

ONE ID

Proposed by Ian Nowland

Abstract:

By abstracting and standardizing the information and purpose of identification cards we can increase the convenience of use for all parties involved. More importantly, by standardizing the way ID data is handled, we can provide a drastic increase in the security of transactions.

Overview:

With the increasing importance of information in society, fraud and theft of information have become increasingly important concerns. Management of personal data is a similarly important and difficult job. Standardization of identification can provide a guaranteed level of security at costs that are much cheaper to society than the proliferation of multiple IDs, centralize data to prevent the unchecked spread of personal details while facilitating the accessibility of necessary information, and, using a reference based system, hide personal details from public sight to provide a much greater level of privacy for all parties.

There are two principles behind the ONE ID standard that make it unique. First is the idea that abstracting the purposes of identification cards enables trusted parties to publish them, allowing the publisher to focus on the security of the ID card and allowing organizations seeking forms of identification to outsource that concern. The second is that by centralizing the information associated with an ID we can protect it easier and control where the information gets utilized, preventing ID theft and fraud. Both of these principles are intrinsically related.

The Card:

Nearly every piece of plastic or paper in your wallet other than cash is an ID. The purpose of an ID card is either to provide authentication that someone is who they say they are, or to provide some sort of authorization, associating someone with some quality or data. That quality can be anything from an age given by a date of birth, to a financial account or frequent flyer miles. We can also sort all the information provided by the ID into two different types: direct and indirect. Direct information is present on the card itself, such as a photograph or date of birth, and allows for quick verification by people checking the card. Indirect information is accessed by referencing an account number on the card with a database where the indirect information is contained.

A standardized ID must provide verification of the identity of the owner of the ID, reference indirect account information, and display direct information. Since the information that needs to be quickly verified is different for many organizations, we set aside an area of the card where information can be listed upon request, and have a card that can be reprinted quickly with the updated information. An additional requirement is that it must be difficult to falsify an ID. While indirect information cannot be falsified, since it is not stored on the card, a forged ID could allow someone to fake direct information, such as a birth date. Since security technologies are constantly improving, the security features required in the card are a minimum standard, with allowance for card issuers to improve upon that standard. In addition to these requirements, we must incorporate technologies for computers to read the ID.

In summary, a ONE ID card must contain a method for a computer to read the card's account number, a direct account number a human can read, an area left to the card issuer to print requested direct information, an area left to the card issuer to add additional security features, and some minimum security features, such as a photo.

By standardizing these features, we encourage the printing of IDs by third parties, such as Visa, Mastercard, and American Express. This allows organizations seeking ID to outsource their printing of IDs to ID publishers, and encourages commercial competition for the ID's price, security features, and convenience.

The Data:

Along with the specifications of the physical format of the ID comes specifications for how the indirect data is handled. Without ONE ID, data is distributed and copied in many different locations among many parties; every credit card company keeps a billing address on hand, for instance. In fact, even companies like grocery stores and convenience stores have been issuing IDs and keeping track of information such as addresses and phone numbers. Not only is this system difficult and unnecessary, it is hard to update and very insecure, as personal data is distributed among so many locations. ONE ID takes steps to rectify this situation.

The data must be handled in a way that will centralize the information. Each ID issuing agency is responsible for maintaining a database of indirect information, keeping said information secure, and keeping a list of which data fields different organizations are allowed to access. This puts all the individual's data in a location that is under a known level of security, and in a central location that is convenient for third parties to reference. The owner of the ID may modify which information is available to whom, providing additional privacy. ID issuers are also required not to release individual data except to registered organizations.

