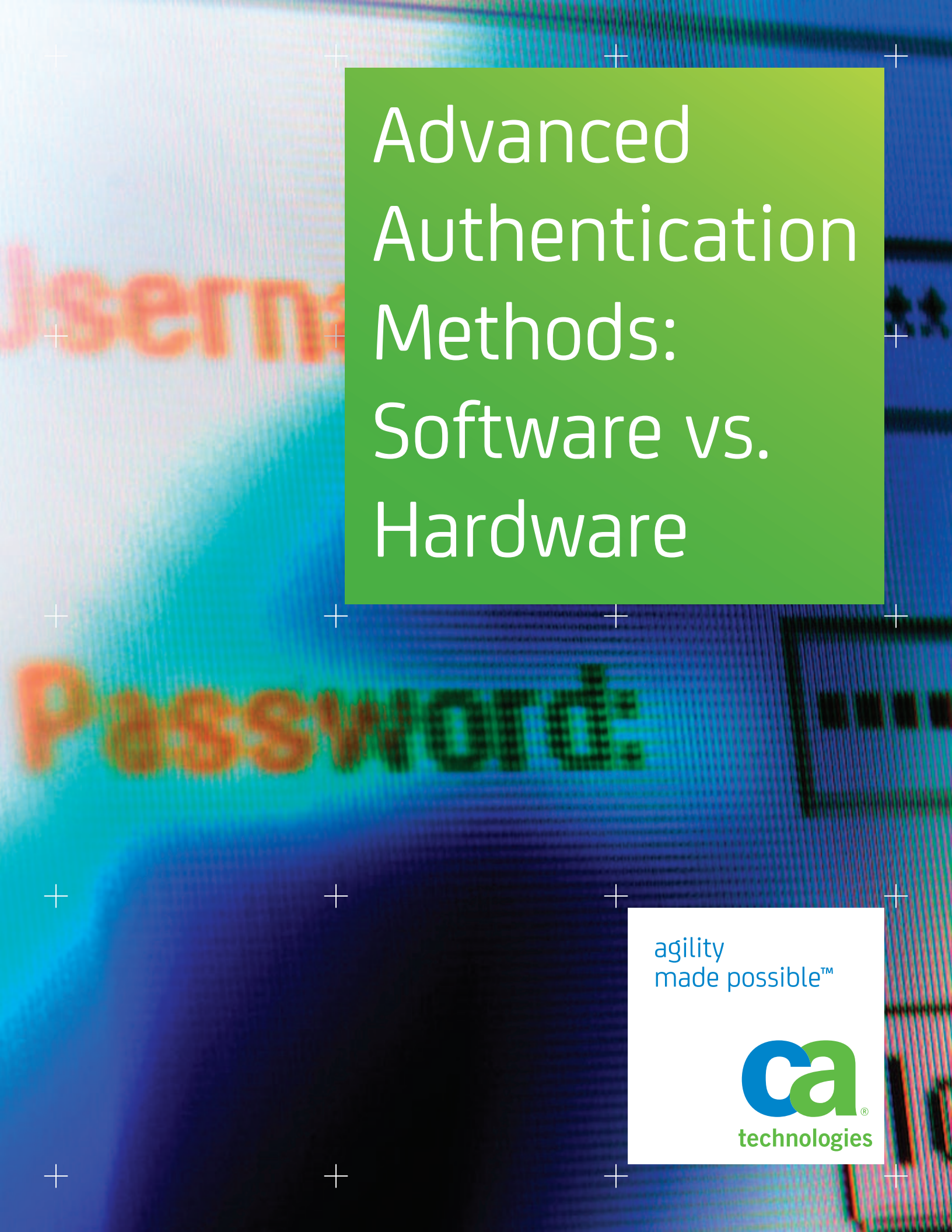


Advanced Authentication Methods: Software vs. Hardware

agility
made possible™

ca technologies

The Importance of Authentication

In the world of technology, the importance of authentication cannot be overstated — mainly because it plays such a central role and touches so many different systems. The Internet is a prime example of this, as practically any action a user takes online begins with authentication.

