



IdenTrust™ & AP Technology

Strong Multi-factor Authentication



The end of 2006 brought with it the deadline for implementation of the Federal Financial Institution Examination Council's (FFIEC) guideline for Multi Factor Authentication (MFA). Financial institutions across the United States took action to shore up weaknesses in their online banking systems for prevention of phishing and pharming attacks by hackers. Also in 2006, institutions realized that strong authentication must be expanded to encompass their other Internet Protocol (IP) based networks such as those carrying ATM and POS transactions. In conjunction with this expansion, auditors also began to assess enhancing money laundering and Bank Secrecy Act (BSA) reporting.

THE NEED FOR STRONG AUTHENTICATION

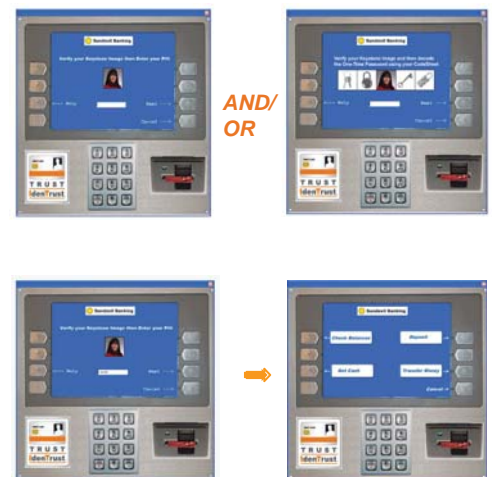
Money launderers establish a legitimate business in the U.S. as a "front" for their illicit activity. They establish a bank account with a U.S. based bank and obtain credit cards and ATM cards under the name of the "front business." Funds from their illicit activities are deposited into the bank account in the United States. While in another country, where their U.S. based bank has affiliates, they make withdrawals from their U.S. bank account, using credit and cards. Money is deposited by one of their cohorts in the U.S. and is transferred to pay off the credit card loan or even prepay the credit card. The bank's online services make it possible to transfer funds between checking and credit card accounts.

The bank that opened the account for the business should conduct appropriate due diligence as part of the account opening process. Under the IdenTrust rule set, the requirement to comply with USA Patriot Act Know Your Customer (KYC) rules holds the institution to stringent guidelines for determining the identity and authenticity of the company requesting the account, and, to determine the legitimacy of the business. The bank should understand the nature of the business and the type of activity expected of the business including the size, frequency, and types of payments that are most typical and be able to track that against the use of the bank's services by the new account holder. The bank should also monitor the business for deposit activity including monitoring for: potential structuring and significant account changes, such as prepayments going to credit cards. By using an IdenTrust, certificate based smart card, doing this type of tracking would be easier.

THE SOLUTION - MUTUAL AUTHENTICATION AND FRAUD TRACKING FOR SHARED AND CARD NETWORKS

With the publication of guidelines for strong authentication requirements and increased vulnerability for card networks from hackers, IdenTrust and AP Technology have partnered to provide a comprehensive mutual authentication and fraud tracking solution for card based transactions. The combination of offerings from these two companies enables the site to be authenticated to the user and the user to the site – mutual authentication. To validate both the user and the site before account access is granted, a card based transaction utilizing an IdenTrust digital identity certificate and AP Technology's Keystone Authentication executes the following workflow:

1. The IdenTrust encrypted digital certificate on the user's EMV standard smart card is read by the device and sent across the network for validation. If the request is returned with a failed validation, the transaction is terminated.
2. In parallel with validating the user's digital certificate, the user's personal photo or Keystone Image (as designated on their personal Keystone CodeSheet) is retrieved from the Keystone Authentication server and posted on the screen. By verifying the appearance of this image, the user knows the ATM is connected to a Trusted network. If the image does not appear or is invalid, then the transaction is cancelled by the user. For additional security in specified geographies, the system can dynamically display additional images along with the user's photo for the purpose of having the user decode a one-time password.
3. Once the user's digital certificate and the device are validated, the cardholder can then proceed with the transaction by entering a valid pin or password with the assurance that it is completely secure from hackers.



IdenTrust Digital Certificates and the Multi-Purpose Smart Card

The IdenTrust digital certificate that is contained on the smart card is issued based on USA Patriot Act-compliant and other federally regulated KYC rules from around the world. IdenTrust policies for identity authentication and validation have been agreed to and documented in a rule set by financial institutions from around the world. These policies (P) incorporate a globally interoperable legal infrastructure (L) and consistent operating rules (O) that utilize a compliance-tested set of partner solutions for the technology (T) access. The IdenTrust PLOT is accepted by 175 countries creating non-repudiation for the transactions utilizing IdenTrust digital certificates. When used, a comprehensive audit trail is created across all banks that are party to the transaction. This enables compliance with requirements that are as stringent as Sarbanes-Oxley reporting, the Suspicious Activity Report (SAR) and other Bank Security Act (BSA) tracking. Fraud tracking and money laundering information are captured each time the certificate is used.



AP Technology Keystone Authentication and Network Validation

AP Technology's Keystone Authentication provides banks with the ability to validate network connectivity and authenticate users as needed through varying applications, such as websites and debit/credit card devices.

The user's *Keystone CodeSheet* – a One Time Password (OTP) decoder – is created via their financial institution's online services and then printed to their local printer, or downloaded to a Personal Digital Assistant (PDA) or mobile phone. This CodeSheet can then be used to gain access to their account/s via the financial institution's website, card or shared network.

Keystone Authentication provides all the security benefits of OTP technology without the expense and logistical issues associated with hardware- or software-based password-generating devices. Unlike other OTP solutions, Keystone offers a built-in anti-phishing component for site/network validation.



Banks have powerful options available to fight fraud when deploying Keystone Authentication. Keystone can be used to provide:

- 1) *OTP-based Mutual Authentication for online banking channels*
- 2) *Network Validation for card networks, when coupled with IdenTrust certificates on EMV standard smartcards*

SUMMARY - GROWING THE SPECTRUM OF TRUST

The IP-based networks carrying card transactions continue to grow in size and importance, yet, to date, they remain vulnerable targets for fraud attack. As communications continue to evolve, users and providers need to have confidence that solutions can be trusted and access is secure. Mutual authentication provides the ideal solution for IP-based network devices by validating both the network to the user and the user to the financial institution to create comprehensive security and a trusted environment in which transactions can occur with confidence.

IdenTrust certificate based smart cards in combination with AP Technology Keystone Authentication provide a powerful solution for complying with audit requirements and also adds the ability to mutually authenticate the user to the site and the site to the user.

AP Technology is a certified IdenTrust Compliant provider. The two companies have joined forces to bring their integrated solution to the financial services industry and create a new level of security and trust for the future of card transactions.

For more information on the IdenTrust™ & AP Technology solution, please contact IdenTrust:

Corporate Headquarters
795 Folsom Street
First Floor
San Francisco, CA 94107
USA

T: +1.415.848.3010
F: +1.415.848.2745
E: sales@IdenTrust.com

European Office
117 Fenchurch Street
London, EC3M 5DY
United Kingdom

T: +44 (0)20 3008.8330
F: +44 (0)20 3008.8331
E: sales@IdenTrust.com

For more information,
visit:
www.IdenTrust.com



TECHNOLOGY

IdenTrust
WE PUT THE TRUST IN IDENTITY