



Web Release

Cardless (card not present) Secure Online Purchasing

Toronto Ontario - On March 23, 2009, aTrust demonstrated its *patent pending* Cardless Secure Online Purchasing System following the Advanced Card Technology Canada's Networking Session held at the Ontario Bar Association.

Digital commerce is still plagued by such things as phishing, identity theft, pharming, man-in-the-middle and denial of service attacks. These serve to diminish confidence in digital commerce and result in significant financial losses to both online vendors and purchasers.

A number of solutions are in use: PKI encryption, security tokens, temporary credit card numbers, and passwords. Experience has shown that each of these methods can be compromised or counterfeited. Identities and credit card data are particularly vulnerable as they must be revealed during online credit card transactions.

aTrust has developed and built a new and unique *patent-pending* security method that will enhance citizen trust and confidence in conducting electronic business and protecting personal information transferred over electronic communication systems.

To compliment its secure identity-verified online banking system, the new aTrust system utilizes a biometric token (FlickerCard™) and aTrust's Electronic Authentication & Civil Identity Credential Service (EACS) which binds the civil identity credentials to the online purchaser's physical identity and their FlickerCard™ serial number. The token and the aTrust's (EACS) are used to conduct secure online purchasing using a "not present" credit or debit card. The EACS and FlickerCard™ render the online purchaser and their credit or debit card information anonymous and invisible to phishing, pharming, man-in-the-middle attacks, identity thieves, and transaction manipulation hackers.

Once the online purchaser's physical identity has been validated and credentials assured, the EACS securely provides for the issuance of temporary credit card information, including a temporary credit card number, temporary credit card verification number and a temporary credit card expiry date.

These temporary numbers are issued by the credit card service provider to the online purchaser by way of a cryptographic optical container which displays on the online purchaser's computer monitor and can only be decrypted by the online purchaser's FlickerCard™. The cryptographic message is decrypted by FlickerCard™ and the temporary credit card information and a one-time password are displayed on the online purchaser's FlickerCard's secure internal display. The online purchaser confirms the transaction to the credit card service provider by entering the time sensitive, one time password, into a password confirmation box. The online purchaser further confirms the transaction to the online vendor by entering the temporary credit card data into the online vendor's credit card payment screen to finalize payment.

The credit card issuer or bank recognizes the temporary credit card data and pays the online vendor the purchase amount while billing the online purchaser's real credit/debit card. In this manner, the true credit card information required for the purchase is not keyed into the computer or displayed on a screen, thereby protecting it from hackers, phishers, credit/debit card identity thieves, and man-in-the middle attacks.

The Cardless Online Purchasing product is available integrated with the aTrust Online Banking product.

About aTrust Inc.

aTrust, a private Canadian company, is an e-Authentication & Credential Services Provider and manufacturer of patented secure, encrypted, and biometrically identity-verified electronic mail software called a-Mail™. aTrust's EACS utilizes FlickerCard™ and SAML 2.0 tokens and infrastructure to provide federated authentication & credential assurance. FlickerCard™ is a microprocessor based, privacy enhanced, personal digital identity token, which provides secure identity-verified (biometric fingerprint) access, transaction manipulation protection, and end to end secure access to online and other applications. a-Mail™ is FIPS 140-2 compliant and also utilizes EACS to provide physical identity authentication and credential assurance.

Contact

Sal Khan — Tel 613-882-1114 email: skhan@atrust.ca