

## **Virtual Credit Card Numbers and Managed Information Cards**

Bob Pinheiro  
Robert Pinheiro Consulting LLC

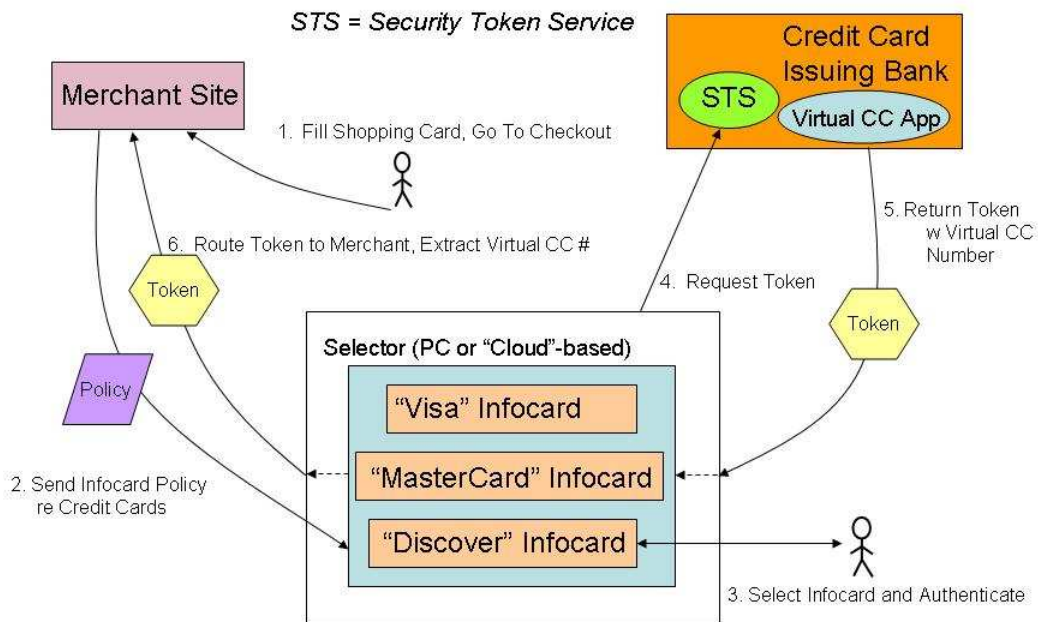
There's a lot in the news these days about data breaches. When those breaches involve credit card data, there's the potential for someone else to put charges on your credit card. The credit card companies have come up with one solution to this problem in the form of “virtual” credit card numbers, which is a temporary random number that substitutes for your real credit card number. Once the number is used to pay a particular merchant, it can't be used by anyone else. So if there's a data breach and a virtual credit card number is stolen, it doesn't matter because the thief can't use it.

But virtual credit card numbers are a bit cumbersome and inconvenient to use, so they haven't gotten much traction. Only a handful of banks offer them. Users first must login to their banking website to generate the numbers, or login to a previously installed application on their PCs to generate the numbers. Then the virtual credit card information must be copied or dragged to the proper places on the merchant's checkout page.

Managed Information Cards<sup>‡</sup> could potentially serve as a consumer-friendly delivery vehicle for virtual credit card numbers. The following diagram illustrates how this might occur:

---

<sup>‡</sup> A good introduction to Information Cards can be found at  
<http://informationcard.net/user-information-center>



1. A user visits an online merchant and wants to make a credit card payment. The merchant's checkout page displays a new payment option that says something like "Use A Secure Electronic Credit Card."
2. The user clicks on the icon for making a secure electronic credit card payment. The merchant's site sends its Information Card policy to the user's Selector, which is a kind of digital wallet that holds the user's various Information Cards. The policy says something like: "I will accept the following credit cards: MasterCard, Visa, Discover Card."
3. If the user's Selector contains a managed Information Card that represents one of these accepted credit cards, the Selector highlights and displays the appropriate Information Cards, and the user selects one. The user then enters a PIN or password to unlock the card.
4. An authenticated request is sent to the Security Token Service (STS) at the user's bank for the issuance of an electronic "token" containing a virtual credit card number and associated information (name, expiration date, security code).

5. The virtual credit card information is generated by an application at the bank that is interfaced with the STS, and the STS generates the electronic token incorporating the virtual credit card information. The STS returns the token to the user.
6. The token is routed by the user to the merchant's site. An application at the merchant's site opens the token, extracts the credit card information, and populates the appropriate fields on the checkout page.
7. At this point, the credit card payment fields on the checkout page are populated with the virtual credit card information, just as if the user had manually obtained this information without the use of Information Cards. The user proceeds with checkout as usual.

#### Potential benefits to merchants, users, and credit card issuers:

- If there is a data breach at the merchant's site and virtual credit card information is stolen, the virtual credit card numbers cannot be used by a thief to post fraudulent charges to the user's credit card account.
- A merchant that accepts virtual credit card numbers (with or without the use of Information Cards) has a higher assurance that an authorized user is making the payment, since authentication is required to generate the virtual credit card number. Merchants are often required to absorb the costs of credit card fraud in the form of "chargebacks" from the credit card companies. Greater use of virtual credit card numbers would reduce fraud and thereby help to eliminate chargebacks.
  - Merchants typically wouldn't know whether a credit card number presented by a customer is the actual credit card number, or a virtual number. The use of Information Cards to deliver virtual credit card numbers to merchants could signal to the merchant that the credit card number is virtual, and hence less risky if stolen.
- Users could shop online more securely, knowing that their true credit card information is not being divulged to the merchant.

#### A Few Issues to Consider

- The software at the merchant's e-commerce site that is necessary to process the secure electronic tokens containing the virtual credit card information could be integrated into the shopping card applications deployed by merchants. Hence the vendors of these shopping cards may need to be "sold" on the concept of including this processing capability into their products.

- Credit card issuing banks will need to deploy the software applications necessary to generate virtual credit card numbers as well as Information Cards and their associated components. In addition, these banks will also need to take a very proactive role in educating their customers about virtual credit card numbers, as well as the Information Cards that will be used by customers to generate and deliver the virtual numbers.
- Authentication of the consumer to the credit card issuing bank is important to ensure that only a legitimate user is generating the virtual credit card number. Today's virtual credit card applications depend on passwords for authentication. Stronger methods of authentication, such as one-time passwords or X.509 digital certificates and private keys, should be used instead for greater security. This authentication may be addition to providing a PIN or password merely to "unlock" the Information Card residing at the Selector.
- Consideration must be given to how consumers will obtain Information Cards, and whether these Information Cards will reside on Selectors on the consumer's computer, or "in the cloud." Strong authentication is especially important for using Information Cards associated with cloud-based Selectors, to prevent others from accessing and misusing those Information Cards.