



Solution Overview



e-Lock Corporation Sdn Bhd

www.elock.com.my
email: info@elock.com.my

September 2006

Table Of Content

Table Of Content	2
Executive Summary.....	3
Overview	3
Limitations Of Some Common Solutions	3
The GRID™ - The Real Answer To Identity Theft	3
Background - Understanding Identity Theft.....	4
Understanding Electronic Identity	4
Common Identity Theft Techniques	4
Phishing.....	4
Pharming.....	4
Keylogging.....	4
Man-In-The-Middle	4
The GRID™ – A Complete Anti-Identity Theft Solution.....	5
The GRID™ – General Overview	6
The GRID™ Authenticator.....	7
Helping Users Authenticate Websites	7
Enabling Strong 2-Factor Authentication	8
The GRID™ 2-Factor.....	8
Device-based Two Factor Authentication	8
Effective Against Man-In-The-Middle Attacks.....	9
Mobility and Device Management.....	9
The GRID™ Shield	10
Who needs The GRID™ ?	11
Banking and Finance – Online Banking.....	11
Internet Service Provider – Online Access	11
Retail – Online Shopping	11
Content Providers – Online Subscription.....	11
Government – Electronic Services.....	12
Corporate – Operations	12
Conclusion.....	13

Executive Summary

Overview

Phishing, pharming, keylogging and man-in-the-middle (MIM) attacks are advanced identity theft techniques used by cyber criminals and fraudsters today to threaten the security of online electronic transactions and to cause huge financial losses to the financial institutions, e-service providers and their customers worldwide.

Limitations Of Some Common Solutions

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

- Anti-spam is only good for blocking email-based phishing but not effective against pharming or keylogging.
- Dynamic keypads will mitigate the risk of keylogging but does not stop phishing or pharming.
- 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 does not prevent keylogging and will 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) cannot stop users from being phished or pharmed, and it is vulnerable to the man-in-the-middle attack.
- Client digital certificates and smart cards are strong authentication solutions but are also cumbersome to manage or costly to deploy.

The GRID™ - The Real Answer To Identity Theft

The GRID is the true solution that will address phishing, pharming, keylogging and man-in-the-middle attacks. The GRID has been designed to address a very fundamental issue about identity theft – "How do I know it is really you and how do you know it is really me?"

The GRID is specifically tailored for e-service providers to strengthen their user authentication process and to protect their customers from identity theft. The GRID allows e-service providers to verify the true identity of their users, and at the same time, helps their users reveal the true identity of the websites.

The GRID is a true two-way two-factor authentication solution. It is a modular solution with the following components:

- **The GRID Authenticator:** Helps user authenticate the e-service websites
- **The GRID 2-Factor:** Provides stronger device-based user authentication
- **The GRID Shield:** Protects user's system from Trojans and Spyware

Depending on the deployment requirements, different module combinations can be selected.

In addition, The GRID is designed to meet the following business objectives:

1. Cost-effective and easy deployment
2. User friendly and hence easy acceptance
3. No change in existing user login process
4. No additional support infrastructure
5. No additional device inventory management
6. Meets regulatory requirements

In short, The GRID is the most effective solution to battle phishing and related crimes today. It is ideal for e-services including online banking, internet services, trade portals, content providers, e-learning sites and any web portal that may be targeted by phishers and fraudsters.

Background - Understanding Identity Theft

Before evaluating any anti-phishing or identity protection solution, it is important to firstly understand the problem – identity theft, and its common techniques such as phishing, pharming, keylogging and MIM.

Understanding Electronic Identity

Normally, each person who is authorized to access an online electronic service, such as e-banking or online trading, is given an electronic identity in the form of a user account which consists of a user ID and a password. Whenever a user wishes to access a particular online service, the user has to:

- 1) visit the website of the online service
- 2) submit the necessary credentials to login, such as user ID and password
- 3) upon successful verification of the user ID and password, the user is granted access.

Cyber criminals and fraudsters typically target its victims at step (1) or step (2) above.

Common Identity Theft Techniques

Phishing

"Phishing" is a trick to lure its victims into believing that a fraudulent website they are visiting is the genuine website, and subsequently revealing their online identity to the fraudsters. Normally, an email with fraudulent content is sent to potential victims with the hope that some of the email recipients will visit a fake website that looks like the genuine website. The victims are then tricked into submitting their login credentials (user ID and password). These login credentials will allow the fraudsters to access the real online service using the stolen identities of the victims.

