



## EzIdentity Platform Next Generation Identity Protection

### Stronger Authentication

EZMCOM offers 2<sup>nd</sup> factor authentication with an end-user transparent **Mutual Authentication** layer for organizations seeking to protect the confidentiality and integrity of sensitive data, communications and transactions. The solution guards against **Man-In-The-Middle, Pharming, Man-In-The-Browser, Script-In-The-Middle** attacks that render One-Time Password based token solutions vulnerable.

#### The Problem:

In 2006, regulators drove financial institutions to add security by implementing strong authentication to prevent fraud and identity theft. To comply with the aggressive deadlines issued by regulators, virtually all financial institution implemented weak forms of authentication such as cookies, pictures, device fingerprinting, IP Geolocation or One-Time password (OTP) tokens.

In the meantime Phishing attack have been upgraded to include Man in the Middle (MITM), Man in the Browser (MITB), Pharming, Trojan Proxy Phishing attacks, which defeats virtually all protections that have been put in place by financial institutions to protect against basic Phishing. MITM attacks, which have been well known in the security and hacking community for years, are now being integrated into easy to use kits and with the availability of MITM Phishing kits.

Hardware solutions typically have issues of distribution, cost of deployment & maintenance for retail deployments and many software based solutions posing cumbersome and steep learning curve for users to the extent of disrupting business, a serious challenge for a commercially viable, mass deployable authentication solution exists.

#### The Solution:

A commercially viable, roaming friendly 2-way SSL (the way SSL was designed to be used rather than only the server having a SSL certificate) implementation that does not rely on easily intercepted 'shared secrets', One-Time Passwords or easily spoofed information such as timezone, IP geolocation. A software based solution that that obviates the overall cost & complexity of implementing a 2-way SSL solution that is easy to use and no disruption in user behavior.

EzIdentity provides an easy to use and familiar *username - password* authentication interface that balance our usability, security & features. Ideal for mass deployments, EzIdentity solution provides compliance to regulatory requirements of strong authentication using its patent algorithms combining concepts of 2<sup>nd</sup> factor authentication and PKI based digital signatures.

The EzIdentity software installs invisibly and runs on a wide range of platforms, making it easy to protect customers, employees, and partners from identity theft and fraud. For the first time, organizations can transparently protect their users from identity theft and fraud, without changing user behavior and or requiring expensive hardware.

#### 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 features and benefits

### Threats and how EzIdentity defeats them

THREATS	DESCRIPTION	HOW EZIDENTITY DEFEATS THE THREAT
<b>Brute Force</b>	The attacker copies the profile file that contains the key to his own workstation and attempts millions of passwords, which eventually leads to the disclosure of the private key.	<p>EzIdentity's patented "Mutual Authentication Payload" technology uses a combination of a PIN and a container fingerprint (CF) as a basis for encrypting the private key. It uses standard encryption algorithms and the patented process to protect the key. The result of this process is that any decryption attempt, with either of the PIN or CF incorrect, will fail to extract the private key. The CF is generated at run-time by the software component of EzIdentity and hence ensures that a copy of the profile file containing the private key to another workstation (i.e. container) does not compromise the private key even if the PIN is brute-forced.</p> <p>A six-character password will anyways have approximately 56.8 billion permutations (upper case, lower case, and numbers), and only of those permutations will unlock the private key within the same workstation (container).</p> <p>If the key decryption fails because an incorrect PIN or CF was generated, the invalid password counter increases by one. The authentication server can block user access after a configurable number of invalid attempts (the default is five) Therefore, the attacker can attempt very few passwords before being locked out.</p>
<b>Challenge/Response (Mutual Authentication Payload) Intercept</b>	The attacker intercepts the encrypted and signed challenge issued by the authentication server and the response from the client. The attacker then uses every possible private key to recreate the signed challenge or the response.	The authentication challenge/response is sent over a secure SSL channel. Even if an attacker were able to break the channel security, this attack still fails because the standard encryption and signature algorithm always ensure the uniqueness of every challenge/response. Only the authorized authentication server or the rightful client (user) can decrypt challenge/response and verify the signature.
<b>Chosen Plaintext</b>	The attacker tests every possible key against a known piece of text that has been encrypted with the public key and can tell when he has discovered the true private key as it would correctly decrypt the plaintext.	The attacker will not be able to mount this attack as neither the plain public key of the user is accessible or is it computationally feasible to generate private key in brute force that may decrypt an encrypted chunk to a chosen plain text.
<b>Fraudulent Administrator</b>	The attacker is a fraudulent administrator who gets access to the user key pair credentials on the server.	<p>A fraudulent administrator may get access to the user credentials, but the administrator cannot use it as it is stored in a PKCS12 container protected with a password that is encrypted with the server public key.</p> <p>The server private key is stored in a security hardware device (HSM) and is not exportable. It is initialized in run-time by the authentication server itself and used only by the authentication server to extract the user private key from the PKCS12 at time when the client is roaming to a new workstation (container) and is initializing the EzIdentity client software. The approach offers non-</p>

