Hard vs. Soft Tokens

Making the Right Choice for Security

HSTE-NB0012-RV 1.0

HYPERSECU®

HYPERSECU INFORMATION SYSTEMS, INC.

#200-6191 Westminster Hwy | Richmond BC | V7C 4V4 | Canada
1 (855) 497-3700 | www.hypersecu.com

The Challenge:

Choosing the right balance between convenience and security.

You understand the security risks of using static passwords. You know it's important to protect your company assets and data, and that two-factor authentication (2FA) is a simple and affordable method of doing so.

Now you're faced with another question: should you choose software tokens or hardware tokens?

It's true that soft tokens offer a degree of convenience. For instance, the digital certificate or application can be installed on personal devices, which many users already keep on their person. There's no need to purchase additional devices.

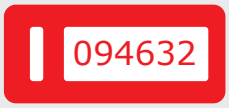
But this is where soft tokens are at a disadvantage when it comes to security: because the digital certificate or one-time password (OTP) application is stored on the device itself, it's not difficult to hack the device and extract that information. Digital certificates can be exported; OTP applications can be tapped into remotely and the data accessed. With how technologically advanced tablets and phones have gotten, there's an ever-growing number of opportunities for hackers to exploit them.

Hard tokens, on the other hand, don't have the vulnerabilities that soft tokens do. As a result, they're a much more secure choice for 2FA.

Comparing the Differences

Software and hardware tokens, also known as "soft" and "hard" tokens, differ in where the application or information is stored. With a software token, the OTP application or PKI certificate isn't stored on a device specifically designed to secure such sensitive data. Instead, it's downloaded and stored on any average computing device such as your mobile phone, tablet, or even the desktop at your office—the very machine you're trying to protect. As a result, the token is "soft" because it isn't tied to a particular hardware device.

Hard tokens, on the other hand, involve two things: the OTP application or PKI certificate itself *and* the hardware device it's stored on. The two can't be separated. With a hard token, the information is kept within that single device, which is designed to keep the information inside secure.

Hard Tokens *vs.* Soft Tokens		
FEATURES	**HARDWARE TOKEN**	**SOFTWARE TOKEN**
Invulnerable to malicious applications that can be downloaded and installed without your notice.	√	X
True two-factor authentication that separates something you have (a token) from something you know (a password).	√	X
Standalone, unconnected device that prevents unauthorized external or remote access by hackers.	√	X

The Risks of Soft Mobile OTP

Software OTP is often stored on the user's phone by installing an OTP application that lets them use their mobile device to access their dynamic one-time password. This also includes SMS OTP, where a code is sent via text message to the mobile phone, which can then be entered to verify the user.

While doing so can be convenient—it eliminates the need to keep track of multiple devices—there are some notable security trade-offs. Phones and tablets have become our personal computers. Remote employees are accessing sensitive company information such as emails and downloading private documents onto their mobile devices. Even employees who work on-site tend to access company data on their phones while away for lunch, during a business trip, or on the commute home. So what happens when the authentication information is stored on the exact same device that's used to gain access?

For one, it's no longer secured with two-factor authentication. For another, it opens both the user and the company to a whole host of vulnerabilities.

- **SIM Card Theft:** Using the Gozi Trojan, hackers can gain access to a device's International Mobile Equipment Identity (IMEI). Using this number, they can file a report that their phone has been stolen and receive a SIM card. Once the SIM card is in their possession, they'll receive all SMS OTP details.
- **OTP Seed Exporting:** Since the OTP application installed on a phone is simply software, its data can be extracted. This includes the sensitive OTP secret key, or seed, that'll allow someone to access your OTP at any time without your knowledge.
- **Malicious Apps:** A number of phone apps are disguised as harmless music or gaming apps, but in reality are malware that can slip through a backdoor to steal information, including your SIM card. 82% of apps read your device ID while 26% know your SIM card information.
- **Inconvenient Downtimes:** Phones and tablets can unexpectedly run out of battery. Even at their best, batteries last for one or two days. Hardware tokens have none of these limitations—batteries can last years, so you'll never have to constantly worry if you have enough battery life for access.

26%

of mobile applications know your SIM card number, which can be used to gain access to your SMS OTP number.

