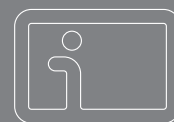


# The Information Card Ecosystem:

## *The Fundamental Leap from Cookies & Passwords to Cards & Selectors*



---

### Table of Contents

- 2 **Introduction**
- 3 **The Cookie/Password Identity Model**
  - Cookies
  - Passwords
  - Identity Silos
  - An Example: Travel Sites
  - Front Channel vs. Back Channel
- 5 **The Card/Selector Identity Model**
  - Information Cards
  - Selectors
  - Providing and Accepting Sites (Identity Provides/Relying Parties)
  - Two Party Relationships (Personal Cards)
  - Three Party Relationships (Managed Cards)
- 8 **Benefits of the Card/Selector Identity Model**
  - Simplicity and Consistency
  - Security
  - Privacy
  - Cross-site Context Sensitivity
- 10 **The Must-Have Benefit: Cross-Site Context Sensitivity**
  - Revisiting the Travel Example
  - Action Cards
  - Password Cards
  - Relationship Cards
  - The Relying Party Awareness Spectrum
- 13 **Living Together in the Information Card Ecosystem**
  - SAML
  - OpenID
  - OAuth
  - XDI
- 14 **Conclusion & Future Work**

### Abstract

The emergence of a long-awaited digital identity layer for the Internet means the evolution from an identity model based on one-dimensional cookies and passwords to a new model based on two-dimensional *Information Cards*. These user-authorized packages of identity data are controlled and managed by a new software tool called a *selector*. The card/selector model gives rise to a new identity ecosystem of card providing sites (*identity providers*) and accepting sites (*relying parties*). It also ushers in a new capability—*cross-site context sensitivity*—that will quickly become an essential feature of next-generation browsing. The paper concludes by looking at the next steps in the evolution of this ecosystem, particularly how it will integrate and adapt to multiple identity protocols.



## Introduction

For over a decade many of the best minds in networking and computer science have wrestled with the requirements and developed new protocols for a digital identity layer for the Internet. This is an extraordinarily difficult task. The layers that exist today—the basic Internet protocol layer<sup>1</sup> and Web content layer<sup>2</sup>—are relatively easy by comparison, since the problems they conquered are primarily technical in nature. But digital identity—how people can prove their identity to Internet sites and applications and authorize sensitive financial, legal, and social transactions—is a much more complex challenge.

At the lower layers, what can be stolen or damaged are primarily bits or pages of information. At the digital identity layer, what can be stolen or damaged are the same credentials a person usually holds in their real-world purse or wallet: proofs of identity, ownership, or membership that are the keys to bank accounts, business accounts, and other highly valuable assets.

These targets attract the same well-financed, organized criminal attacks that take place today against banks, museums, governments, and other storehouses of value in the physical world. For this reason, the industry has been slow to move beyond the basic “cookie/password” model for network identity developed to support e-commerce on the Web. As useful as this model has been, it is now holding us back in much the same way character-based interfaces held us back before the advent of graphical user interfaces (e.g., Mac and Windows).

This white paper details the fundamental leap now happening from the cookie/password model up to a new model represented by Information Cards and selectors. This model does not replace the cookie/password model any more than GUIs replaced command lines, but it will, like GUIs, unlock a watershed of new value for users and businesses alike.

---

<sup>1</sup>The layer based on the TCP/IP internetworking protocol that forms the basic substrate of the Internet.

<sup>2</sup>The layer based on the HTTP hypertext protocol and HTML web page format used by web browsers.

# The Cookie/Password Identity Model

## Cookies

It is hard to use the Internet today without using cookies, yet they remain largely misunderstood by most Internet users. As explained by the Wikipedia article<sup>3</sup>:

*The term "HTTP cookie" derives from "magic cookie", which is a packet of data a program receives and sends out again unchanged. Magic cookies were already used in computing when Lou Montulli had the idea of using them in Web communications in June 1994.<sup>[32]</sup> At the time, he was an employee of Netscape Communications, which was developing an e-commerce application for a customer. Cookies provided a solution to the problem of reliably implementing a virtual shopping cart.<sup>3</sup>*

Essentially cookies enable a Web site to remember the relationship with a particular Web user—anything from the simple fact that the user has visited the site before, to the fact the user has an account filled with preferences, privileges, profile data, and usage history that can be used to richly customize the site.

## Passwords

Whenever a site does remember sensitive or private data about a user, it is critical to protect it by authenticating the user each time they return. To do that, the Web has adopted the same basic authentication mechanism used in most local networks: usernames and passwords.

Essentially your username/password has become the "ticket" to renewing your cookie at most websites today, a dance all of us go through countless times daily.

