



**Stop Identity Theft  
with  
Transparent Two-Factor Authentication**



**e-Lock Corporation Sdn Bhd**

December 2009

# Table Of Content

---

- Table Of Content ..... 2
- Executive Summary..... 3
- 1. Introduction ..... 4
  - 1.1 The Issue – Identity Theft ..... 4
  - 1.2 The Impact..... 4
  - 1.3 The Challenges ..... 5
- 2. TheGRID – Stop Identity Theft ..... 6
  - 2.1 Two-factor Authentication ..... 6
  - 2.2 Mutual Authentication ..... 6
  - 2.3 Key Benefits..... 7
  - 2.4 How It Works ..... 7
  - 2.5 Comparison ..... 9
- Contact Information ..... 10

# Executive Summary

---

## The Issue

The increasingly rampant identity theft activities such as "phishing" have made the traditional password authentication inadequate.

## The Impact

Identity theft has led to unauthorized access to information, and in many cases, financial losses due to unauthorized financial-related transactions.

## The Challenges

The challenges for mitigating this issue include:

- Can the solution stop all kinds of identity theft activities?
- Can the solution be easily implemented to thousands of users?
- How to keep the total cost of ownership low and manageable?

## Common But Inadequate/Cumbersome Countermeasures

Although there are numerous solutions available in the market, most of them are merely partial solutions to the problem, cumbersome to implement or too costly.

- Question and answer challenge response is still vulnerable to phishing because an ignorant user can still be simply tricked to reveal such information.
- Server identification by displaying a known secret text/image of the user will still fail when there is a man-in-the-middle between the user and the server.
- Token-based authentication (both hardware tokens and SMS-based tokens) is vulnerable to man-in-the-middle attacks.
- Client digital certificates and smart cards are strong authentication solutions but are also cumbersome to manage or costly to deploy.

## The Solution

TheGRID is a user device identification and authentication solution commonly used for the following purposes:

- Two-factor authentication to double verify user identity during login to a web portal
- User device restriction to deter unauthorized account sharing

TheGRID solution offers the following benefits:

- Cost-effective and easy deployment
- User friendly and hence easy acceptance
- No change in existing user login process
- No additional support infrastructure
- No additional device inventory management
- Meets regulatory requirements

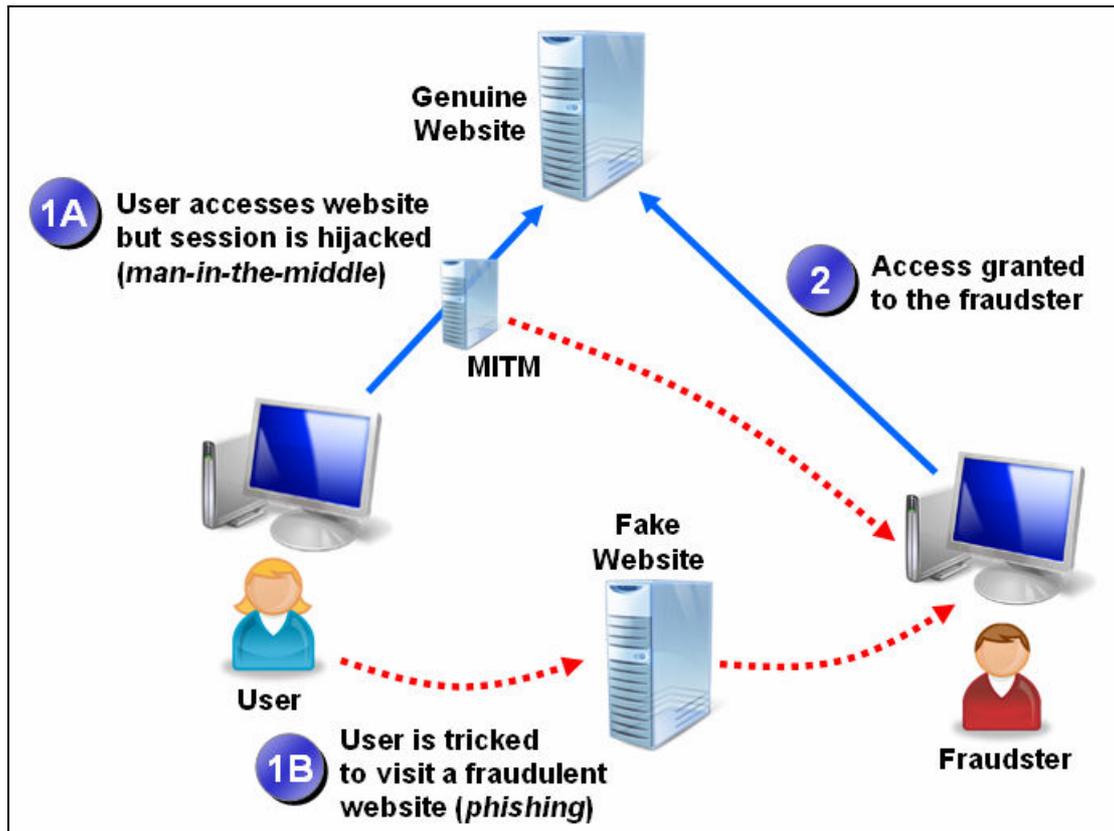
TheGRID has been deployed by online web portals from across the industry:

