Strong Authentication

An Essential Component of Identity and Access Management

WHITE PAPER

Executive Summary

Driven by many factors—including consumer demands for enhanced security, compliance pressures and a desire to re-energize the growth of e-business—leading enterprises are developing strategies for identity and access management (I&AM). As they do so, they are coming to view a well-established technology, strong authentication, in a new light. Unlike password protection, which remains pervasive despite its known shortcomings, strong authentication meets one of the core requirements of I&AM: it enables organizations to verify user identities with high degree of certainty, and thus enhances online trust.

Based on interactions with large enterprise customers and its unique perspective within the security industry, RSA Security believes that strong authentication will play an increasingly broad and important role, both in enterprise and consumer environments—with the first large-scale consumer deployments likely to occur within the coming years.

With a long record of success in strong authentication and leadership in other technologies foundational to I&AM, RSA Security is well-qualified to assist organizations that want to implement strong authentication, either in the context of an I&AM initiative or as a stand-alone solution.

RSA SECURITY® | Confidence Inspired™

TABLE OF CONTENTS

I. IDENTITY AND ACCESS MANAGEMENT: A NEW FRAMEWORK FOR AUTHENTICATION

Leading enterprises in virtually every industry are rethinking their strategies for identity and access management (I&AM) and, by extension, for user authentication. Distributed approaches to identity management, which have long been viewed as good enough security" for most purposes, are now being scrutinized in the light of several harsh realities. These include:

- Skyrocketing rates of identity theft, including widespread theft and misuse of online identities;
- Persistent consumer fears about security and privacy, and a subsequent resistance to doing business online;
- Increased compliance requirements, which hold companies responsible for safeguarding sensitive information and documenting business processes for audit and control purposes;
- Intense pressures to manage security-related infrastructure costs; and
- The adoption of new technologies, such as federated identities and web services, that promise to bring new value to supply-chain relationships.

Many Challenges, One Common Solution

All of these challenges point in the same direction: the need for more secure, efficient and flexible ways to manage user identities and access privileges. In research conducted for RSA Security, 82% of respondents said that identity and access management is a high priority for their organizations, and many have enterprise-level I&AM initiatives currently under way. These efforts are designed to provide immediate benefits in the form of enhanced security, increased user convenience through single sign-on (SSO) and reduced cost and administrative burden. However, they also share an ambitious long-term goal. Leveraging a common infrastructure, they will deliver centralized identity management services that not only span the enterprise but also securely manage relationships with customers, partners and suppliers.

Rethinking the Authentication Challenge

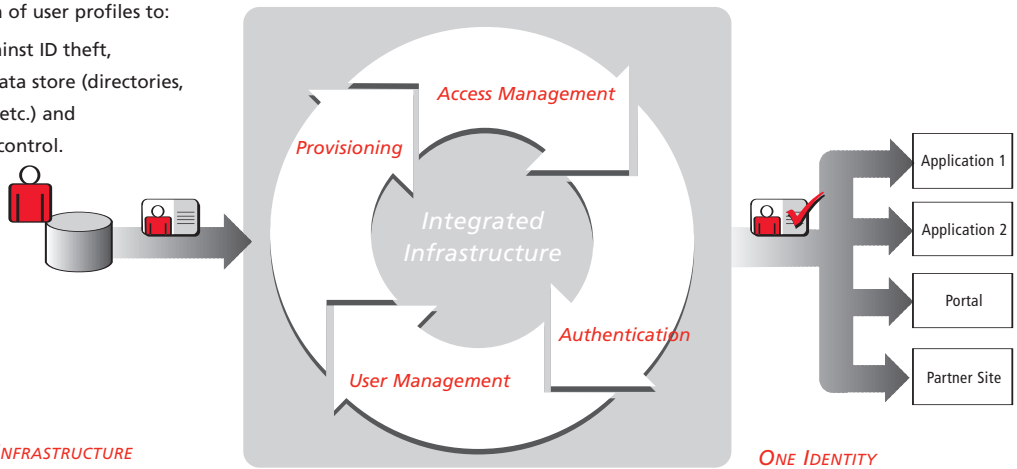
Within this framework, the task of user authentication takes on a whole new importance. Rather than unlocking an application here and there, a user's credentials will unlock a whole universe of resources—whether for a legitimate user or a successful impostor. Suddenly, it becomes critically important that an enterprise know, with certainty, who is on the other end of a network connection. And suddenly, "good enough security" may no longer be good enough.

For all these reasons, leading enterprises are looking more carefully at how they authenticate users, asking, "When are passwords adequate? And when do I need stronger authentication?"

