

# EzIdentity: Adding Protection to SSL VPN 2FA moves into the mainstream

"About 80 per cent of VPN installations now include some form of Two-Factor Authentication (2FA) security; whether tokens, one-time passwords or USB devices." These findings were based on interviews with 20 leading vendors including Juniper, Citrix, Checkpoint, Cisco, SonicWall and their distributors. – 2008 Study report by Frost and Sullivan.

This proves that 2FA is no longer a niche security solution appropriate only for the largest multi-nationals; it is now a mature, mainstream solution that is specified by the vast majority of corporate and public sector organizations to secure their remote user access.

VPN delivers easy, anywhere access but is each remote user really who they claim to be?

## Identity is Trust

The popularity for SSL VPN systems is due to the increased demand from our users to provide Anywhere Access to our most sensitive business systems. We need to allow our trusted users to connect to our core business applications from any convenient computing device across any public Internet or wireless link, and VPN technology is making this much easier to deliver. However, this new Anywhere Access approach puts the Identity of our users at the centre of our security model, with the critical question being: 'Is each remote user really who they claim to be?'

In any system trust is based upon the individual's identity to access resources. For instance, at airport we show our passport and visa to an Immigration Officer, similarly an on-line user is challenged by their organization's VPN server to present their 'digital identity' which comprises their Username plus their Authentication Credentials.

## Identity Theft is the biggest threat

Your users' digital identities become very critical to your critical business systems. If a user's user-id and password is stolen then that user's entire digital identity is compromised. In the wrong hands the stolen identity can be used to impersonate the victim and gain access to your most sensitive resources. This is Corporate Identity Theft. It is difficult to protect your systems once you have suffered Identity Theft. An imposter can present stolen identity to your VPN systems, and will be allowed to enter without further challenge. It is an attack to organization and its business.

## Few questions to ask

We must take a long hard look at:

- How we authenticate the identity of each remote user?
- How we issue these identity credentials to our users? Is user name and static password enough?
- How we manage and support our users over their working life to keep their identities secure and private at all times?

## Static Password problem

Unfortunately still many organizations are applications like CRM, HRM, Email, DMS etc accessible through their VPN. Their VPN server with the 'username & static password' combination is all that stands between their most sensitive business information and hostile prying eyes.

Static passwords are 'weak authentication' which can be easily cracked by key logger, over the shoulder sniffing, brute force, man in the middle attack, Trojans. Employees always keep simple to remember password and repetition is a very common mistake Your Gmail password will be same as your organization's password. Once username and password has been hijacked, that person's entire digital identity is vulnerable and the attacker instantly acquires all the privileges of his/her victim. All this can happen without the victim being aware for them to report it to administrator. With the weak authentication provided by standard passwords you can never be really sure that a user is who they claim to be.

## Simple, strong and cost effective

A One-time Password, generated from a hard or soft token, can make authentication credentials strong. We need to make it impossible for hacker to attack and hijack the user's credentials.

Typically a user must present two different forms of credential:

- "Something the user knows": username & password.
- Plus "Something the user has": This Second Factor

Authentication (2FA) can be a soft/hard token that generates One-Time password. We know passwords are free but password management is not. To simplify password management, One Time Passwords are good solution as their inherent property is -One Time Password expires after one use. Even if hacker sniffs it, no compromise as OTP is already expired.

# EzIdentity: Platform, its features

## Off the shelf solution

### EzIdentity: Authentication Platform

EzIdentity delivers a strong authentication to will keep the good in and the bad out. It offers least cost, least maintenance software as well as hardware 2FA One Time Password tokens with complete life cycle management system ready to plug and play with existing enterprise's systems.

#### What is it in for me? (VPN Provider)

- Compelling Add-on: Give simple yet stronger protection to enterprise and their employees for VPN driven access.
- 'No cost Service': Complete software 2FA solution with software tokens to give no hidden cost solution.
- Generate Revenue: Adding value to your services where customers will pay extra to get needed protection.

#### What is it in for Customer? (VPN User)

- Enhanced protection: Strong authentication through enforcement of 2FA: something the user has (the token) and something the use knows (the PIN code).
- Simply to use: End-users simply use the OTP generated by token and type their PIN code to get the two-factor capabilities.
- Easy to choose: Single user can carry token wallet (2 or more tokens) and use accordingly in case they forget either one.