For example, while it's true that basic information gathering on the Web (i.e., Google searches, Wikipedia, etc.) is often unrestricted, users looking to conduct personal and professional business (e.g., online banking) or perform transactions (e.g., online sales or purchases) will almost always encounter some type of authentication. As authentication has become more pervasive and important in the technology space, the challenges of implementing and maintaining it have grown as well. For starters, the number of online interactions is increasing everyday — as is the amount and value of data they produce — and systems are getting more distributed and complex (e.g., cloud computing, software as a service (SaaS), etc.).

Alongside these increases, attackers are getting more organized and sophisticated, and they are able to more easily mount and fund attacks than ever before. Yet as entire communities spring up around the creation and distribution of advanced attack tools, organizations and their customers are struggling to protect sensitive data and user privacy.

Finally, in the midst of all this change, it has become commonplace to hear about hackers attacking major corporations, stealing critical business and personal information from servers and leaking that information online. It's gotten to the point where people are fed up with yesterday's security techniques — they're asking, "What can we do? Is there an authentication method that can truly protect us from these types of attacks?"

Authentication Basics and Technologies

It should come as no surprise to anyone who has ever used a computer that the initial form of authentication — the user name and password — is still the widest used, factoring into nearly 80% of authentication events. After all, it's cost-effective, scalable and easy to administer and use. That said, a number of recent trends have created a need for stronger, more innovative authentication methods.

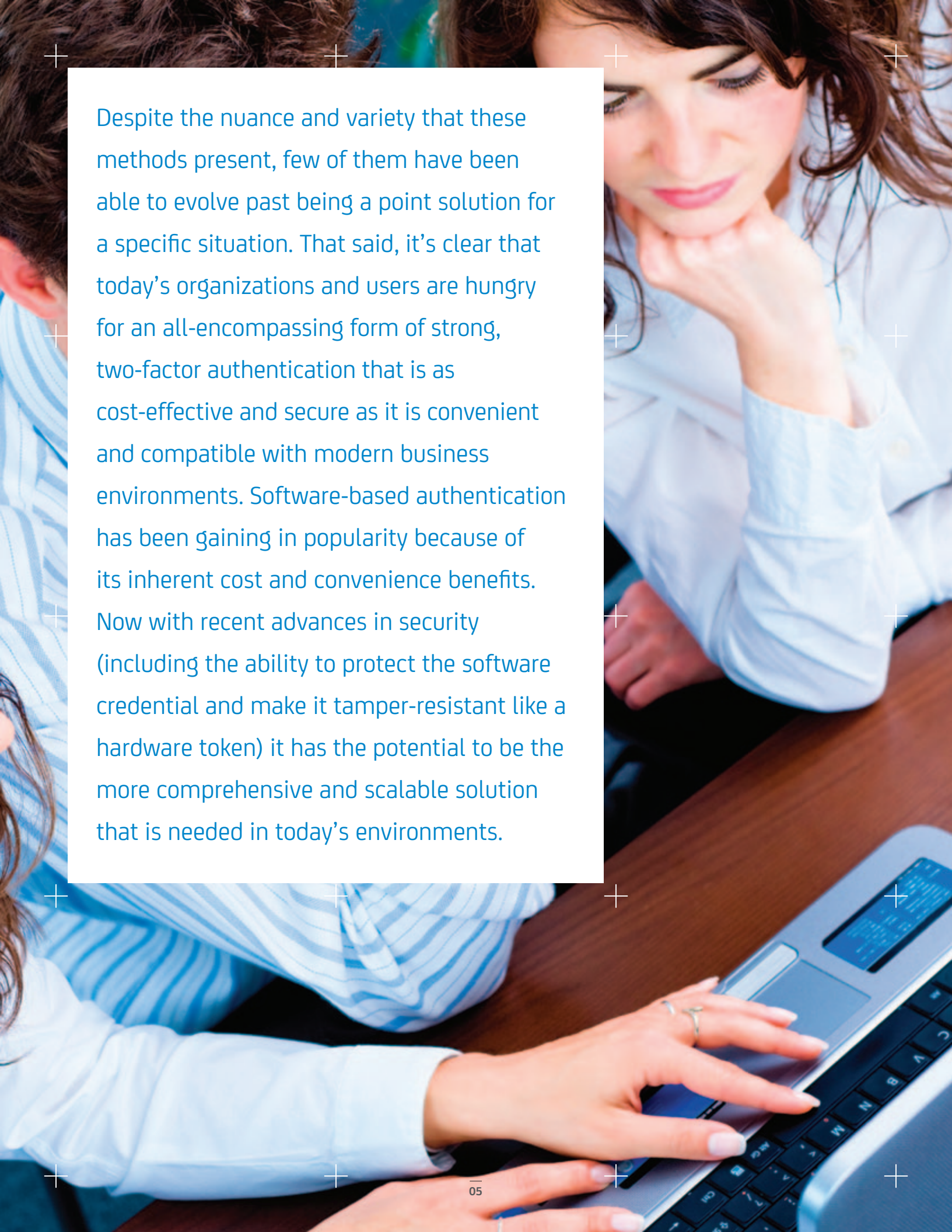
For one, the number of users — from employees to partners to customers — have exploded, essentially multiplying the points of exposure and risk businesses must address. The types of data that need to be protected have changed as well, with more personal and business-critical information being stored in portals and online applications. For example, many organizations expect their employees, partners and customers to access sensitive information and provide data online as a regular part of their interactions. Finally, devices continue to evolve, so any authentication method has to be compatible with laptops, smartphones, tablets and whatever comes next.

