

Windows CardSpace Information Cards and secure2trust



 info@avocosecure.com

US: +1 415 839 9433

International: +44 207 851 6070

www.avocosecure.com

© Avoco Secure 2009 - All rights reserved.

Avoco Secure Ltd

Windows CardSpace¹ provides a type of information card in the form of a software token, that is used as a method of digital identity.

Windows CardSpace information card is a client application that comes pre-installed with the Windows .NET 3.x Framework. The information card runs on the desktop as an identity selector for CardSpace Cards created or issued

Windows CardSpace information card is based on an identity meta-system, architecture consisting of:

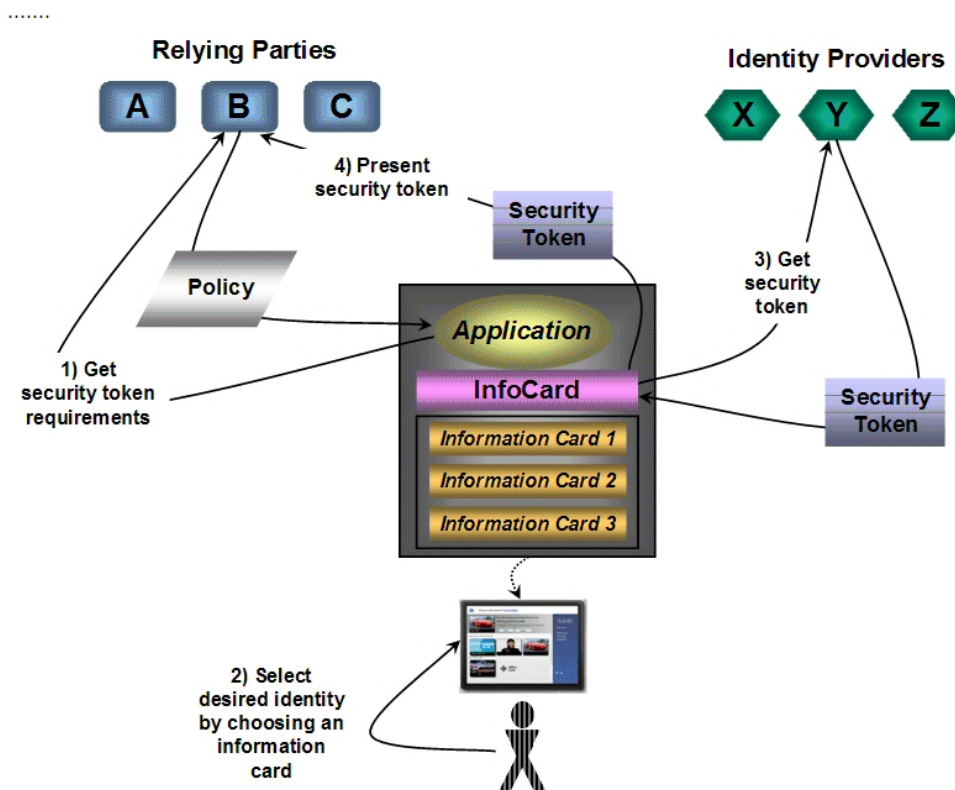
1. Identity Providers (companies who issue cards to their customers, employees, *etc.*)
2. Users (individuals who have a card issued that they can they use as their identity to log onto websites, *etc.*)
3. Relying parties (applications, services and similar that use an identity to authenticate a person to then authorise an action such as logging onto a website, accessing a documents, *etc.*)

A Card is either issued by the Identity provider to a user, or a user can self-issue a card. Each card holds a number of 'Claims' associated with that user which are subsequently used to identify them when the card is used. These claims include identifiers such as name, email address, *etc.*

When a user needs to use a card with a supporting application (relying party) to access a resource (such as a secure2trust protected document or a website that supports logon through information cards) the CardSpace desktop interface opens and the user can choose a card to identify themselves. The information in the card is sent to the relying party over a secure SSL connection and the software token is encrypted to ensure that the user's identity is secured. If the relying party successfully authenticates the user's identity, then an authorisation policy associated with the relying party application or service, is invoked and the user can gain access to the resource (website, documents, *etc.*).