One User

Centralization of user profiles to:

- Protect against ID theft,
- Leverage data store (directories, databases, etc.) and
- Centralize control.



One Infrastructure

Integration between I&AM components and with user applications across the entire enterprise provides compelling business benefits:

- Cost reductions,
- Enhanced security and compliance, and
- Business enablement and revenue opportunity.

One Identity

Enhanced user experience through:

- Single sign-on,
- Federated ID and
- Web services.

II. PASSWORD PROTECTION: NOT ALL IT'S CRACKED UP TO BE

Introduced in 1963 to protect timeshare systems, password authentication gained wide acceptance based on its three chief attributes: it came free with each application, was easy to use and provided adequate security for the great majority of purposes.

Forty years and many generations of technology later, passwords remain pervasive. (See the sidebar *Passwords vs. Strong Authentication: Where Things Stand Today*—page 2.) However, the original three value propositions for password protection—cost-effectiveness, ease of use and security—has been turned upside down.

Distributed password protection is costly

In many organizations, the proliferation of "free" security applications spawned a distributed, decentralized infrastructure for identity management. (In one financial services firm, RSA Security found more than 100 application-specific authentication systems.) Costly to manage and maintain, these "archipelagos of security" are one of the factors driving the growth of enterprise-wide identity management initiatives.

Distributed passwords are a barrier to action

While one password can be described as "easy to use," any number beyond three or four constitutes a nuisance. In corporate environments, where users may need to access 15 or 20 different applications to do their jobs, password authentication creates a low-level but persistent drag on employee productivity. Additionally, for applications that are infrequently used, passwords are easily forgotten and result in time-consuming calls to the help desk.

In consumer environments, the inconvenience that results from having multiple passwords has a different effect: A user who can't immediately access a protected resource will frequently abandon the effort and, in many cases, never bother to come back. This has an impact on revenues, customer loyalty and an organization's reputation for being easy to do business with.

Table 1. Prevalence of Existing Security Measures

	Used universally	Significant use	Used moderately	Very little use	Not used at all
Password protection	60%	32%	7%	1%	0%
Two-factor authentication (tokens)	8%	19%	25%	17%	32%
Two-factor authentication (biometrics)	1%	3%	9%	22%	66%
Smart cards	4%	12%	11%	19%	54%

PASSWORDS *VS.* STRONG AUTHENTICATION: WHERE THINGS STAND TODAY

While password protection is still widely used, security professionals recognize that it does not provide adequate protection for high-value applications and information. For example, in a survey of 250 security and IT executives, *60% reported that their enterprises still use passwords as their only form of user authentication*[1]. This is despite the fact that only 22% of those same executives rated password security as being highly effective.

In response, many organizations have implemented stronger forms of authentication for selected applications. As Table 1 shows, 44% of participants said their companies make significant or moderate use of token-based two-factor authentication; 32% make significant or moderate use of smart cards; and 12% do the same for biometrics.

How do CSOs rank the effectiveness of these different methods? While only 22% said that passwords are a highly effective security method, 48% said that token-based two-factor authentication was highly effective and 45% said biometrics are. This suggests that CSOs will opt for strong authentication any time the economics are sufficiently compelling.

Weak passwords pose a serious security threat

Password protection is relatively easy to defeat, even for low-tech thieves. With so many passwords to keep track of, many users subvert secure practices in the interests of convenience. They choose passwords that are easy to guess, use the same password for multiple accounts and/or leave passwords where they can be copied or stolen, all habits that increase the likelihood of online identity theft. For technology-savvy thieves, cracking tools—which are widely available on public web sites—automate the theft of encrypted passwords, exposing poorly constructed passwords in a matter of minutes.

[1]For more details, see the RSA Security White Paper, *The CSO Perspective on Security Threats, Data Protection and Identity and Access Management Solutions*, available at www.rsasecurity.com.

It should come as no surprise then that the misuse of password-protected identities is the starting point for a wide variety of online crimes. These include hacking, identity theft, credit fraud, online vandalism and intrusions to plan future network attacks. These actions can have serious consequences for the user and the targeted business—doubly so if the breach is publicized.

Passwords can be made stronger—to a point

Centralized solutions for identity management make significant progress in addressing the shortcomings of traditional distributed password protection. For example, through directory management, they reconcile multiple existing user identities into a single identity and password, which can authenticate the user to multiple resources in a single sign-on (SSO) or reduced sign-on environment. This enhances user convenience and dramatically reduces the administrative burden associated with passwords.