In response to these trends, a variety of authentication technologies have hit the market over the years. To better understand what they are and how they compare to the user name/password combination, it helps to be familiar with the standard authentication factors — something you know, something you have and something you are — and how each technology leverages them to power its authentication capabilities.

- **Something you know** is a bit of knowledge committed to memory, such as a password or an answer to a secret question.
- **Something you have** is an item that is owned or carried, such as a smart card or similar hardware device.
- **Something you are** is a physical attribute that can be identified, such as a fingerprint or voice.

Below are some examples of existing authentication technologies and how they utilize the three factors:

Technology	Description	Factor	Use-case	Pros	Cons
Biometrics	Measures physical characteristics of a user, such as fingerprints, eye geometry, facial features, voice patterns, etc.	▪ Something you are	High-value physical security, including military bases, data centers, vaults, etc.	▪ Cutting-edge tech ▪ Works well as an extra factor	▪ High cost ▪ Can be inconvenient for user ▪ Can create false positives and false negatives
Smart cards	Cards that contain cryptographic keys based on public key infrastructure (PKI) and are used as part of an authentication protocol	▪ Something you have (card) ▪ Something you know (PIN)	High-value military and government applications	▪ Strong security ▪ Two-factor authentication	▪ High cost ▪ Requires readers or drivers installed on PC
Browser certificates	PKI-based digital certificate that gets installed in a browser; leverages a private key and a password	▪ Something you have (browser key) ▪ Something you know (password)	Internet and Intranet browsers	▪ Stronger than single-factor authentication	▪ Not a true two-factor solution, as private key and password are not independent ▪ Subject to brute-force attacks
Hardware OTP tokens	A hardware device that generates a one-time password (OTP) and is generally used in conjunction with a traditional password	▪ Something you have (hardware) ▪ Something you know (password)	Typically used for access to a set of sensitive applications by a subset of employees (one or more tokens)	▪ Strong security ▪ Two-factor authentication ▪ Ease of integration	▪ High cost ▪ Can be inconvenient for user (extra login step, separate item to carry) ▪ Creates questions about chain-of-custody
Unprotected software token	Typically a local OTP file used in conjunction with a password	▪ Something you have (software file and code) ▪ Something you know (password)	Same as hardware tokens but easier to distribute and scalable to larger groups	▪ Two-factor authentication ▪ Lower cost	▪ Security issues related to various threats, such as brute-force and man-in-the-middle attacks ▪ Requires a one-time registration process
Secured software credentials	A protected local PKI-based or OTP file used in conjunction with a password	▪ Something you have (software file) ▪ Something you know (password)	Full set of employee, partner and customer use cases	▪ Strong security ▪ Two-factor authentication ▪ User convenience ▪ Lower cost ▪ Scalability	▪ Requires a one-time registration process