Registered organizations are required to not retain past immediate use personal information whenever they access data fields other than the ID number. This means that when information about an individual is needed, the information is referenced from the database, used, and then deleted or overwritten. Since the registered organization can keep a record of the ID number, they can record a transaction while still keeping the details anonymous, by noting that the transaction was with said ID number. There is no need to record further data fields because they can look them up if they need to use them later. In addition, organizations may keep data about individuals, but only in one of two ways: they may add data fields to the database the ID issuer keeps, fields that only they and the individual can view or access, and they may keep a database of their own information about the individual, but it cannot contain any information that is already present in the main database, except the ID number which is used to reference the main database. By only containing the ID number and not the individual's name, the data fields of the organization's database are effectively anonymized. When keeping their own database of information, they must register what fields of information they are tracking on their own with the ID publisher. This keeps the information effectively centralized.

All of this is easiest to understand through examples.

Examples:

Let us say that Alice has an ID issued by Visa. Alice is currently visiting the doctor and needs to present her ID so they can register the doctor visit and update her medical records. She presents her ID, which has the number that all her records are

under. The hospital verifies Alice's identity by checking the photo of her ID and other security features incorporated into the card. Then they check her records. The hospital stores her records, but Visa has a data field under her name for which hospital holds her records, so that in an emergency, a quick swipe of her ID from whichever hospital picks her up and the information will quickly be available. Alice feels safe that her records are confidential, since the hospital doesn't have a name attached to any of those records, only an ID number. Since Visa will only reveal Alice's information to people who are registered to use that information correctly, Alice's information has the benefit of being both secure through anonymity, and yet still quickly accessible. If Alice was to switch hospitals or health care providers, the hospital would either upload Alice's medical records to Visa, or transfer them to another hospital licensed through Visa, with Alice's permission.

From the hospital's perspective, and that of the insurance companies as well, the arrangement is convenient. The personal information is in a conveniently accessible and organized location. In addition, not only can they quickly be sure they are not mistaking Alice for any of their other patients, but they are outsourcing all of their concerns about identification to the ID issuer.

Suppose Bob registers to drive. He goes to his state's DMV and successfully takes the test. His state registers his ID number and adds to his account that he is licensed to drive several classes of vehicles, and that the license will expire at a certain date. There is no need for the state to print a license, since his ID incorporates all the security features they desire, and any police officer can check Bob's driving record with a swipe of Bob's ID. However, for ease of use, the state prefers to have Bob's license type listed as part of the direct information on Bob's ID card. They request the direct information to be added to Bob's ID, and a new card to be printed. Bob can still drive with his current card in the meantime, since the information is in the database. The state also benefits from this arrangement, since they know the latest standards of security are being incorporated into the card by Visa, and they don't have to worry about printing secure identification of their own.

Bob's new card arrives in the mail. In addition to having his driving license visible, it has a different account number. As soon as Bob activates the new card, his old card's number will become useless. Visa will electronically notify all the registered users who keep records of any of Bob's information that the number associated with that information has changed. In this way Bob is protected in case anyone gets hold of his old ID card, and Visa and all the registered organizations are protected from Bob trying to use his old ID to falsify information. A similar process would occur if Bob lost his ID card.

In another example, Bob was just caught speeding, but not in his home state. While some states keep the driving records on their own in a similar way to how Bob's hospital records are kept, his home state prefers to simply add data fields concerning his driving record to his Visa account. The state trooper that has currently pulled Bob over checks his ID, verifying Bob's identity, and looks at the visible information showing that Bob is licensed to drive. The state trooper then swipes the ID and has access to all the information he needs, straight from Visa. He can record the ticket. However, he doesn't need to record the address or any of Bob's personal information other than the Visa ID number. If Bob fails to pay his ticket and the state needs to issue Bob a reminder, it simply references Bob's account to look up the name and address, and then as soon as the reminder is printed, the memory gets overwritten. Bob retains his anonymity except for the actual moment of printing.

To illustrate how the account can be modified, today Alice has just moved to a

new town. She updates her address with Visa. Since everything else checks her address at the time of mailing, that's all she has to do; she doesn't have to change her address with anyone else. After that, she goes to the library, since she enjoys reading. She signs up for an account with her new library. They take her ID number and put an account with it, registering with Visa that they are keeping a record of information regarding Alice's borrowed books, associated with her ID.

