solid pre-existing digital identification tools and verification measures, various services are not able to move online safely. In other cases, too many different entities are involved to easily verify an individual's identity or attributes. Examples of identity-centric tasks that are difficult to implement with today's identity technology include

Without solid pre-existing authentication measures, various services are not able to move online safely

- accessing healthcare information,
- managing legal documents,
- managing government services,
- state and local licensing,
- applying for scholarships,
- applying for loans,
- age-restricted transactions,
- utility account setup,
- opening certain financial accounts, and
- identifying trading partners.

Through its national addressing system for residences and businesses as well as its vast network of retail locations, the U.S. Postal Service has the right data, reach, and customer relationships to fill an important gap in the digital identity ecosystem, verifying the link between citizens and their digital identities.

[6] Many users employ PIN numbers that are too short to be secure, passwords that involve common names or personal details, or other passwords that can be easily guessed.

By enabling people to link their real-world identity to a digital identity, the Postal Service could serve as vital infrastructure for creating new digital services and make identity-centric transactions more convenient and secure. At the same time, the Postal Service could serve to strengthen online privacy for digital identities.

By building on its long history of connecting the nation and its position as the most-trusted government entity,[7] the Postal Service is in a unique position to protect customer privacy with clear and binding privacy regulations similar to those implemented for First-Class Mail.® The Postal Service could fill a critical gap in today's identity ecosystem: digital identity services with strong privacy protections suitable for use with government services, e-commerce offerings, and other identity-centric applications not possible with today's technology.

Use of such services would be entirely voluntary; individuals must be able to determine when and where to use their digital identities. People have multiple digital identities and few individuals are likely to assign their real-world identity to all of them. It must be recognized that the right of Internet users to remain anonymous for many interactions is an important part of what drives digital innovation and change.

Currently, there are several formal initiatives to explore the use of digital identities by government agencies and to encourage an interoperable standard for identity on the Internet. If the Postal Service can act swiftly, it is in a position to create and enhance an important part of the infrastructure for online commerce and eGovernment.

Background

Identity, Authentication, and Attributes

A **digital identity** refers to a collection of attributes related to a specific person or organization. Most Internet users have several digital identities issued to them as they sign up for email addresses, create accounts on websites, or access their office computers from home. For example, when you register for a new account at an online store, you create a new digital identity. You are asked to choose a password, so that in the future you can prove that you control that identity. This process of verifying that you control an identity is called **authentication**. When users enter their email address and password to access an account on a website, they are authenticating that they control that identity.

The details of your online identities are called **attributes.** Similar to a driver's license, revealing your digital identity to a third party discloses certain personal details. While your driver's license lists your name, address, age, and details about your physical appearance, a digital identity used for eCommerce may include details like your email

[7] U.S. Postal Service, "Statement from Postmaster General Patrick Donahoe on the Fiscal Year 2013 Budget of the U.S. Government," February 13, 2012, http://about.usps.com/news/national-releases/2012/pr12_0213FYbudget.pdf, and Ponemon Institute, "U.S. Postal Service Tops Ponemon Institute List of Most Trusted Federal Agencies," June 30, 2010, http://www.ponemon.org/news-2/32.

address, name, phone number, and shipping address. If you have a digital identity, such as an account with an online store, you may be able to place orders faster, find details about your order history, and add items to a wish list, although not every eCommerce website implements these features.

A Trust Framework and Its Components

Within the digital identity field, a **trust framework** is a certification program that enables a party who accepts a digital identity credential to trust the identity, security, and privacy policies of the party who issues the credential and vice versa.[8] It ensures that the user can have confidence in all parties in a given identity ecosystem.

The organization that issues a digital identity is called an **identity provider**. In the case of a driver's license, the identity provider is the state government. In the case of an email address, the identity provider is the company that hosts your email. The identity provider is not always the only organization to rely on the attributes in that identity. Just as there are many organizations that use your state-issued driver's license to determine your age, residence, or record your identity to deter fraud, other entities can rely on an online identity created by a trusted third party.

Organizations that rely on an identity issued by another entity are called **relying parties**. Several popular web services, including Facebook, Google, and Twitter, encourage people to use identities that these services provide for efficient authentication with other third-party services. Not incidentally, many such web services use these logins to gather behavioral profiles. For example, you may use your Facebook account as your identity when participating in an online discussion forum. In that case, the online discussion forum is a relying party, because it is relying on an identity provided by Facebook. Unlike a driver's license, digital identities often allow the owner to control the specific attributes they reveal. For example, when using a driver's license to verify your state of residence, you reveal information that may not be relevant, such as your date of birth — a detail that is unrelated to the question of where you reside. This information may not be needed for a transaction and therefore would not need to be shared.[9]

Today's digital identities are generally unfit for use with services that require a verified link between a digital identity and a real person

Today's digital identities tend to be limited to attributes provided by the end-user, making them generally unfit for use with services that require a verified link between a digital identity and a real person.[10] Additionally, today's identity services may expose

[8] Open Identity Exchange, "What is a Trust Framework," 2010, http://openidentityexchange.org/what-is-a-trust-framework.
[9] See Appendix B for a list of commonly used terms.
[10] Some users of high security applications are given physical tokens with dynamic codes to strengthen authentication. Tokens are typically used in addition to passwords and PINs. A token must be held in the user's possession to assure security and allow digital access. Tokens are expensive, cumbersome, and often misplaced or lost.

sensitive information to the identity providers in ways that the users are unaware of, raising questions about the suitability of today's services for use with financial, health, and government services.

There is potential, however, for a digital identity solution to emerge that enables certain sensitive, identity-dependent transactions to take place on the Internet with an expectation of privacy and convenience. By creating a way for web services to authenticate the real-world attributes of digital identities, the Postal Service could reduce fraud, increase customers' privacy, and expand the possibilities for new online services.

Existing Digital Authentication Solutions

Passwords

Internet users are familiar with the username and password pattern that is the most common method of managing Internet identities. When creating an account at a website, users are often asked to enter their email address and choose a username and a password.

Passwords and Fraud

Many users choose the same password across all of the websites that they visit; their entire online identity can be revealed by hacking a single website. For example, in 2011 hackers made a serious breach into networks operated by Sony, exposing millions of passwords that Sony left unencrypted. When comparing the passwords of users who had accounts on both Sony's services and other popular sites that were hacked, researchers found that most users had reused their password across multiple accounts.[11] In this case, users who had one password stolen now had all of their online accounts at risk.