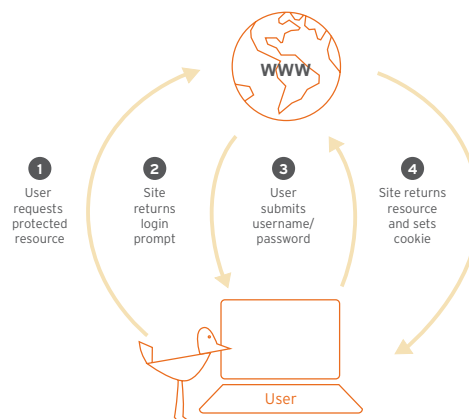


Fig 1: The ubiquitous cookie/password identity dance

Of course, this means the Web also inherited the well-known security and usability problems associated with username/password authentication. What wasn't anticipated is how badly the Web would multiply these problems:

- *Password fatigue*: The sheer size of the Web means suddenly users need an order of magnitude more usernames and passwords than were ever required on a local network.
- *Inconsistency*: The variety of websites and web programming languages means the rules for entering usernames and passwords vary greatly across sites, further confusing users.
- *Phishing*: No one controls the Web, so anyone can try anything to trick anyone else. Many users (and sometimes even professionals) can't tell the difference, leaving us highly vulnerable to sophisticated phishing attacks.<sup>4</sup>

<sup>3</sup>See [http://en.wikipedia.org/wiki/HTTP\\_cookie](http://en.wikipedia.org/wiki/HTTP_cookie).

<sup>4</sup><http://en.wikipedia.org/wiki/Phishing>

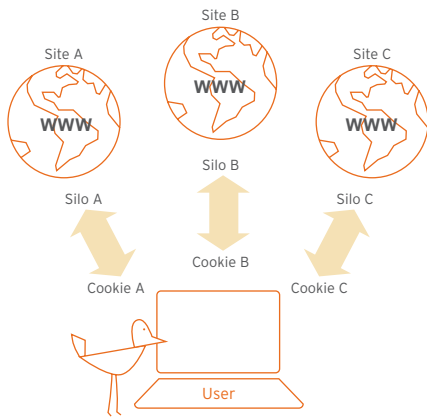


Fig 2: With cookies/passwords, each relationship is its own identity “silo”

## Identity Silos

As bad as the usability and security problems with usernames and passwords are, they are not the primary drawback of the cookie/password model. There is a more fundamental limitation: for security and privacy reasons, each user/site relationship is confined to its own identity “silo”.

The reason: each cookie serves primarily as a key to the user’s data in the site’s own back-end data stores. While each site may store a great deal of valuable data from or about the user, cookies do not provide a mechanism for the user to share that data *across* sites. The user is essentially “starting over again” building a new profile and storing new data at each new website.

## An Example: Travel sites

An example painfully familiar to any frequent business traveler is the experience of researching and booking a trip using multiple Web travel sites.

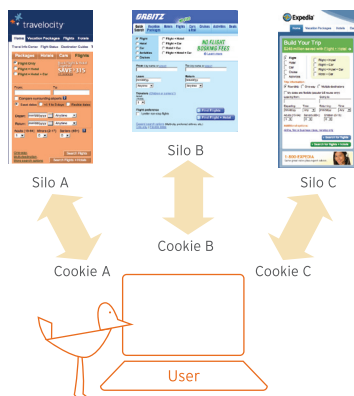


Fig. 3: Each travel site can recognize you are a returning user...but nothing more

You start at the first site, enter all the trip details, and view the results. Then, to see the alternatives available from a second site, you do it all over again. And again and again for each additional site, even though your own context—the trip and its details—stay the same throughout.

## Front Channel v.s. Back Channel

Because the cookie/password model does not directly support sharing data across sites, two workarounds have evolved. The first is for site A to redirect a user to site B, and include special parameters in the URI (Web address) for the redirect. This is called the *front channel*, because it goes directly through the user’s browser, although it is almost always hidden from the user.

The second option is direct data sharing between the website’s own back-end servers, called the *back channel*. This completely avoids the need to involve the user or the user’s browser.

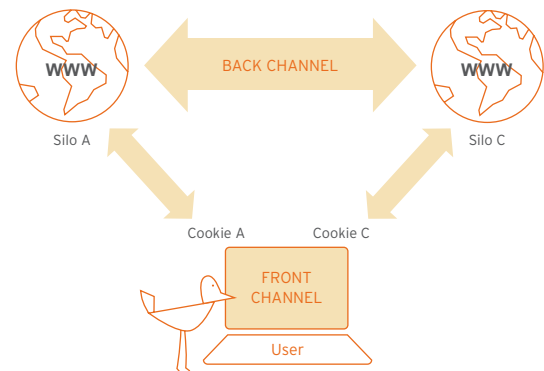


Fig. 4: Front-channel vs. back-channel data sharing

Both methods can work, and both have their own security and privacy challenges (particularly unpermitted back-channels). But the real issues with the cookie/password model are:

- It was never designed for sharing identity data *between* sites, only to track user state at a single site.
- Neither workaround—front channel or back channel—puts the user at the center, understanding and controlling the data sharing taking place.
- The user has no ability to be directly involved, to share identity on their own, without being mediated by a site.

So what would it take to put the user at the center, in control, directly involved? How could identity data flow between sites in a way that was safe, does not threaten the user’s privacy, serves the user’s interests, and lets the user take advantage of the value of data and relationships they have developed in different contexts?