Despite the nuance and variety that these methods present, few of them have been able to evolve past being a point solution for a specific situation. That said, it's clear that today's organizations and users are hungry for an all-encompassing form of strong, two-factor authentication that is as cost-effective and secure as it is convenient and compatible with modern business environments. Software-based authentication has been gaining in popularity because of its inherent cost and convenience benefits. Now with recent advances in security (including the ability to protect the software credential and make it tamper-resistant like a hardware token) it has the potential to be the more comprehensive and scalable solution that is needed in today's environments.

The Evolution from Hardware to Software

Because they are one of the only devices to combine two-factor authentication with a relative ease of integration in IT environments, hardware OTP tokens have proven to be one of the more popular authentication technologies in past years. Yet, while they compare favorably with such options as biometrics and browser certificates, tokens have many disadvantages when weighed against a newer approach to authentication: secured software credentials.

For one, hardware OTP tokens have started to lose their reputation for strong security. Since they are physical items that are manufactured and shipped to various locations (e.g., distributor, customer, branch locations, etc.), they have a number of attack points — which means that organizations and their end users have to rely on the security of their vendors and partners to ensure their protection. Also, hardware OTP tokens do not provide adequate protection from the newer Internet threats, such as man-in-the-middle attacks.

On the other hand, software-based solutions have been gaining popularity recently because of lower costs and easy scalability. While unprotected software tokens have been criticized for an inability to protect the token from brute-force attacks, secured software credentials are able to provide the cost and scalability benefits companies expect, with the strong protection they require.

Even though software has many clear advantages over hardware, many organizations continue to use hardware tokens because they feel their keys are more secure with that physical layer of protection. They think, “With unprotected software on a device, what’s to stop someone from locating the file and running brute-force attacks on it?” For many types of software, that is a fair question to ask, but what if a two-factor authentication software credential had a built-in “patented technology” that protected the key like a physical enclosure? Businesses would finally have a way to marry the cost, convenience and scalability benefits of software with the tactile security and peace of mind they get with hardware tokens.

In order to fully appreciate the benefits that secured software credentials have over hardware tokens, it helps to analyze their characteristics through a variety of lenses — particularly those that business owners find important, such as cost, convenience, security and disaster recovery.

Cost

Cost breaks down across three categories:

- Manufacturing/Acquisition
  - Hardware has to be made, shipped, inventoried, distributed and tracked
  - Software can be created as needed on the fly
- Operational
  - Hardware has to be inventoried, distributed, allocated and tracked
  - Software can be created as needed on the fly
- Lifecycle
  - Hardware has a vendor-determined lifetime and a lengthy replacement/renewal process
  - Software has a customer-specified lifetime and a rapid replacement/renewal process

Convenience

- Hardware Tokens
  - A token has to be carried; if it's forgotten, the user has no access
  - If a token is lost, the recovery process can be lengthy
  - Issuance and replacement require human involvement
  - Users dislike having to carry multiple tokens for multiple accounts
- Secured Software Credentials
  - Users can choose to carry the software credential on a PC, USB device or phone
  - If it is lost, it can be revoked immediately and easily replaced
  - It supports self-service issuance, replacement and management
  - Multiple software tokens are as easy to carry as one

Security

- Hardware Tokens
  - Keys are burned into tokens at the manufacturer's location
  - Complex chain-of-custody as token goes from manufacturer to vendor to distributor to customer
  - Each stop along the way is another potential attack point
  - Customer security is dependent on how well the vendor protects the keys
- Secured Software Credentials
  - Keys are generated in the field by a customer's server
  - No chain of custody or vendor site concerns (fewer attack points)
  - Protection against man-in-the-middle and brute-force attacks
  - Security remains under a customer's policies and control

Disaster Recovery

- Hardware Tokens
  - It takes time for vendors to ship new tokens to users
  - Creates costs around downtime and purchase/management/shipment of new tokens
- Secured Software Credentials
  - Compromised credentials can be revoked instantly
  - New credentials can be generated and delivered quickly and without cost

Some Best Practices and Two-Factor Authentication Software Credentials

At this point, it should be fairly obvious that for all of their diversity of features and benefits, many existing authentication technologies fall short by being too costly, too cumbersome and — in some cases — too weak. For organizations concerned about their security, that's a particularly sobering thought.