Additionally, centralized identity management solutions make it much easier to implement, automate and enforce secure password practices in a consistent way, for example by guiding users to create strong passwords that incorporate a range of non-alpha characters, by compelling them to change their passwords on a regular basis—by requiring that they only memorize one strong password instead of several.

Unfortunately, even the most disciplined password management practices cannot overcome the strongest cracking tools, which employ brute force attacks and exhaustive dictionary techniques to systematically test possible password combinations against encrypted password files. With only modest computing power and sufficient time, a determined cracker can expose strong passwords—and gain access to any resource they are designed to protect.

Furthermore, with centralized password solutions that enable SSO, a thief only needs to obtain one thing, a password, to gain the "keys to the kingdom." For many organizations, this alone is sufficient reason to decide that passwords do not provide adequate protection for user identities.

Lastly, centralized approaches don't address the problem of orphan accounts that may still exist in the original distributed security applications. Such accounts, which some analysts believe comprise as much as 60% of all online identities, can provide entry points for intruders to access individual applications.

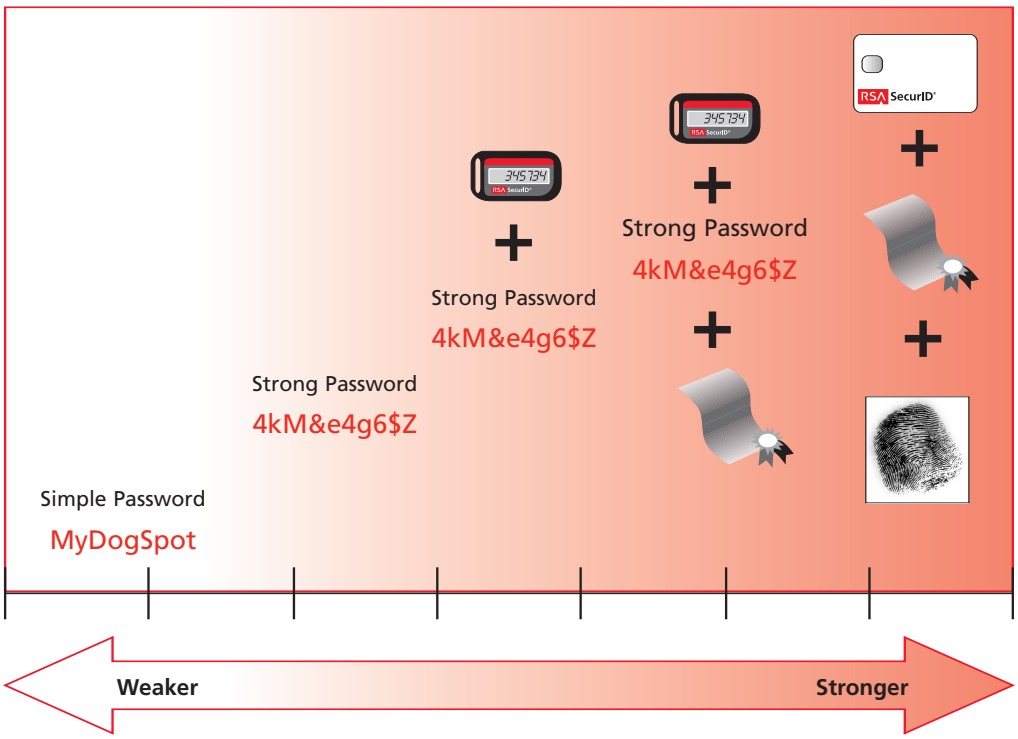


Figure 2.
Authentication Factors
Organizations can enhance security by requiring users to present multiple credentials or "factors". The more factors required, the greater the level of protection.

III. STRONG AUTHENTICATION: A STRONGER VALUE PROPOSITION, TOO

For those applications where password protection does not offer a sufficient value proposition, strong authentication is the only logical alternative. That's because an effective solution not only strengthens security but also enhances user convenience and reduces infrastructure costs.

Enhancing Security

What distinguishes strong authentication from password-based authentication? From a security perspective, the key difference is that a user must provide significantly stronger proof of identity before being granted access to protected resources. Typically, this proof is established by presenting multiple forms of identity or "factors." The more factors a user must present, the more secure an application is considered to be. (Password solutions only require one identifier and are therefore considered the least secure.) Identifiers fall into three broad categories:

- *Something only the user knows.* This includes passwords and confidential PINs.
- *Something only the user has.* This is usually a physical device (e.g., a token or smart card) that contains a unique and hard-to-defeat identifier (for example, a one-time authentication code or an encrypted digital certificate).
- *Something only the user is.* This category includes biometric identifiers that are unique to an individual, such as retinal or fingerprint scans.