# The Card/Selector Identity Model

The answer is a new model—a model that leaps beyond the cookie/password model the same way graphical user interfaces (e.g., Mac/Windows) leapt beyond the character-based user interfaces (e.g., DOS/Unix command line) that preceded them.

The history of where and how the Information Card model emerged is beyond the scope of this white paper—it is recounted in several other industry publications and books.<sup>5</sup> However we can summarize by saying that the model was pioneered by Kim Cameron and his team at Microsoft, inspired by the set of requirements for Internet-scale digital identity that Cameron labeled the *Laws of Identity*.<sup>6</sup> It has since been embraced and generalized by many others in the industry, including the open source [Higgins, Bandit](#), and [OpenInfoCard](#) projects, and the members of the non-profit [Information Card Foundation](#) (ICF).

The system—technically known as the *Identity Metasystem*<sup>7</sup>—consists of the components and protocols described in this section.

## Information Cards

Information Cards are visual metaphors for digital identities that people use online. Information Cards (capitalized as a proper noun, like “the Web”) are analogous to the physical cards most people carry in their purse or wallet.

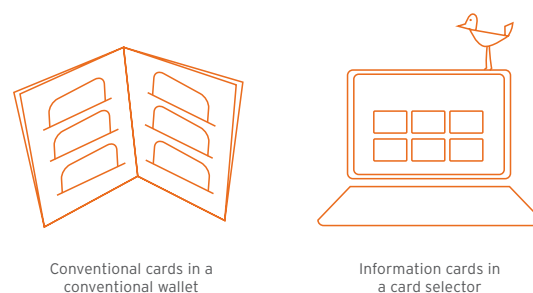


Fig 5: Information Cards are the digital version of physical cards in a wallet

Although the format for the data in an Information Card is standardized—much the same way mag-stripes or bar codes are standardized on ordinary plastic cards—different cards support different kinds of attributes. Attributes can include names, roles, interests, employee numbers, addresses, voter registrations, memberships, age categories, payment information, medical information and almost anything else. Cameron called these attributes *claims* to emphasize that they are assertions made either by the user or by some third party and are thus to some extent equivocal. Cards are themselves XML files that can be offered by card issuing websites, and can be imported into and exported from card selectors (see below).

You can see a variety of Information Cards being offered today by visiting the ICF’s directory of *Featured Card Projects*.<sup>8</sup>

<sup>5</sup> For example, see *Understanding Windows CardSpace*, V. Bertocci et al, Pearson Education, ISBN 0-321-49684-1

<sup>6</sup> Ibid, pp 92-107. Also <http://www.identityblog.com/stories/2004/12/09/thelaws.html>.

<sup>7</sup> [http://en.wikipedia.org/wiki/Identity\\_Metasystem](http://en.wikipedia.org/wiki/Identity_Metasystem).

<sup>8</sup> <http://www.informationcard.net/card-projects>

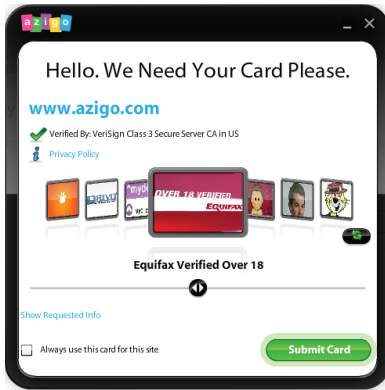


Fig 6: A selector is to Information Cards what a browser is to Web pages

## Selectors

The same way conventional plastic cards are grouped together and guarded in a physical unit such as a wallet or purse, Information Cards need to be grouped together and protected on your computer or mobile device. This application is called a *card selector* (often shortened to *selector* the same way the term “web browser” is shortened to “browser”). The name derives from the action of selecting an Information Card from your set of stored cards to perform an identity transaction just like selecting a card from your purse or wallet to perform a transaction in the real world. In essence a selector is to Information Cards what a browser is to Web pages.

Most selectors are client applications that are triggered by browser plug-ins or capabilities built into the browser. Your selector automatically pops up whenever you need it to login to a site, fill out a form, or authorize a transaction—an experience similar to the integrated password management capabilities of Apple Keychain<sup>9</sup>, except it works across the entire Web.

Selectors are smarter than conventional wallets in many ways. For example they can automatically filter your Information Cards to display only the set that fulfill a particular request. So, when checking out and paying at an e-commerce site, your selector can only show you payment cards, or when scheduling a doctor’s appointment, show you only health cards.

Selectors let you import and export your “cardfile”—your collection of Information Cards. Some selectors store this file on your local device (hard drive, phone, etc.) Other selectors allow you to store it on a USB key, smart card, or other portable store. Still others store it “in the cloud” as a service so you can access the same cardfile from multiple selectors installed on different devices.

