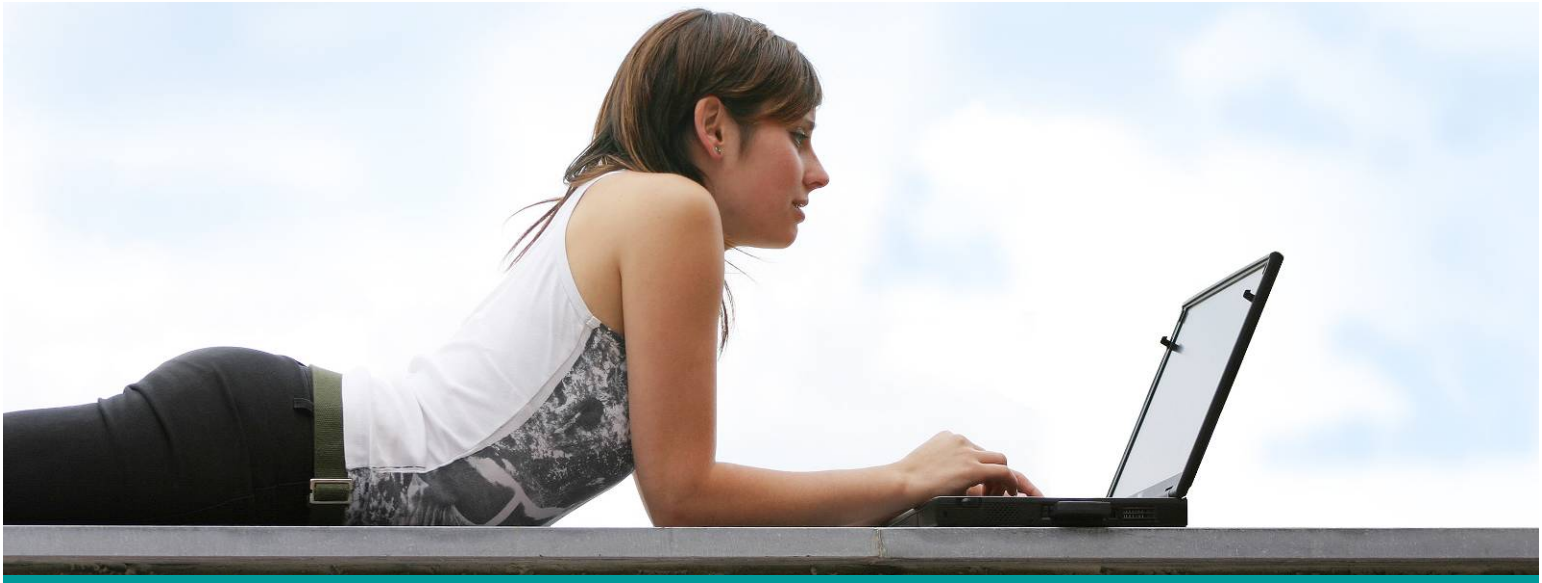
Enhanced Single Factor, 2 Factor & Multi-Factor Authentication Solutions

featuring

Next Generation One Time Passwords, PINs & Enhanced Knowledge Based Authentication

SyferLock™



The Authentication Spectrum

Utilizing SyferLock's Approach to Cross and Cover the Authentication Spectrum

The story and problem are enduring for organizations and security conscious individuals: traditional reusable passwords are at the "breaking point", and no one solution seems to be adaptive enough, flexible enough and secure enough to help with the ever increasing and ever changing business cases and user needs. SyferLock Technology has created one of the most secure, adaptive and flexible systems to help address the "breaking point". Key features:

- Deviceless One Time Password Generation
- Zero Foot Print – No Additional Client-Side Hardware or Software
- Greatly Reduced TCO
- Highly Flexible, Adaptive and Customizable

Static/Reusable Password — **2FA / Multi-factor**

Static / Reusable Passwords and PINs

At one end of the authentication spectrum you have reusable passwords that are weak and vulnerable against the most prevalent and easily executed attacks.

Attempts to make them "limited time passwords" i.e. expire every 30,60,90 days add no real strength to the threat matrix, but add a real Total Cost of Ownership (TCO) burden to users and organizations.

Even with the known weaknesses static passwords are the most pervasive form of authentication for the majority of users.

2 Factor and/or Multi-Factor

At the other end of the spectrum you have 2 factor, or what has historically been called strong authentication.

While delivering increased strength from One Time Password generation and "having something", traditional hardware and the very nature of the "something you have" unfortunately create real limitations.

Heavy burden on TCO and limited deployment force organizations to go bare due to budget constraints even in the needs and mandates of regulatory bodies and guidelines (e.g. PCI, SOX, FFIEC, HIPAA, BASEL).

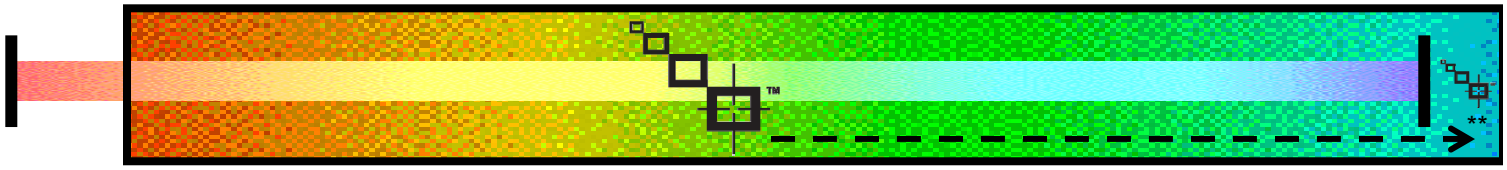
Also the challenge still exists to have a secure, un-intrusive "plan B" for lost, stolen, or broken devices.

SyferLock

The Authentication Spectrum

Utilizing SyferLock's Approach to Cross and Cover the Authentication Spectrum

Static/Reusable Password **2FA / Multi-factor**



** SyferLock's AutoToken™ technology provide 2 Factor and Multi-Factor standards

---

Filling the Void and Covering the Spectrum

SyferLock Technology's unique approach and methodology address the large part of the spectrum between insecure static/reusable passwords and costly, cumbersome two-factor solutions . SyferLock delivers proven, effective security through one time passwords or PINs, while allowing IT security a viable alternative to static passwords delivering greater information access control.

