# Kid Cards:
# Protecting Children Through Their Parents

**Privo / Denise Tayloe: http://www.privo.com**
**Parity / Paul Trevithick: http://www.parity.com**

**ABSTRACT**
This paper describes a system wherein parents register information about themselves and their children at a website. The site generates an electronic, visual "kid card" for use by the child. The child holds this card in an electronic "wallet" and uses the card to access age-restricted content areas. The child's parent is given notice of the child's attempts to enter these areas and provided with a web based control panel to manage the child's access rights. The parent can control which sites the child can access as well as which functions (e.g. chat, uploading images, etc.) are allowed on that site.

**Keywords**
Filtering, searching, identification, verification, parental controls, identity management, information cards.

**Functional Goals**
This solution is able to:
☑ Limit harmful contact between adults and minors
☐ Limit harmful contact between minors
☑ Limit/prevent minors from accessing inappropriate content on the Internet
☑ Limit/prevent minors from creating inappropriate content on the Internet
☐ Limit the availability of illegal content on the Internet
☑ Prevent minors from accessing particular sites without parental consent
☑ Prevent harassment, unwanted solicitation, and bullying of minors on the Internet
☑ Other – allow parents to continuously monitor and control their children's access to Internet content

**PROBLEM INTRODUCTION**
1. Children have access to many sites that bring them into contact with malicious adults. To reduce that threat, some of these sites would like to create age-restricted areas. However this requires being able determine the age of site visitors with reasonable assurance while staying in conformance with applicable law. The proposed solution fulfills this requirement by allowing the site to gate access to participants who are either too old (e.g. adults) or too young (e.g. still younger children) to these areas. It does so by requiring the child to use an Information Card (i-card) to log in the site (or a specific area of the site). This technology conveys through a secure channel to the site a set of claims about the child (e.g. their age or age range) that have been asserted earlier by the child's parent or another responsible party.

2. A related problem is that many parents need to be able to selectively restrict their child's access to entire websites or to certain functions (e.g. chat or posting images) at a website. The proposed solution permanently and securely links the child's i-card to a parental control website that enables the parent to manage such permissions.

**PROPOSED SOLUTION**
The solution builds on i-card technology as shown in Figure 1. For readers unfamiliar with i-cards, a primer is provided in the next section.

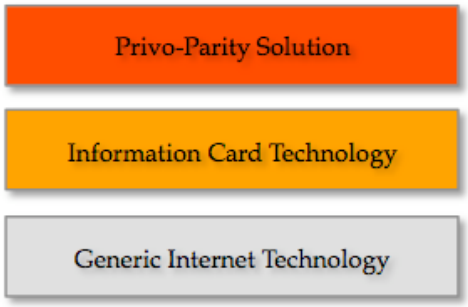


*Figure 1, Solution Layers*

**Information Card Primer**
I-card technology is based on a set of network protocols (e.g. WS-Trust) and security token data formats (e.g. SAML 1.1). These standards are the key to i-card inter-operability, and have been made available on an open, royalty-free basis. All commercial and open source i-card software relies on these protocols to achieve interoperability. In June 2008 the Information Card Foundation [1] was launched by leading implementers of i-card technology including Microsoft, Google, PayPal, Equifax, Novell, and Oracle.

I-cards are enabled by a new component called an *identity selector* (Figure 2) that must be integrated with a user's browser on their computer or mobile device. This selector acts as a kind of digital wallet holding a set of visual i-cards. Both commercial and open source selectors are available today in versions compatible with IE, Firefox and Safari browsers and compatible with Microsoft Windows™, Apple OSX™ and Linux operating systems. The CardSpace™ [2, 3] selector ships with Microsoft Vista™ and has been available since early 2007. Other commercial selectors are available from Novell (DigitalMe™ [4]) and will soon be available from Parity

(Azigo.com™ [5]). The latter two are based on the open source Eclipse Higgins code base [6].

