

EzIdentity Platform Next Generation Identity Protection

Future Proof Strong Authentication (2FA)

For organizations seeking to protect the confidentiality and integrity of sensitive data, communications and transactions, EZMCOM offers solutions that increase the security of authentication with a layered approach consisting of 2nd factor tokens, a **Mutual Authentication** layer & transaction signing for guarding **Man-In-The-Middle, Pharming, Man-In-The-Browser, Script-In-The-Middle attacks** that otherwise render 2FA tokens vulnerable.

The Problem:

Regulatory authorities across the globe have acknowledged the threat of Phishing to financial institutions and called for stronger authorization and authentication for their online customers. In the U.S., Securities and Exchange Commission has warned users of keystroke-logging software, phishing scams and traditional snoops as ways fraudsters could obtain access to online brokerage accounts and steal money.

As more and more people trade online, there has been also a rise in the number of hack attacks where your resources are used by hackers to make profits for themselves. These attacks are often carried out by stealing your identity and then accessing your online account with an online trading firm. Let us first understand how these hackers work.

The first thing the hacker needs to do is to steal your username and password. There are numerous ways in which they can do this. And new ways are being developed all the time. Once they have your user name and password they can easily access your account and buy or sell whatever they want to. Exactly the way you do. So this hacker is most likely to sell all the shares that you have accumulated, and with the money he thus receives will buy shares on micro-caps.

What are micro-caps? Also known as penny stocks these are thinly traded stocks.

What the hackers do is by buying shares of that micro-cap with your money he drives up the price for the particular share. Once the price is quite high he sells his own holdings at a considerable profit. The money is then wired to an account in a different country or a series of straw men and dummy corporations are used to transfer it to their account. As online trading get increasingly easy many investors drop their guard. Financial institutions just cannot take it easy on the net and need to implement minimum authentication security to address this challenge to the online trading industry.

Phishing still remains the main method that fraudsters use to attack financial institutions; though simple and cost-effective, it yields lucrative results. However, as financial institutions across the globe continue to deploy strong authentication, fraudsters are also finding more sophisticated ways to launch attacks. As the fraud landscape evolves, financial institutions will come to face more advanced threats, specifically Man-in-the-middle and Trojan (malware) attacks.

Man-In-The-Middle attacks:

“This is a common and predictable attack. As an industry, we need to accept that solutions not incorporating strong client and server authentication cannot survive the Internet. Ten years ago, this was evident with the advent of key SSL mechanisms. It’s time to put them to work.”

Eric Greenberg, Former leader of Netscape’s security group, which originally created SSL

“All the kit-using criminal has to do is register a phony domain name, then plug that and the URL of the real Web site into the software’s administrative control panel. The kit then communicates in real time with the target IP address and uses a proxy to redirect content from the legitimate site to the bogus URL; thus the user interacts with actual content from, say, his own bank, adding to the deception. The fake URL squats between the consumer and the target -- that’s where the “Man in the Middle” phrase comes from -- and captures all data from user to bank or bank to user.”

Gregg Keizer, InformationWeek New Phishing Toolkit Poses Danger to Consumers

“Two-factor authentication is not useless. It works for local log-in, and it works within some corporate networks. But it won't work for remote authentication over the Internet. I predict that banks and other financial institutions will spend millions outfitting their users with two-factor authentication tokens. Early adopters of this technology may very well experience a significant drop in fraud for a while as attackers move to easier targets, but in the end there will be a negligible drop in the amount of fraud and identity theft

Bruce Schneier, April issue of Communications of the ACM

EzIdentity Platform

Layered Defense, Future Proof

Layer-1: Second Factor Authentication (2FA)

The first layer of defense - a One-Time Password (OTP) easily eliminates a wide spectrum of Phishing attacks. The OTP is available for the user in the form of Hardware or Software Token allowing the implementation of Layer-1 in a significantly cost effective way by harnessing the power of Software based approach.