You can see listings of the selectors available for different browsers and operating systems today in the ICF’s [Guide to Selectors](#).<sup>10</sup>

## Providing and Accepting Sites (Identity Providers/Relying Parties)

In the card/selector identity model, sites and applications may play either or both of two roles: a) providing Information Cards, b) accepting them. The former is called an *identity provider* and the latter a *relying party*. Together with the user’s selector, these three points form the essential triangle of relationships at the heart of the Information Card ecosystem.

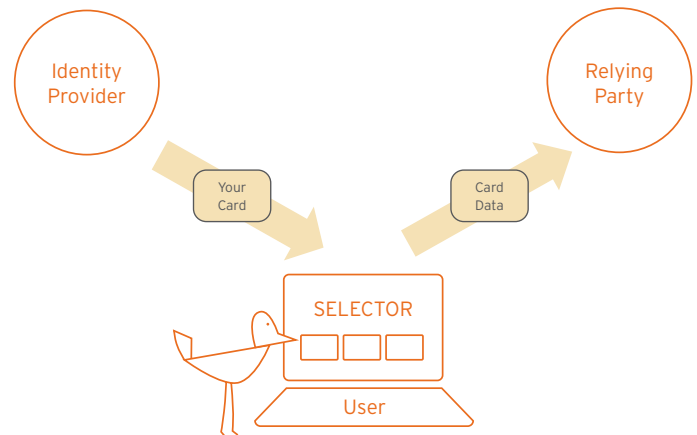


Fig. 7: The essential triangle of relationships at the heart of the Information Card ecosystem

<sup>9</sup> [http://en.wikipedia.org/wiki/Apple\\_Keychain](http://en.wikipedia.org/wiki/Apple_Keychain).

<sup>10</sup> <http://www.informationcard.net/selectors>.

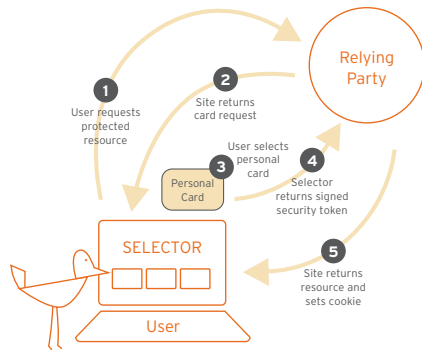


Fig 8: Protocol flow in two-party relationships using personal cards

## Two-Party Relationships (Personal Cards)

To emulate the functionality of the cookie/password model, only two of the three roles are required. This is not surprising—in a “silo” there are only two ends to a relationship.

In this scenario, the Information Card can be provided directly by the user, the same way users provide their own usernames and passwords today. Management and storage of such a *personal card* is handled directly by the selector, and the resulting security token is signed by the user’s own security token service before it is sent to the relying party.

Personal cards may currently include up to 14 standard claims representing the most commonly-requested site registration data: name, email address, telephone number, birthdate, gender, etc.<sup>11</sup> Users can create as many personal cards as they need to represent the different “personas” (packages of personal identity data) they most frequently wish to share.

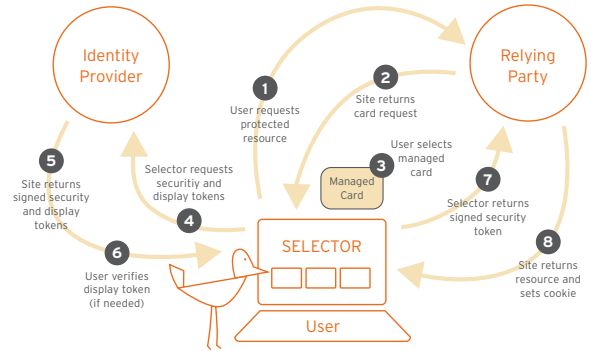


Fig 9: Protocol flow in three-party relationships using managed cards

## Three-Party Relationships (Managed Cards)

Although the card/selector model can add significant value to two-party relationships (see the next section), its real power is in enabling three-way relationships. In this case, the Information Card and claims are provided by a third-party—the identity provider. A user can obtain such a *managed card* from any identity provider willing to offer one. The user can simply visit the provider’s website to download the card (their selector can automatically import and store it), or it can be emailed, included on a disk, etc.

To use a managed card, the selector still receives an Information Card request from the relying party and prompts the user to select a card satisfying the request.<sup>12</sup> However at that point, the selector requests both a signed Information Card security token and a signed *display token* from the third-party identity provider. This Request for Security Token (RST—step 4) must include the necessary authentication token for the user.<sup>13</sup>

The identity provider validates the authentication token and returns the signed tokens (step 5). The selector checks the signature on the display token to verify it, then (if requested by the user), confirms with the user that this is the information he/she wants to share (step 6). If so, the selector forwards the signed security token to the relying party, who can independently verify the identity provider’s signature.

Managed cards may be used to transmit any set of claims data defined by an identity provider and requested by a relying party. Because claims are defined using URIs (the standard identifier for all resources on the Web), it is truly an open information exchange ecosystem usable by any community of sites anywhere on the Web.

<sup>11</sup> Technically they may contain other claims, but these are the ones define in the Identity Metasystem Interoperability Specification V1.0 Committee Draft from the OASIS IMI Technical Committee: <http://docs.oasis-open.org/imi/identity/v1.0/cd/identity-1.0-spec-cd-02.pdf>.