Pharming

"Pharming" is a more advanced identity theft technique but with the same objective as phishing – to steal electronic identity. Rather than distributing fraudulent emails and exploiting user ignorance, pharming quietly diverts users who are trying to visit a genuine website to a look-alike fraudulent website where their identity will be stolen.

Keylogging

"Keylogging" is a technique used to steal user ID and password when a user submits these login credentials to the genuine website. This is normally achieved by firstly infecting the user's system with a "Trojan Horse" or spyware that quietly records all the keystrokes of the user. The recorded keystrokes including the user ID and password typed by the user will be periodically sent to the criminals.

Man-In-The-Middle

As its name implies, a "man-in-the-middle" (MIM) is positioned between a user and the targeted e-service website. Typically, the MIM will relay information back and forth between its victim and the genuine website to steal the login credentials or to hijack the login session. The strength of such an attack is that the user will think that the MIM is the genuine website since all the information presented appears to be correct, and likewise, the e-service website will believe that it is communicating directly with the user since all the login credentials are correct.

Man-In-The-Middle is an advanced attack that will circumvent many two-factor authentication schemes that require the users to submit additional authentication codes because the users do not know that they are actually submitting these additional security information via the MIM.

In the next section, we will explain how The GRID will address all the above issues.

The GRID™ – A Complete Anti-Identity Theft Solution

The GRID solution has been conceived and designed based on thorough understanding of the issue of identity theft and the associated techniques such as phishing, pharming, keylogging and man-in-the-middle attacks.

By analyzing carefully the requirements for an effective solution against identity theft, we can conclude the following:

1. Phishing has been highly successful because many users could not differentiate between the genuine websites and their fraudulent counterparts.
2. Pharming exploits our trust on the website address information that can be modified by hackers.
3. Keylogging can be successful because the user's PC can be easily compromised.
4. Man-In-The-Middle attacks are possible because a general user will not be able to detect the presence of the man-in-the-middle. In addition, since the MIM is able to relay all the login credentials as well as the additional factors of authentication, it is also difficult for the e-service website to detect the presence of the MIM.

Based on the above, The GRID has been developed to fulfill the following technical criteria:

1. Help users easily recognize genuine websites and detect the fraudulent ones.
2. Identify the genuine website without depending on website address information.
3. Block the user from accidentally connecting to known phishing websites.
4. Help users minimize the risk of infection by keylogging spyware.
5. Allow the e-service provider to request for additional factors of authentication to complement the existing user ID and password authentication.
6. Detect the presence of MIM and prevent submission of additional factors of authentication when the MIM is present.

Furthermore, The GRID was designed with the following key business objectives:

1. To remain cost effective for both initial rollout and maintenance
2. To implement easily for the e-service providers
3. To allow easy large scale deployment
4. To minimize training required for users
5. To eliminate changes to existing login processes
6. To minimize additional operation workload
7. Minimize additional support infrastructure requirements
8. To scale easily to accommodate large user base
9. To deliver a long term solution for e-service providers

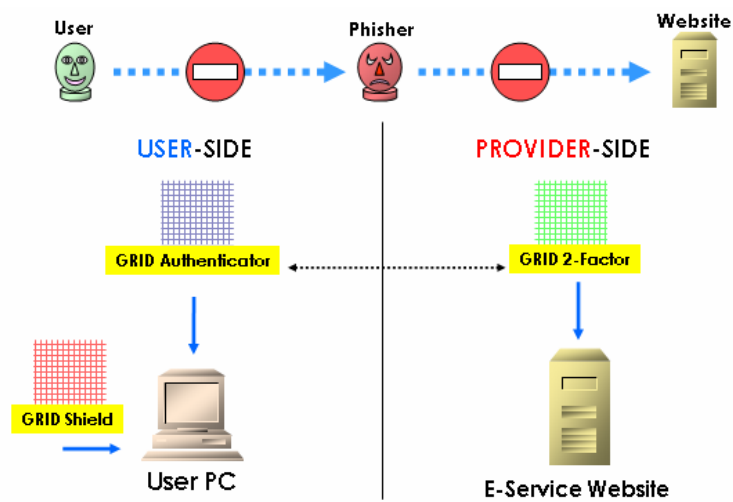
The GRID offers all the above benefits to ensure smooth implementation and operation.