¹ More information on Windows CardSpace Information card can be found here:
<http://www.microsoft.com/windows/products/winfamily/cardspace/default.msp>

Overview of CardSpace Identity Meta-System



Source: Microsoft

Information Card Types

Information Cards can be either:

- Personal – self-issued by the user on their desktop
- Managed – issued by a trusted third party such as a company, bank, etc.

Managed cards are a much more secure and controllable method of using information cards, because the cards are created and managed by a central, trusted, issuing party who can verify an individual's identity, rather than created by an individual. In addition, the issuer can associate any claim with the card, for example, employee number, department, security clearance level, etc. making the card more relevant to its purpose.

The claims associated with an issued card are managed and owned by the 'authority' which is the company that supplies the cards. The claims are managed and controlled by this authority and as such, can be changed and revoked as required, providing, potentially a mechanism for changing and revoking policies associated with resources such as websites and documents.

Issuing Information Cards based on the Windows CardSpace Selector

Information cards based on Windows CardSpace, can be issued by any organisation that provides a method of obtaining a card (e.g. an appropriate website) and a Security Token Service (STS) that can handle requests made by the Microsoft WS-Trust protocol to return an encrypted and signed token.

Avoco Secure provides a toolkit that allows a trusted party, such as a bank, etc. to issue information cards. For further details please see our demonstration site here:

<https://www.secure2cardspace.com/>

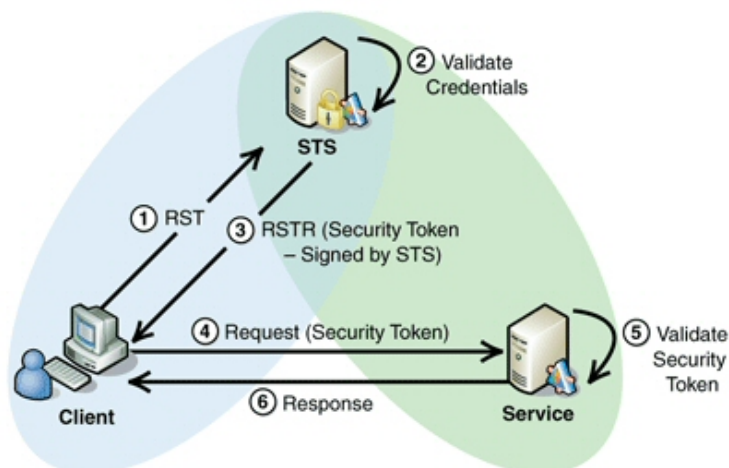
To issue an information Card, the Issuing party must set up a website that allows any required Claims to be presented by the user, or to be associated with the user by the issuing authority itself. These claims form the basis of that users information card.

The STS acts as a brokered authentication service to check the user's claims and to provide a security token to prove the user has been authenticated with the STS. The client presents this security token to the web service, which in turn checks that the token was verified by the trusted STS as authenticated.

The security tokens are encrypted and communicated *via* SSL.

Overview of Architecture for Managing Windows Information Cards

1. Client – this is the Windows CardSpace application on the desktop
2. STS – this is the web service that validates the claims presented by the client and once authenticated, generates a security token
3. Service - this is the web service that requires authentication of the client (*via* the security token) to authorise the user