<sup>12</sup> The request can either be encoded as an HTML object tag or an XHTML tag on the relying party’s web page, or it can be described in a linked WS-SecurityPolicy request. See <http://docs.oasis-open.org/imi/identity/v1.0/cd/identity-1.0-spec-cd-02.pdf>.

<sup>13</sup> At present four types of authentication are specified: X.509 certificates, Kerberos, username/password, and personal cards. Using a personal card to “back” a managed card is particularly convenient for users.

# The Benefits of the Card/Selector Identity Model

## Simplicity and Consistency

The first and most obvious benefit of the card/selector model is how it simplifies and standardizes identity transactions regardless of the site, domain, application, or information involved. Some of the world's leading security architects believe this is actually the hardest problem in Internet security.

To quote Ben Laurie, a leader of Google's Caja project<sup>14</sup>, "Ideally, all login should be achieved via a uniform mechanism (i.e. the selector)—regardless of the underlying protocol or transaction." In fact this characteristic of the model was so important that it was Cameron's seventh and final Law of Identity:

*The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.*<sup>15</sup>

The card/selector model fulfills this requirement by providing one standard user ceremony for all types of authentication and authorization transactions. On the Web, this ceremony is always triggered in the same way: clicking the icon representing an Information Card, just as you would click the icon representing an RSS feed or the Search button at the end of a search bar.

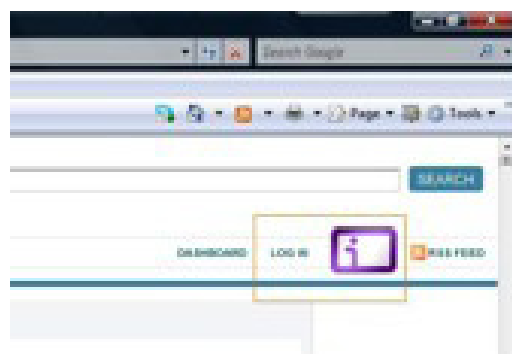


Fig. 10: The standard icon that always triggers an Information Card selector

This click is always followed by the same user experience: selecting the desired card from your selector "wallet" (or being informed you do not have a card with the necessary claims).

<sup>14</sup> [http://en.wikipedia.org/wiki/Caja\\_\(programming\\_language\)](http://en.wikipedia.org/wiki/Caja_(programming_language)).

<sup>15</sup> <http://www.identityblog.com/stories/2004/12/09/thelaws.html>, Law Seven

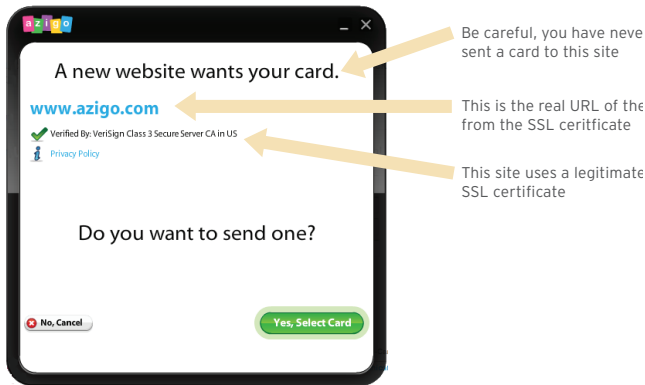


Fig. 11: The user is always alerted the same way when entering a new relationship

## Security

Beyond simplifying and standardizing the user experience, the card/selector model is such an important advancement in Internet security that the subject requires its own white paper (see *Future Work*). However let us at least summarize the main points:

- *Eliminates password fatigue.* Gone is the need to remember or type usernames and passwords for a multitude of sites.
- *Builds in strong anti-phishing protection.* Eliminate passwords and you eliminate the ability for them to be snooped by spyware or phished out of users via all manner of social attacks.
- *Automatic new site warning.* With the plethora of Web login options today, browsers often cannot tell if you already have an account at a site. In fact some sites deliberately obfuscate this to increase security. But selectors actually make it very easy—they automatically warn you whenever a new site is asking for a card, alerting you instantly if you are being phished.<sup>16</sup>
- *Selector-to-user authentication.* The same way you can immediately recognize your own real-world wallet, you can immediately recognize your own selector. This presents an even higher barrier to phishing, pharming, and other social attacks.
- *Built-in strong cryptography.* Some architects consider the card/selector identity model a “GUI for PKI”, i.e., a way of bringing the same type of usability to public key infrastructure that graphical user interfaces brought to command-line PCs. Certainly it sets a much higher bar for the cryptographic protection of common security credentials.

## Privacy

What the card/selector model can do for Internet security it can also do for privacy. For example, a selector can standardize the ability to inspect the privacy policy associated with any Information Card-based data sharing. And it can ensure that all identity data is shared with appropriate confidentiality safeguards in transit.