The GRID™ – General Overview

The GRID is a complete solution to battle identity theft. It is an ideal solution for e-service providers to deploy at their e-service portals as well as for the customers. The solution consists of three main components:

- The GRID Authenticator
- The GRID 2-Factor
- The GRID Shield

Each component can be implemented independently to achieve different security objectives. However, when combined, the components work as a single formidable solution to battle even the most advanced identity theft method like MIM.



Essentially, The GRID adopts the following approach:

1. Minimize the risk of users losing their login credentials to phishers and fraudsters
2. Prevent phishers from unauthorized access even if they have valid login credentials

Generally, the process of authentication is as follows:

Step 1: The GRID Authenticator ensures the user that he is connecting to the real website
 Step 2: Upon successful authenticating the website, only then the user's login information is released together with the user's device ID (representing the 2nd factor). Here the GRID 2-factor authenticates if the user is logging in from a registered device.

Step 1 and Step 2 achieve a true 2-way 2 factor authentication process. User authenticates the website first, and subsequently the website authenticates the user device.

The GRID Shield is provided to ensure that the user's system environment is not susceptible to unauthorized installation of programs such as Trojans, spyware, etc.

Note that the entire process of 2-way authentication is transparent to the user. In the background, The GRID adopts the following techniques to perform authentication:

- Realtime identification and verification of websites
- Verification based on whitelist, blacklist, website certificate and protected web address information
- Two factor authentication using user device serial number or secure browser cookies
- Realtime security alerts and blocking of known phishing sites.

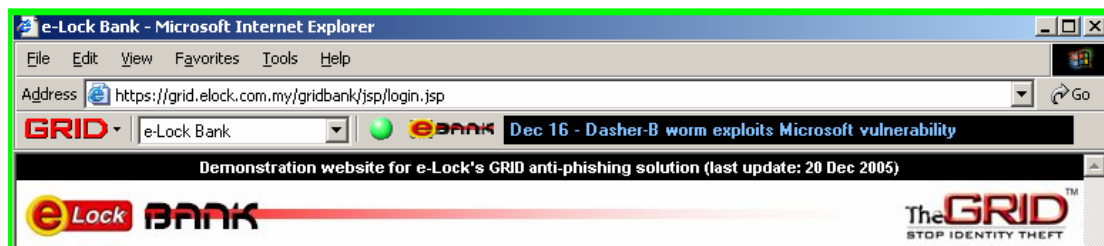
The GRID™ Authenticator

The GRID Authenticator provides end users with the first layer of defense against phishing, pharming and man-in-the-middle attacks. Its primary purpose is:

- To ensure that users connect to the genuine e-service website
- To warn users when the website cannot pass the stringent verification tests
- To block users from visiting known active phishing websites

In other words, it helps the user answer the question – “Is it really you (the genuine website)?”

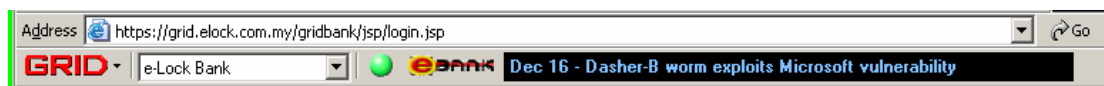
The GRID Authenticator is implemented as a light-weight web browser plug-in that can be easily distributed to the masses. Once installed, The GRID Authenticator will appear as a toolbar within the web browser as shown below:



Helping Users Authenticate Websites

The featured e-service websites will be shown in a dropdown menu to allow the user to easily select and visit the e-service website. (A featured website is an e-service website that participates in The GRID authentication program.)

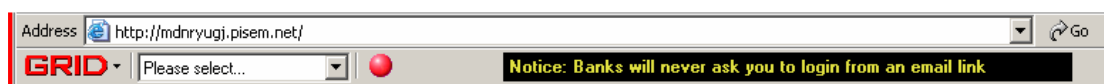
More importantly, whenever a web user visits a featured website, The GRID Authenticator will perform a series of very stringent and technical tests on the visited website, using e-Lock's advanced and patent-pending web authentication technology. Subsequently, it will inform the user on whether the website is authentic using an easy-to-understand "traffic light" system. In this case, the traffic light will turn "green", indicating that the visited website is a genuine featured website. The "green" color will become a form of assurance to the user that the visited website is genuine and trustworthy. An example is shown below:



