Digital ID and eGovernment

Phillip J. Windley, Ph.D.

phil@windley.org
http://www.windley.com

Governments are vitally concerned with identity and yet, paradoxically, most governments have been largely unwilling to take a leadership role in the digital identity arena.

As commonly used, the term "digital identity" refers to a set of properties about an individual that are associated together and available in electronic form. Identities, digital or otherwise, are assumed to be unique. Normally when we talk about identity, we think of people, but that need not be the case. For example, vehicles have unique identities and states go to great lengths to establish and secure those identities in the form of vehicle titles.

When most entities talk about "digital identity" they are more concerned with the properties that the identity has than they are with tying that identity to a specific person. For example, Amazon.com is happy if the identity presented has two specific properties: a valid credit card number with a balanced in the credit limit and a valid address for delivery. The credit card company just cares that the bill gets paid regularly. Even the post office only cares about locations, not the people at those locations.

This is not the case with Government. In almost every case, Government cares deeply that the identity is tied to a specific person. Sometimes this is because that identity is associated with an authorization for that person to perform certain actions in the physical world, like drive a car or practice medicine. In other cases, its because the identity might be used to do something as severe as put take away the person's freedom or even put them to death.

The Driver's License as Identity

The driver's license represents the one of the clearest examples in the physical world of the three functions we associate with identification. In one simple document that you can carry around in your wallet, it supplies:

- **Identity** – the driver's license lists a number of properties about a person that identify that individual, including name, address, and so on.
- **Authentication** – most driver's licenses carry a simple biometric called a picture which can be used by almost anyone to authenticate the license against the individual presenting it.
- **Authorization** – the primary purpose of the driver's license is to indicate what vehicles the government has authorized the individual to legally operate, and under what conditions.

In the United States, the state issued driver's license is, for better or worse, the gold standard for identity. Every other form of ID is an afterthought. You can use

something else to get on a plane or verify your identity when you cash a check, but hardly anyone does.

States didn't set out to create an identity instrument when they created driver's licenses. They were doing exactly what the instrument is called: licensing drivers. But once it had been created it filled a need beyond what it was designed for and was quickly co-opted to a new role: establishing identity. Even now, if you ask the head of your state's driver's license bureau about the driver's license as an identity instrument, they're likely to deny that it has any such purpose.

There are no standards for driver's licenses and they vary widely across the 50 states in what information they convey; some states don't even require a picture. Furthermore, as a rule, states have put more information on the driver's license than what is required to establish an authorization to drive. For example, one could argue that if the sole purpose of the driver's license were merely indicating authorization to drive, the address of the person is irrelevant. In fact, their name is probably irrelevant as well in that case. In truth, the use of the driver's license goes well beyond driving authorization, including information about blood type and even whether or not the carrier wishes to be an organ donor.

Governments and Identity

Governments are vitally concerned with identity. I would argue that identity is a foundational piece of almost everything a government does. Here are some examples of governmental activities that affect or make use of identity.

Vital Records. Governments took over the function of keeping vital records sporadically during the 19th century---mostly for public health reasons. The records that are most applicable to identity are the birth and death certificates. In some states, simply possessing a birth certificate is enough to establish identity for the purpose of gaining a driver's license.

Permitting. Governments spend most of their time authorizing someone to do something or prohibiting someone from doing something. To be effective, they have to know who they are authorizing or prohibiting.

Contracts. Governments have a responsibility for building a set of laws under which commerce can flourish and people can live their lives. Inherent in this responsibility is the need to identify the parties to contracts and other agreements.

Public Safety and Criminal Justice. Governments obviously play a large role in public safety and are the only game in town in the area of criminal justice. Identity is a big part of that. In fact, one could argue that the sole purpose of a trial, establishing guilt or innocence, is largely an identity problem. The police gather a set of properties that are connected with the crime and then the prosecutor tries to prove that the suspect on trial has those properties. Once we have verified the identity of the suspect as the one who actually committed the crime, we lock them away.

Passports. The federal government issues passports to US citizens to verify citizenship. In general function, it is very much like a driver's license. It lists identifying traits and properties, includes a picture for authentication purposes, and authorizes the rights of citizenship to any authenticated possessor.

The Proper Role of Government in Digital Identity

I think its fascinating that even though governments depend on identity as a core component of their activities, governments in the US have, almost universally, failed to take an active role in developing the means to identify citizens in the digital world.

While I believe that governments have a vital and proper role to play in establishing and issuing foundational identity documents, I believe that their role ends there. I do not believe that governments need to be in the business of creating directories or other infrastructures used in the processing or validation of identity other than for their own use.

As part of their duties in establishing the foundation or digital identity, I think states have three key artifacts that they should address: vital records, driver's license, and digital certificates.

Vital Records

As I mentioned before, one of the roles that states play in the area of identity in the physical world is in keeping vital records. States keep vital records in databases, but when you want a copy for your use, they print you out a certified paper copy of the electronic record. At this point, I know of no state that issues birth and death certificates as digital documents. In some states you can view an image of the document on the Internet, but it is not a certified copy that can be used for any purpose other than information. One ought to be able to file a life insurance claim online, for example, using a digital copy of the death certificate and a digital signature.