#### "3-2-1" to go secure

Administrator:

3. Procure EzIdentity (appliance or software)
2. Install EzIdentity.
1. Configure EzIdentity to User Directory.

Operator:

2. Select the user from user group.
1. Assign the 2FA token(s) to the end user.

User:

1. Activate token(s) and use.

EzIdentity offers 4 web interfaced portals to enable "3-2-1" steps. Let's look at them.

#### Simplified Administration & Management

Administration Portal: is used to configure & integration EzIdentity with Enterprise's directory server(s) and create logical groups of users. The admin can select tokens to be made available for these groups.

Operator Portal: This token-user life cycle management portal is available for the operator. The operator assigns, un-assigns tokens to users, set PIN policy and perform the helpdesk functions associated with the tokens and users.

Management Portal: is available for the administrator to monitor the services and their availability. It also allows Logs Collection, Backup & Restore, Customize & Configure SMTP Mail Server & SMS gateway settings and many other product features.

User Portal: is extended for the end users to allow them to get their tokens assigned by operator. It guides user with step-by-step instructions for download, activate and test the token. This portal can we made available for intranet as well as internet based users.

Each of the portals can be configured for its authentication (admin, operator, manager and users) with existing directory server. Optionally, owing to out-of-band channel utilized in User Portal, the authentication for the portal may be switched off.

#### Why EzIdentity? Differentiating Features

Choice of tokens: EzIdentity offers a wide variety of software & hardware tokens to meet each individual enterprises cost, usability and their user's lifestyle.

Multiple customer integration: EzIdentity is a centrally deployable identity protection platform that integrates with various Enterprise's applications for strong authentication. The users can use same tokens for various applications.

Token Wallet: EzIdentity gives flexibility to each user to have more than one token in its token wallet. Incase you do not have access to your favorite token; you can use your other token in the interim. No CRM support is needed.

Ready Made Platform: EzIdentity is available as appliance or software installation. Installation to configuration time is less than 30 minutes.

Scalable: EzIdentity provides simply 3 click configuration for Load balanced, High Availability configuration.

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

# EzIdentity Data Sheet

## Technical specifications

### EzIdentity Appliance Specs

R-Series	Concurrent Users
R-3000	Up to 100
R-6000	Up to 500
R-10,000	1,000+

EzIdentity appliances allows single standalone, HA and HA-DR configuration with multiple appliance deployments.

### Software Installation

Server Platform Coverage:

- Windows 2003 Server SP1 & above
- SuSe Linux Enterprise Server 10.1 & above

### Appliance Specifications

Per Appliance specifications

- 1U 19" (IEC Rack compliant)
- 2 X (Dual Gigabit Ethernet NIC)
- Additional 1 HBA Card for SAN interface

### Director Support (user data storage):

- EzIdentity LDAP (Inbuilt)
- Active directory v1.1
- LDAP Directory v3

### Support for external Databases:

- Oracle XE
- DB2 Express
- MYSQL v5 onwards

### Authentication Services offered as:

- Java remote EJB calls
- Web Services (over HTTP and HTTPS)
- ISAPI Filter for IIS 5.0 and above
- IAS Extension for Windows 2003 Server Family

### Token Security Algorithms:

- OATH (HMAC OTP) for OTP generation
- 3DES, SHA-1 combination for credential protection

### Interoperability

- RADIUS interface.
- Web Services interface (free SDK available).
- Basic Authentication by HTTP Web Server
- SAML 2.0

### Tokens supported

Software tokens:

- PC Token
- Mobile Token
- Web Token
- SMS OTP

Hardware Tokens:

- Mini Token
- Pocket Token
- Card Token
- Data Flash Drive Token

### Contact Information

America (North and south):

Pravat Mishra

[pravat@ezmcom.com](mailto:pravat@ezmcom.com)

+1-510-396-3894

EZMCOM, Inc. ([www.ezmcom.com](http://www.ezmcom.com))  
575 N Pastoria Ave.,  
Sunnyvale,  
CA 94085