However, from a privacy perspective, perhaps the most important benefit is that the card/selector model opens an entirely new way to *move identity data sharing to the front channel*. This not only puts the user in control, but makes it fully transparent what data is being shared with whom. User can be confident they are granting the appropriate permissions for the right data to the correct party.

When this new dynamic is established, users won’t “freak out” when personalized services are offered across sites. In fact they will come to expect and demand it, because it may in fact be the most significant benefit the card/selector model has to offer, as described in the next section.

<sup>16</sup> Even if you do submit a card to phishing site, unlike submitting a password it doesn’t give them anything—your selector automatically creates a new security token for every new site, so the phisher can’t use the token they received at the real site.

# The Must-Have Benefit: Cross-site Context Sensitivity

In his widely cited book, *Crossing the Chasm*<sup>17</sup>, Geoffrey Moore asserts that any new technology, to achieve ubiquity, requires a *must-have value proposition*. As powerful as the simplicity, consistency, security, and privacy benefits of the card-selector model are, it might be debatable whether they are "must-haves". After all, the Web is being used today by hundreds of millions of people today who do not yet enjoy those benefits.

But if we stand back and look at the underlying need that originally drove development cookie/password model (as quoted in the Wikipedia cited above)...

*[HTTP cookies were invented by an] employee of Netscape Communications, which was developing an e-commerce application for a customer. Cookies provided a solution to the problem of reliably implementing a virtual shopping cart*

...it reveals that what *really* drove the invention of cookies was solving the Internet shopping problem. People *needed* to share identity data across web pages ("intrasite context") to make e-commerce easier. And that was just across the pages from a single site!

From this perspective, it is much easier to see the breakthrough benefit of the card-selector model: it allows users to easily and seamlessly share identity data *across different sites* the same way cookies let them do it across pages from the same site.

This capability is referred to as *cross-site context sensitivity*. Let's see how it works.

## Revisiting the Travel Example

Recall that under the cookie/password model, a user must re-enter their trip information into each travel site, one by one, for as many "silos" as it takes to book a trip. Even if you login to each site, that site only remembers your trip details at that site. There is no *cross-site context sensitivity*.

Contrast that with: you go to your favorite travel site, click once to login with an Information Card, enter your trip details, and do a search. The site stores your trip details so they are available to you through a managed Information Card from that site.

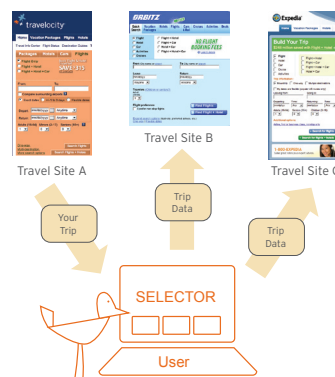


Fig. 12: Cross-site context sensitivity with travel sites

Now you go to the second site, click once to login with that same managed Information Card, and instantly your trip search results are shown to you. No separate username/password, no navigating menus, no entering data. Just results.

And the same for every other travel site that accepts an Information Card with standard claims describing a travel itinerary and preferences (standards that already exist within the travel industry).

Now multiply this experience by every other type of task that takes you across multiple Internet sites. Product research. Technical support. Paying bills. Buying insurance. Movie reviews. Health care. Government licenses and permits. Who would want to browse without it?

<sup>17</sup> [http://en.wikipedia.org/wiki/Crossing\\_the\\_Chasm](http://en.wikipedia.org/wiki/Crossing_the_Chasm)

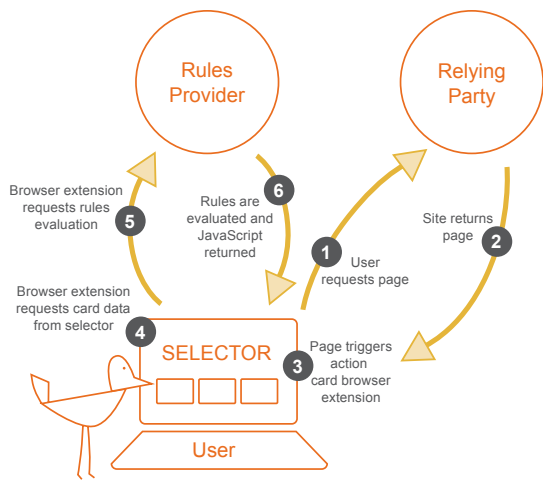


Fig. 13: Action cards use associated rules to augment displayed browser content

## Action Cards

The previous scenarios require sites to become Information Card-enabled before a user begins receiving the benefits. But cross-site context sensitivity provides enough value to overcome this chicken-and-egg problem. In other words, it can add value to your browsing experience *even before sites become card-enabled*. This new niche of the Information Card ecosystem is called *action cards*, and here's how they work.

When you download an action card into an enabled-selector, it comes with an associated set of rules from a *rules provider* that augment your browser display when you visit relevant sites.

Those rules are triggered by the pages you visit.<sup>18</sup> When you load a relevant page, the action card browser extension first requests the relevant card data from your selector, then requests evaluation of the associated rules from the rules provider. The rules provider then returns JavaScript code to the browser extension to augment the page displayed by your browser.