Layer-2: Mutual Authentication

The use of only one-way SSL security (only the website has an SSL certificate instead of two-way, which is the way SSL was designed to be used), reliance on easily intercepted 'shared secrets', or easily spoofed information such as timezone, IP geolocation are primary reasons for failure of existing authentication measures. Moreover, the overall cost & complexity in implementing a 2-way SSL solution with the end-user education or the provisioning of a pure out-of-band authentication & authorization solution using SMS or voice-calls or even deploying specialized hardware tokens capable of transaction signing pose many other business related challenges to enterprises that need a strong yet easy to use solution.

EzIdentity provides a one-stop multi-layer, multi-token authentication platform that becomes a single gateway to a host of software and hardware based authentication solution that balance our usability, security & features with its patent pending algorithms to bootstraps 2FA (software or hardware) with added layers of security transparent to end-users using strength of digital signatures to provide mutual authentication similar to a 2-way SSL & transaction signing working in a virtual out-of-band channel.




- Transaction Integrity
- Variety of Tokens
- OATH Compliant
- Software and Hardware
- Protects Hacking 2.0

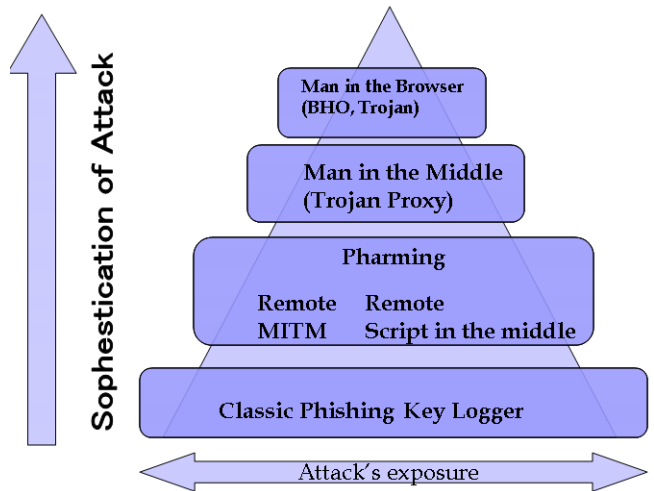


- 2nd Factor Authentication
- Variety of Tokens
- OATH Compliant
- Software and Hardware
- Protects Hacking 1.0

EzIdentity Platform features and benefits

EzIdentity Protection

EzIdentity Authentication Methods	Attacks						
	Classic Phishing	Key logger	Pharming	Remote MITM	Remote Script in the middle	Man in the Middle (Trojan Proxy)	Script / Browser in the Middle (Trojan Proxy)
Layer-1 (2FA Token)	✓	✗	✗	✗	✗	✗	✗
Layer-1 + Layer-2 (EzAuth)	✓	✓	✓	✓	✓	✗	✗
Layer-1 + Layer-2 + Layer-3 (EzAuthX)	✓	✓	✓	✓	✓	✓	✓



EzIdentity Benefits

Ease of use: End-users simply use the OTP generated by token (software or hardware) and type their PIN code to get the two-factor capabilities. Enhancement of 2FA tokens with Mutual Authentication is provided in a transparent way to the user without changing customer or 2FA token behavior.

Compelling ROI: Maximize ROI on existing 2FA tokens by enhancing their security. Minimal IT enablement required.

Standards-based: Implements Open standards of Cryptography and FIPS compliant algorithms. RSA, PKCS, EMV Cap v2, OATH compliant standards

Compliance: Standards and regulatory compliance for identity, privacy, policy enforcement, audit and authentication services (Sarbanes-Oxley, Basel II, GLBA, HIPAA, FFIEC and more).

Enhanced security: Strong authentication through enforcement of two-factor authentication: something the user has (the token) and something the user knows (the PIN code). In addition, Mutual Authentication: something that you are (a digital finger print) guards against Man-In-The-Middle (MITM) phishing attacks.

One Stop Solution: Allows multiple applications to integrate and implement various configurations of security as deemed necessary by the application. A centrally managed solution that can provide software tokens, hardware tokens to PKI Based tokens and multiple layers of security.

Future-ready: Future-proof investment through extensible platform capable of plug-and-play support of an increasing family of EzIdentity tokens as well as support for a broad range of 3rd party tokens.