Unique Features of the Grid Data Security Solution

- Utilizes a user's existing password and organization's account directory

- Absolute zero client footprint and deviceless in nature

- Lower TCO and lightweight aspects allow for complete user coverage

- Bolsters and works in conjunction with other factors and security measures

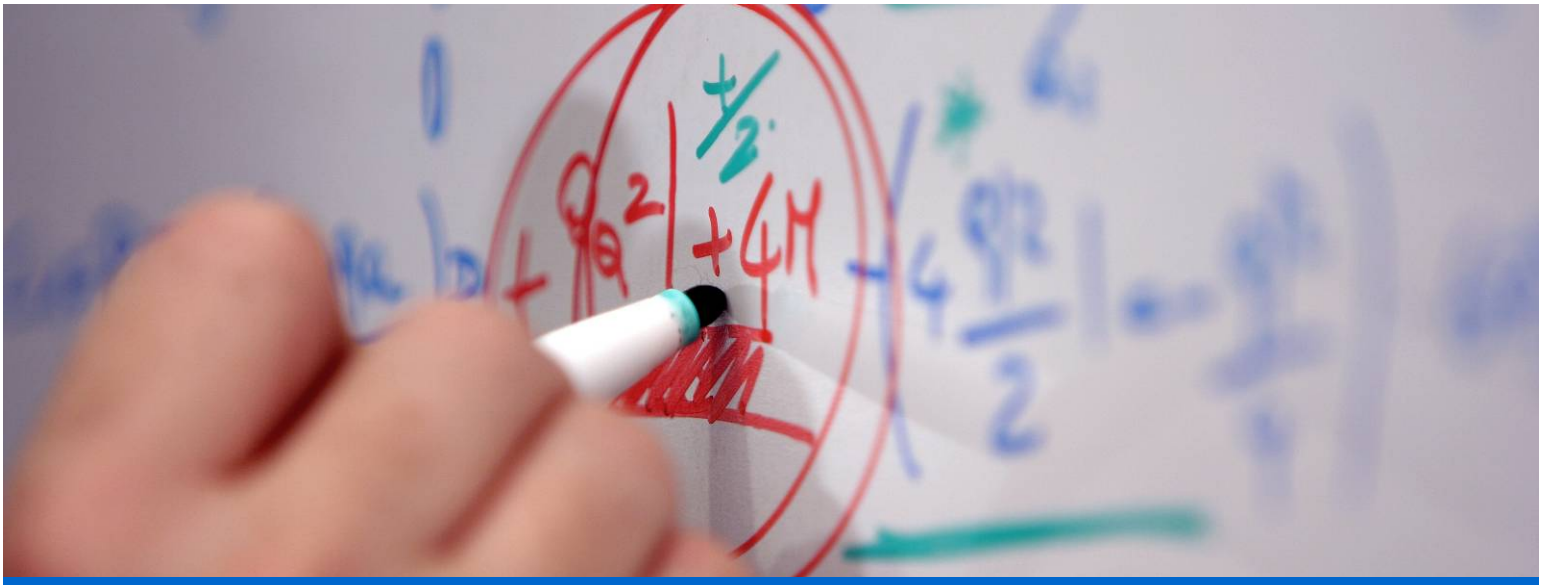
---

Critical Security Benefits Delivered

Grid's OTP system eliminates or mitigates the following attacks:

* Key loggers
* Shoulder surfing
* Brute force attacks
* Phishing
* Replay attacks
* Stored browser passwords
* Dictionary attacks
* Password sniffing and interception

SyferLock



The Patented Approach & Methodology

Next Generation One Time Passwords & Enhanced Authentication

SyferLock Technology delivers a family of patented products offering a paradigm shifting approach to next generation One Time Passwords (OTPs) and access to computers, networks and the internet. SyferLock has engineered an enhanced authentication methodology and system providing *deviceless* OTPs allowing Users with a simple, more secure way to access information leveraging their *existing* passwords.

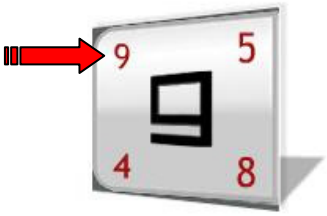
Our solutions deliver unparalleled flexibility through a solution allowing for diverse and evolving authentication needs. The zero footprint aspect allows and provides d*eviceless*, One Time Password generation without any extra client-side hardware or software – ANYWHERE, ANY MACHINE, MORE SECURELY™. Finally, the methodology allows the creation of a layered approach to current authentication processes: stand alone, or used in conjunction with other factors.

Utilize and Leverage the *Existing* Password

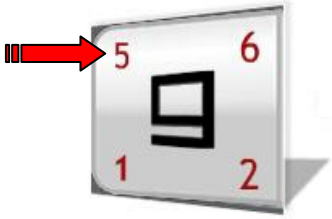
Grid starts with the first factor! Leverage the pervasive use of passwords. It is estimated that 99% of all authentications use static passwords or PINs. Another estimate shows that 95% of authentications use only the first factor of static passwords/PINs. Take the familiarity of a static password, allow the user to continue its use, but now use Grid's innovative system to convert the static password to a dynamic One Time Password consisting of a randomly changing string of numbers.

Grid accomplishes this One Time Password by the power and process of simple substitution. At log-in, substitute the real password with randomly changing numbers! A substitution cipher with the strength of one-to-many. It starts with a single cell that contains a letter or character (or the possibility of any other password character from which users can construct their passwords). Each character has a number (or cryptogram) that sits in each of the four corners of the cell. These cryptograms change at every login or at every screen, UI or page refresh (see below figures) In addition, the cryptograms are fully customizable from the value they display to where they are displayed (i.e. Corner or Position - North, South, East and West).