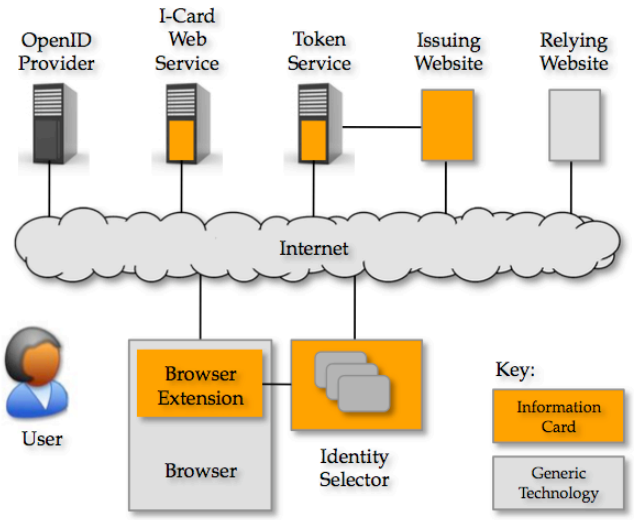


*Figure 2, Information Card Components*

Some Higgins-based selectors (e.g. [5]) rely on a hosted I-Card Web Service as shown in Figure 2 that, among other things, synchronizes cards across a single user's multiple browsers and devices. If the user has an OpenID or i-name they can use it as their master selector account name and master password.

Cards are issued by an Issuing Website as shown in Figure 2. This site makes them available to users as downloadable links. Issuing sites also implement a Token Service that generates security tokens as requested by the selector when the user attempts to use the issued card at a relying site. Commercial Token Service offerings have been announced by IBM Tivoli [7], and others.

The Relying Website is a website that is capable of accepting i-cards for sign in, payment, age verification, or other purposes. Two small changes are required in the site. First the site must add a few lines of HTML to their site that indicates the set of attributes, called *claims*, required by the site. Second, the site must be able to validate a security token when it is posted to the site via the user's browser and selector.

### *Generic I-Card User Experience*

In brief, the relevant user experience involves the user: (1) downloading or activating an i-card selector to work with their browser, (2) downloading i-cards from card issuing sites into the selector "wallet", and (3) visiting relying websites where the user simply clicks on an icon to open up their selector and display the set of cards the site will accept for the resource the user is trying to access. The user selects the card they wish to use, and a secure, digitally-signed token is transmitted to the site to grant the user access.

Just as a browser can read web pages from any web server, a selector can collect cards from any card-issuing website. At each site, the user is authenticated and his/her claims verified using whatever method that site chooses to employ. Once satisfied, the site generates an i-card that the user imports into their selector by clicking a download link.

In the case of the *managed* i-cards discussed here, it is important to understand that the card itself contains only metadata (a description of other data)—not the actual claim *values*. The managed card is an XML document with elements that include the name of the card, the background image of the card, and the set of the types (but not the values) of attributes supported by the card and its associated token service endpoint. A card could, for example, indicate that it supports the claim types of first name, last name, postal code, and email address. More to the point, the card might hold a claim type whose Boolean value is the truth of the statement that the card holder is less than 16 years of age.

Instead of relying on usernames, passwords and form filling, sites that accept i-cards rely on digitally signed tokens provided by the user's selector. To request such a token, the site displays the standard icon shown below on the home page (or any other page where data is needed).

*Figure 3, Information Card Icon*

When the user clicks on this icon, their i-card browser extension retrieves an HTML or XML description of the site's policy specifying the set of required and optional claims it needs. The browser then opens up the user's selector in a window showing only the card(s) whose set of supported claim types is the same set (or a superset) of the claims requested.

The user selects one of the cards by clicking on it and authenticates to the card as required (e.g. by entering a PIN). The selector sends the authentication materials to a token service (typically co-resident with the data systems supporting the card issuing website). The token service returns a token that is signed using encryption keys derived from the SSL domains of both the relying site and the issuing site. The selector then POSTs this token to the relying site.

For example, if the relying site had requested a Boolean claim as to whether the user was less than 16 years of age, and the user selected a card that supported this claim type and the user was properly authenticated to submit it, then the relying site would receive that Boolean value in a digitally signed token from the issuing site. By verifying the signature, the relying site can now trust this assertion to the extent that it trusts the issuing site.