Passwords are frequently compromised via a technique called "phishing," in which a user is emailed a link to log-in to a malicious website that is impersonating an official web page. The web page may request that the user enter their username and password or other sensitive details. Instead of logging the user into the web service as they expect, the malicious website captures the user's details for further fraud.

Passwords are also easy for computers to guess. Researchers at Cambridge University analyzed a sample of 70 million passwords with the cooperation of Yahoo!, and found that around 1 percent of accounts had passwords easily guessed by a computer.[12] More sophisticated guessing techniques can yield even better results.

[11] Troy Hunt's Blog, "A brief Sony password analysis," June 6, 2011, http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html.
[12] Joseph Bonneau, "The Science of Guessing," http://www.cl.cam.ac.uk/~jcb82/doc/B12-IEEESP-analyzing_70M_anonymized_passwords.pdf.

Due to the difficulty of motivating users to choose secure passwords, rampant password re-use by users, and the relative ease of phishing and hacking to compromise identities, password-only account systems are a weak link in the digital identity ecosystem.

The complexity of managing fragmented digital identities means a greater exposure to fraud

For many less experienced Internet users, the complexity of managing fragmented digital identities means a greater exposure to fraud. It is impossible to come up with a reliable estimate of the impact of fraud on the Internet in the United States, as scams increasingly traverse different communications media and borders. Some estimates of annual worldwide Internet-related fraud run into tens, or even hundreds, of billions of dollars.

Passwords and Identity

Username and password schemes can secure individual access to an online account, but they can only ensure that the user has control of an online identity. Passwords, by themselves, do nothing to authenticate that a given user is who or what they say that they are. Another shortcoming of the username and password pattern is that users must find a way to authenticate their identities for each individual service. Each banking website, each government agency, and each medical provider may have a different way of verifying that an online identity is controlled by a particular person. Fraud during this verification process can expose even more of a user's identity than a phishing scam.

The difficulty of making these processes easy to use, compounded with the risk of fraud, has limited the feasibility of online services that require strict identity control. While solutions exist to help technically inclined users overcome the burden of controlling many multiple online identities, as discussed below, these solutions leave large segments of the population with a greater exposure to fraud and diminish opportunities to participate in the digital economy. Further, the fear of lack of privacy in itself prevents some users from ever using even basic Internet commerce offerings.

Corporate Single Sign-On Services

In response to the shortcomings of password authentication, several large Internet companies have designed identity services that are easier to use. Single sign-on services allow a website owner to accept verification for an identity from a trusted third-party. For example, users can sign in to the National Public Radio (NPR) website using accounts from other websites including Facebook, Google, and Twitter. While single sign-on services alleviate the need for users to remember many different passwords, these services have their own shortcomings. Some of the companies issuing these identities compile detailed behavioral profiles of their users by tracking user behavior across the Internet. These profiles are used to tailor advertising to that individual based on their activity across multiple websites. The use of today's single sign-on services could be suboptimal for web services with an expectation of privacy, including managing government services and dealing with sensitive healthcare information.

Additionally — and very importantly — single sign-on identities do not verify specific attributes or that users are who they say that they are. For example, you can create a Facebook profile listing residence in a city other than the one where you live or under any name that you choose. A single sign-on identity only verifies that a particular Internet user controls the data in an account on a website, making today's single sign-on identities insufficient for trusted applications or those needing to deal with the specifics of real-world identity.

OpenID

OpenID is a decentralized single sign-on solution, meaning it sets an interoperable standard for organizations to share and issue identities. It was developed in 2005 as a collaborative effort among leaders in the digital identity community. Currently, two nonprofits are involved with OpenID: Open Identity Exchange provides certification for identity providers and OpenID Foundation, manages the trademark and promotes the OpenID standard. Both groups are supported by leading technology companies.[13]

OpenID is a specification for creating identities that can work across multiple websites. Any person or organization may create an identity, and web services that support OpenID can accept those identities even when the identity was not originally created at that site. Used by many single sign-on services, OpenID can help reduce the number of different accounts a user must maintain across the web.

OpenID is a promising approach to Internet identity because it utilizes existing technology…but cumbersome for the average Internet user

For example, users with an OpenID are able to log on to the NPR website with a process similar to that used for a single sign-on identity issued by a corporation. If the OpenID is issued by the user themselves or another party that does not track users' activity across multiple websites, then the user retains a greater measure of privacy than those using a single sign-on identity issued by a tracking and advertising business. This means that OpenID technology may present an opportunity for services that are identity-centric or deal with information more sensitive than shopping and social networking.

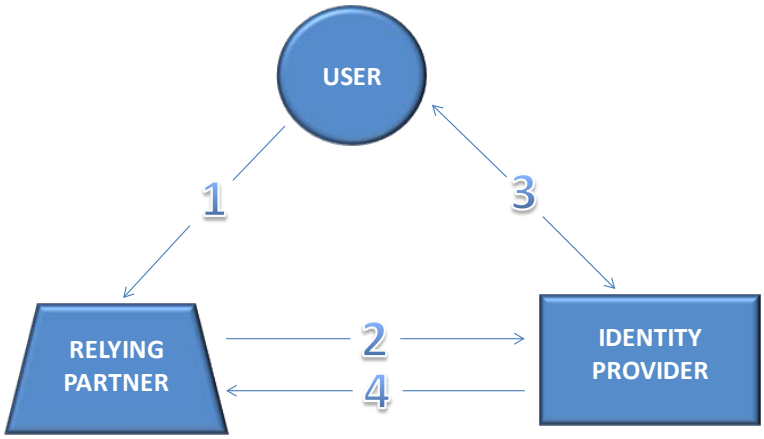
OpenID is a promising approach to Internet identity. OpenID requires no additional software other than the standard web browser, and OpenID itself utilizes other open-source specifications for transferring data and authentication. This ease of adoption has resulted in 9 million sites using the technology, with over 1 billion identities created within the ecosystem.[14]

The OpenID specification allows trusted third parties to verify attributes of a specific identity (see Figure 1). For example, the Postal Service could act as a trusted third party to verify the street address of a user and authenticate the user's identity. When

[13] For example, both groups include board members from Google, Microsoft, PayPal, and Symantec.
[14] OpenID, "OpenID 2009 Year in Review," December 16, 2009, http://openid.net/2009/12/16/openid-2009-year-in-review/.

appropriate, the user could choose to reveal some real-world attributes of their identity to do business online. Users have a choice of which attributes they would like to reveal, perhaps only revealing their state of residence rather than their full street address. The mechanisms for sharing attributes of an identity are designed to protect individual user privacy and choice. They also help to protect the universe of users at large.