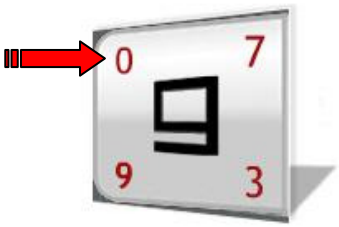
Login 1



Login 2



Login 3…



SyferLock

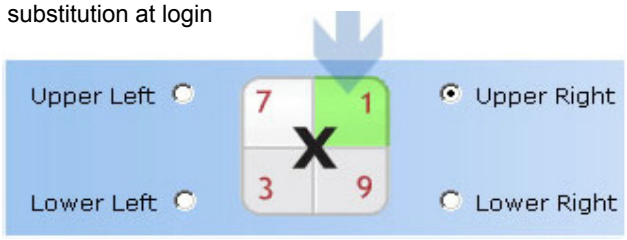
The Patented Approach & Methodology

Next Generation One Time Passwords & Enhanced Authentication

Account Setup - A Simple 2 Step Process

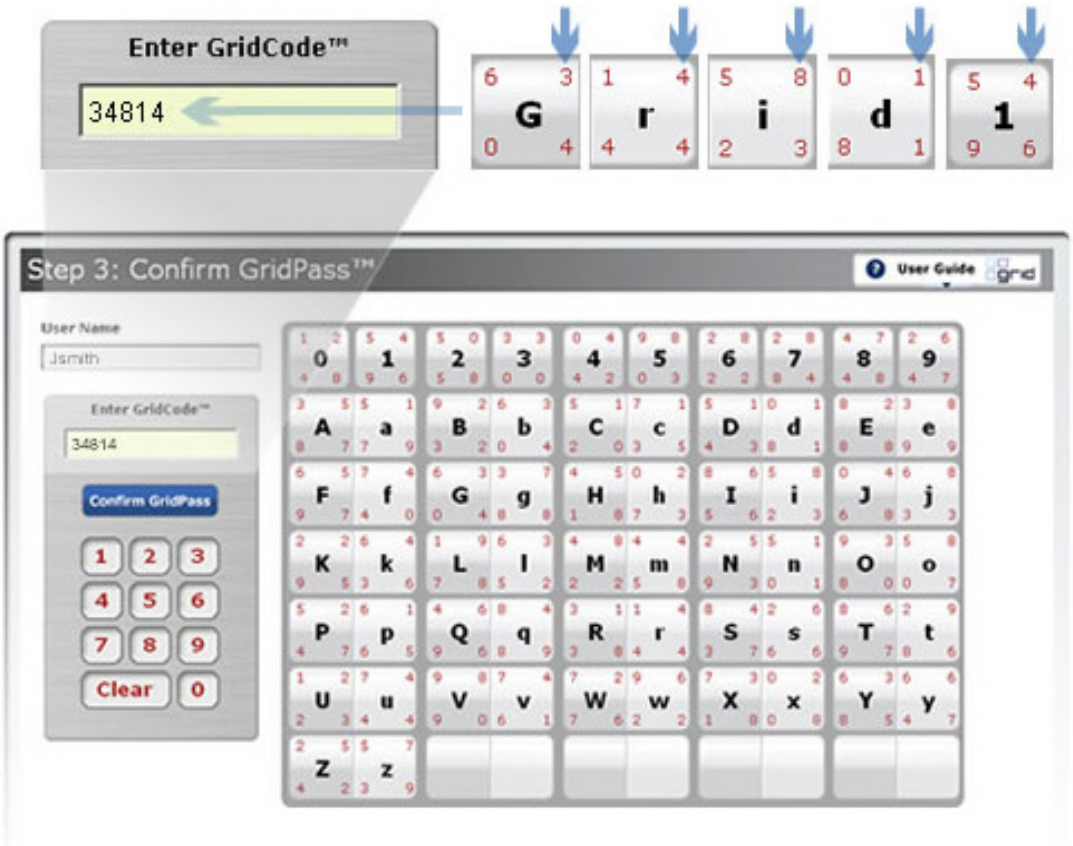
Step 1: The user will enter their existing domain password.

Step 2: The user now chooses which corner to use for substitution at login



User's Reusable Password becomes a One Time Password

At login, users simply refer to the security grid user interface[1]. Looking at the keys corresponding to the characters of their password and the selected target corner, the user will enter the number of the target corner as their GridCode. Upon every refresh and/or new login, the corner numbers randomly change, creating a new one-time password.



[1] The grid user interface can be completely customized through MyGrid™ technology allowing a wide variety of layouts, designs, and languages and/or character sets.

SyferLock

Tuneable, Adaptive and Flexible Security

Next Generation One Time Passwords & Enhanced Authentication

GridAdvanced™ Security Grid UI

The GridAdvanced solution allows greater endpoint security by offering a wide array of security features to its users.

GridBasic™ Security Grid UI (shared corner version shown)

The GridBasic solution delivers key security benefits while making its integration and deployment straightforward and unintrusive.

SyferLock

Tuneable, Adaptive and Flexible Security

Next Generation One Time Passwords & Enhanced Authentication

Grid2Form™ Security Grid UI

The Grid2Form solution allows two vectors to be utilized leveraging the user's password coupled with a one time PIN. Ideal for where PINs are used but enhanced security is warranted.

	EFFECTIVE SECURITY AGAINST	KEY FEATURE(S)
GridAdvanced™	✓ Key Logging ✓ Shoulder Surfing ✓ Replay ✓ Stored Browser Information ✓ Session capture/observation ✓ Brute Forcing	- Advanced feature possibilities - Unparalleled zero footprint security - Endpoint security benefits
GridBasic™	✓ Key Logging ✓ Shoulder Surfing ✓ Replay ✓ Stored Browser Information ✓ Brute Forcing	- Ease of Integration
Grid2Form™	✓ Key Logging ✓ Shoulder Surfing ✓ Replay ✓ Stored Browser Information ✓ Brute Forcing	- Offers two vectors of security - Improves the security of static PINs