However, there are some steps businesses can take to improve authentication security, such as:

- Review password policies and have users change passwords periodically
- Add risk-based authentication for user logins and to measure the risk of individual transactions
- Consider replacing hardware tokens with secured software credentials

As identity theft and online fraud becomes more commonplace, organizations are trying to find a good balance between strength of security and level of inconvenience for employees, partners and customers. When combined with a strong password policy, risk-based authentication can leverage rules, parameters and analytical modeling techniques to add an extra layer of protection and reduce exposure to fraudulent activity — without annoying end users or creating a high rate of false positives.

Finally, for organizations that are looking to expand their use of strong authentication or trade in their cumbersome, aging hardware tokens for a more secure and cost-effective two-factor authentication software credential, CA Technologies offers two such solutions in CA ArcotID® and CA ArcotOTP.

"Perhaps one of the weakest links in accessing important Internet assets is a strong tie between the user and the areas they have the right to access. The use of a simple user-name/password mechanism is truly a weak link. What is unique about Arcot's approach is that it is both strong and people-friendly."

– Dr. Taher Elgamal, PhD at Stanford University and inventor of SSL while at Netscape

CA ArcotID

CA ArcotID is a secured software credential that combines protection for digital IDs like that of a hardware smart card with the lower cost and simplicity of a software solution. It provides strong, two-factor authentication that allows organizations to replace simple username/password or OTP tokens with the strength of PKI — without changing the user experience. The solution provides strength and security, while also being easy to use and invisible to the end user.

CA ArcotOTP

CA ArcotOTP is a mobile authentication application that turns a smart phone, tablet or other mobile device into a secure authentication tool that creates a one-time-password and eliminates the need to carry additional hardware. It is cost-effective, easy to integrate into existing systems and convenient for end users.

Cryptographic Camouflage

Both CA ArcotID and CA ArcotOTP employ patented Cryptographic Camouflage key concealment technology. Cryptographic Camouflage protects the keys from password-guessing brute-force and dictionary attacks. Reviewed and vetted by leaders in the field and based on established security best practices, Cryptographic Camouflage provides secured software credentials allowing organizations to implement two-factor authentication completely in software.

"Since the innovation of public key cryptography 25 years ago, people have been struggling to secure the private key without the assistance of hardware. Arcot's innovative Cryptographic Camouflage has solved the problem. Finally there is a cost-effective and convenient means to strongly authenticate users and transactions over the Internet without the need for cumbersome hardware."

– Dr. Martin E. Hellman, Professor Emeritus at Stanford University and inventor of PKI

Conclusion

In an ever-evolving business world that is as active on the Web as it is in brick and mortar, having effective authentication technology has gone from a luxury to a necessity. And, as high-profile stories about online attacks and compromised data continue to see the light of day, companies need to ensure that their authentication solutions are not only resistant to attacks, but also easy-to-use, flexible and cost-effective.

With CA ArcotID and CA ArcotOTP — as well as the patented Cryptographic Camouflage they employ — CA Technologies combines strong, two-factor authentication technology with the low cost and convenience of a software solution, helping today's companies stay ahead of the security curve and mitigate the risks of attacks.

For more information about CA ArcotID and CA ArcotOTP, please visit *ca.com/replacetokens*.

CA Technologies (NASDAQ: CA) is an IT management software and solutions company with expertise across all IT environments — from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies' innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 relies on CA Technologies to manage evolving IT ecosystems.

ca® technologies