Figure 1: OpenID and Third Party Verification



1. User logs into Relying Partner's website
2. Relying Partner contacts Identity Provider to authenticate the User
3. Identity Provider asks User to authorize using identity with Relying Partner
4. If/When User allows, Identity Provider sends credentials to the Relying Partner and the User is logged into the website

OpenID remains cumbersome for the average Internet user. The process of creating and using an OpenID is unfamiliar to most users. Also, under the current specification for OpenID, creating an OpenID with a third party (instead of issuing one's own ID) can expose more information to the identity provider about a user's behavior than an average Internet user may realize.

While OpenID remains as vulnerable to phishing as other single sign-on systems, these issues are likely to be overcome by improving its design. The OpenID Foundation continues to update and evolve the specification in response to the experience of web developers and feedback from the information security community.

Pilot Projects for a Digital Identity Ecosystem

Government agencies, other posts and the private sector are responding to the shortfalls of today's identity capabilities by forming organizations to develop and advance interoperable standards for digital identity.

The National Strategy for Trusted Identities in Cyberspace Initiative

In May 2012, the Federal Government's Chief Information Officer unveiled a new Digital Strategy emphasizing that government "must ensure confidentiality, integrity, and availability by building security into digital government services."[15] Prior to this, recognizing the need to establish a framework for trusted identities online, the White House has issued an administrative mandate to establish an "identity ecosystem" that gives both organizations and Internet users a greater degree of confidence in the identities of those they do business with online. In a proposal released in February of 2012, the National Strategy for Trusted Identities in Cyberspace (NSTIC) created federal support for a steering committee in a private sector-led effort to develop an identity ecosystem, involving stakeholders from industry, federal and local government, and privacy, civil liberties, and consumer advocacy organizations.[16]

NSTIC has committed funding and other support to establish the steering committee and undertake pilot projects to explore digital identity models; it envisions implementation of a functioning identity ecosystem by 2016.[17] NSTIC aims to create a norm in digital identity management whereby institutions and users are able to conduct identity-related business online in a voluntary fashion, thus giving individuals control over what private information is disclosed. NSTIC encourages interoperability and government adoption of the resulting digital identity platform. In discussing and defining potential authentication solutions, NSTIC and other organizations use the definition of four levels of authentication assurance provided by the National Institute of Standards and Technology (NIST); levels 1 and 2 are the most commonly employed.[18]

Open Identity Exchange

Distinct from the OpenID Foundation, which manages the specification to implement OpenID, the Open Identity Exchange is a certification listing service for open trust frameworks. The Open Identity Exchange has developed a certification for identity providers in conjunction with the General Services Administration (GSA). Certified identity providers as of March of 2012 include Google, PayPal, Verisign, and Equifax. A pilot program enables the National Institutes of Health (NIH) to accept OpenID credentials from certified private-sector identity providers.[19]

---

[15] Digital Government: Building a 21st Century Platform to Better Serve the American People, Office of Management and Budget, http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

[16] National Institute of Standards and Technology, "Administration Releases Strategy to Protect Online Consumers and Support Innovation and Fact Sheet on National Strategy for Trusted Identities in Cyberspace," April, 15, 2011, http://www.nist.gov/public_affairs/releases/whitehouse_nstic.cfm.

[17] John Fontana, "NSTIC doc outlines transition to privately led ID effort," ZDNet Identity Matters, February 8, 2012, http://www.zdnet.com/blog/identity/nstic-doc-outlines-transition-to-privately-led-id-effort/224?tag=search-results-rivers;item0.

[18] For definitions of the four levels of authentication assurance, see Appendix C.

[19] Open Identity, "Open Identity Exchange Commences Open Government Pilot with National Institutes of Health," March 3, 2010, http://openidentityexchange.org/press-releases/nih-announces-oix-pilots-2010-03-03, and National Institutes of Health, "Open Identity for Open Government at NIH," http://datacenter.cit.nih.gov/interface/interface245/open_gov.html.

International Posts and Secure Identity Across Borders Linked

In a recent survey of postal operators conducted by the Universal Postal Union, more than a third of the 15 industrialized country respondents stated that they currently provide digital identity services. Other postal operators, particularly in Europe and the Arab region, continue to expand such offerings.[20]

According to 2011 research from The Information Technology & Innovation Foundation, 16 European countries provide a digital identity for its citizens.[21] In Europe, the Secure Identity Across Borders Linked (STORK) project aims to create reciprocal recognition of digital identities provided by European nations. The project is made up of partner entities from the public and private domains. It is funded in part by the European Commission and encompasses several pilot projects currently in progress across the continent, including international change-of-address services.

STORK creates a template for a platform to share identity data, while allowing the end user to maintain control over what data is sent to what website. As the European Union strives to strengthen consumer privacy protections, STORK's platform aims to protect privacy by transferring only the minimum data needed to create a transaction and allowing individuals to completely delete all of their information from the system if they choose.[22]

Features of the Digital Identity Ecosystem

Today's framework for digital identity addresses several problems successfully: the need to verify the identity of websites themselves for transmitting secure information, the existence of an open platform, and ever-improving tools to help users manage multiple identities.

Several unaddressed needs remain; these gaps represent an opportunity for new identity services. Solving these issues will expand the possibilities for digital services to use identity information efficiently, saving costs, reducing fraud, and adding convenience for individuals and organizations.