States should be checking that a birth certificate exists for each driver's license they issue, that only one driver's license has been issued for that birth certificate, and that no corresponding death certificate exists. This is made more difficult by the fact that vital records are stored in each of the fifty states separately and in some states not even stored at the state level but in counties instead. So, when someone applies for a driver's license in one state, the system would need access to the vital records in all fifty states to make a proper check. What is needed is a national clearinghouse for the information. EVital is a Federal program that will link state vital records to the Social Security Administration for the purpose of expediting the issuing of social security numbers and benefits. With such a system in place, using it to validate and verify vital records for other purposes, such as establishing identity, would be a natural evolution.

Driver's License

States need to recognize that the driver's license is an identity card and start treating it like one. We could more properly refer to this as a state ID card, but the moniker "driver's license" has stuck, so we might as well keep using it. Further, the driver's license ought to be based on smart card technology and contain identifying information in some standard format that can be used in a variety of situations to form the basis of identity. One could present their driver's license in an online

transaction the same way that one presents it in the physical world. Of course, some means of authentication besides the picture would need to be used.

I believe that homeland security is going to be a driving force in the use of the driver's license as a national identity document. The federal government is unlikely, for political reasons, to begin a national ID card program, but they could force states to use common standards, including smart cards, that would create a *de facto* national ID card system. For such a system to be useful for things besides homeland security, a broad range of technologists will have to be involved in its creation.

Digital Certificates

No paper on digital ID and eGovernment would be complete without a look at digital certificates. Governments turned to digital certificates and their associated digital signatures early on as a way to solve the digital ID dilemma. In truth, digital signatures have largely failed to deliver on their promise and most have stopped looking to them as a replacement for physical signatures. I think that Government's inability to clearly see its role in providing the foundational structure in digital identity is a significant contributing cause for this failure.

Instead of recognizing the key role that they play in establishing identity in the physical world and then seeking to play a similar role in the digital world, governments turned to commercial entities to create, authenticate, and sell digital certificates (i.e. act as certificate authorities).

I argue that issuing digital certificates is a proper role of Government given the Government's obvious interest in identity and its *de facto* role in identity by issuing driver's licenses, passports, and other identity documents. Even so, no state government has taken on the role of certificate authority. There are a few who are issuing digital certificates to their citizens, but they use a commercial certificate authority to do so.

I believe that this has been one of the primary causes for the spotty use of digital certificates in electronic government and commercial transactions. They are prohibitively expensive in many cases. This expense helps mitigate the risk that certificate authorities assume for misidentifying someone. Governments can (and frequently do) indemnify themselves against such risk and could issue digital certificates that are at least as trustworthy as the state issued driver's license at a very low cost. In fact, such certificates could be routinely issued as part of the process of issuing a driver's license if the license was based on smart card technology.

Conclusion

Governments have long played a role in identity in the physical world, but have abdicated their responsibility in this area for digital identity. In the US we have a healthy skepticism of government identity programs, which is one of the hurdles government involvement in digital identity will have to overcome. Even so, imagine what commerce in the physical world would look like if no driver's license existed and states had never assumed responsibility for vital records. Certainly commerce

would have not come to a standstill, something would have filled the vacuum, but the look of commerce would be very different. Governments have a responsibility to establish societal scaffolding in support of commerce. I contend that the dissonance that we experience by having government serve as the foundation for identity in the physical world, but not in the digital world is partly responsible for many of the problems we face in using digital identity and a significant source of friction in electronic transactions. Serving as the foundation for identity is a proper role for government and we should work to bring it about in the digital world.

About the Author

Phillip J. Windley is a nationally recognized expert in using information technology (IT) to add value to the business. Dr. Windley regularly consults with businesses on this topic. He is particularly interested in the areas of interoperability, web services, XML, and digital identity. Dr. Windley is a frequent author and speaker on these topics and authors a free, daily web-based newsletter at www.windley.com. His web-site contains numerous white papers in these areas and others.

Dr. Windley served from 2001-2002 as the Chief Information Officer (CIO) for the State of Utah serving on the Governor's Cabinet and as a member of his Senior Staff. In this capacity he was responsible for effective use of all IT resources in the state and advised the Governor on technology issues. During his tenure, the State was repeatedly recognized by many national groups for its excellence in the areas of IT and eGovernment.

Prior to his appointment as CIO, Dr. Windley served as Vice President for Product Development and Operations at Excite@Home, managing a large, interdisciplinary team of product managers, engineers, and technicians developing and operating large scale Internet and e-commerce products. Prior to joining Excite@Home, Dr. Windley served for two years as Chief Technology Officer (CTO) of iMALL, Inc. an early leader in electronic commerce. Dr. Windley has been a professor of Computer Science at Brigham Young University and the University of Idaho. At BYU he founded and directed the Laboratory for Applied Logic. Windley received his PhD in Computer Science from the University of California, Davis in 1990. Prior to doing graduate studies, Windley worked for 4 years as a nuclear metallurgist and a member of the technical staff at the Department of Energy's Division of Naval Reactors.

Copyright Information