

TEXTKEY FAQs

Next-Generation Authentication
for Your Website, VPN and Apps



TextPower, Inc.
888-818-1808



THE NEXT-GENERATION OMNI-FACTOR™ AUTHENTICATION SYSTEM

The world's first patent-pending Omni-Factor Authentication™. Protect websites, VPNs and apps with an industry leading seven factors of authentication verified by the user sending a simple text message FROM their cellphone.

What is TextKey™?

TextKey™ is a multi-patented next-generation omni-factor authentication system that is highly secure, simple to install and easy for users. It can be used to protect web sites, Virtual Private Networks (VPNs), apps or any other data that requires privacy, confidentiality or restricted access. It works by having users text a simple message via standard SMS into the TextKey™ system to authenticate their identity.

Who needs TextKey™?

Small and medium-sized businesses (SMBs), enterprises, financial institutions, medical facilities or others that want to protect intellectual property, sensitive records, transactions or other important information from theft or illegal access.

Don't companies already protect their web sites?

Most web sites are only protected by the standard user ID and password process simply because more effective protection has been too difficult, cumbersome or expensive for the average business to implement.

The established and industry-accepted best practice for protecting a web site from intruders that goes beyond ID/password protection is a "two-factor authentication" system. The two factors mean that the authentication process requires two things:

1. Something you know. In most cases this will be a user ID and password, or occasionally security question "challenges" (e.g., "What is your mother's maiden name?") to which, presumably only the user would know the answer.
2. Something you have. In most cases these "things" are a security "token" which the user must carry with them all the time in order to access the web site. These tokens typically take the physical form of key fob (similar in size and appearance to a vehicle's remote entry gadget), a special card with an embedded microchip or a USB thumb drive.

If it's better why don't all web sites use two-factor authentication?

Two-factor authentication systems can be complex, difficult to install, constant work to maintain and are typically very costly. Only companies with significant

information technology resources have been able to implement these systems in the past.

What makes TextKey™ different?

TextKey™ is a next-generation authentication system. It replaces complex, costly and high-maintenance systems with a simple approach that leverages the power of advanced messaging technologies and a cellular phone's "fingerprint."

Many companies that have a need for security haven't taken the appropriate steps to secure their environments because of the complications and expense. TextKey™ offers a way for companies of any size to implement authentication quickly and inexpensively.

The TextKey™ approach eliminates:

- Significant up-front expense of other two-factor authentication systems
- Complex installation of hardware and/or software
- Man-in-the-Middle and Man-in-the-Browser hacks
- Purchasing and maintaining an inventory of "tokens"
- Tracking, replacing and maintaining these tokens
- Lost or misplaced tokens or insufficient supply when needed
- Learning curve for users

Why is TextKey™ more secure than other authentication systems?

Every cellular phone ever manufactured contains a unique device identifier (a "UDID") that serves as the "fingerprint" of that device. While hacking or spoofing may work on common two-factor authentication systems because they receive, not send, text messages, the TextKey™ system eliminates this hacking by using the fingerprint of the phone to verify that the message is being sent by a legitimately authorized phone and not a "spoofed" number. A text message cannot be sent into the TextKey™ system without the cell phone carrying the correct UDID.

Furthermore, two-factor authentication systems rely on information being input into a browser by a user. Typically someone using a cell phone receives a text

message containing an authorization code and then must enter the code that appears on the token or cell phone's screen into a field on the web page. By definition this opens the process to "man-in-the-middle" (MITM) or "man-in-the-browser" (MITB) hacks that compromise the security of the entire process.

TextKey™ uses a patented process that completely eliminates any information being entered into, or shared through, the browser. All communication occurs on a secure server-to-server connection outside of the browser environment and thus excludes, by definition, any possibility of MITM or MITB attacks.

How does it work?

When a login is attempted on a protected web site or VPN a numeric code will appear in an overlay box that the user must text into the TextKey™ system from their cell phone. Without our system receiving the proper code from the proper phone it will not authorize the login to your site. The overlay box prevents the user from entering anything into the web page until either the correct code is sent into the TextKey™ system or a timeout occurs, reverting the user back to the original login page.

All the user has to do to authenticate their identity is send a simple text message from their cell phone. There are no apps to download or update, no smartphones are required, nor is there any hardware or software to maintain on the server side. There are no tokens to buy, distribute, track and replace. **A standard text message from a standard cell phone is all it takes to authenticate the user.**

Is it difficult to set up on my web site?

If your web site already uses a simple user ID and password system, more than 90% of the work is done.

How can this be so simple to implement and yet so secure?

We've designed TextKey™ so that most of the work is on our end, not yours. One simple block of code, which we provide to you, gets copied and pasted into the HTML on your login page. A few additional lines of code, which we also provide in PHP, .NET or

Javascript, get installed on your server to complete the secure communication between your server and ours.

You can register the cell phone numbers associated with each user ID that you wish to authorize on a simple web page or by using our API to connect to our server. In either case the only information that must be registered on our site is the user's ID and the cell phone number associated with it. TextKey™ never requires any new credentials and never requests your password. The user ID that you use on your company's web site is required for verification and matching to your mobile number but it is stored in a "hashed" format and therefore cannot be read or retrieved by anyone, ever.

How long does it take to implement it?

TextKey™ can be installed on a typical web site in a few hours. Your mileage might vary, of course, but TextKey™ is designed so that our infrastructure does the heavy lifting; the majority of the code and processing occur on our system, not yours. Compare that to the days or weeks of implementation typical of other systems.

TextKey™ doesn't require any hardware or software that might interfere with your regular operations. It doesn't require timing synchronization with your server or additional devices (tokens, key fobs, etc.) to be issued to your users, so it all happens quickly.

Implementations may vary based on the complexity of your application, desired features, etc., but the only thing that is required for TextKey™ to work is to have a cellular phone number associated with each user ID and to have that information registered on our system.

How can it be secure if you have the user IDs?

TextKey™ does not maintain your user IDs in any readable format; after you enter them through our registration system they are fully encrypted and unreadable by anyone – ever.

Can I see how it works?

- You can view an animated, 2-minute video of the principle behind TextKey™ here:

<https://vimeo.com/32399918>

Who is behind TextKey™?

TextPower, Inc., created and provides TextKey™ services. The company provides mission-critical alerting services for utilities, municipalities and universities. Our infrastructure is built with clustered server failure protection and is completely geo-redundant.

In short. TextKey™ is powered by the most robust and reliable text messaging system anywhere.

27134-A Paseo Espada
San Juan Capistrano, CA 92675

Talk to us about it at:
888-818-1808

TextPower Inc.