Verification of Real-World Attributes

In order to support an expectation of privacy and a need for strong identity, government agencies, businesses, and citizens will require a way to authenticate the real-world identity of an Internet user by verifying user attributes. Current verification procedures are fragmented across organizations, creating inefficiencies and adding barriers to

[20] The UPU is also currently in the early stages of developing a postal identity standard. See Appendix A for an overview of digital identity models used for the provision of eMailbox-type services.
[21] The Information Technology & Innovation Foundation, *Explaining International IT Application Leadership: Electronic Identification Systems*, September 15, 2011, http://itif.org/publications/explaining-international-it-application-leadership-electronic-identification-systems.
[22] STORK (Secure Identity across Borders Linked), "FAQs," www.eid-stork.eu/index.php?option=com_content&task=view&id=55&Itemid=76#stork_faq_5.

providing online services. For example, users may be required to have separate online identities and accounts to manage the distribution of government benefits and to securely access their healthcare information online. Each organization the user communicates with adds another layer of complexity and another process for verification.

The standards for addressing in the physical world have acted as a catalyst for communications and commerce. Similar infrastructures should exist in the digital world

There are potential macroeconomic diseconomies without a reliable national digital identification and address system online, even one that is optional for consumers. In the physical world, standards for addressing have acted as a catalyst for communications and commerce by making it simple for businesses and individuals to locate and deliver information and goods to customers around much of the world. Similar infrastructures should exist in the digital world as activities shift online. Simplifying the process of verifying a user's real-world identity online would expand the possibilities for bringing government services into the digital world. By providing the user with a digital identity that can be used for these kinds of services, agencies could more easily offer their services online, and users could utilize those services effortlessly.

If citizens were able to use their verified identities for transactions outside of government services, several positive trends might emerge. First, the more widely usable an identity is, the less friction there is to widespread adoption. Secondly, the use of verified real-world attributes is not a problem unique to government. Businesses could build on the new opportunities created by a secure identity infrastructure, bringing new services to market and strengthening existing ones. As digital identity security increases, the cost of fraud to businesses will decline.

While there are pilot programs in progress to certify commercial single sign-on services for government use, for-profit single sign-on services would be inappropriate for many applications where there is an expectation of privacy. Current pilot programs do not yet define a solution for identity verification that operates at Internet scale. The programs explore use of single sign-on services with government services, but in a limited environment where the identity of the user may be prescribed outside of the single sign-on service.

Users can only make choices about privacy when their options are clearly presented

Transparent Privacy Policies

Users can only make choices about privacy when their options are clearly presented. Most websites today feature a privacy policy, typically reached via a link at the bottom of a web page. Users are often asked to agree to a website's privacy policy before creating their account. Yet this is unrealistic in practice, as typical privacy policies are often long and complex. Researchers from Carnegie Mellon recently suggested that it

would take the average Internet user 76 workdays to read all of the privacy policies that they encounter in a year.[23]

Even if consumers reviewed the privacy policies they encounter, the Internet's premier identity providers lack a precedence of strong privacy protection. In 2011, Facebook settled with the Federal Trade Commission over changes to their privacy policy that shared users' information and bypassed their privacy preferences.[24] And in March of 2012, the Federal Trade Commission began examining whether Google has misrepresented its privacy practices to consumers.[25] Google has acknowledged that it intentionally bypasses the privacy settings in the Safari web browser in order to track users across the web.[26]

In cases where users are accessing sensitive services online or revealing real-world aspects of their identity, the implications of privacy choices must be made clear to users and must be respected. Without a framework of trust and transparency between digital identity providers and the users they service, today's digital identity management capabilities are inappropriate for use where there is a strong expectation of privacy.

Neutrality

Market forces can create additional conflicts for uses of these identities, including an incentive for anticompetitive practices. The Internet is a neutral infrastructure; one that does not select the winners or losers in the marketplace. By forcing users to choose between for-profit identities in order to digitally engage with their government services, users could be left with no options that protect their privacy. A neutral provider of identity infrastructure would allow greater marketplace innovation and diminish the incentive of identity providers to limit the interoperability of their identities.

Today's economic incentives for identity providers stem from their ability to track users

As an example of these politics at play in the current marketplace, consider the criticism that today's large-scale identity providers rarely accept identities authenticated by other providers. For example, you cannot log into Google's services using an identity other than one issued by Google, but Google encourages you to use your Google identity with other providers. Because today's economic incentives for identity providers stem from their ability to track users, it does them little benefit to utilize identities provided by other organizations. Placing those same limitations on one's ability to access financial, government, or health services would force the user to maintain a number of digital identities, which would be detrimental to the user and promote inefficiencies.

---

[23] Aleecia M. Mcdonald and Lorri Faith Cranor, "The Cost of Reading Privacy Policies," *ACM Transactions on Computer-Human Interactions,* 0380 No. 3, http://www.mendeley.com/research/the-cost-of-reading-privacy-policies/#.
[24] Byron Acohido, "Facebook settles with FTC over deception charges," *USA Today*, November 29, 2011, http://www.usatoday.com/tech/news/story/2011-11-29/facebook-settles-with-ftc/51467448/1.
[25] Julia Angwin, "Google Faces New Privacy Probes," *Wall Street Journal*, March 16, 2012, http://online.wsj.com/article/SB10001424052702304692804577283821586827892.html.
[26] Jon Brodkin, "US, Europe investigate Google's bypass of Safari privacy settings," *Ars Technica*, March 16, 2012, http://arstechnica.com/tech-policy/news/2012/03/us-europe-investigate-googles-bypass-of-safari-privacy-settings.ars.

Personal Choice

If users find it more convenient to use an identity issued by a for-profit identity provider, and accept the possibility that sensitive information is likely to be tracked in data compiled by the identity provider, then those users should be able to utilize any identity service that they choose. It must remain up to the user to decide what organizations to trust with their information.

Ideally, Internet users will have many options available to them. More possibilities for online services would be created in an ecosystem where the users are able to choose to employ multiple identities or remain anonymous, as they see fit. Perhaps many users will choose one single identity, provided and verified by an entity that they trust. Some users may use multiple identities: one for sensitive applications and another where convenience is the primary concern.

Today's advanced Internet users are able to partition their online identities in ways that add an element of privacy protection. Other users are completely comfortable disclosing their online activities in exchange for valuable services. And some users choose only to participate in the online world anonymously. All of these options should be preserved in the online identity ecosystem, even as more are presented that bolster the users' privacy options.

Opportunities for the Postal Service in Digital Identity

The Postal Service has a long history of bringing together citizens, government, and commerce. How people connect has changed significantly. The expanding digital economy presents a challenge to bring these values to new environments. It also presents a starting point for the development of new digital products and revenue streams.

