

A One-Page Introduction to Windows CardSpace

Michael B. Jones, Microsoft Corporation, January 2007

© 2007 [Microsoft Corporation](#). All rights reserved.

Many of the problems facing the Internet today stem from the lack of a widely deployed, easily understood, secure identity solution. Microsoft's Windows CardSpace software and the "Identity Metasystem" protocols underlying it are aimed at filling this gap using technology all can adopt and solutions all can endorse, putting people in control of their identity interactions on the Internet.

One problem people face is knowing whether they're at a legitimate web site or a malicious site. This is an identity problem: a problem with reliably identifying authentic sites to their users. People also face numerous problems in identifying themselves to the sites they use. Username/password authentication is the prevailing paradigm, but its weaknesses are all too evident on today's Internet. Password reuse, insecure passwords, forgotten passwords, and poor password management practices open a world of attacks by themselves. Combine that with the password theft attacks enabled by counterfeit web sites and man-in-the-middle attacks and today's Internet is an attacker's paradise. CardSpace is part of the solution to all of these problems.

The Windows CardSpace software enables people to maintain a set of personal digital identities that are shown to them as visual "Information Cards". These cards are easier to use than passwords. Furthermore, they employ strong cryptography, making them significantly more secure than passwords and other information typed into web forms. There are three participants in any digital identity interaction using CardSpace:

- **Identity Providers** issue digital identities for you. For example, businesses might issue identities to their customers, governments might vouch for the identities of their citizens, credit card issuers might provide identities enabling payment, online services could provide verified data such as age, and individuals might use self-issued identities to log onto web sites.
- **Relying Parties** accept identities for you. Online services that you use can accept digital identities that you choose and use the information provided by them on your behalf, with your consent.
- **You** are in control of all these interactions. You choose which of your digital identities to have and which to use (or not to use!), at places where they are accepted.

Windows CardSpace and interoperable Information Card implementations by others enable the Internet to move beyond sole reliance upon username/password for sign-in. By using Information Cards, people will no longer need a username/password pair for every web site they log into. Because no passwords are used, they no longer need to be remembered, won't be reused between sites, and can't be stolen and used by others for fraudulent purposes.

Beyond being used to log into sites, Information Cards can also facilitate other kinds of interactions. The Information Card model provides great flexibility because cards can be used to convey any information from an identity provider to a relying party that makes sense to both of them and that the person is willing to release. One possibility is online age verification, with identity providers providing proof-of-age cards, and relying parties accepting them for purposes such as online wine sales; other attributes could be verified as well. Another is online payment, where merchants could accept online payment cards from payment issuers, containing only the minimal information needed to facilitate payment.

Microsoft's Windows CardSpace software is based on open communication standards and interoperates with numerous components built by others, both for Windows and for other platforms. Together, these implement an interoperable "Identity Metasystem". CardSpace can be used to provide identities both for web sites and Web Services applications. CardSpace is Microsoft's contribution to a widely accepted, broadly applicable, inclusive, comprehensible, privacy-enhancing, security-increasing identity solution for the Internet.

For more information, see <http://cardspace.netfx3.com/>.

