



IdenTrust™: Beyond SSL and Multifactor Authentication

Eliminating Man-in-the-Middle Attacks with IdenTrust™

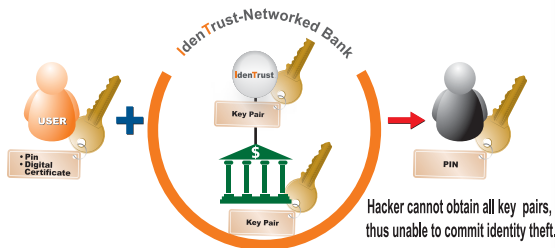
A Preventative, Proactive Approach to Securing Electronic Transactions

Many financial institutions believe that they are protected from man-in-the-middle (MITM) attacks because they encrypt data using a Secure Socket Layer (SSL) protocol or offer multifactor authentication. But the fact is that fraudsters can easily bypass SSL or outwit multifactor authentication. The only fail-safe approach to protecting your institution from an MITM attack is to create a reciprocal trust relationship between all parties in an electronic transaction with mutual authentication.

The Problem



The Solution



The Reality: More Needs To Be Done to Protect Institutions Against MITM

Industry groups and regulatory bodies have been vocal about the flaws of most current Internet authentication practices. For example, according to the Financial Services Technology Consortium (FSTC):

"Better institution-to-customer authentication would prevent attackers from successfully impersonating financial institutions to steal customers' account credentials; and better customer-to-institution authentication would prevent attackers from successfully impersonating customers to financial institutions in order to perpetrate fraud."

As the FSTC notes, clearly more must be done to prevent insidious MITM attacks. The "more" is mutual authentication.

Still Vulnerable to MITM Attacks

During a MITM attack, a third-party can read, insert and change messages between two unsuspecting parties. By intercepting the message, the third-party can access confidential information, steal account numbers, make changes to contracts, the list goes on. An MITM attack can take the form of eavesdropping, denial-of-service or phishing.

SSL protocol does not protect against these attacks. Public Key Infrastructure (PKI) communications rely on a cryptographic system of two keys: a public key and a private key known only to the recipient of the message. The only requirement for SSL to work is that the client trusts the server.

Most Web-based applications do not require client-side certificates to create a reciprocal trust relationship between the client and the server. This lack of reciprocal relationship provides the opening for a MITM attack. Applications such as online banking are particularly vulnerable.

Like SSL, one-time passwords (OTP) also fall short in protecting against MITM attacks. OTP only authenticates the client; the user does not know to whom they are speaking. A fraudster can create a pharming site and present their own certificates for encrypted sessions, fooling the client into believing that they are who they say they are. The user enters his or her password—which is then intercepted by the fraudster.

Benefits

Prevents MITM Attacks

By design, the IdenTrust Trust Network creates a trusted relationship between all parties in an electronic transaction.

Provides Mutual Authentication for Highest Levels of Protection

Mutual authentication is inherently more secure than multi-factor authentication.

Strong Credentials

IdenTrust has provided identity validation to global financial institutions, corporations and government agencies for almost a decade.

Real-Time

Using OCSP, IdenTrust validates identities when they are needed: in real-time.

Non-Repudiation

IdenTrust's Trust Network limits the liabilities of each of the relying parties.

Certificate Policies Ensure Security

IdenTrust Certificate Policies govern policies for access control, client and user authentication, digital signing and non-repudiation.

Guaranteed Assurance

Financial institutions from around the world are members of the IdenTrust Trust Network.

The IdenTrust Mutual Authentication Solution

Mutual--or two-way--authentication refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity.

IdenTrust prevents MITM attacks by providing mutual authentication in two ways:

- creating a secure channel between parties
- requiring a reciprocal trust relationship between the client and the server

To make global electronic communication and commerce less risky and more cost effective, IdenTrust™ relies on the PLOT – policies, legal and operational framework, and access technology for globally interoperable identity authentication. IdenTrust is recognized by major government and regulatory bodies in more than 175 countries. Key features of the PLOT:

- Policies and procedures developed by financial institutions around the world provide comprehensive authentication
- IdenTrust identities are globally interoperable under uniform private contracts
- Customer agreements are valid, binding and enforceable in countries where members offer the IdenTrust Service
- Complete, hosted environment enabling a full spectrum of trusted identity services

How Mutual Authentication Works

In a mutual authentication scheme, the server creates a key encrypted with the server's private key. The server then asks for client authentication. The client uses his or her private key to encrypt back another key which the server then decrypts.

By creating this encrypted tunnel that no one else is able to penetrate, each party in the transaction is absolutely certain they know and can trust each other.

Under the IdenTrust Rule Set, the keys used to create the secure channel session and the keys used to authenticate the signing and relying parties are kept separate. IdenTrust issues each certificate holder both a utility certificate and an identity certificate. The utility certificate is used for encryption; data confidentiality and integrity; and SSL and secure key distribution. The identity certificate is used for digital signing.

The Network of Trust

IdenTrust's Identity Certificates govern access control, client authentication and user authenticity including SSL, digital signing and non-repudiation. Identities are validated in real time giving the IdenTrust community secure Internet connections and validation of the signing and relying parties at the time the identity is being relied upon.

By partnering with financial institutions, IdenTrust has leveraged their risk and liability expertise and created the only truly globally interoperable, limited liability, non-repudiable method of conducting electronic commerce: mutual authentication.

About IdenTrust™

IdenTrust is the global leader in trusted identity solutions, recognized by global financial institutions, government agencies and departments, and commercial organizations around the world. IdenTrust enables organizations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimize investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust, smarter, faster, and more cost effectively.

The only bank-developed identity authentication system, IdenTrust provides a unique legally and technologically interoperable environment for authenticating and using identities worldwide. The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (P.L.O.T.) to create a comprehensive environment for issuing trusted identities. IdenTrust is the only company to provide a solution incorporating all four of these elements. Customer agreements are valid, binding and enforceable in more than 175 countries. IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Competing offerings, in contrast, rely on a dizzying maze of public laws that vary from jurisdiction to jurisdiction. Additionally, the IdenTrust Trust Infrastructure maintains the privacy of each and every transaction processed by reading only digital certificate information, not the message itself.

For more information on the IdenTrust™ Man-in-the-Middle Solution, please contact:

Corporate Headquarters
55 Hawthorne Street, Suite 400
San Francisco, CA 94105
USA

T: +1.415.486.2900
F: +1.415.486.2901
E: sales@IdenTrust.com

European Office
288 Bishopsgate
London, EC2M 4QP
United Kingdom

T: +44 (0)203.008.8330
F: +44 (0)203.008.8331
E: sales@IdenTrust.com

For more information,
visit:
www.IdenTrust.com

IdenTrust
WE PUT THE TRUST IN IDENTITY