For example, today you can download an action card that reminds you to obtain your AAA (American Automobile Association) membership discount from any merchant offering it. Now when you book a trip at a travel site, for instance, the [AAA Discount Reminder](#) card can automatically pop up a AAA discount reminder *even if the travel site is not yet Information Card-enabled*.

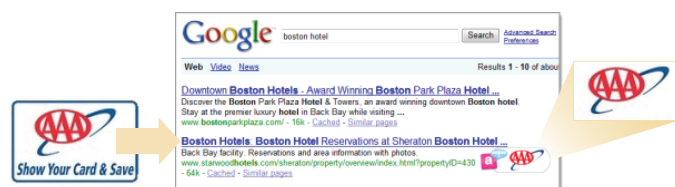


Fig. 14: The AAA Discount Reminder action card

Another groundbreaking action card goes to the heart of one of the most important issues of our time: global warming and the need to restore environmental balance. The [ChoixVert](#) card works with a ruleset developed by [Project ChoixVert](#) and [Kynetx](#) to tell you, as you are browsing, which companies you are visiting are known for their commitment to environmental responsibility.

For details on these and other action cards, visit the ICF's [Featured Card Project](#) directory.<sup>19</sup>

## Password Cards

Earlier we mentioned how the role of a selector is similar to that of an operating-system level password manager such as Apple KeyChain. While the ideal is to eliminate as many passwords as possible, the reality is that for the foreseeable future many websites will continue to rely on them. By incorporating support into the selector for automatic form-filling of usernames and passwords, we provide immediate utility to the user, increasing the incentive to install a selector and making it more attractive for sites to add support for Information Card login.

Legacy usernames/passwords can be securely managed using a special type of action card called a *password card*. While the password-manager function of most browsers—or third-party password manager products—can perform a similar function, the advantages of using a selector include:

- Legacy password management can be integrated into the same simple, consistent user experience as other Information Cards.
- The user's usernames and passwords can be made available on multiple browsers across multiple computers and devices using cloud-based synchronization services.
- A certain measure of anti-phishing protection can be provided.
- Both password cards and other Information Cards can use the same secure store.
- A selector is smart enough to detect when a site/application upgrades to a stronger authentication mechanism, such as an Information Card, and seamlessly migrate the user to this new method.

<sup>18</sup> Technically, they are triggered by URIs that appear on the page or the URI of the page itself.

<sup>19</sup> <http://informationcard.net/card-projects>

## Relationship Cards

Cross-site context sensitivity enables user-controlled identity data to be shared directly and immediately over the user's front-channel. But what if the user wants an ongoing data sharing relationship, i.e., wants to provide the relying party access to a specified portion of the user's data over time—or even automatically push data updates such as a change of email address, postal address, phone number, marital status, etc.?

This is the function of another evolutionary step for Information Cards: *relationship cards*. A relationship card allows user-controlled back-channel data sharing. It adds the metadata necessary for a relying party to access a user's back-end data store via a standard data sharing protocol such as ID-WSF, Portable Contacts, XDI or others. Relationship cards are under active development by the [Higgins Project](#) and should appear on the market in the latter half of 2009.

## The Relying Party Awareness Spectrum

The evolution of action cards, password cards, relationship cards, and other innovative card types means the Information Card ecosystem no longer needs to wait for relying party adoption before it can start to flourish. Rather there is a new way to think about this evolutionary path: the Relying Party Awareness Spectrum.

In the left portion of this spectrum, cards and selectors are delivering value to users before the relying party is even aware of their existence. Unlike a cookie-capable browser, which does nothing for a user unless a site supports cookies, a selector with password and action cards makes an attractive proposition for users.

The right portion of the spectrum shows the steadily increasing value for both the user and the relying party as the latter becomes card/selector aware and supports progressively richer card types. This is the part of the spectrum where network effects kick in, driving the card/selector model towards ubiquitous adoption.