SyferLock

Self-Service 2 Factor & Multi-Factor Authentication

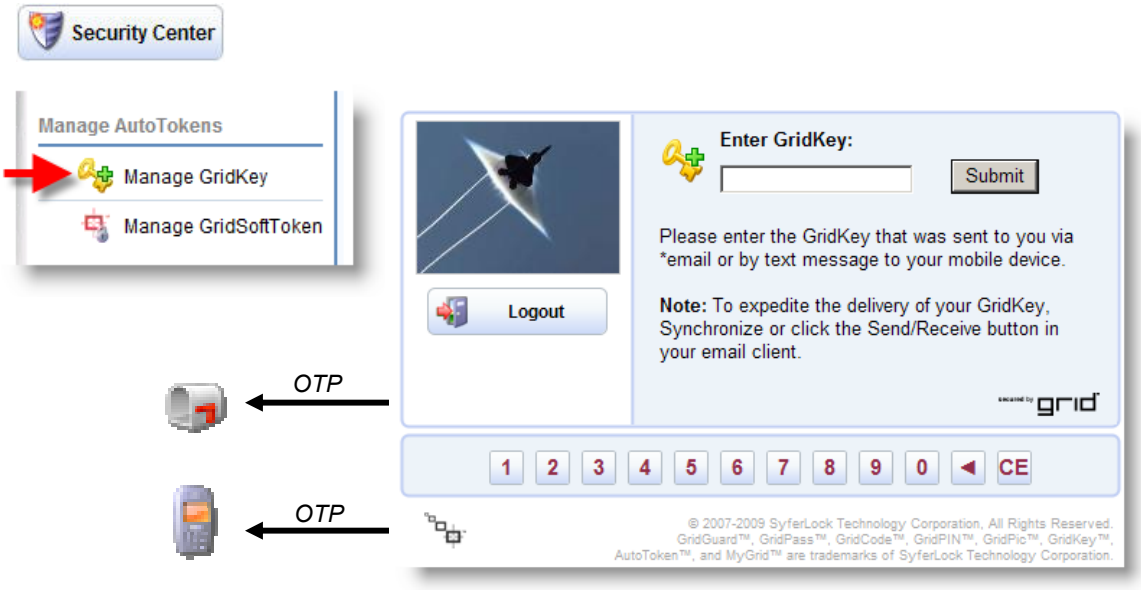
SyferLock's AutoToken™ Technology

Self-Service 2 Factor & Multi-Factor Authentication

SyferLock offers deployments and their users the ability to self-service 2FA through its AutoToken™ technology. AutoToken™ is a 2FA feature that allows the user the option to bolster their authentication with an additional layer or layers of security - by sending a one time password (OTP) to either an email account or phone via SMS text message, by locking their account access to a device, or a combination thereof.

AutoToken™: *GridKey*™ Out-of-Band Authentication

GridKey™ is a 2FA feature that allows the user the option to bolster their authentication with an additional layer of security - by sending a one time password (OTP) to either an email account or phone via SMS text message.



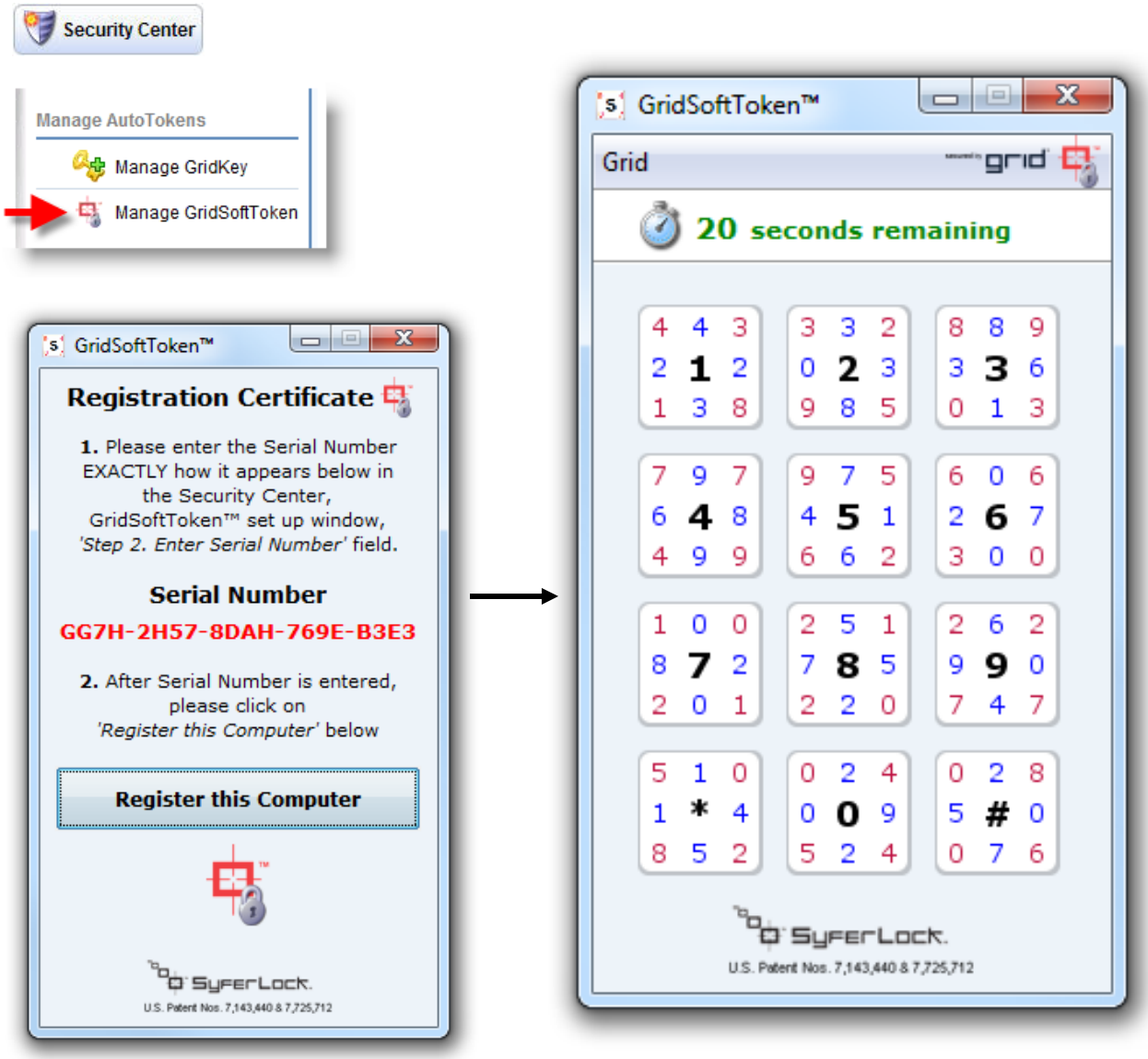
Competitively unique to SyferLock is that the GridKey™ will only be generated and delivered AFTER the user applies and completes a *deviceless* "multi-token" OTP authentication process at their initial login - creating unparalleled secure access. The SyferLock system leverages the user's *existing* password and it is securely entered as an OTP through SyferLock's patented methodology and security grid UI.