In entering the world of identity provisioning, the Postal Service will have to determine the optimal level of authentication needed. While in-person application provides the highest level of security, it also makes sign-up more difficult and expensive. There is an inherent trade-off between the rigor of the authentication and customer convenience that affects the rate of adoption. It may be best to adopt a multi-level authentication protocol, allowing higher-level transactions only with a similar level of authentication, while maintaining minimum levels of authentication for simpler transactions.

By taking the role of a trusted entity to verify attributes of identity, the Postal Service can use key parts of its existing infrastructure[27] to create a valuable service. The service would provide a strong link between real-world identities and digital identities, backed by clear and strong privacy procedures, thus enabling government and businesses to better meet the growing expectation for digitally accessible transactions. It would add capabilities to the digital identity ecosystem at a time when these features are needed.

[27] This includes its current website, usps.com, and customer databases.

As a Trusted Third Party Online

The Postal Service could serve as a trusted third party for verifying an individual's location of residence with the individual's permission. When using a verified identity online, customers could choose what to reveal about their real-world identity in a given transaction, with specificity ranging from street address to region, state, county, city, or ZIP code. Through the U.S. National Change of Address (NCOA) system the Postal Service could verify the past addresses of individuals and businesses.[28]

Figure 2: The Postal Service as a Trusted Third Party

1. User requests a digital identity from Identity Provider
2. Identity Provider creates a verification request with the Postal Service
3. The Postal Service verifies the identity of the User either in-person or using change of address data
4. As a Trusted Third Party, the Postal Service provides verification of the User's physical identity for the Identity Provider

Utilizing OpenID's protocols for attribute exchange, the Postal Service could verify these attributes for organizations that act as digital identity providers. After successful verification, identity providers would allow customers to reveal the attributes to relying parties.

As an Identity Provider

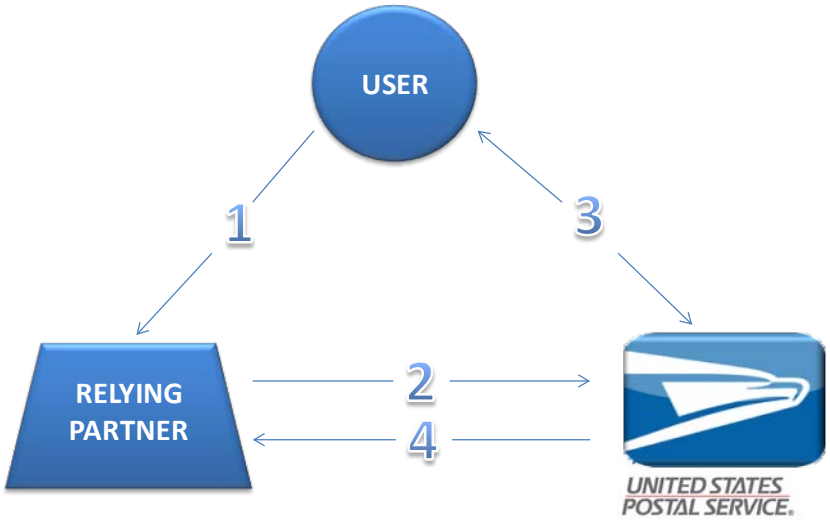
In addition to verifying attributes of identities issued by other organizations, the Postal Service could act as an identity provider itself. The Postal Service could directly verify attributes of individuals and organizations online. Digital identities issued by the Postal Service could operate according to the OpenID standard and work within the existing identity ecosystem. Customers could use their identities for all of their online transactions, or use their identity only for transactions that handle sensitive information.

[28] Currently, data in the NCOA system is stored for four years. For more information on the NCOA, see U.S. Postal Service Office of Inspector General, *eMailbox and eLockbox: Opportunities for the Postal Service*, Report No. RARC-WP-12-003, November 14, 2011, http://www.uspsoig.gov/foia_files/RARC-WP-12-003.pdf.

At the request of a customer, the Postal Service could share the customer's verified location and identity details with relying parties, such as retailers or service providers.

The digital identity could also traverse back into the physical world as an identifier for a number of different access tools. For example, it could serve as the core identifier on a postal-centric smart card that would not only provide access to postal services, but provide digital authentication and serve as a platform for other government and commercial entities to offer additional services.[29]

Figure 3: The Postal Service as an Identity Provider



1. User logs into Relying Partner's website
2. Relying Partner contacts the Postal Service to authenticate the User
3. The Postal Service asks User to authorize using identity with Relying Partner
4. If/When User allows, the Postal Service sends credentials to the Relying Partner and the User is logged into the website

Verifying Attributes Physically for Digital Identities

The Postal Service can verify the mailing address of individuals or organizations several ways. With a nationwide network of locations and postal carriers reaching every door, the Postal Service could provide in-person verification or verification-by-mail services. The Postal Service already provides such services for the processing of passports, having collected 5.6 million passport applications in 2011 alone.[30] With permission from an individual, the Postal Service could verify a specific individual's control over an online

[29] U.S. Postal Service Office of Inspector General, *The USPS Global Card: A Conceptual Analysis of a Smart Card Platform*, Report No. RARC-WP-12-006, February 13, 2012, http://www.uspsoig.gov/foia_files/RARC-WP-12-006.pdf.
[30] U.S. Postal Service, "Postal Facts," http://about.usps.com/who-we-are/postal-facts/welcome.htm.

identity by matching an address and incoming mail, and checking physical identification. The NCOA system, in addition to helping people receive their mail at new locations, could provide accurate and up-to-date verification of an address.[31]

Many existing processes for verifying addresses utilize the Postal Service. For example, some businesses will mail a postcard with a unique code to an address they are attempting to verify. The resident will enter the unique code onto a website to prove they reside at that address. While repeating this process for multiple services is not optimal, this use of the postal system demonstrates businesses' reliance on current postal services.

Identity Provisioning and Revocation

The Postal Service's existing "brick and mortar" locations are a major advantage for identity services. In order to provide a new digital identity for a customer, physical verification of their mailing address would be required.[32] By offering these services in-person at a retail location or with verification by their letter carrier, customers could work with an organization they trust to keep their information updated and secure. The Postal Service reaches every residence and business in the United States.