- Online securities trading (e.g. SBI Securities, Japan)
- Online fund transfer (Tune Money Cash Card)
- Online banking (e.g. Alliance Bank)
- Online paid content provider (e.g. PricewaterhouseCoopers eTax virtual library)

# 1. Introduction

## 1.1 The Issue – Identity Theft

Identity authentication is the process of examining the genuineness of a claimed identity. In the case of a website authenticating the identity of its user, the typical approach is requesting the user to supply the user's login ID and a secret password supposedly only known to the user and the website. However, the increasingly rampant identity theft activities have made the traditional password authentication inadequate. The common technique used is "*phishing*", where users are tricked to divulge their passwords. There are also reported cases of "man-in-the-middle", where the user's login session is hijacked.



## 1.2 The Impact

The impact of identity theft could be any of the following:

- Loss of confidential information, if the stolen account grants access to confidential personal or business information.
- Financial losses, if the stolen account grants access financial-related transactions such as Internet banking or online stock trading.

## **1.3 The Challenges**

### ***Effectiveness***

Firstly, the solution used as a countermeasure to identity theft should be effective against both the common attacks such as phishing and also the advanced attacks like man-in-the-middle.

### ***Ease of Implementation***

Next, the solution should be easily integrated with the existing the website and practical to be deployed to large number of users with minimum efforts. Also, the solution should require minimal user involvement and if possible, totally transparent to the users.

### ***Cost Considerations***

Lastly, the solution should be cost-effective even for large scale deployments to thousands or millions of users. It should also minimize both initial investments and ongoing operation and maintenance costs.

## 2. TheGRID – Stop Identity Theft

TheGRID is a user-end device identification and authentication solution commonly used for the following purposes:

- Two-factor authentication for additional validation for logins or transactions
- User device identification and restriction to deter unauthorized account sharing