Self-Service 2 Factor & Multi-Factor Authentication

SyferLock's AutoToken™ Technology

AutoToken™: *GridSoftToken*™ 2 Factor Device & Superior User Authentication

SyferLock offers deployments and their users the ability to leverage their existing computer or laptop as the 2nd factor "something you have" versus having to buy additional "hard tokens". The users already "have" their machine, why not leverage that? GridSoftToken™ is a Java Network Launching Protocol (JNLP) application that is downloaded to the user's computer or device. The GridSoftToken™ when initially downloaded, leverages various underlying hardware and its associated ID information to determine and generate a unique machine serial number, which is displayed on the registration screen. This serial number is specific to the machine and cannot be used from any other device. This serial number in combination with the device's current time, is used as the unique "seed" to generate the security Grid's UI cryptograms used to login.



Self-Service 2 Factor & Multi-Factor Authentication

SyferLock's AutoToken™ Technology

AutoToken™: *GridSoftToken*™ 2 Factor Device Authentication *PLUS* Increased User Authentication

If 2 Factor security is mandated or required and if you are paying for this additional layer of security, why accept only device authentication? SyferLock's proprietary technology delivers not only 2 Factor device authentication, but also delivers a much higher level of USER authentication as well.

Figure 1. below, SyferLock's GridSoftToken™, is what would be presented to the user of that computer or device when requesting authentication. The password, or in this case PIN, is not presented to the user "in the clear". Figure 2. shows a traditional soft token as created by one of the security industry's leading manufacturers and as *you* can see, anyone possessing access to the computer or device can read and then input the code for authentication.

Figure 1. SyferLock GridSoftToken™

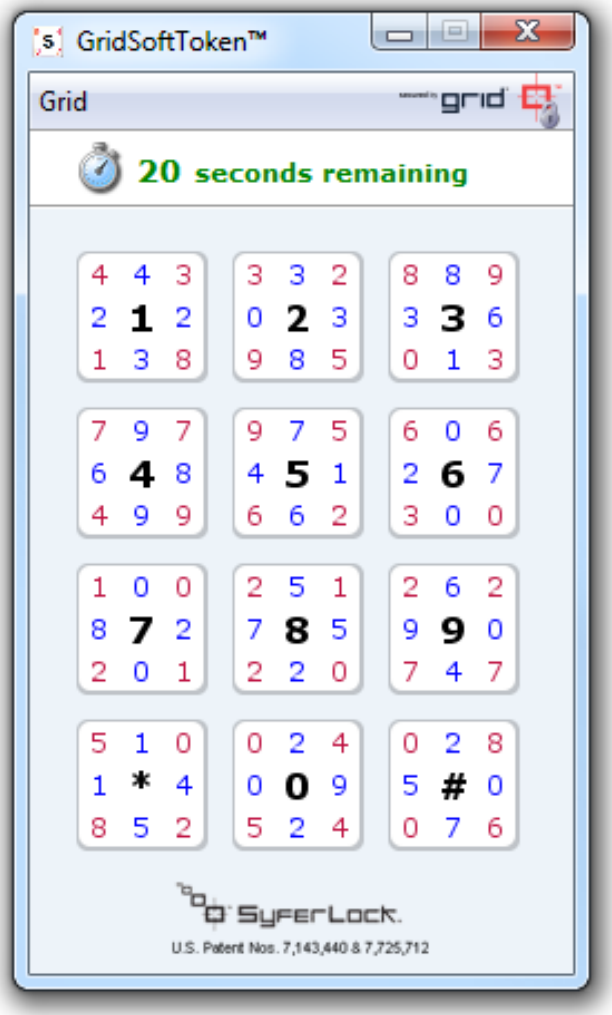
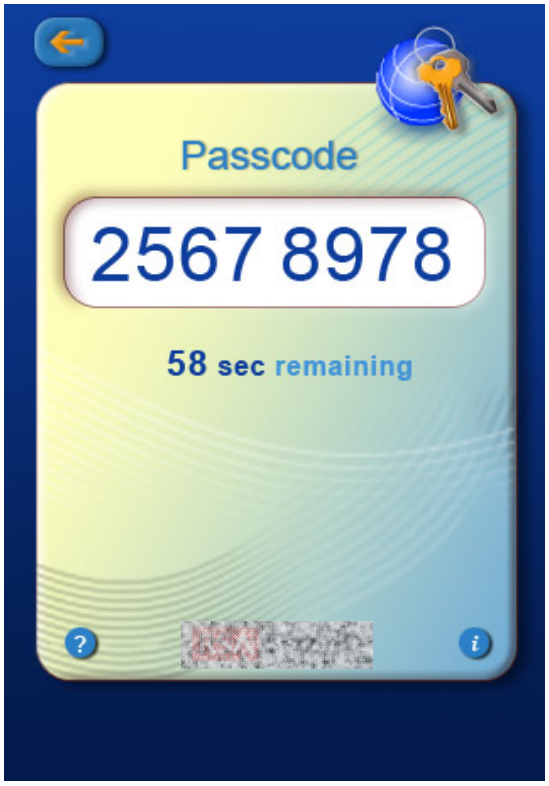