One responsibility of an identity provider is revoking compromised identities. If customers lose control of their identities, they must notify identity providers to prevent unauthorized use of the identity online. Even the revocation process can be a target for fraud online.

Protecting Privacy and Security

Backed by the Privacy Act of 1974 and the legal protection of First-Class Mail, the Postal Service has a long-established history of clear, direct, and effective privacy practices with legal standing. This history means that the Postal Service is in a unique position to provide identity services built on a foundation of privacy and trust, an aspect of digital identity left unaddressed by today's identity providers. Verification of identity attributes and identity services can be delivered in a way that protects the individual's privacy. Being bound by mail privacy laws, the Postal Service could fill critical gaps in the identity ecosystem and provide a clear, concise privacy statement that prevents the Postal Service from sharing any information with any parties other than those customers choose.

The Postal Service is in a unique position to provide identity services and to fight against fraud

The Postal Service also has unique strengths in the fight against fraud. The Postal Service offers protection under federal law through two law enforcement organizations: the Office of Inspector General and the Postal Inspection Service. These law

[31] U.S. Postal Service Office of Inspector General, *The USPS Global Card: A Conceptual Analysis of a Smart Card Platform*, http://www.uspsoig.gov/foia_files/RARC-WP-12-006.pdf.
[32] The Postal Service already verifies addresses for mailers through a number of address hygiene services.

enforcement organizations currently investigate crimes that include using a false identity and fraud. The reach and experience of these two organizations serve as a valuable tool for the enforcement of customers' privacy and security — a tool that could readily be adapted to fulfill a wider role in the digital sphere.

Evolving Role in Authentication and Digital Identity Services

The Postal Service has experience both in providing physical authentication services for federal agencies such as the Department of State's Office of Passport Services and in providing such services for its own products, ranging from Change of Address requests to registration for the new gopost™ parcel lockers. In the digital world, the Postal Service has also amassed experience in providing secure online storage of personal information, including the encryption used to manage the AMS and NCOA databases as well as the administration of the Click-N-Ship® postage program.

This experience, along with a reputation for trust, brings the organization the necessary credibility to engage in this arena. As the framework for an online identity ecosystem evolves, the Postal Service has begun to engage with key players from government and industry. Whether as an active participant with industry and government representatives developing the NSTIC framework, as a potential partner to participants in the NSTIC and OpenID pilot programs, or working with federal government agencies to develop a single sign-on across the .gov domain, the Postal Service has been and must continue to be engaged as an identity framework rolls out over the coming years.

The need for a Postal Service role in federal online identity management is significant. In this era of limited resources, federal agencies are reducing their physical footprints and seeking ways to reduce costs. Simultaneously, the same agencies are seeking to reach Americans through innovative eGovernment programs requiring identity and attribute authentication. Whether vetting identification for the Department of Agriculture or verifying physicians in the roll-out of the Center for Medicare and Medicaid Services' ePrescribe Program, such programs provide an obvious role for the Postal Service.

Adoption and New Applications

If the Postal Service were able to provide Internet users with the ability to share information about their real-world identity through their physical identity, innovators would set to work finding profitable applications for this information. Each expansion of capability available to entrepreneurs is followed by a wave of start-up businesses exploring new potential concepts. For example, when a user's current physical location became available to websites through smartphones, new businesses emerged to utilize that data. Participants in the digital economy ultimately decide the fate of these new ventures.

One possible application using the Postal Service's authentication services is Peer-to-Peer Escrow. As background, the Internet has enabled an expansion of peer-to-peer commerce. Websites such as eBay and Craigslist make it easy for individuals to connect with people in their community or even internationally for the purpose of trade;

bartering; or selling used goods, crafts, and services. This expanded economy has provided new ways for criminals to defraud citizens in possibly receiving counterfeit goods, or on the other side, in possibly receiving counterfeit payment.

If both the buyer and the seller were able to register their identities digitally with a service that facilitated payment for the transaction (or "escrow service"), they would be able to lower their fraud risk. By using their digital identities, authenticated by the Postal Service, the buyer and the seller could reveal their information only to the trusted third party. This would deter fraud, better enable law enforcement to address a growing problem, and provide a legitimate sense of security and privacy to the buyer and the seller.

This hybrid of digital identity verification and escrow is a theoretical service that illustrates the potential for the use of authenticated digital identities in the Internet economy. By creating digital identities that interoperate with the open standards on the web, the Postal Service could enable new businesses to emerge, as well as help existing organizations to be more secure, efficient, and convenient for their customers.

Revenue Opportunities

Digital identity services provide several revenue opportunities for the Postal Service. For example, when working as a trusted third party to verify limited attributes of existing identities, the Postal Service could charge either a value-based per-use fee or an annual access fee to the identity providers for which the Postal Service verifies attributes.

For services with a high expectation of privacy, identities issued by the Postal Service may be ideal. When functioning as an identity provider, the Postal Service could charge organizations that rely on Postal Service-verified attributes to complete commercial transactions.

Automated billing of per-use fees is a common revenue model for open Internet platforms. For example, Google Maps allows businesses to utilize its data for commercial purposes. The first 25,000 requests in a day are free. After that, businesses pay $4 for each additional 1,000 requests. A more liberal license is available for large-scale users, which includes technical support and availability agreements, starting at $10,000 annually.[33]

Implementation Considerations

Integration with Existing Identity Ecosystem

The existing identity ecosystem is large. Billions of these identities exist on the Internet today, and they are a critical part of the digital economy. To fill the gaps in service

[33] "Google puts a limit on Free Google Maps API: over 25,000 daily and you pay," *The Guardian,* Technology Blog, October 27, 2011, http://www.guardian.co.uk/technology/blog/2011/oct/27/google-maps-api-charging.

outlined in this paper, the Postal Service should implement its identity services in a way that interoperates with the existing identity ecosystem.

Over time, OpenID may develop into a platform on which to build a strong, identity service with a focus on user privacy

Although still under development, OpenID demonstrates the power of an open platform and the ability for the specification to evolve and meet new challenges. Over time, security will increase, usability will improve, and OpenID may develop into a platform on which to build a strong, privacy-centric identity service.