Historically, two-factor authentication—which is similar to the model established for ATM cards and machines—has been the most common form of strong authentication for users. To prove identity and gain access, an individual must present two factors: a token or smart card and a confidential PIN. As with an ATM card, a criminal must steal the physical device and have access to the user's PIN in order to impersonate that user. This "raises the bar" sufficiently to discourage many identity thieves, who typically will move on, looking for an easier target.

Enhancing ROI

Strong authentication solutions can be leveraged across multiple applications, with one identity used to authenticate the user to a range of protected resources. As an organization adds strong authentication to a growing universe of resources and users, initial infrastructure investments and ongoing administrative costs (such as user management and help desk support) are amortized across a wider resource base, thus enhancing return on investment.

Creating a More Satisfying User Experience

Increasingly, strong authentication projects are being implemented in conjunction with web access management to provide single sign-on (SSO) to multiple applications or reduced sign-on. This allows users to navigate seamlessly across applications and domains and reduces the number of passwords that need to be remembered.

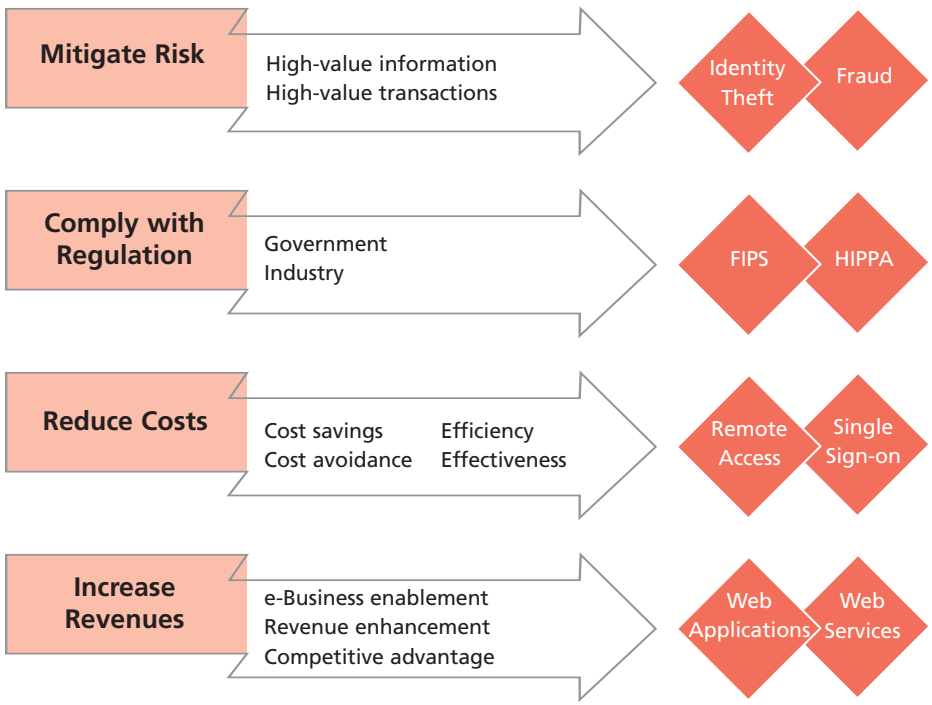


Figure 3. Identity & Access Management Market Drivers
Powerful forces are driving organizations to implement enterprise-wide initiatives for identity and access management (I&AM). In a survey conducted for RSA Security in 2003, 59% of security executives said their organizations had recently implemented or were currently involved in I&AM projects.

Means and Ends

Strong authentication solutions can incorporate a range of authentication methods, including one-time authentication codes, digital certificates, PINs and passwords and biometric identifiers. In turn, those identifiers can be stored and transported in different containers, including hardware and software tokens, smart cards and USB tokens. These diverse elements can be combined to meet a range of requirements for security, ease of use and total cost of ownership. (For a discussion of the various advantages and trade-offs of different strong authentication methods, see Appendix A.)

IV. FAST FORWARD: WHY THE USE OF STRONG AUTHENTICATION IS POISED FOR GROWTH

Historically, the adoption of strong authentication technologies has progressed at a leisurely rate. This is due to a number of factors including a lack of urgency regarding security issues, concerns about user acceptance of strong authentication (which typically requires some behavioral change) and perceptions that some technologies, in their early incarnations, were complex to deploy and support.

However, all these underlying factors have changed and there are compelling reasons to believe that large enterprises will accelerate their adoption of strong authentication during the next two to three years, creating pressures on their competitors and supply chain partners to do so as well. Some of the forces that RSA Security sees driving this shift are summarized below.