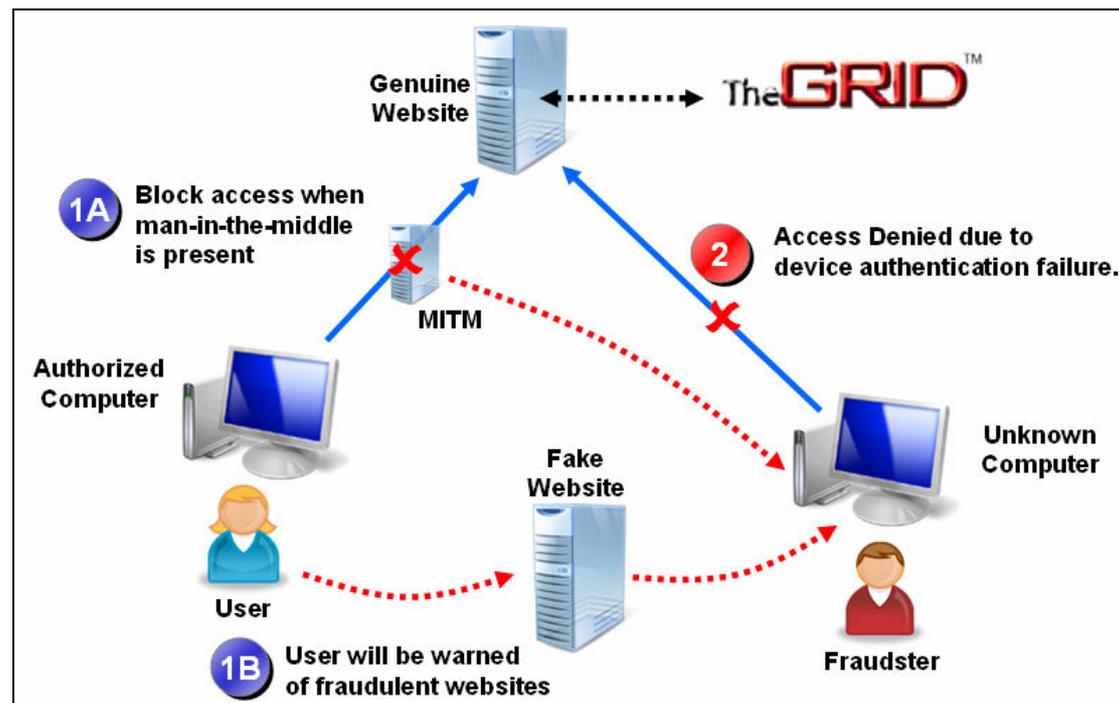
This section focuses on objective to stop identity theft.

### 2.1 Two-factor Authentication

TheGRID implements two-factor authentication using the user's device as the additional proof of user's identity.

Two-factor authentication is the introduction of "*something the user has*" as the additional proof of identity to complement the existing proof based on "*something the user knows*" (the password). This additional proof could be anything that is owned by or in possession of the user, and has previously been made known to the website through a registration process.

Zero physical deployment can be achieved by rephrasing "*something the user has*" to "*something the user already has*"! Since it is something that is already with the user, no additional physical item needs to be delivered to the user.



By registering the set of devices used by the user to access the website and associating the set of devices to the user's login ID, two-factor authentication is achieved by uniquely identifying the user's device and verifying it with the list of registered devices for that particular user. The device registration process can easily be incorporated seamlessly into a website's existing login workflow.

### 2.2 Mutual Authentication

TheGRID implements mutual authentication by providing users with a friendly tool to identify a known genuine website.

The centre of attention on web authentication has normally been the user authentication performed by websites. However, one often overlooked aspect of web authentication is the website authentication by the user. In fact, the successes of recent phishing attacks owe a great deal to the inability of users to distinguish between genuine websites and the fraudulent website replicas. TheGRID addresses this very important issue which is typically not addressed by some other alternative approaches. Mutual authentication is also known to be effective against the "*man-in-the-middle*" attacks.

This is an optional feature normally implemented in the second phase of TheGRID deployment after the two-factor authentication has been fully deployed.

## **2.3 Key Benefits**

### **2.3.1 Security With Total Convenience**

TheGRID secures online businesses without compromising user convenience. Customers will continue to enjoy the same login experience while the underlying two factor authentication works in the background.

### **2.3.2 Control and Confidence**

TheGRID allows customers to easily and completely control where they can access the website from. Users will have confidence that no one else can access their online accounts even if their login credentials have been stolen.

### **2.3.3 Website Identity Assurance**

TheGRID performs stringent website verification so that users can now be assured of the true identity of the website they visit with just a casual glance, and will less likely be victimized by online scams and fraudulent websites.

### **2.3.4 Easy Deployment**

TheGRID solution can be quickly and easily deployed over the web to the masses with virtually zero deployment cost.