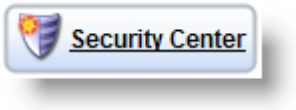
Figure 2. traditional soft token



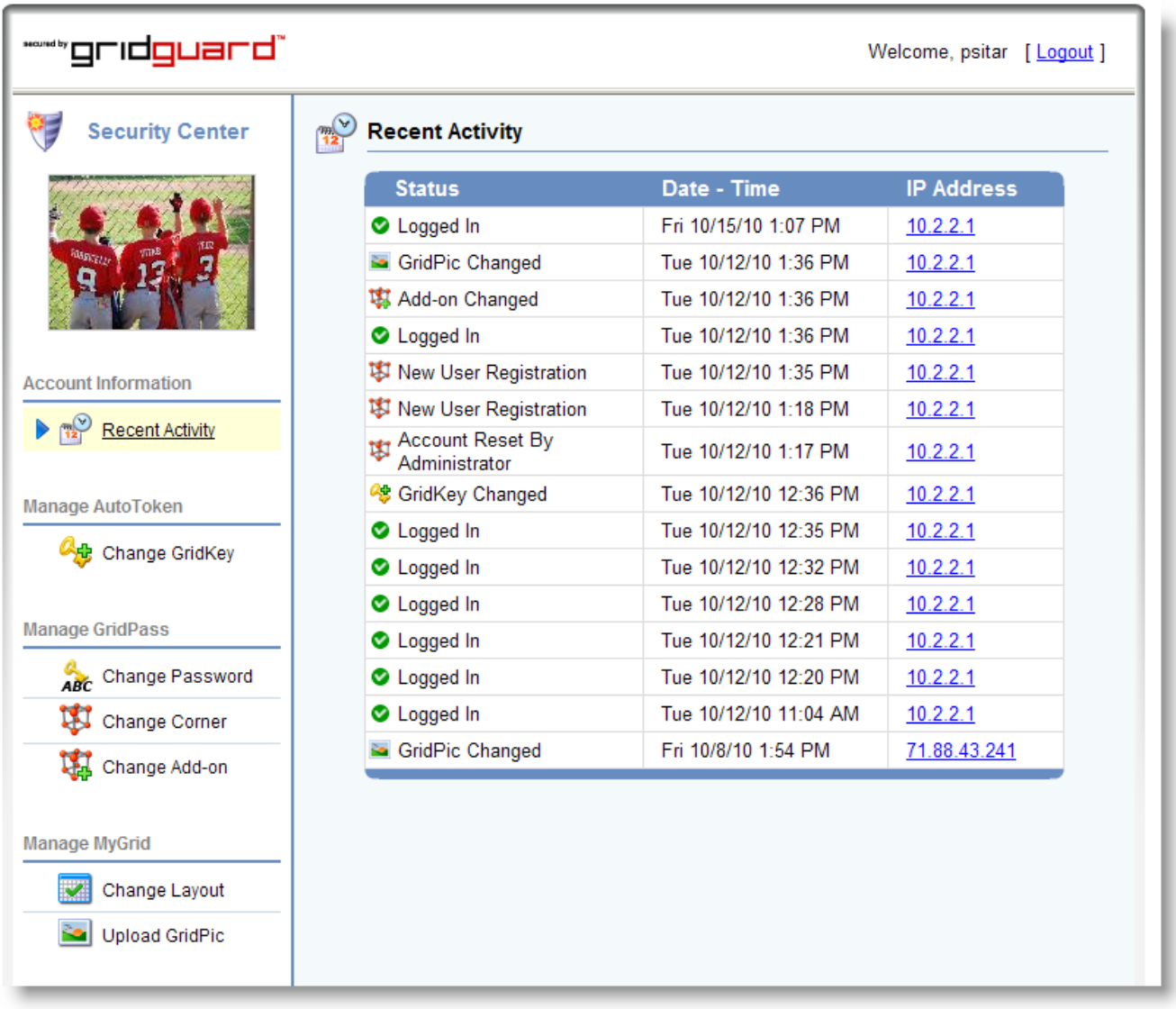
SyferLock.

Completely Customizable for Optimal User Experience

Next Generation One Time Passwords & Enhanced Authentication



Empowering users with critical, self-service, security features



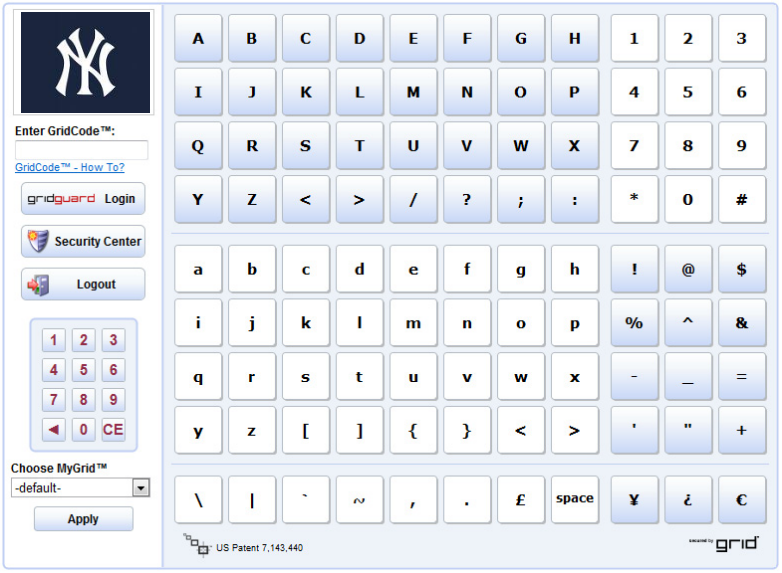
- Allows you to use existing passwords
- Makes all passwords device-less one time password
- Universal Access always on security – from any machine, anywhere
- Detailed account monitoring and analysis
- Complete self service escalating security features to combat key-logging, sniffing, phishing, even continuous screen capture
- Self-service 2 factor authentication capabilities
- Self-service customized UI and languages