As one last example, Bob is making a purchase with his ID. He has previously specified which credit account he wants his ID to pull money from when making purchases from specific vendors. The vendor verifies Bob's identity, then swipes the ID. Visa receives a request from a licensed vendor to make a purchase to Bob's account. Visa then sends the money from the account Bob has specified to the account the licensed vendor has specified. Not only is the transaction entirely between parties Visa trusts (and therefore Bob and the vendor trust) but no financial details are ever revealed publicly. This adds many layers of security to the transaction than currently exist. This also allows credit companies to use further security schemes very easily such as rotating account numbers.

It is worth pointing out that while I have used an ID issued by Visa as an example, Alice or Bob could just as easily have received their IDs from a state that hasn't outsourced this ID printing to third party vendors yet. In this case, the purchase still works, except that the account the state database lists as preferred for making purchases isn't managed by the same agency. Again, none of the financial details are revealed publicly at any time.

Foiling ID Theft:

Now let us say that someone has stolen Alice's ID. They want to use it to make a purchase. They proceed to a merchant and attempt the purchase. Several barriers are present to protect Alice. First, the vendor should first verify that the ID is Alice's. If the photo and other security information doesn't match, it is obviously a stolen ID. If additional security features are present to verify the owner of the ID, such as a pin number that must be typed before Visa will release any of Alice's information, that will also foil the attempt. Since Visa will not interact with organizations who are not registered, and any vendor who swipes IDs that it doesn't verify risks losing their registration, the incentive is for IDs to be checked. In addition, as soon as Alice is issued a new ID, her old ID will become useless, as the account number will be outdated. When the thief tries to use the old ID he will be easily caught.

Another risk is that someone forges an ID with Alice's number, but using a different picture. Just as before, any additional security features such as a pin number would easily stop this attempt at ID theft. This sort of fraud is also easily preventable by having Alice's photo be one of the pieces of information that gets returned from Visa to the vendor. If the photo Visa sends doesn't match the photo on the ID card, the fraud is easily revealed. Again, if the vendor doesn't comply to these basic security standards, they risk losing their registered status with Visa.

The majority of other cases are protected behind the double blind nature of the way the data is handled. In most transactions, Alice's information isn't even present, only his ID number, which is useless to anyone Visa doesn't trust. Anyone Visa does trust still has their accessing of Alice's information recorded, for verifiability. If some of Alice's information is stolen, such as the medical records at her hospital, she is again protected by his ID number: her records are anonymous until Visa verifies which name goes with that ID number, which they wouldn't do unless they trusted the requester. If they suspect an organization's database has been compromised they can

easily issue new ID numbers to all the at risk individuals, effectively randomizing all the information again. All of Alice's personal information is either as secure as her ID issuer can make it, or completely anonymous. Any breach of privacy of Alice's information is also easily accountable for since the data is centralized.

Alice receives the benefits of security, privacy, and convenience from her card, while organizations benefit from a fully secure ID they can trust to verify Alice's identity at every transaction, along with the benefit of centralized information, whenever they need it.

Summary:

Recently, the Real ID act was passed. This act will set Federal standards on driver's licenses, perhaps the archetypal identification today. While this will provide some consistency to identification, there are many advantages we could gain by setting into place a commercial standard. A commercial standard would encourage commercial competition of security features, price, and convenience. In addition, with a commercial standard we can set some rules on data management.

The ONE ID standard is meant to be compatible with driver's licenses, and implemented in such a way that it can be compatible with future Federal standards as well. By specifying minimum features of the identification cards, additional features can be added to make the card compliant with any other standard, and yet still allow room for improvement. ONE ID's format is meant to go beyond physical identification and use the computer science principles of abstraction to extend security beyond just having a card with a photo, and it is past time for it.