**Privo-Parity Solution**

We will describe the solution from a user experience point of view, review some key technical details and then provide more business-related highlights and issues. For brevity we will simply refer to *parent* instead of saying "parent, guardian or other responsible adult."

*User Experience*

The parent creates an account on the Privo Website, as shown in Figure 4, where detailed personal information can be entered and verified using traditional methods. The parent also creates a set of records for each of their children. These linked child records include identifying information about the child such as name, date of birth, etc.

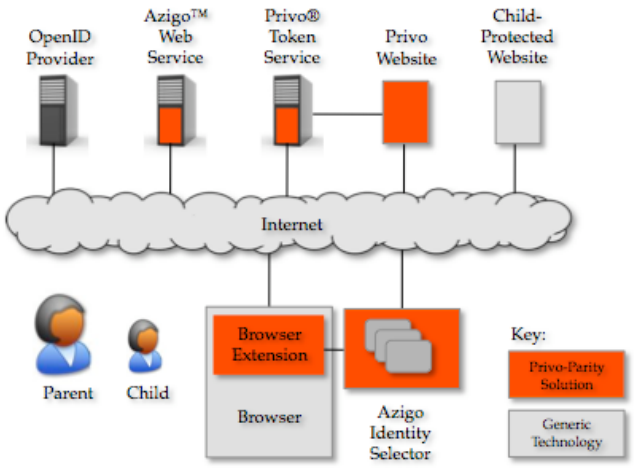


*Figure 4, Privo-Parity Solution*

Once the parent is registered and creates an account for the child, the child can go to the Privo site and populate that account by entering their permitted attributes. These values are used to link their account to their parent's account. The site displays a visual PrivoCard™ for Kids that the child can import with one click into their selector. If the child does not already have a selector, the parent or child can download and install one for them.

If a social networking site such as MySpace [8] were to become i-card compatible, the site would display the icon/button shown in Figure 3 at any page gating entrance to age-restricted areas. When the child clicks on this icon, the selector appears and the previously issued "Privo Kid Card" will be displayed within it[1]. The child clicks on this card and enters their personal PIN number to unlock it. If the parent, using the parental controls section of the Privo site, has designated that this child should have access to this area of MySpace, then the child is granted access.

*Technical Details: Linking Parent and Child*

The heart of the solution design lies in the interactions between the Privo Token Service and the Privo Website. The parent's account on the Privo site not only provides the linkage between their own identity and that of their children, but also provides a rich set of parental control pages that indicate at a coarse level what sites a particular child may enter, and at a fine level what functions and/or areas (e.g. chat, image galleries, etc.) the child may access within the site. We consider now the detailed sequence of steps when a child called Johnny clicks on the i-card icon on the hypothetical MySpace site.

As described earlier, behind this icon is MySpace's policy describing the set of claims it requires in order for a visitor to enter. We'll assume for this example there is a section of the site appropriate only for children less than 16 years old. Embedded in the page containing the i-card icon would be a special object tag that contains a parameter whose URI would be "age-less-than-16".

After Johnny's selector displays the Privo Kid Card and Johnny clicks on it and enters his PIN, the selector requests a token from the token service associated with the card. We will assume that the WS-Trust protocol is being used between the selector and the Privo Security Token Service (STS). Johnny's PIN number, along with the set of MySpace-required claims, the relying site domain, and other information is sent in a *Request for Security Token* (RST) message to the STS.

The STS is linked with the account records at the Privo site. If this is the first time that Johnny has attempted to enter this section of MySpace, then the parent is notified (e.g. via email or IM) of the attempt. This notification will include a link to the parental control page for Johnny. The parent can choose to approve access to this site and specify permissions for specific areas or functions of the site. The parent's preferences and approvals, along with the values of the age-related Boolean claim, are encoded as the values of the claims in a SAML token that the STS signs and returns to the selector as its *Request for Security Token Response* (RSTR).[2]

The selector then POSTS the token to MySpace, where it is validated and used to allow or disallow access to pages and functions of the site.