SyferLock

Completely Customizable for Optimal User Experience

Next Generation One Time Passwords & Enhanced Authentication

Alpha Landscape
Security Grid UI

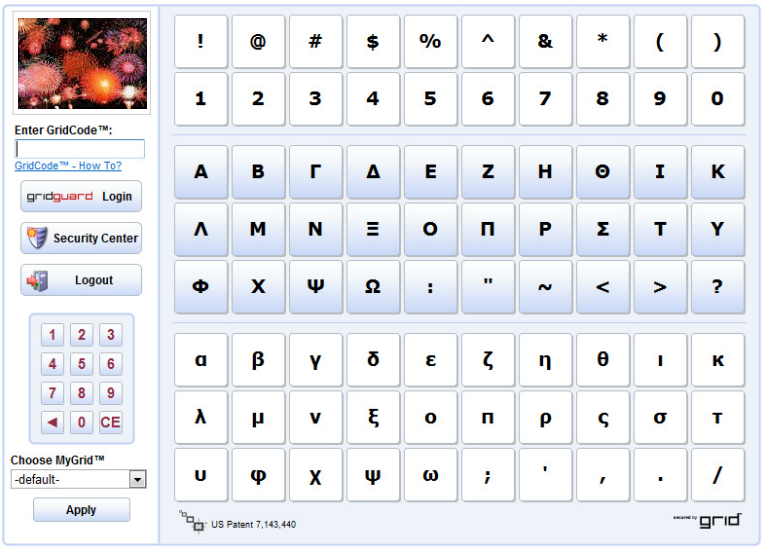


Alpha Number Pad
Security Grid UI

QWERTY
Security Grid UI

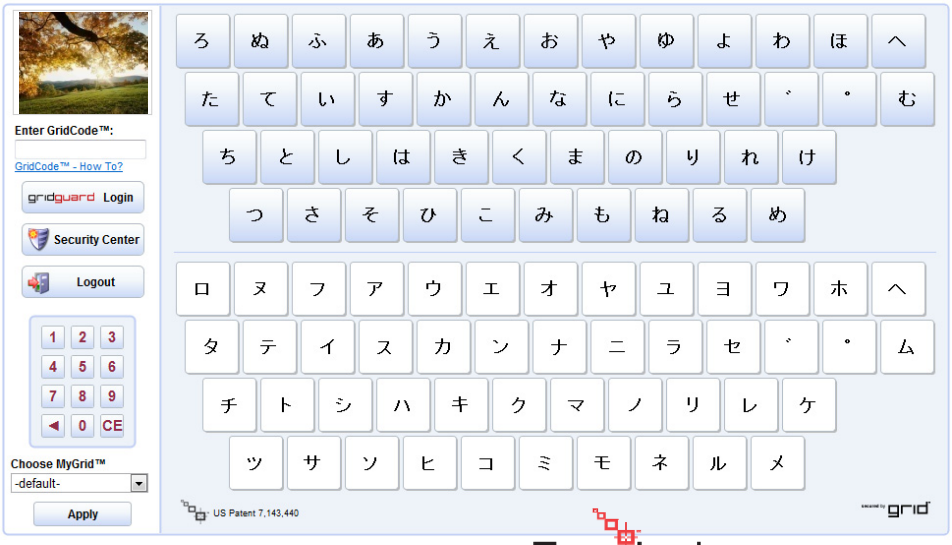
Completely Customizable for Optimal User Experience

Next Generation One Time Passwords & Enhanced Authentication



Greek
Security Grid UI

Arabic
Security Grid UI



Japanese
Security Grid UI

SyferLock

SyferLock Technology Products

Enhancing the Security of Key Applications

Securing Your Future with SyferLock's Authentication Systems

Do you truly know who's accessing your information?

Unfortunately, security that leverages static, reusable passwords has proven easy for hackers to beat.

As more and more individuals are leveraging the flexibility of doing business (professionally and personally) from remote locations, the need for reliable and secure application access is essential. The GridGuard™ authentication system can provide this reliability and security as it is based upon something you know (a password) and something you know (a target corner or position) – providing an increased reliable level of user authentication than a static or reusable password. By converting your existing password into a secure one-time password (OTP), remote user will be protected against many common security threats.

- ✓ **Secure one-time password that changes at every login**
- ✓ **Anomaly detection through Account History**
- ✓ **Self Service approach providing significant decrease in help desk/support calls.**

SyferLock offers enterprises a range of user authentication options, helping to identify users before they interact with mission-critical data and applications through Remote Authentication (SSL VPN), Intranets & extranets, E-mail, Microsoft Windows Desktops, GridGuard Services (SDK, custom integrations).

Product	Description
GridOne™	The GridOne™ solution works within the guidelines of a portal environment, providing organizations a solution that is as easy to deploy and administer. With GridOne™, no interaction with a desktop is required—that is, no need for an install , therefore no client side software maintenance. Equally important, there are no tokens to manage. GridOne™ is a device-less solution where authentication can occur from anywhere a web URL is available.
GridGuard™	The GridGuard technology provides enhanced authentication for Remote Access, Outlook Web Access and SharePoint . Some of the supported remote access solutions include Juniper SA SSL VPN , AEP Netilla, Citrix Access Gateway, Connectra – Checkpoint and others. For further details on the solutions that GridGuard™ supports, contact SyferLock directly.
GridPro™	GridPro™ offers enterprises a solution for the personal computer leveraging a Microsoft Windows® operating system platform. This solution consists of a login application (replacing the standard Windows login) that presents a user with a Grid for authentication.
Grid Services	SyferLock offers an Software Developers Kit (SDK), as well as for those organizations where resources (time/people) are limited so developing off of the SDK is not an option , SyferLock can provide that service (customized solution). Custom solutions include, but not limited to JAAS, Servlet Filters and many more. For further details on our Grid Services, contact SyferLock directly.
Grid2Go™	Grid2Go is a two-factor authentication system based on SyferLock's patented authentication system and methodology. The system leverages current-generation "smart" mobile devices such as the Blackberry and iPhone as the second factor in the authentication process.