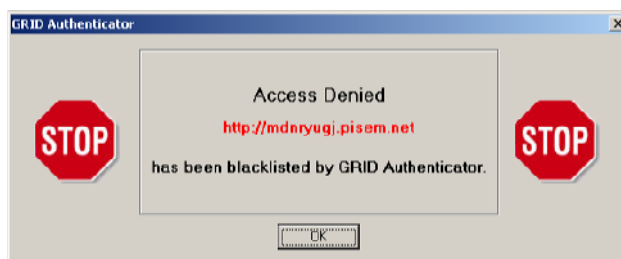
On the other hand, if a web user is tricked into visiting a fraudulent website but believing that it is the genuine website, The GRID Authenticator traffic light will not turn green. Since the normal "green" indicator is not shown, the user will notice the difference and be more aware of a potential scam.

For non-participating websites, The GRID Authenticator will remain passive and hence will not display any authentication status.

However, for known and confirmed fraudulent websites, they will be blacklisted by The GRID Authenticator. In this case, the traffic light will turn red indicating a no-go. An example is shown below:



In addition, access to such blacklisted websites will be blocked by the GRID Authenticator. A sample blocking dialog box will pop up to stop the user from proceeding further.



With this easy to understand traffic light system, a non-technical user can now easily identify a trustworthy participating website by looking for the “green” color indicator. When the GRID Authenticator gives the green light for a participating website, it is safe for the user to proceed with the login process; otherwise the user should never proceed.

Besides verifying websites, the GRID Authenticator also plays an important role in educating the users on security practices and issues. The GRID Authenticator will receive and display security news and alerts from trusted sources.

Enabling Strong 2-Factor Authentication

When The GRID Authenticator is used in conjunction with The GRID 2-Factor, the e-service login authentication can be enhanced with the powerful device-based authentication using user device serial number as the second authentication factor. Please refer to the GRID 2-Factor section for details.

The GRID™ 2-Factor

The GRID 2-Factor provides a cost effective mechanism for e-service providers to enable two-factor login authentication. The GRID 2-Factor will complement any existing user ID and password authentication, and will help to prevent unauthorized access even when the user ID and password have been stolen from the user.

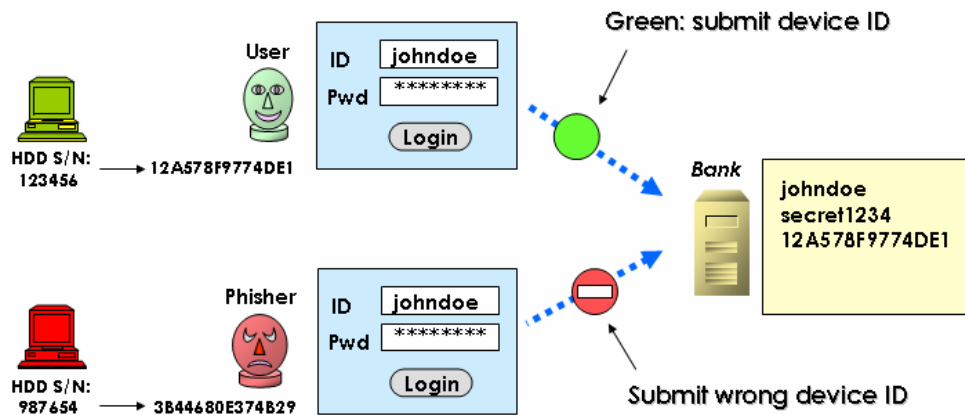
The GRID 2-Factor consists of an authentication server to be deployed at the e-service site, and communicates with the e-service web application. Upon user login, the web application will firstly perform the routine user ID and password verification, and then request the GRID 2-Factor authentication server to perform the additional authentication.

Device-based Two Factor Authentication

The GRID 2-Factor functions by associating each user with a trusted device (or a group of trusted devices). Now, it is necessary for everyone to login using valid login credentials from a registered trusted device. In other words, a phisher will not be able to access the e-service even if the user ID and password have been stolen using phishing, pharming or keylogging techniques because the phisher is not accessing the e-service from a registered device.