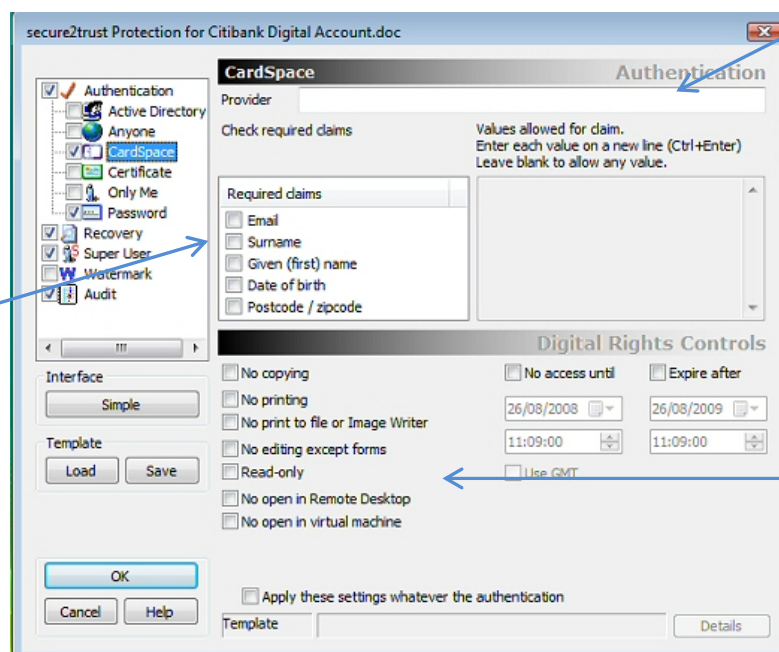


Source: Microsoft

Using Windows CardSpace Information Cards with secure2trust

secure2trust (the relying party) allows you to protect documents so they can only be accessed by a specified Windows CardSpace Information Card/s. You can also specify a security policy that is then associated with a document accessed by a specific information card user: For example, preventing a user from copying or printing content from a document.

To set access to a document to be controlled using a Windows CardSpace information card, you will need to choose **CardSpace** using the secure2trust authentication options menu and choose the claims associated with that information card holders card. If the card is a managed card, issued, for example, by your organisation you can specify that only a card issued by a certain provider (for example, your organisation) can be used for access, thus increasing the security of the access control. In addition, if your organisation has issued the card, then if you revoke that card, access to the document will also be revoked.



Enter the url of the card issuer to ensure only this issued card is used for access

Set the CardSpace claims you wish to match up to control access to the document

Set a security policy to be applied if access is successful

Receiving a Document Protected To Allow Access Using a Specified CardSpace Information Card

The following steps show the process when accessing a document protected with a users Windows CardSpace information card: In practise this process takes seconds to complete.

Step 1

User receives a document (by email, across a network, *via* a datacenter, through the Cloud, *etc.*) that has been protected so that it can only be accessed with a specified users Windows information card.

Step 2

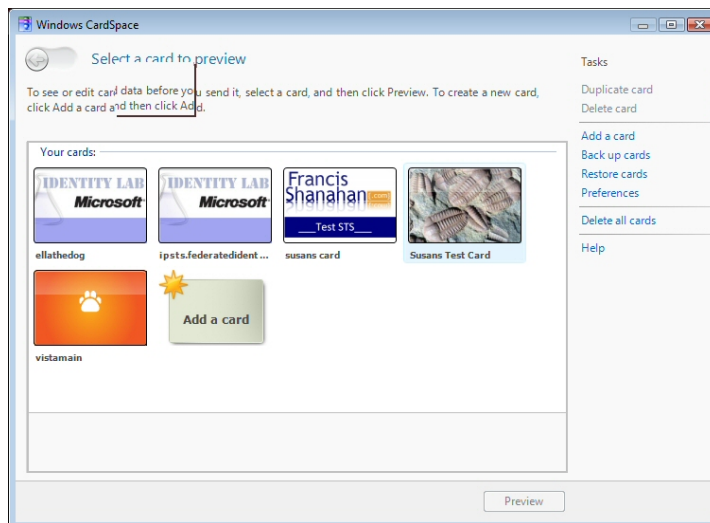
User attempts to open the document in the usual manner

Step 3

On attempting access, secure2trust (relying party) asks for the user to supply their CardSpace information card

Step 4

This opens the Windows CardSpace user interface:



The user chooses the correct card from this interface and clicks **Send**

Step 5

Clicking Send initiates a request to the card issuing authority (the issuer) to return a secure token representing the claims within the card

Step 6

The token is returned and secure2trust checks the token against the claims specified when the document was protected. If they match, the document is opened and any associated security policy on how the document can be used is applied.

Using Windows CardSpace Information Cards to Control Access to Documents