Consumer Demand for Increased Security

During the initial phase of e-commerce, enterprises enjoyed a period of rapid growth that was fueled by early adopters. However, the proverbial "low-hanging fruit" has long since been harvested and companies now struggle with how to entice the next 20% or 30% of their users into transacting business online. The economics for doing so are compelling and companies have tried many approaches to expand their user base. However, they have discovered that most consumers are unmoved by "cool" technology, innovative services or the promise of convenience. Instead, users have made it clear that security is their top concern, and they are willing to sit on the sidelines until that concern is addressed.

Large companies are starting to get the message. Across several key industries, RSA Security sees leading firms poised, for the first time, to adopt strong authentication for consumer applications. These leaders will position enhanced security as a competitive differentiator and will offer it as a premium service to security-minded users. As this begins to happen, competitors will be motivated to follow suit, and consumers will come to demand enhanced security. Companies that fail to respond may find themselves playing "catch up" in a fast-changing, security-hungry market.

Stronger Protection Against Insider Misdeeds

Another factor driving adoption of strong authentication is the realization that internal users commit a significant percentage of online misdeeds, often facilitated by password-based identities. In one widely publicized case, a help desk employee at a credit-service agency stole passwords that were used by his accomplices to steal thousands of credit reports and run up millions of dollars in fraudulent transactions.

In response to incidents such as this, companies are expanding their use of strong authentication beyond VPN and employee remote access applications. For example, many now require two-factor authentication for login to desktops, mobile systems and the network. This approach thwarts intruders who might otherwise gain access via an unattended system. Additionally, if a laptop is lost or stolen, strong authentication constitutes a significant barrier to viewing sensitive corporate data stored on the laptop and to accessing the network via the laptop. In some scenarios, employees use traditional passwords for accessing low-risk applications and two-factor methods for high-value applications.

Similarly, many enterprises use strong authentication to validate partners and independent contractors before allowing access to extranets and intranets. RSA Security sees this frequently among customers in all industries but especially in financial services, healthcare and manufacturing.

The Growth of Supply-Chain Solutions Based on Federated Identity

Looking ahead, the growth of strong authentication will also be driven by the security and ease-of-use requirements of federated identity solutions. Federated solutions will enable organizations in a "circle of trust" to provide their users with the convenience of secure single sign-on (SSO) across multiple partner sites. In the same way that a driver's license issued by one state or country is accepted in other jurisdictions, a user identity that has been authenticated by one partner will be trusted by the other partners, eliminating the need for the user to be authenticated or authorized multiple times.

If the user chooses, relevant "context" information can also be federated over to partners, eliminating the need to input the same data repeatedly. In an enterprise environment, this might include a user's company affiliation, e-mail address, job title and level of purchasing authority—information that can, for example, streamline the purchase of goods and services. In a consumer environment, the user's home address and credit card information could be federated to partner sites, along with relevant information about transactions recently carried out on those sites. In a commonly used example, a consumer who books an airline ticket for a vacation could allow information about his or her travel plans, for example dates of arrival and departure, to be made available to an auto rental agency and a hotel chain, facilitating faster booking of those accommodations.

Figure 4. USB Token
A number of factors are expected to drive wider adoption of strong authentication. One of these is the emergence of new authentication technologies that address varied requirements for mobility, security and total cost of ownership. For example, USB tokens combine the convenience of a plug-and-play device with secure storage of multiple digital credentials.

Figure 5. Authenticator Types
Two-factor authenticators come in a variety of forms suited to different business needs: smart cards, SMSdelivered access code, software and hardware tokens.

In a federated environment, even strong passwords may not provide sufficient proof of identity to justify this level of trust among partners. Instead, strong authentication will be a prerequisite.

Compliance Pressures on CSOs

A fast-growing body of laws and regulations hold companies accountable for protecting sensitive personal or business information that has been entrusted to them and for documenting business processes and transactions for audit and control purposes[2]. Many security executives now rank compliance among their top two or three concerns[3].