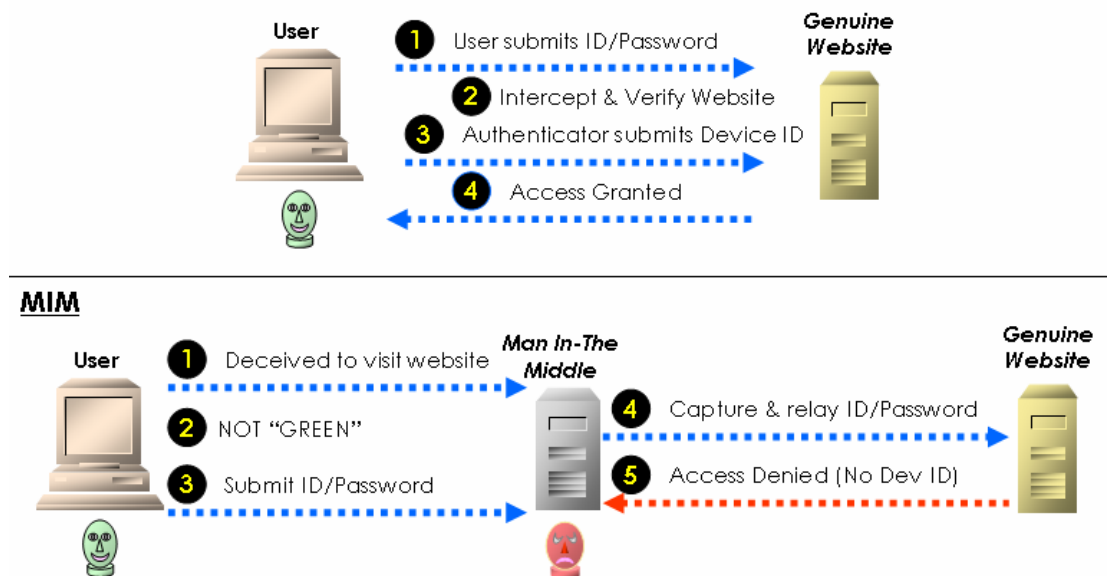
The GRID 2-Factor supports two types of user-device association:

- a) When used as an independent component, user devices are tagged with secure browser cookies;
- b) When used in conjunction with The GRID Authenticator, user devices are identified using secure hash signature of hardware serial number.



Effective Against Man-In-The-Middle Attacks

The combination of The GRID Authenticator and The GRID 2-Factor provides one of the most robust two-way two-factor authentication mechanism that is not vulnerable to man-in-the-middle (MIM) attacks today. The GRID Authenticator will NOT transmit the device identification if a website fails the stringent genuine website test as described in the previous section. Hence, in the case where a MIM is present, the MIM will not receive the secret device identification and will therefore fail the two-factor authentication of the e-service website: Please see the illustration below.



Any other two-factor authentication systems that require users to enter and submit the additional authentication codes are vulnerable to man-in-the-middle attacks. This is because the user will not be able to detect the presence of a MIM and can be easily tricked into submitting the additional authentication codes.

Mobility and Device Management

One question often raised is whether user's mobility will be impeded with the association of a user account to fixed devices. The answer lies in the flexible self-management capability of The GRID system. The device management function is made available normally as part of the existing e-service website (pre-built program templates are available to the e-service provider for quick integration). A user may easily add a new authorized device or delete an existing registered device by accessing the device management screens from an existing registered device.

A typical workflow for a user to register a new authorized device is as below:

- 1) A user logs on to the e-service website from a registered device associated to the user's account
- 2) The user accesses the device management feature and makes a request to allow a new device to be registered.
- 3) The GRID will record this request and issue a "device registration ticket" to the user. The ticket will be valid for a fixed period of time (typically 24 - 72 hours, subject to e-service provider's policy) and will contain a user-defined one-time registration code.
- 4) When the user logs on from another device (i.e. the device to be registered) within the ticket validity period and with the correct user ID, password and the one-time registration code, this new device will be registered as an authorized device for this user.

The entire process above can be performed by the end user without involving customer service personnel of the e-service provider. This mobility scheme provides a good balance between security and flexibility.

In summary, The GRID 2-Factor supports the following management features:

- a) Same user on multiple registered devices – when users need to log in from multiple trusted devices (such as home PC, office PC, notebook, etc).
- b) Multiple users on the same device – when more than one users share the same PC (such as when a home PC is shared by members of the family).
- c) Users can self-manage their trusted devices, such as to register new trusted device or to revoke a registered device, all without intervention from the e-service provider.
- d) Full audit trail on user access and device management is available to the e-service provider.

The GRID™ Shield

The GRID Shield is a powerful software for defending the user's system against infection by Trojans and spyware. By blocking unauthorized copying and downloading of malicious programs such as keyloggers, user login credentials are protected from being stolen due to keylogging activities.