### **2.3.5 Easy Maintenance**

TheGRID solution requires no maintenance. There is no end user security device to maintain.

### **2.3.6 Low Cost of Operation**

TheGRID solution requires virtually no operating cost by utilizing your existing web infrastructure.

## **2.4 How It Works**

### **Two Factor Authentication**

TheGRID will only allow access from devices that has been registered by the user. The registration process is simple and straightforward with just one step required of the user – to perform a quick email verification.

The registration workflow is outlined below and also illustrated in the diagram below:

1. User logs in at a device that has never been registered by the user.
2. TheGRID detects that this device is not one of the registered devices and hence denies access. However, an email will be sent automatically by TheGRID to the user's email address that has previously been registered with the website. The website displays a page informing the user about the login failure and requests the user to check the verification email.
3. The user clicks a hyperlink on the verification email which triggers TheGRID to verify the email link and registers the user's current device.

4. TheGRID redirects the user back to the web portal. Any subsequent login from this registered device should be successful without any intervention, as described in the previous section.

The user login experience will not change with the introduction of TheGRID. The redirection to TheGRID server is automatic and happens in just a very brief moment. Once the user has entered the existing login ID and password, the next screen seen by the user is the main screen of the website. Please note that the user is not required to perform any additional steps for the two-factor authentication to take place. Device identification and verification takes place in the background without any user's intervention.

### ***Mutual Authentication***

TheGRID solution comes with an additional component called TheGRID Authenticator that can optionally be deployed to the users in the form of a web browser add-on to enable mutual authentication.

TheGRID Authenticator is configured with technical information about the genuine websites. Whenever a user visits a known website, a quick but stringent website identity verification process will take place to ascertain the integrity of the website. Fraudulent websites and man-in-the-middle systems will always fail the website verification process.

In addition, TheGRID Authenticator will only submit the two factor information to a trusted genuine website after a series of stringent website identity verification to prevent the security information from falling into the wrong hands. Hence, TheGRID solution is not vulnerable to phishing or even the man-in-the-middle attacks.

TheGRID Authenticator is an optional feature and should only be implemented when deemed necessary. It should be deployed in a later project phase after the standard two-factor authentication has been fully deployed.

## 2.5 Comparison

	TheGRID	Hardware OTP Token	SMS OTP Token
<b>Features</b>			
Two Factor Authentication	Yes	Yes	Yes
Genuine Website Identification	Yes	No	No
Blacklisted Site Blocking	Yes	No	No
<b>Effectiveness</b>			
Anti-phishing	Yes	Yes	Yes
Anti-Man-In-The-Middle	Yes	No	No
<b>Ease of Use (End User)</b>			
First-time Registration	Registration of user devices via email/web	Activation of token via web	Registration of phone number via web / ATM
Normal Day-to-day Usage	No action required	Enter token code	Wait for text message and then enter OTP
Physical item to bring along	None	Token	Mobile phone
<b>Ease of Deployment</b>			
New Hardware	Auth Server	Auth Server, tokens	Auth Server, SMS Gateway
Physical Delivery	None	Delivery of tokens by courier service	None
Speed of deployment to millions of users	Immediate, as and when user logs in	A few weeks	Immediate or over a few days, subject to registration method
<b>Cost</b>			
Initial Costs	Licensing, Servers, Implementation	Licensing, Servers, Implementation, User Tokens	Licensing, Servers, Implementation, SMS system
Operation / Maintenance Costs	Servers	Servers, Tokens	Servers, SMS system, Messaging
Additional Growth Costs	Licensing	Licensing, Tokens	Licensing, Messaging

# Contact Information

---

Company	e-Lock Corporation Sdn Bhd
Address	Business Suite, 19A-26-3A, Level 26, UOA Centre 19 Jalan Pinang, 50450 Kuala Lumpur, Malaysia.
Phone	+ 60 3 2166 2981
Fax	+ 60 3 2166 2982
Website	<a href="http://www.elock.com.my/">http://www.elock.com.my/</a>
Email	info@elock.com.my