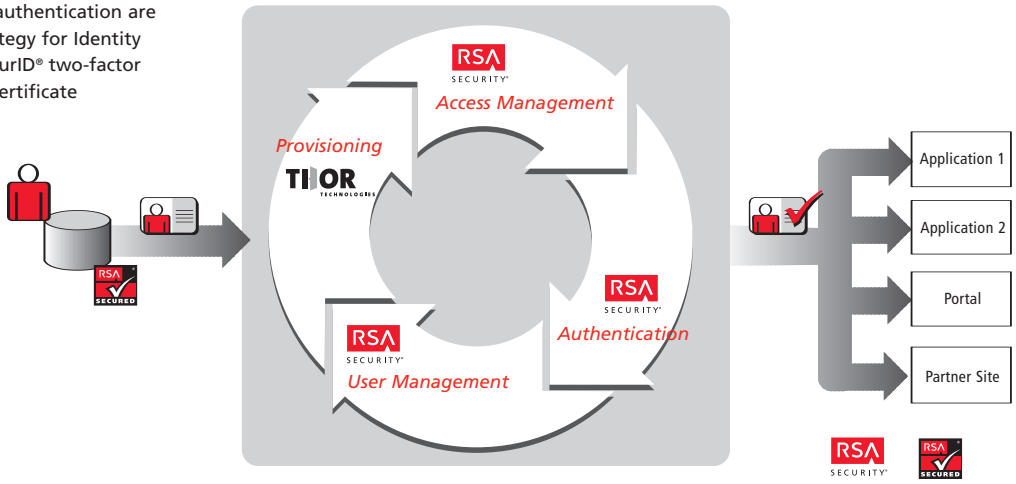
While there are many dimensions to compliance, a number of laws have implications in the realm of strong authentication. For example, in the U.S., the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare-related organizations that have custody of sensitive patient data to reliably validate a user's identity before granting that individual access to the data. Because passwords don't provide the proof of identity that HIPAA requires, many companies have implemented strong authentication solutions for individuals requiring remote access.

In numerous countries, laws have been enacted to ensure that digital signatures provide the protection that is necessary to reliably authenticate online transactions and communications. For example, the European Union (E.U.) Directive for Digital Signatures defines the legal, technical and policy criteria that digital signatures must meet in order to ensure E.U.-wide acceptance.

[2]These include the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act, Food and Drug Administration (FDA) 21 CFR Part 11EU, the California Data Protection Act, the European Data Protection Act and various digital signature directives.

[3]In the previously mentioned survey of CSOs conducted for RSA Security, 24% of respondents said compliance had the most impact on their company's awareness of security issues — ranking second only to the September 11 terrorist attacks (30%) and well ahead of viruses (18%), hacking (12%) and identity theft (6%)

Figure 6. RSA Security's I&AM Strategy
RSA Security solutions for strong authentication are part of the company's overall strategy for Identity and Access Management. RSA SecurID® two-factor authentication and RSA® Digital Certificate management software integrate seamlessly with RSA® Access Manager web access management and with other components of the I&AM infrastructure. In the future, all of these products will converge to a single I&AM platform that offers a common set of services.



Enhanced Usability and Economics

Many organizations have been slow to adopt strong authentication due to concerns about user acceptance and total cost of ownership (TCO). However, this situation is changing as new technologies offer more diverse value propositions, mature technologies become more efficient and cost-effective and authentication investments are leveraged across a wider range of applications and users.

For example, a new generation of USB tokens address a wide range of strong authentication challenges. USB tokens can securely store multiple credentials on one device, greatly reducing the security risks and infrastructure costs that result from maintaining multiple authentication methods. They are small and highly portable, which helps ensure user acceptance. In addition, because USB ports are now built into virtually all computers and many consumer devices, the tokens don't require a card reader—which reduces cost of ownership.

Even as new technologies emerge, well-established authentication technologies continue to improve. For example, hardware token vendors have developed web-based user self-service solutions that reduce the administrative burden and costs of distributing physical tokens. Similarly, certificate-based solutions, which initially gained a reputation for being complex, have made significant advances in ease of deployment and the automation of administration and management tasks.

In addition to all these forces, which are helping to drive point solutions for strong authentication, an additional "pull" is being created by identity and access management initiatives.

V. VIEWING STRONG AUTHENTICATION IN THE CONTEXT OF IDENTITY AND ACCESS MANAGEMENT

In business relationships, both online and off, identity is the foundation of trust. The more an enterprise knows about a person—who they are, what they do and who already trusts them—the easier it is to evaluate how much trust to extend to that individual.

The pervasive lack of trust in online environments and the subsequent push for I&AM strategies is driven, in large part, by the fact that traditional online identities are highly unreliable. It is simply too easy to fabricate a false identity or to steal a legitimate one. One of the primary goals of I&AM is to create valid and accurate user identities that are extremely difficult to compromise—and therefore can be trusted in online transactions and communications.