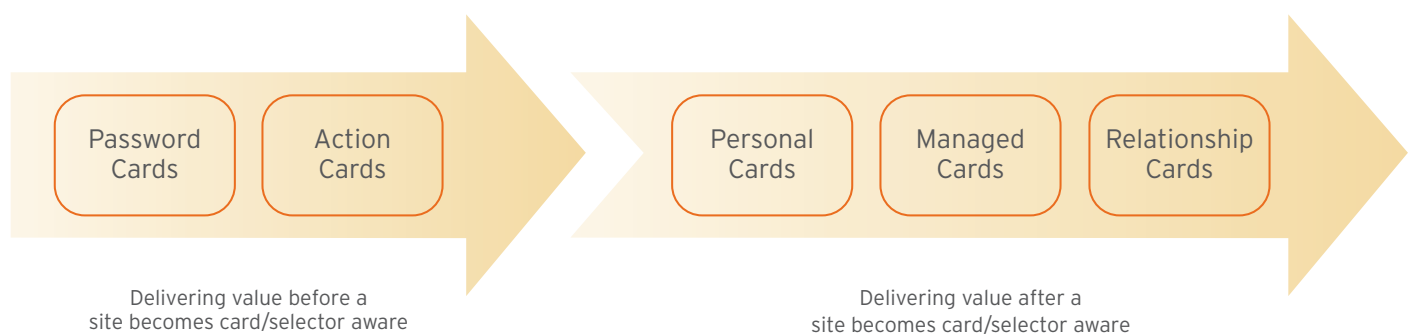


Fig. 15: The Relying Party Awareness Spectrum

# Living Together in the Information Card Ecosystem

New card types are just one example of how the Information Card ecosystem, like any living system, is starting to grow, evolve, and adapt. Although the current Identity Metasystem specifications are based on the WS-\* family of protocols, another key evolutionary step is adaptation and integration of other identity protocols that were not originally designed for the card-selector identity model. Some of these protocols are well advanced in their own evolution, so this is critical to developing a healthy, harmonious system.

Each of these will be the subject of a white paper from Information Card Foundation in the coming months (see *Future Work*); only a summary can be provided here.

## SAML and ID-WSF

The term SAML (Security Assertion Markup Language), refers to the syntax and semantics of SAML XML assertions in security tokens as well as the protocol used to transport those tokens between identity providers and relying parties. Most identity providers, all selectors and most accepting sites and applications rely on SAML security tokens for identity information exchange. Beyond SAML tokens, there is work underway to integrate the SAML (as well as the ID-WSF) protocols “underneath” the Information Card metaphor.

## OpenID

OpenID emerged from the open source community as a lightweight, easily-deployed authentication protocol based on HTTP redirection. With OpenID, users are able to login and exchange basic registration attributes with websites using their own OpenID identifier and password (versus having to register a new username and password at each site).

OpenID and Information Cards are in fact quite complementary. For example, the three weakest areas of OpenID are user experience, security and privacy. These are Information Cards strengths—for instance an OpenID service provider may accept an Information Card instead of a password to authenticate an OpenID user, thereby adding a layer of anti-phishing protection.

For its part, OpenID provides a way for service providers to offer a *Web selector*: a service that makes the user’s Information Cards available via an OpenID account. With a Web selector, a user can still login to relying parties using OpenID when the user does not have direct access to their own client-side selector. Using extensions to OpenID Attribute Exchange, the Web Selector can even exchange attributes security tokens to the relying party.

Conversely, if a user already has one or more OpenID accounts, a Web selector can represent them as a set of Information Cards that can be used with card-enabled relying parties.

## OAuth

OAuth is often characterized as the authorization counterpart to OpenID. Although they in fact have different roots, OAuth does apply the same lightweight, HTTP-based design to distributed authorization, and is often used in the same environments and deployments as OpenID. As with OpenID OAuth is weak in the user experience area, especially in more complex use cases involving delegation. A number of groups are exploring how both the Information Card user experience metaphor and relationship cards can be applied to OAuth.

## XDI

XDI (XRI Data Interchange) is the youngest of these protocols; it is still in development at the OASIS XDI Technical Committee. XDI is not an identity protocol, rather is a special RDF vocabulary and serialization form designed primarily for structured data sharing. This approach is particularly suited to cross-domain semantic mapping, data portability, and authorization portability, so it is a good fit for user-permissioned back-channel data sharing via relationship cards.

# Conclusion & Future Work

## Conclusion

What started several years ago as the Identity Metasystem, the roots of which were in single vendor (Microsoft), has now evolved into a living, breathing Information Card ecosystem with contributions from all corners of the globe. The driving DNA of this ecosystem is the evolutionary leap from cookies and passwords to cards and selectors.

While this sets a new standard for Internet usability, security, and privacy, ultimately the greatest benefit for users and sites alike will be cross-site context sensitivity. As cookies did in the last decade, Information Cards that enable users to safely carry contexts across sites will be the key to the next generation of Internet browsing. This in turn will drive forward the next evolutionary step: integrating other identity and data sharing protocols into the Information Card ecosystem.

## Future Work

The evolution of a digital identity layer for the Internet is a tremendously broad, deep, and vital topic that cannot be encompassed in a single white paper. This is the first in a planned series of white papers from the Information Card Foundation and its members. Other titles currently planned in this series include:

- *Lexicon of the Information Card Ecosystem*
- *The Information Card Security Model*
- *The Information Card Privacy Model*
- *OpenID and the Information Card Ecosystem*
- *SAML and the Information Card Ecosystem*
- *XDI and the Information Card Ecosystem*
- *Action Cards: Safe Web Augmentation with Information Cards*
- *Password Cards: Adapting Information Cards to the Legacy Web*
- *Relationship Cards: Dynamic Data Sharing with Information Cards*

To be informed when new titles in this series are published, please subscribe to the [Information Card Foundation blog](http://www.informationcard.net/blog)<sup>20</sup>, or directly to the White Papers page<sup>21</sup> of the ICF website.

---

<sup>20</sup> <http://www.informationcard.net/blog>.

<sup>21</sup> <http://www.informationcard.net/white-papers>.