The NSTIC and Open Identity Exchange initiatives both aim to increase the adoption of this technology within government. By working with these organizations, the Postal Service could develop a revenue stream in providing identity services to other government agencies, the healthcare industry, and other entities with which individuals share their identity profile.

User-centric Privacy

The potential for abuse of privacy is a valid concern for any identity service. Although the Postal Service has a longstanding tradition of keeping individual information private, some of its revenue models based in the physical world will not translate to the digital. A strong commitment to privacy can be displayed if the default settings of the service are to maintain the strict confidentiality of customers' information. Adoption will be stifled if users believe that keeping their information current will result in increased amounts of unwanted physical or digital communication from advertisers.

Any information-sharing should only be under circumstances where users opt in and have granular controls over what attributes are shared and with whom. If serving as an identity provider, the Postal Service should not store any information about the specific websites a customer authenticates with. In order to keep user privacy paramount, no behavioral information should be logged or stored.

A Building Block for Web Services

Beginning in 2011, The U.S. Postal Service Office of Inspector General (OIG) Risk Analysis Research Center (RARC) began publishing a series of white papers that explore a positioning for the Postal Service in the digital economy. For each opportunity defined in the series, including eMailbox and eLockbox services, digital identity services may be part of the foundation.

While building an interoperable identity service is a much larger undertaking than creating a username and password authentication system, it may be a requirement of moving the Postal Service further into the digital age. The Postal Service currently offers accounts online for both individuals and mailing organizations. Improving the interoperability of accounts within existing Postal Service products could be a logical first step towards building an expanded identification service.

A Platform for New Applications

Part of the potential for the Postal Service in offering digital identity services is the organization's ability to create a platform in addition to a simple digital identity service offering. While customers can utilize a service for a specific use, a platform would enable new products and services to be created, enabled by the core technology of verifying real-world attributes of digital identities.

Technology — Cost and Internal Capabilities

Establishing an interoperable identity service is not a one-time investment. In addition to customer service, verification services, and revocation and security responsibilities, the technology that serves as a foundation to digital identity will continue to improve. Services built on this technology will adapt as well.

Today's open identity ecosystem, largely driven by OpenID technology, is an evolving standard. The OpenID Foundation improves the specification on a regular basis, responding to the challenges presented by real-world implementation. This process of adaptation is an open one. If the Postal Service becomes a stakeholder with a long-term investment in this technology, participating in the creation of new versions of the OpenID standard is an important step in strengthening the digital identity ecosystem.

Partnering with outside organizations could provide a shortcut …but is unlikely to provide privacy benefits

How the Postal Service could best develop this technology and participate in its evolution is open to further exploration. Partnering with outside organizations could provide a shortcut to development, but the rebranding of existing identity technology in itself is highly unlikely to provide the privacy benefits required to make a strong impact in today's market.

Liability

A digital identity solution used to manage valuable information is a target for fraud. Criminals attempt to access information that can be used for identity theft by taking control of a user's online identity, either through exploiting security deficiencies or tricking users into giving away control.

New identity services should be supplemented with a legal review of the liability created by providing these services. If a customer's information is compromised and a fraudulent transaction completed, what protections are in place for the customer, the relying party, a trusted third party, and the identity provider? New protections or limitations for the use of identity services may be necessary as conditions of using identities provided or verified by this system.

Currently, no comprehensive federal law or regulation covers the security of sensitive personal information by the federal sector or related liability in the event of breach or fraud. Instead, a web of federal laws, regulations, and guidance apply, reflecting a

"sectoral approach" to the protection of personal information.[34] Major legislation passed by Congress in areas such as financial services, health care, and the Internet, has created a framework with multiple organizations maintaining enforcement authority, ranging from the Veterans Administration to the Federal Trade Commission to the new Consumer Financial Protection Bureau. This web of statutes presents a challenge, but should not prohibit or discourage the Postal Service from further engagement.

As the Postal Service considers partnering with federal and even state and local government agencies, it must evaluate and develop sensible liability provisions that spread responsibility among accountable parties and minimize risk. As a self-insured entity, the Postal Service has elected to pay for losses itself rather than purchasing insurance in the private market. This policy should be reviewed, together with an examination of examining new digital identity and attribute authentication services and how risks could be shared with other agencies.

Regulatory Issues

Before even planning digital services, the Postal Service should consider whether the product would be allowed under current postal regulations. By law, the Postal Service is restricted to offering "postal services" or specifically grandfathered "nonpostal services." Current law, however, grants significant leeway to the Postal Service in providing services to other parts of the federal government.

In 2011, the Office of Inspector General engaged a leading regulatory expert to conduct an extensive analysis of the current regulatory environment. She concluded that current regulations, particularly in the provision of eGovernment services, do provide a legal path for the Postal Service to offer a number of digital services. Many new products that bridge the gap between the physical and digital worlds, such as those in this paper, may be characterized as complements or digital versions of existing postal products.[35]

The Postal Service is on the brink of missing a critical opportunity to find its own role in the digital economy and shape the future of identity on the Internet

Further, one could argue that offering digital identity services not only helps to bridge the gap between the physical and digital worlds, but also plays a vital supporting role in in continuing to bind the nation together. As the digital revolution continues to rage, providing such services across the nation reflects a modern interpretation of the Postal Service's Universal Service Obligation in providing a secure and trusted channel for communications and commerce.

[34] U.S. Congressional Research Service, *Federal Information Security and Data Breach Notification* Gina Stevens,January 28, 2010, http://www.fas.org/sgp/crs/secrecy/RL34120.pdf, p. 1.
[35] U.S. Postal Service Office of Inspector General, *Bridging the Digital Divide: Overcoming Regulatory and Organizational Challenges*, Report No. RARC-WP-12-004, November 22, 2011, http://www.uspsoig.gov/foia_files/RARC-WP-12-004.pdf.

Conclusion

With pilot programs already in place through NSTIC and OIX, the Postal Service is on the brink of missing a critical opportunity to find its role in the digital economy and shape the future of identity on the Internet. While technology leaders in both the public and private sectors have yet to develop and agree on common standards and protocols, they are progressing and could begin testing even an imperfect prototype. The Postal Service needs to take an active role in order to keep pace with an evolving industry, an industry that will dramatically expand once more rigorous identity authentication is available for highly sensitive offerings. Any potential offering from the Postal Service should include appropriate and enforceable privacy safeguards to allow the further growth of both eCommerce and new communications applications and enhancements.