THREATS	DESCRIPTION	HOW EZIDENTITY DEFEATS THE THREAT
		repudiation.
<b>Man-in-the-Middle</b>	The attacker intercepts the credentials and data while they are in transit. In this case, the attacker appears as the target server to the user and as the user to the target server.	The most insidious phishing attack is the Man-in-the-Middle. Protection from this type of attack is unique to EzIdentity solution. Each Challenge (Mutual Authentication Protocol: MAP payload) from the server contains information about the server that issued it. The EzIdentity client automatically verifies the MAP payload to confirm that it is connected to the correct server before generating its own encrypted and signed response. If the server match is not found, the EzIdentity client will abort the session and the attacker will not be able to complete the authentication.
<b>Pharming</b>	The attacker poisons the DNS server and redirects users to the fraudulent web site. Users do not suspect anything because the redirect happens even when the user selects the web site from a saved favorite or actually types in the correct URL.	As mentioned above, each MAP Payload issued from the server contains information of the server and the domain that issued that Challenge (MAP Server Payload). The EzIdentity client automatically checks to confirm that it is connected, via SSL, to the right domain before accepting the challenge (MAP Server payload) before encrypting and signing the response (MAP Client payload). If the domains do not match, the EzIdentity client will abort the session and the attacker will not be able to complete the authentication.
<b>Phishing</b>	The attacker targets unsophisticated users and fools them into entering their credentials into a fake web site. This usually occurs when a criminal sends an email impersonating a customer service organization from a legitimate business (such as a bank or payment site) and asks recipients to click on a URL to perform account maintenance or verification. The link takes them to a fraudulent site, which prompts them for their valid credentials.	One key advantage of the EzIdentity solution is the implicit implementation of two-factor authentication to protect users from phishing attacks. Assuming phishers can convince a user to disclose their password/PIN, they are still unable to impersonate the user as they don't have the second factor (a trusted and EzIdentity initialized workstation). The phisher needs both what the user has (the EzIdentity profile file on a trusted workstation) and what the user knows (the Password/PIN).  The initialization of the EzIdentity profile file on a trusted workstation is achieved by utilizing any out-of-band authentication to establish the identity of genuine user and the workstation on which EzIdentity is getting initialized.
<b>Replay Attack</b>	The attacker stores a copy of the user encrypted and signed response (MAP Client payload) and replays it to the site.	The EzIdentity authentication involves a PKI-based challenge/response model where the response sent to the server for verification always contains a unique One-Time usable code. The server decrypts and verifies the digital signature of response and accepts the particular response only if the One-Time usable code is verified. The uniqueness of the response defeats the replay attacks.
<b>Key-Logger</b>	The attacker installs key-logging malware that captures every keystroke and mouse click on the computer and periodically sends that information over the internet to the criminal who created it.	EzIdentity's pointing device enabled PIN Pad thwarts logging malware. The PIN-pad is a virtual keyboard that shows up on the screen; users enter their password by clicking with a mouse on a screen-based key pad. The user will not use the keyboard to enter the password and is hence protected completely from keyboard loggers.
<b>Malware Browser Memory Attack</b>	The attacker attempts to find the private key in the memory of a system that has initialized the EzIdentity in roaming mode on a browser of public	EzIdentity private key is accessed only briefly in memory when the user provides the password and the encrypted and signed response is generated. EzIdentity leverages on a memory that managed securely as a sandbox that has restricted file-system and network access, as well as access to browser internals.

THREATS	DESCRIPTION	HOW EZIDENTITY DEFEATS THE THREAT
	Internet kiosk.	Immediately after response generation, the private key and password are cleared from memory; only the response (encrypted and signed – MAP Client payload) is sent back to the authentication server. In public internet kiosks, EzIdentity recommends the roaming user to initialize EzIdentity for a single browser session. The EzIdentity profile file gets removed and unusable after a single browser session.

## Comparison between EzIdentity and other authentication technologies

	MITM	Pharming	Phishing	Replay Attack	Key Logger
EzIdentity	↑	↑	↑	↑	↑
OTP Tokens	↓	↓	↓	↔	↔
Risk Based Analysis	↓	↓	↑	↔	↓
Personal Assurance	↓	↓	↑	↓	↓
Virtual Keyboard	NA	NA	NA	NA	↑
Identifying Questions	↓	↓	↑	↓	↔
SMS/e-mail/IVR	↔	↔	↑	↔	↓
Scratch Cards	↓	↓	↔	↓	↔

## Comparison between EzIdentity and PKI authentication

	Brute Force	Script-In-The-Middle*	MITM	Roaming convenience	Cost of deployment
EzIdentity	↑	↑	↑	High	Low
PKI Token (Hardware)	↑	↓	↑	High	High
Client SSL Certificate	↓	↓	↑	Low	Medium

**Script-In-The-Middle:** Malicious JS/VB Script in a Phishing website uses the PKI Token to sign a fraudulent transaction.

Legend: ↑= Full protection; ↔= Partial protection; ↓= No protection

## About Us

EZMCOM designs, develops, markets and supports identity protection products for the financial world, business and commerce over converging wired and wireless data channels.

Copyright © 2007-2008 EZMCOM, Inc. All rights reserved.