McAfee Report, 2014

The Risks of Soft PKI

Software certificates and PKI are at an equal disadvantage to soft OTP applications, if not more so. While it's rare for an OTP application to be stored on a desktop, it's much more common with digital certificates. Many users install their certificate, along with their private and public keys, right onto their desktop computer. This means in addition to being vulnerable to theft or loss, internal threats, and malicious applications, soft certificates are also:

- **Vulnerable to being hacked during the key pair generation process.** With PKI, the private key must be kept safe. It holds the ability to decrypt messages, sign emails and documents, and verify your identity. When the key pair is being generated on an unsecured device like a laptop, the keys can be hacked and the information stolen.
- **Open to more hacking opportunities.** Computers are left on for extended periods of time. Some employees even leave their desktop on 24/7, choosing to put it to sleep instead of shutting it down overnight. This leaves a wide window open for malicious activity to take place.
- **Vulnerable to keylogger attacks.** If your system has been compromised, the PIN to your PKI could be stolen with keylogger software.

Once a hacker has the authentication details in hand, they can proceed to not just read encrypted details, but also digitally sign things like malware using the certificate to make it look as if the program is a legitimate piece of software—something that can be further used to exploit a company. Proper management and security of digital certificates is crucial.

PKI Security Regulations

Because of the risks that come with soft PKI, many countries and institutions have regulations around making sure that the type of PKI being used is secure enough to guard against critical data theft.

» In areas like the U.S., Asia, and Europe, the law requires that key pair generation takes place on a PKI token or card in order to be admissible in court. If the signing, encryption, or authentication didn't take place on a hardware PKI token or card, the evidence may be disallowed.

» The U.S. government, including military, requires its authentication devices to be FIPS 140-2 certified. Due to its physical tampering regulations, only hardware devices can be designed to meet those standards.

Consider Hardware Tokens for 2FA

Despite the risks of soft tokens, many still opt to use them due to their convenience. It's important to consider your company's specific needs and to integrate 2FA as smoothly as possible into the organization's existing infrastructure. For some, a soft token may be all that's needed. For others, though, hard tokens may seem more daunting and expensive than they really are when in fact the security gained could far outweigh the financial risk of a data breach.

The consequences of security incidents are usually preventable. The Online Trust Alliance (OTA) reports that in 2013, **89% of incidents could have been averted** had proper security measures been in place. While security measures aren't foolproof against human error, they can help reduce them. Employees can have a tendency to lose their mobile devices, forget to log off of work computers, and leave office doors unlocked by mistake. Some might still write their passwords down and leave them near their work station. Using hardware tokens to instill true 2FA means the impact of these errors can be greatly reduced.

Hardware tokens can reduce the impact of human errors, such as forgetting to log off, leaving offices unlocked, and writing down passwords.

Take into account the impact when a company's security is compromised.

- **Financial losses incurred can reach millions.** Many have heard by now of Target's infamous data breach that cost the giant company $148 million, but Target isn't a unique case, nor are breaches limited to retail chains. Healthcare, education, and industrial organizations can all be affected. A report by the Ponemon Institute estimates that in 2014, U.S. businesses lost on average **$5.5 million as a result of data breaches.**
- **Loss of trust and reputation.** Businesses are built on trust that's earned from partners, investors, and customers. On top of the immediate financial losses, a damaged reputation could take years to repair—costing the company even more.
- **Time and money must be invested in damage control.** Once a security breach has occurred, steps must be taken to repair the damage and prevent it from ever happening again. This takes a lot of time and money, which could've been used to secure the company initially. The Poneman Institute notes that **companies continue to spend more money after the fact trying to reduce the consequences of a data breach.**
- **Losses must now be regained.** Even a large business can struggle to regain their finances and reestablish their reputation. For smaller companies with limited resources, the consequences could be irreparable.

Get Started with Hypersecu

Hypersecu offers a wide line of multi-factor authentication solutions to secure your business, including OTP, PKI, and smart card readers. Our flexible products are designed to suit your needs no matter the size of your business or the industry you're in. If you're not sure what's right for you, we're happy to provide consultation to work out a customized solution that covers all of your information security challenges.

Learn More

We provide demos of our products upon request and our expert consultants are ready to answer your questions. Contact us or visit our website at www.hypersecu.com to learn more.

Hypersecu Information Systems, Inc.
#200-6191 Westminster Hwy
Richmond, BC V7C 4V4 Canada

Email: sales@hypersecu.com | Phone: 1 (855) 497-3700