[1] If this is the first time an i-card icon has been clicked on in the current browser session then the child may, depending on security settings and preferences, have to enter a "master" password before the selector window will appear.

[2] If parental notice and consent had not already been set up, the original RST message would time out and Johnny would be told in a message box to try again later after his parent has had a chance to respond.

*Other Considerations*

On the Internet today, there is no standard way to convey *verified* claims about yourself. Typing self-asserted data entered into forms is the coin of the realm. Among the consequences are: (i) An entire generation of children have taught themselves to lie about their age to gain access to restricted content, and (ii) predatory adults can easily claim to be children. In this paper we have proposed a solution, but there are barriers to adoption:

- For the solution to be *used*, parents must register themselves and their children at sites like privo.com. In most cases they will also have to download and install an identity selector (although over time this will less frequently be the case).
- A large-scale public relations/evangelism effort is required to build awareness that such a solution exists.
- Although Privo has already been providing the core capability of the solution described here to major corporations, many people are still unaware that such a solution is possible within the existing legal regimes (e.g. COPPA, etc.)
- Relying websites must become comfortable with the underlying i-card technology, which is relatively new.
- Despite a thriving ecosystem around the technology, the adoption challenges facing any Internet-scale technology are large, and we are at the beginning of a multi-year adoption curve.
- We believe that the direct financial costs to relying websites (e.g. social networking sites) of implementing this solution are affordable, however it is unclear if there is sufficient legal and/or social pressure to motivate them to implement solutions such as the one described here.

## COMPANY OVERVIEW

Privo, founded in 2001, is a privately held corporation based in Northern Virginia servicing Fortune 1000 companies and nonprofits in their efforts to comply with existing federal children's privacy legislation and social or legal pressure to obtain parental consent. Denise Tayloe, a founder and the CEO, has been a leader and industry expert in the consultation, certification and the development of child-protection technology.

Parity, founded in 2000, is a privately help corporation based in the Boston area. Parity is in private beta test of its Higgins-based Azigo hosted identity selector. Paul Trevithick, is Parity's CEO, the chair of the Information Card Foundation, and the founder of the Higgins project and participates in several other projects related to Internet identity.

## BUSINESS MODEL OVERVIEW

"Privo Kid Cards" require a level of underlying identity verification and/or vouching. The existing PrivoLock™ applications are consumed and paid for by organizations which have a social need or legal requirement to process verifiable parental consent. The "Privo Kid Cards" are available as an option as part of the PrivoLock approval process. The "Privo Kid Cards" are also available as an option for parents to purchase through the registration process of the Protect My Child Registry™. "Privo Kid Cards" will be available for purchase towards the end of 2008.

Parity's Azigo selector is a downloadable browser toolbar and hosted service that will be freely available to anyone. Azigo provides one convenient place to control a person's online identity and relationships. Since Azigo is entirely controlled by the personal account holder, e-merchants and other websites will pay Azigo (Parity) to create and maintain high-quality relationships with their customers.

## CONTACT INFORMATION

Denise Tayloe Denise Tayloe of Privo may be reached at dtayloe@privo.com or at (703) 932-4979.

Paul Trevithick of Parity may be reached at paul@parity.com or at (617) 513-7924.

## CERTIFICATION

The authors certify that they have read and agree to the terms of the Internet Safety Technical Task Force Intellectual Property Policy.

## REFERENCES

1. Information Card Foundation. Available at http://informationcard.net/.
2. Microsoft CardSpace. Available at http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx/.
3. Bertocci, V., Serack, G., and Baker, C., Understanding Windows CardSpace. Addison-Wesley, 2008.
4. Novell DigitalMe. Available at http://www.bandit-project.org/index.php/Digital_Me/.
5. Parity Azigo. Available at http://azigo.com/.
6. Eclipse Higgins. Available at http://eclipse.org/higgins/.
7. IBM Tivoli Federated Identity Manager. Available at http://www-306.ibm.com/software/tivoli/products/federated-identity-mgr/
8. MySpace: http://www.myspace.com