Eliminating Man-in-the-Middle Attacks Using IdenTrust® Mutual Authentication

What is a Man-in-the-Middle Attack?

During a man-in-the middle (MITM) attack, a malicious third-party actor can read, insert and change messages between two unsuspecting parties. By intercepting the message, the third-party can access confidential information, steal account numbers or passwords, make changes to contracts, etc. An MITM attack can take the form of eavesdropping, denial-of-service or phishing.

Are Financial Institutions Protected Against Man-in-the-Middle Attacks?

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 multi-factor authentication. But the fact is that fraudsters can easily bypass SSL or outwit multi-factor authentication. A MITM attack can result in reputational risk; this is a multi-billion dollar problem which can close businesses down.

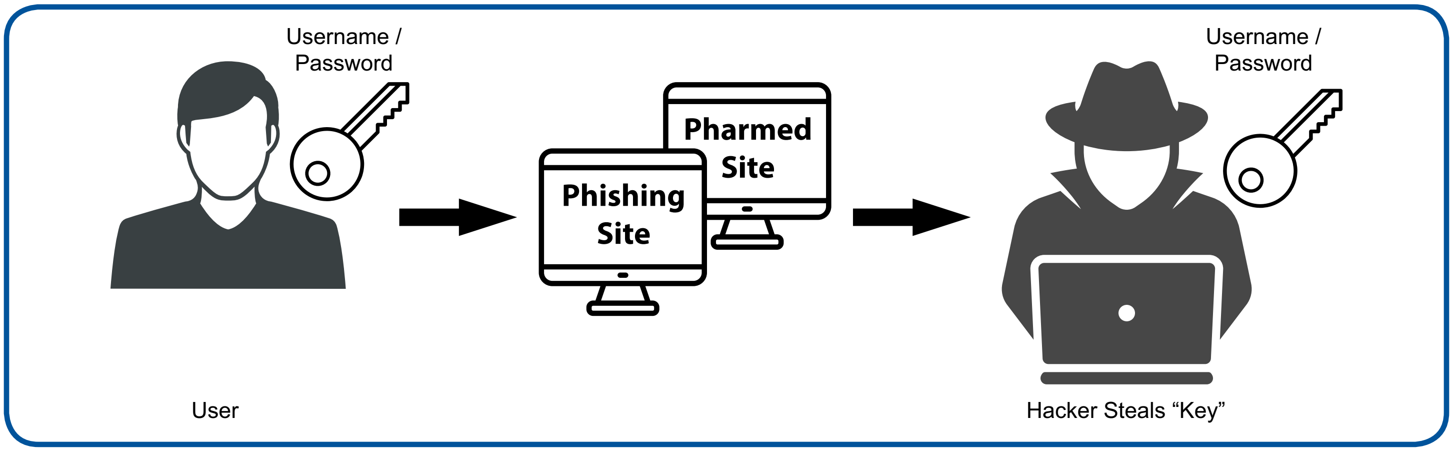
The Problem

Secure Socket Layer (SSL) protocol does not protect against these man-in-the-middle (MITM) attacks. Public Key Infrastructure (PKI) communications rely on a cryptographic system of two (2) keys: (1) a public key; and (2) 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.

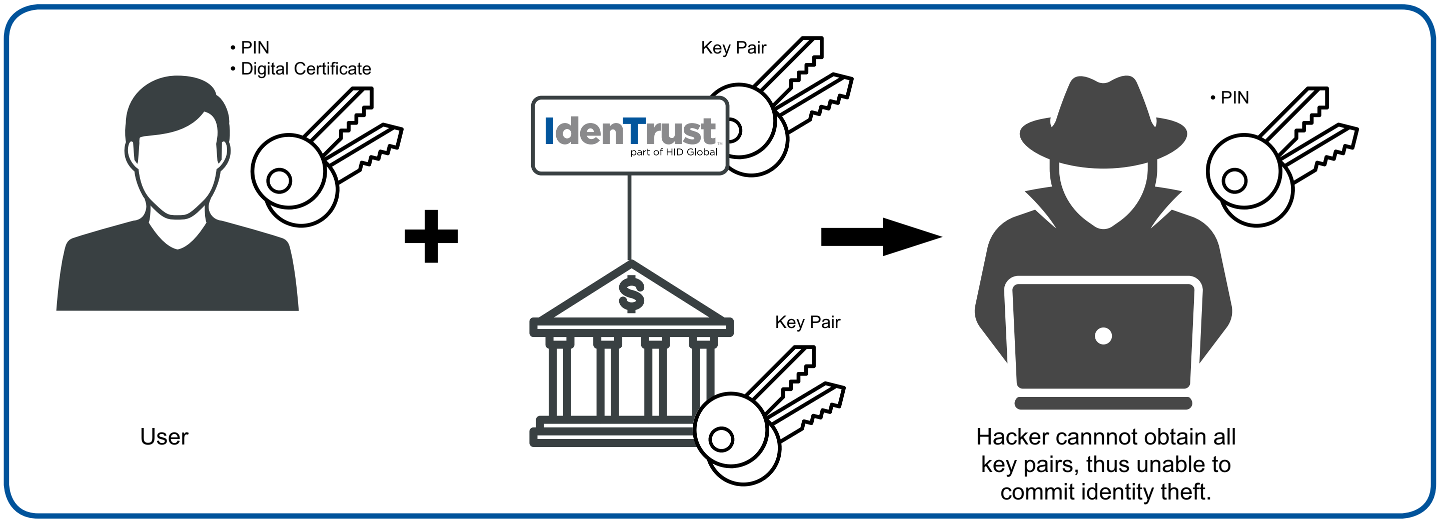
Graphically, the problem looks like this:



The Solution

The only fail-safe approach to protect your financial institution from a man-in-the-middle attack is to create a reciprocal trust relationship between all parties in an electronic transaction using mutual authentication.

Graphically, the solution looks like this:



How Mutual Authentication Works

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.

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.

The IdenTrust Mutual Authentication Solution

IdenTrust prevents man-in-the-middle (MITM) attacks by providing mutual authentication in two ways:

- Creating a secure channel between parties; and
- 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 Framework, Operations Hosting and Technology) Rule Set which provides legally binding trust for online transactions with customers and partners.

PLOT is a trusted Rule Set for identity authentication that was created by global financial institutions. The PLOT Rule Set ensures that identities are issued, validated and utilized in a standardized way inside and outside a financial institution, nationally and internationally. As a result, IdenTrust identities are globally interoperable under private contracts recognized by countries belonging to the World Trade Organization.

Key features of the PLOT Rule set include:

- Only the total combination of the PLOT components (i.e., Policies, Legal Framework, Operations Hosting and Technology) provides a comprehensive solution to risk management in digital transactions.
- Policies and procedures developed and agreed to by financial institutions around the world provides a comprehensive approach to authenticating identities.
- IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Other systems require public law for digital signatures to be effective.
- Customer agreements are valid, binding and enforceable in countries that comply with United Nations, World Trade Organization and FATF guidelines.
- IdenTrust delivers a complete, hosted environment to enable a full spectrum of trusted identity services.

Under the IdenTrust PLOT 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 benefits of the IdenTrust mutual authentication solution include:

- **Prevention of MITM Attacks:** By design, the IdenTrust Trust Network® creates a trusted relationship between all parties in an electronic transaction.
- **Mutual Authentication for the 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 Validations:** Using OCSP, IdenTrust validates identities when they are needed: in real-time.
- **Non-Repudiation:** The IdenTrust 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 Network of Trust

IdenTrust 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 global, interoperable, limited liability, non-repudiable method of conducting electronic commerce: mutual authentication.