Safeguarding User Identities

Once an identity has been created, it is protected through a number of security mechanisms. These may include rogue-account detection capabilities within the provisioning function, as well as the practice of encrypting identity data stores to thwart the theft of user identities by hackers and other intruders. When users go online, strong authentication is the primary form of protection that ensures trust in online identities. Regardless of the strong authentication method chosen, a well-designed solution will:

- Provide strong proof of identity as the basis for granting access to protected systems and applications;

- Enable secure single sign-on, when deployed in conjunction with web access management;
- Thwart online identity theft by ensuring that a user's credentials are hard to compromise;
- Render stolen identity information less useful in committing online crimes because that data is not the basis for granting access and
- Ensure after-the-fact accountability for reporting and audit purposes.

In addition to these functional benefits, strong authentication provides compelling evidence to users that an organization takes seriously their concerns about security and privacy.

VI. CONSIDERATIONS WHEN CHOOSING A STRONG AUTHENTICATION PROVIDER

Accustomed to thinking of strong authentication in a limited context, many organizations don't see the intimate connection between strong authentication and identity management. This failure to "connect the dots" can have costly consequences down the road, for example, if today's point authentication investments don't align well with future I&AM initiatives.

An experienced vendor, with a strategic vision for I&AM and practical expertise in strong authentication, can help an organization articulate the role that strong authentication plays within I&AM framework. Conversely, a vendor can help ensure that stand-alone projects for strong authentication take into account future I&AM plans, or initiatives already under way in other parts of the organization.

RSA Security: Providing Leadership in Strong Authentication and I&AM

RSA Security is well qualified to help enterprises address the challenges of strong authentication within the framework of I&AM. With a brilliant heritage in security technologies, the company is a recognized pioneer, market leader and innovator in this field. Equally important, RSA Security's strong authentication continues to be an integral part of the company's strategy for identity and access management.

At this moment, RSA Security identity management solutions are helping organizations worldwide leverage the power of online identity to increase security and trust, enhance employee effectiveness, strengthen partner relationships and reduce business process costs. With a rock-solid foundation in industry standards and a stellar track record for ease of integration and interoperability, these solutions also help position organizations to participate in environments that incorporate federated identity and web services technology.

An Incremental Approach

Recognizing that implementation of I&AM is 3- to 5-year undertaking, RSA Security helps an organization articulate its vision for I&AM in the context of its most pressing business and security challenges and its future business goals. Offering a pragmatic and flexible approach, RSA Security encourages enterprises to start their I&AM journey from the point that is most relevant to their needs. This may be user management and provisioning, strong authentication, web access management, single sign-on (SSO) or federated identity. In any case, an organization can implement I&AM in a phased approach, proceeding at its own pace.

Thought Leadership

On this journey, RSA Security provides insight into where identity management technologies are heading along with guidance on how to ensure investment protection for today's I&AM investments. This perspective is gained through the company's technical and business leadership in key standards bodies, such as the Liberty Alliance and WS-Security, and through the work of RSA Laboratories, which pursues research and provides state-of-the-art expertise in security technologies.

Market Leadership Today

Within the larger framework of I&AM, RSA Security is an established market leader in strong authentication. Built on 20 years of experience, the company's solutions help address the need for strong protection of user identities, easy integration and deployment of security infrastructure and cost-effective user administration.

To meet varying requirements for security, portability and cost of ownership, RSA Security offers diverse authentication methods.

- *RSA SecurID® tokens* have been deployed to 15 million users around the globe and are widely recognized by an authentication code that changes every 60 seconds. Rugged and highly portable, self-contained hardware tokens are small enough to clip on a key chain. As an alternative, software tokens can be installed on client devices—such as PCs, laptops and personal digital assistants (PDAs)—which eliminates the need to carry a separate hardware token.
- *RSA SecurID Smart Card solutions* can allow an organization to combine multiple credentials and security functions on one device and infrastructure, thus increasing user convenience while consolidating costs. Helping to provide secure storage for RSA SecurID functionality, passwords and digital certificates, a single device can enable employee badging, building access and network access.
- *RSA SecurID USB tokens* are similar to smart cards in that a token can store multiple credentials on one device. However, this solution uses a different form factor: a small, rugged token that can plug into any USB port to deliver the user's credentials.
- *RSA® Digital Certificate Management solutions* can enable an enterprise to issue, validate and manage credentials that are based on x.509 digital certificates. These solutions have already proven their value in authenticating users, devices (such as servers, mobile phones and cable modems) and transactions. For example, RSA® e-Sign capabilities within the RSA Digital Certificate solution help enterprises to add legally binding digital signature capabilities to web-based forms and e-mail. In web services environments, RSA Security certificate solutions are designed to provide a mechanism for discrete web services to reliably authenticate themselves to other web services.
- *Biometric credentials* enhance proof of identity by adding biometric identifiers, such as fingerprint and retinal scans, to RSA Security's strong authentication devices—either smart cards or USB tokens. This application is most commonly used in government and high-security environments.