The GRID Shield is available as an optional download for all users of The GRID Authenticator. Once installed, The GRID Shield will block all known and unknown spyware from infecting the user's system. A user can momentarily disable The GRID Shield to allow for authorized program installation.

Unlike other anti-virus or anti-spyware programs, The GRID Shield does not rely on virus patterns and signatures. The GRID Shield will prevent any executable programs from being installed unless specifically allowed by the user. The GRID Shield is highly robust and cannot be bypassed even for attacks which compromise system administrative privileges.

The GRID Shield is effective against Trojans and spyware with executable file types including exe, com, sys, dll, ocx, vxd, scr, pif, vbe.

Who needs The GRID™ ?

The GRID is a robust two-way two-factor authentication system suitable for both commercial applications and daily business operations across the various industries.

Banking and Finance – Online Banking

Issue

The banking and finance sector has been the primary target of identity theft crimes. Approximately 90% of the phishing scams target the financial institutions where customers using the online financial portals are often the victims.

How will GRID help?

The GRID protects online financial portals with robust device-based two-factor authentication and at the same time provides the customers with an easy and yet reliable means for identifying genuine websites.

Internet Service Provider – Online Access

Issue

Internet service providers are the next major targets where users' access login credentials are stolen for the unauthorized access. Such identity thefts affect the monthly bills of both broadband and dial-up Internet users, especially those charged based on bandwidth usage.

How will The GRID help?

The GRID stops bandwidth thieves from enjoying unauthorized access by requiring them to prove their identities using devices owned by the actual users.

Retail – Online Shopping

Issue

The retail sector is another target of the identity theft criminals where online shopping account login credentials are stolen. The criminals may be able to access shopping records and delivery addresses so that further crimes can be undertaken, and worse still if the shopping website keeps credit card information.

How will The GRID help?

The GRID ensures a pleasant online shopping experience by helping shoppers identify the genuine shopping portals and preventing phishers from logging from unauthorized devices.

Content Providers – Online Subscription

Issue

The providers of online content such as movies, music and electronic newspaper, face a different issue – the abuse of subscription account by the genuine users rather than identity theft. One person may sign up for an online subscription but the account login credentials are shared among many people, contributing to a loss in potential revenue for the content provider.

How will The GRID help?

The GRID can be tuned to restrict a user to login from a limited number of locations to prevent mass sharing of a single paid account, and therefore helping the content providers to prevent users' usage abuse and violation of subscription agreement.

Government – Electronic Services

Issue

Many government departments and agencies have started to offer online services. These online websites may contain confidential personal information such as the social security number, balance of employee provident fund, etc., which might be of interest to identity thieves.

How will The GRID help?

The GRID helps establish trusted e-government services and protects public interest with its robust two-way two-factor authentication.

Corporate – Operations

Issue

In general, enterprises today use various business applications for internal and external use, including private intranet applications, ERP and CRM systems, customer service portals and partner portals. However, most of these business applications only provide one-way authentication based on ID and password, which is definitely not adequate.

How will The GRID help?

The GRID helps to strengthen the authentication by complementing any existing authentication mechanisms of the enterprise application. One good example would be web-based email access: The GRID adds device-based authentication to the standard email login ID and password authentication so that only users logging in from designated locations will be granted access to minimize the risk of infiltration within enterprise network.

Conclusion

The combination of all The GRID modules provides both the e-service providers and their customers a complete defense against phishing, pharming, keylogging and man-in-the-middle attacks.

Firstly, The GRID Authenticator helps users differentiate genuine e-service websites from their fraudulent imitations, hence minimizing the risk of users unknowingly submitting user IDs and passwords to the phishers and fraudsters.

Secondly, The GRID 2-Factor offers the e-service providers a robust two-factor authentication mechanism to verify user logins based on registered devices owned by genuine customers. End-user mobility is not sacrificed where users are allowed to have multiple registered devices. When used in conjunction with The GRID Authenticator, this mechanism will still be effective against the advanced man-in-the-middle attacks. This provides the last line of defense against identity theft.

Finally, The GRID Shield provides end-user system protection against keyloggers by preventing unauthorized installation of Trojans and spyware.

The GRID is the only complete solution today against phishing, pharming, keylogging and man-in-the-middle attacks. It is one of the most practical approach to providing two-way two-factor authentications for mass markets.