

## Protecting Online Customers from Emerging Phishing Attacks

### Strong authentication without impacting Business

For organizations seeking to protect online customers from emerging phishing attacks, the challenge is two folds: a **low-cost** solution that can be rapidly deployed to **large volume** of users and provide strong authentication capable of guarding **emerging threats** such as **Man-In-The-Middle, Trojans, Pharming attacks** without disrupting the convenience of user experience.

#### Product overview:

A 100% software-based authentication solution that uniquely balances usability, cost and security features. Consumer- and business-facing portals can benefit from EzIdentity's ability to enable rapid deployments that protects against emerging threats such as MITM, Trojan, Pharming, **without changing user behavior or requiring expensive hardware.**

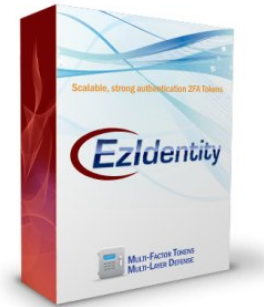
The solution uniquely defeats MITM attacks through its built-in Public Key Infrastructure (PKI) technology. EzIdentity creates a secure, application layer communication session that ensures mutual authentication between the client and the application or portal. **Transparent to the end user**, this application layer 2-way SSL alike secure channel ensures that the user is connected to the correct web domain before sending a digitally signed One-Time pass code as an added authentication factor.

A layered security approach provides defense-in-depth against unknown forms of MITM, Trojans. Even if a savvy attacker is able to defeat the first layer, sophisticated risk analytics of EzIdentity trigger an out-of-band (SMS, USSD, IVR, e-mail) secondary authentication. At its core, EzIdentity provides an **adaptive authentication engine**

designed to determine when to trigger its secondary out-of-band authentication and what type of method to use. These decisions are based on risk levels, institutional policies, customer segmentation, and the access channel getting used (Internet | Mobile | Phone). Such a defense-in-depth approach adds a cryptographic check (viz. OATH OCRA) of the originating and completed transaction, along with binding of the transaction to a user to ensure immunity against known and unknown forms of MITM. When the user is positively identified, the adaptive nature of the authentication engine ceases to trigger the secondary authentication unless the analytics engine detects an anomaly.

EzIdentity monitors online activities of the user in the background and logs proof positive digital forensic details for fraud analysis. This empowers IT and Risk teams with the capability to trail, trace and track down the details of a device or workstation (point of origin) of a suspected user activity for analysis of fraud claims and dispute resolution.

EzIdentity provides unprecedented software security for online customers with its patent authentication protocols methods while preserving the ease-of-use critical to the success of any authentication solution and online business.



#### 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](#)

#### Two-factor authentication:

"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](#)

#### User experience impacts Business:

"Authentication solutions that drive customers away are not good ones. Research indicates that customers expect you to provide the protection -- not ask them to take extra steps or pay extra for protection"

[Dave Cullinane, CISO for eBay](#)

## Protecting Online Customers from Emerging Phishing Attacks

### EzIdentity Features and Benefits

| Feature                         | Benefit  |
|---------------------------------|--|
| Requires no additional Hardware | Reduces initial cost, complexity and deployment time versus hardware solutions; eliminates ongoing hardware maintenance/support.   |
| Clientless solution             | No need of installing any authentication software programs, Drivers or ActiveX or Netscape Plug-in installable. Seamless support in browsers, Operating Systems.   |
| Transparent user experience     | Appears to user as password authentication; no user retraining required.   |
| Virtual Keyboard option         | Provides the option of a pointing device driven keypad for entering Password. Protects against keystroke and mouse click loggers.  |
| Mutual Authentication           | 2-way SSL alike mutual authentication is implemented at application layer. Ensures that digitally signed authentication credentials of the user are submitted only if the user is connected to the legitimate server.        |
| Multi-Factor Authentication     | Although transparent to the user, a digitally signed one-time usable pass code is transmitted on behalf of the user. Binds a user with a trusted device (access terminal).   |
| Defense-in-Depth                | Based on configurable policies, guard against unknown forms of MITM and merging threats by triggering out-of-band secondary authentication that binds a user transaction with a user (viz. OATH OCRA or Digital Signatures). |
| Adaptive Authentication         | Identifies anomalies in user online activity or transactional behavior and triggers secondary out-of-band authentication and minimizes authentication requests.  |
| Fraud analysis                  | Monitor and log user's online activities and collect actionable, proof positive network and point of access (terminal) details for fraud analysis and dispute resolution.  |

User environment:

- Firefox 1.5.x, 2.0.x, 3.0 • IE 6, 7 • Opera 9.x • Safari 2.x, 3.x
- Win XP, Win Vista, MAC OS X (10.4.10, 10.5), Win 2000 Professional, Win 2003 Server
- JRE 1.4 and above

### About EZMCOM:

EZMCOM is a leading provider of strong two-factor authentication and digital signature solutions. EZMCOM's software offerings are compliant with industry standards including OATH, PCI DSS. Tier-1 banks and other enterprises use EzIdentity to protect the identities of millions of employees, partners, and consumers worldwide. Organizations also work with EZMCOM to comply with regulations or legislation such as FFIEC, Sarbanes-Oxley, and HIPAA. Visit us at <http://www.ezmcom.com>.