SyferLock

SyferLock Technology Products

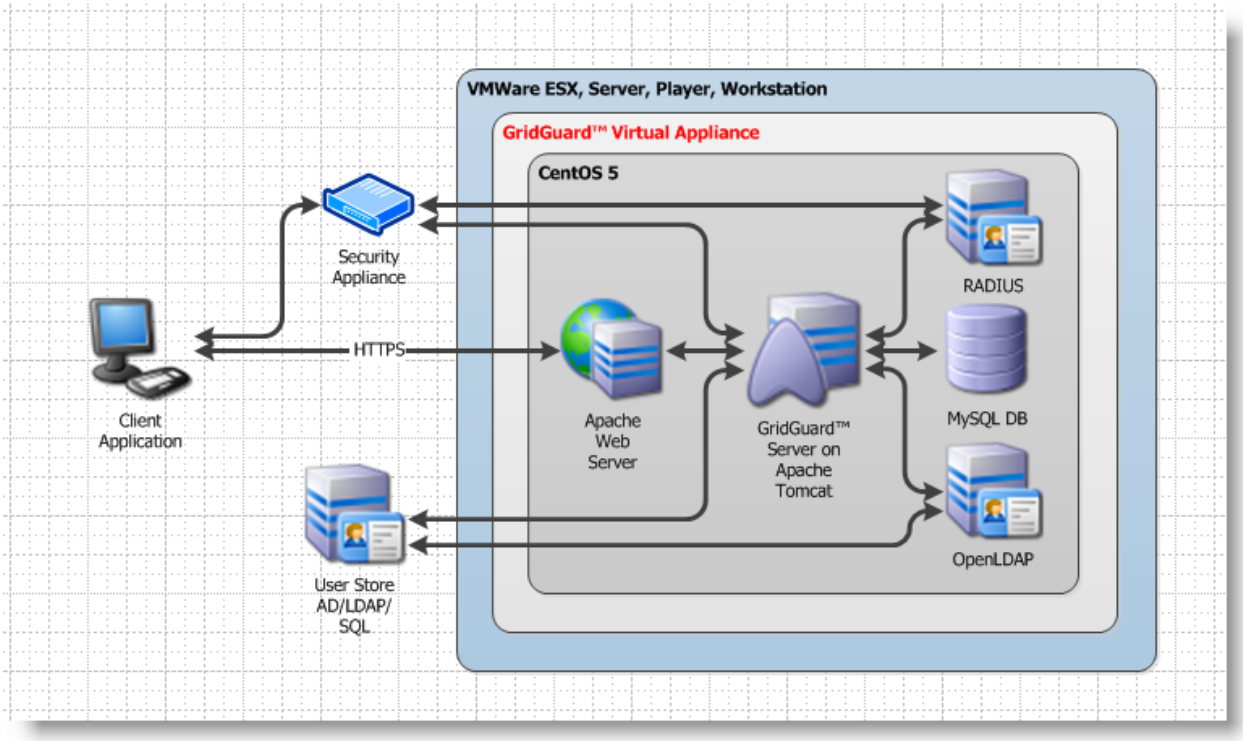
Enhancing the Security of Key Applications

GridGuard™ Virtual Appliance

To allow our customers to easily acquire, deploy and manage a pre-integrated solution stack, GridWare™ is now available as a virtual machine; the GridGuard™ Virtual Appliance.

The virtual appliance is built on a CentOS 5 Linux operating system. The pre-integrated solution stack includes the following components:

- Apache Web Server 2.2
- GridServer™ software 3.5.0
- MySQL 5.0 Database server
- GridRADIUS™ server
- Apache Tomcat Server 6.0
- OpenLDAP 2.3 server
- Oracle/Sun Java JDK 6.0



The GridGuard™ Virtual Appliance is currently supported on the following VMWare virtualization platforms only.

- VMWare ESX, ESXi
- VMWare Server
- VMWare Player
- VMWare Workstation

The product roadmap includes plans to make the virtual appliance available in Open Virtualization Format (OVF) format which will run on any industry standard virtualization platform.

There are also options allowing the software stack to be deployed as a physical appliance.

SyferLock Technology Products

Enhancing the Security of Key Applications

INTEGRATED PLATFORMS (partial list)

Manufacturer	Product	Version
CA SiteMinder	WAM R12SP1, SP2	
Checkpoint	Connectra	R66
Cisco	ASA 5500 Series	>= 6.2
Cisco	ASA 5500 Series	< 6.0
Citrix	Access Gateway	4.6
Citrix	Netscaler VPX	8.1, 9.X
IBM	Tivoli Access Manager for Enterprise SSO	Any
Joomla	Joomla	1.5
Juniper	SA2000 SSL VPN	6.2R1
Microsoft	Outlook Web Access (OWA)	2003, 2007, 2010
Microsoft	UAG	2010
Microsoft	TMG	2010
Microsoft	Windows	XP, 7
OASIS	SAML	1.1, 2.0
SonicWall	SS-VPN 2000	
SonicWall	Aventail EX Series	>=10.0

SYSTEM REQUIREMENTS

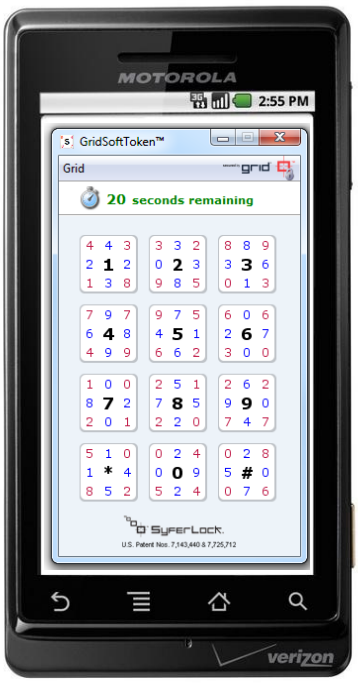
Component	Memory	Disk Space	Additional Considerations
GridCore™ Server	1GB Min	500 MB	Can reside on an existing or Virtual image, etc
LDAP Proxy	500 MB Min	50 MB	Can reside on existing Grid Server, Virtual image, etc.
User Directory	___	___	Reference the supporting documentation for system requirements.
Database (Login)	___	___	Reference the supporting documentation for system requirements.
Authentication Support/ User Store	___	___	LDAP, Active Directory, Novell eDirectory, IBM Directory Services / Tivoli Directory, Custom Data Bases (+ associated professional services)

SyferLock

SyferLock Technology Products

Coming to market ...

SyferLock's patented authentication system and methodology, delivering unparalleled flexibility and security, will be released to the OpenID users. This will allow users to never have to type or transmit a static password to those sites accepting OpenID credentials. SyferLock's OpenID platform will be the most secure OpenID offering that is currently available.



SyferLock's superior security and flexibility will allow mobile devices to become an even more powerful security tool in the authentication process. The mobile device can be utilized as a hard token equivalent and replacement, and due to SyferLock's patented approach, its higher level of user authentication will server as an added layer of security in the case of lost or stolen devices.

SyferLock will also be one of the strongest tools available to lock the device itself, bolstering the current approaches offered today.

GridPro™ will now complement its Windows XP GINA replacement login technology, by creating the same enhanced authentication for Windows 7. When local or domain access must be secured, SyferLock's GridPro™ offers a valuable security alternative.

SyferLock Technology Corporation

Company & Contact Information

SyferLock Technology Corporation

250 Pequot Avenue
Southport, CT 06890 USA
Phone 203-292-6268
Fax 203-292-5440
Email info@SyferLock.com
www.SyferLock.com

Grid is Green! No Additional Hardware. No Additional Heating. No Additional Cooling. No manufacturing, shipping or postage costs required.