A MIGRATION PATH TO THE FUTURE

RSA Security's solutions for strong authentication are evolving to incorporate standards for web services and federated identity. In the future, they are designed to converge to a single enterprise platform that offers common services for user management and administration. With an eye to the future, RSA Security continues to explore approaches to strong authentication that will help enhance security and drive down cost of ownership while supporting the larger goals of identity and access management.

CLOSING THOUGHTS

Distributed approaches to identity management no longer meet the demanding requirements of today's complex enterprises. In their place, identity and access management strategies are taking shape, allowing organizations to address strategic goals such as enhancing security, reducing infrastructure and administrative costs and enabling new business opportunities.

Deployed to protect a far wider range of resources than in the past, strong authentication will play an important role in this new environment, enhancing trust by providing conclusive proof of user identities.

Prudent organizations will plan identity management projects with strong authentication in mind. Conversely, point solutions should be planned and deployed within the framework of I&AM. In all these matters RSA Security can help provide organizations with the insight, vision and technology expertise that is required to ensure lasting success for their initiatives.

ABOUT RSA SECURITY INC.

With more than 15,000 customers around the globe, RSA Security provides interoperable solutions for establishing online identities, access rights and privileges for people, applications and devices. Built to work seamlessly and transparently in complex environments, the Company's comprehensive portfolio of identity and access management solutions—including authentication, web access management and developer solutions—is designed to allow customers to confidently exploit new technologies for competitive advantage. RSA Security's strong reputation is built on its history of ingenuity and leadership, proven technologies and long-standing relationships with more than 1,000 technology partners. For more information, please visit www.rsasecurity.com.

APPENDIX

Form Follows Function: Evaluating Diverse Authentication Methods and Form Factors

In planning a strong authentication strategy, an organization can choose from a range of authentication methods and forms factors. Different combinations of methods and form factors offer different value propositions in terms of security, portability, scalability, ease of use, reliability and cost of ownership. For organizations that want to evaluate the merits of different strong authentication methods, RSA Security offers a consistent, structured framework and calculator, the Authentication Scorecard. This vendor-neutral tool, available at www.rsasecurity.com, can help organizations select the most appropriate technologies for their mix of authentication challenges.

Self-contained hardware tokens. While the underlying technologies differ from vendor to vendor, these devices are similar in that they autonomously generate a secure authentication code that either changes frequently or is only good for a single use. This dynamic quality makes it difficult for a would-be intruder to compromise a user's online identity. Self-contained tokens get high marks for security, portability and ease of use. Drawbacks include the cost and administrative burden of distributing and revoking physical tokens.

Software tokens deployed on hardware devices. A number of vendors offer software versions of their self-contained hardware tokens. Typically, software tokens are deployed on multipurpose client devices—such as a PC for desktop authentication or a laptop or PDA for mobile authentication- using the device both as a container for the credential and as a source of computing power to generate the credential. By leveraging existing infrastructure, this approach eliminates the need for users to carry a separate authenticator and eliminates costs related to the distribution of physical tokens. However, the client device must be physically present, which limits portability. Additionally, software tokens are not considered to be as secure as self-contained hardware tokens.

Smart cards. Smart cards make it possible to consolidate multiple credentials (passwords, certificates and biometrics) on one device and infrastructure to support multiple security applications, including employee badging, network access and building access. This can enhance user convenience and eliminate duplicate infrastructure. The most significant drawback to this approach is the requirement that card readers be installed at every access point. This adds to deployment and management costs and limits the portability of a user's credentials.

USB tokens. Though relatively new, this form factor has been greeted with early enthusiasm. Small enough to carry on a key chain, these devices combine some of the strengths of self-contained tokens (portability, ease of use) with those of smart cards (e.g., the ability to store multiple credentials on one device, including passwords, digital certificates and biometric identifiers). Because they can be plugged in to any USB port, USB tokens can be used to authenticate users to a wide range of hardware devices and the networks on which those devices reside. Considerations include the costs of token distribution.

Mobile devices. Wireless phones and PDAs can also be used to immediately deliver one-time authentication codes to a user, via text messaging, as part of the login process. This is viewed as an economic way to provide strong authentication for web-based consumer applications. However, a user's ability to immediately receive an access code can be affected by "dead spots" in their wireless service.

RSA SECURITY®

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

SA WP 0804