Appendices

Appendix A A European Postal Perspective

Key Issues and Outlook

For European posts, authentication is at the heart of the development for eMailboxes and other digital applications, including eGovernment and hybrid (digital-physical) mail options. There is a wide divergence between the authentication systems in use. Final design drivers are based on local circumstances and legislation around eSignatures. If third party identities are valid and useable, they should be considered as an alternative or complement to in-house processes. For example, four Nordic countries leverage the authenticated identities used in the banking system.

- Finland's protocol is the simplest, with users continuing to use their banking ID as a user name or choosing a new username and password.
- Denmark uses the banking identity initially and then changes it to a higher level of authentication.

Switzerland operates two systems: one is fairly straightforward, and the other is unique, where users hold a hard certificate in a token (USB stick).

Market Directions

There is increasing discussion on providing differentiated levels of authentication and credentials based on the level of services accessed. Thus, light authentication could be used for simple eMailbox access, with more rigorous authentication if payment or access to eGovernment services is part of the transaction.

Authentication for eMailboxes and other applications is likely to remain tied to banking applications where possible. OpenID standards are not likely to be adopted unless they are accepted and used by the banking sector.

There is growing interest in using mobile phones as a delivery channel. In addition, European posts are reviewing bio-metric authentication methods. These are currently not proven or used techniques for digital identity authentication.

See Table 1 for detailed information on how authentication is handled by five European posts.

Table 1: Examples of Digital Identity Models in Europe*

Postal Operator	Name of Service	Overview	Verification Method
Post Nord (Denmark)	eBoks	Authentication utilizes banking ID, legal address, and social security number. User name is social security number with self-selected password. One-time scratch code card is delivered to home phyiscal address for multi-factor process.	Online via banking information.
Itella Post (Finland)	NetPosti	Two ways to register: through bank identity or national chip card. Also can register at Post Office.	Online via bank process, utilizing social security number or in-person with issuance of one-time password.
Deutsche Post (Germany)	EPostBrief	Uses Deutsche Post's own "Postident" on-line certification process.	In-person, validated against Government databases.
Poste Italiane (Italy)	Poste mailbox	Uses Poste Italiane's own on-line certification process.	In-person, validated against government tax codes and social security number.
Swiss Post (Switzerland)	Swiss Sign	Online registration and validation against national data bases. Creates legal Public Key Infrastructure-based electronic certificate for digital signature. Certificate offered in computer neutral USB token which authenticates digital signature and allows remote application management and upgrading.	In-person.

*Digital identity processes used for eMailbox registration

Source: Strategia Group and decision/analysis partners, in cooperation with the U.S. Postal Service Office of Inspector General, 2012

Appendix B Commonly Used Terms

Term	Description
AMS	The U.S. Postal Service's Address Management System, which is a proprietary database of all addresses and addresses in the U.S.
Attributes	Descriptions of characteristics; details or components of online identities.
Authentication	The process of establishing confidence in the identity of users or information systems.
Digital Identity	Collection of attributes related to a specific person or organization within a given context, either fact-based or fictional.
Identity Ecosystem	A set of technologies, policies, and agreed upon standards that securely support communications and transactions. Key attributes of the Identity Ecosystem include privacy, convenience, efficiency, ease-of-use, security, confidence, innovation, and choice.
Identity Provider	An organization that issues a digital identity.
Intermediary	Same as Trusted Third Party. See below.
NCOA	The U.S. Postal Service's National Change of Address System is a registry of addresses for individuals, businesses and organizations who have moved or changed addresses in the U.S.
NSTIC	National Strategy for Trusted Identities in Cyberspace, a White House initiative to develop a more secure identity ecosystem, involving public, private, and nonprofit organizations.
OpenID	A decentralized single sign-on solution initially developed in 2005 and under continuous revision. Open ID technology has protocols for attribute exchange among digital entities and uses standard software.
Phishing	An attack in which the user is lured and tricked (usually through an e-mail) into interacting with a counterfeit Verifier or Relying Party and revealing attributes of user identity.
Relying Parties	Organizations that rely on an identity issued by another entity.
Single Sign-On	An authentication process that allows a user to enter one name and password to access multiple online applications from different organizations.
Token	A physical object used to access digital information by an authorized user.
Trust Framework	Certification program enabling a party who accepts a digital identity credential to trust the identity, security, and privacy policies of the party issuing the credential and vice versa.
Trusted Third Party	An entity that authenticates user identity (through verification of attributes) and that is not otherwise participating in the communication or transaction.
Verification	The process of establishing confidence in attributes of users or information systems.

Sources: U.S. Postal Service Office of Inspector General Risk Analysis Research Center (RARC), National Institute of Standards and Technology (NIST), National Strategy for Trusted Identities in Cyberspace (NSTIC).

Appendix C Levels of Authentication

Following are excerpts from the requirements for each of the four levels of authentication assurance as defined by the National Institute of Standards and Technology (NIST):[36]

> …the party to be authenticated is called a *Claimant* and the party verifying that identity is called a *Verifier*. When a *Claimant* successfully demonstrates possession and control of a token to a *Verifier* through an *authentication protocol,* the Verifier can verify that the Claimant is the Subscriber named in the corresponding credential. The Verifier passes on an assertion about the identity of the Subscriber to the Relying Party.[37]

Levels 1 and 2 provide the lightest authentication, which may involve pseudonyms (false names). In most cases, only verified names may be specified in credentials and assertions at Levels 3 and 4:

Level 1
Although there is no identity proofing at this level, the authentication mechanism provides some assurance that the same Claimant who participated in previous transactions is accessing the protected transaction or data. Since identity proofing is not required, names and credentials and assertions are assumed to be pseudonyms.

Level 2
Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information, although the credential may assert a pseudonym. A wide range of available authentication technologies can be employed.

Level 3
Level 3 provides multi-factor remote network authentication. At least two authentication factors are required. At this level, identity proofing procedures require verification of identifying materials and information.

Level 4
Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 is based on proof of a possession of a key through a cryptographic protocol. At this level, in-person identity proofing is required.

[36] National Institute of Standards and Technology, *Electronic Authentication Guideline: Information Security*, Special Publication 800-63-12011, December, 2011, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.
[37] Ibid., p. 17.