

RSA SecurID® Authentication

A Better Value for a Better ROI

The value of the RSA SecurID® authentication solution goes far beyond the technical features and benefits of the RSA SecurID token. When you purchase RSA SecurID authentication, you are not only protecting your network and network-based applications, but also investing in a security solution that is manageable, scalable and easily deployable — now and over time. RSA SecurID is not “just a token” — rather, it is a security solution that offers, when compared to competitive products, significantly lower total cost of ownership (TCO) and higher return on investment (ROI).

The objective of this paper is to highlight the value of the RSA SecurID time-synchronous authentication solution by analyzing the RSA Security solution against various competitive products. We will explore how RSA SecurID authentication helps to mitigate network security risk, reduce costs, increase revenues, achieve compliance and, perhaps most importantly, protect your investment in authentication technology as your e-security needs grow over time.

RSA SecurID Authentication
A Better Value for a Better ROI

Table of Contents

I.	e-Security and Trust	1
	1.1 Financial Losses	1
	1.2 Passwords Aren't Enough	1
II.	What is Two-factor Authentication	1
III.	RSA SecurID Value Points	2
IV.	The ROI of RSA SecurID Authentication	4
V.	Investment Protection	8
	5.1 Securing VPNs	8
	5.2 Securing Wireless Devices	9
	5.3 Securing Digital Certificates	9
VI.	Conclusion	10
	About RSA Security	10

I. e-Security and Trust

A strong network security solution is the foundation of e-business. Without a strong security solution, there is no trust between customers, partners and employees. And without trust, e-business is ineffective. We all know that effective e-business is critical to increasing revenues and profits. In addition, you can incur substantial losses (financial and others) if your network or applications on your network are breached. Two-factor authentication helps you not only to establish the trust on which e-business revenues and profits are based, but also to protect you and your e-business from losses due to unauthorized access.

1.1 Financial Losses

Continued computer security breaches and corresponding financial losses underscore the increasing need for two-factor authentication. Consider the following statistics from the 2001 "Computer Crime and Security Survey" developed by the Computer Security Institute (CSI) with the participation of the Federal Bureau of Investigation's (FBI) Computer Intrusion Squad:

- 85 percent of respondents detected cyber attacks within the last 12 months;
- 64 percent of respondents acknowledged financial losses due to computer breaches;
- 187 companies reported a total of \$377,828,700 in quantified financial losses — that's an average loss of approximately \$2 million per company; and
- The most serious financial losses occurred through theft of proprietary information and financial fraud.

1.2 Passwords Aren't Enough

Many companies are comfortable with protecting their high-value information and transactions with a password. A simple password security policy may be effective for protecting non-critical data and does not require the purchase of additional hardware and software but usability issues (memorizing passwords), administrative issues (calls to the help desk) and security issues (password hacking tools) render a password-only authentication policy inadequate for protecting high-value information. One way to strengthen your authentication policy is by adding factors such as tokens, smart cards, digital certificates and biometrics. The most common form of multi-factor authentication is two-factor authentication using a token or smart card as the second form of identification.

II. What is Two-factor Authentication?

The most popular example of two-factor authentication is a typical ATM banking scenario — you combine something you know (your password) with something you have (your ATM card) to prove that you are who you say you are.

Most IT professionals would agree that two-factor authentication is vital to effective network security. But which two-factor authentication solution is right for you? There are multiple types of two-factor authentication: challenge-response, event-synchronous and time-synchronous authentication. RSA SecurID authentication is based on patented, time-synchronous technology.

The following outlines some of the differences between the various methods of authentication — and the reason why time-synchronous authentication is most efficient.

Challenge-Response

1. User enters user name and password
2. Server sends 8-digit challenge
3. User enters 8-digit challenge
4. 8-digit response is displayed on token
5. User enters 8-digit response, and is validated

Event-synchronous

1. User activates next token code by pushing a button on the token (the "event")
2. User enters user name and passcode (the passcode is an event-produced token code + the user's PIN)
3. Server authenticates by matching user passcode with server passcode (server passcode is generated based on the next "event" in the sequence)

Time-synchronous

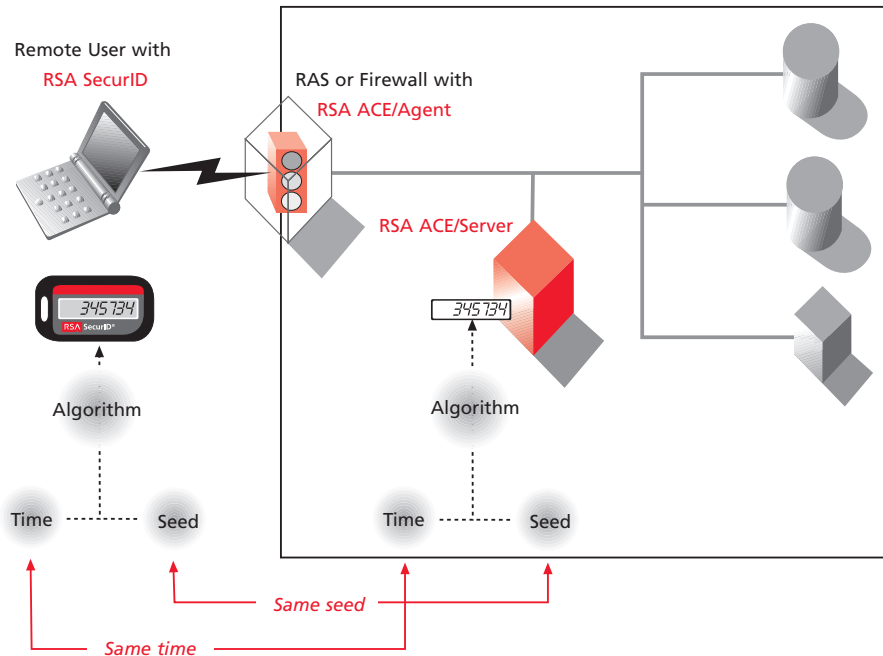
1. User enters user name and passcode (the passcode is a four- to eight-digit random token code + the user's PIN)
2. Server and token compute token code by combining seed record and current Greenwich Mean Time
3. Server authenticates user by matching user passcode with server passcode

Challenge-response authentication proceeds through a laborious 5-step process that is prone to user error. Event synchronous authentication follows a three-step process in which the token code is based on the next number in the sequence, not a random number generation scheme, which makes the device prone to hacking.

In time-synchronous authentication, both the token and the server (RSA ACE/Server®) have internal clocks that are synchronized (hence, "time-synchronous"). They also have identical seeds (a "seed" is the starting value used by a random number generation routine to create a pseudo-

RSA SecurID Authentication A Better Value for a Better ROI

Figure 1: Time Synchronized Authentication



fewer instances of a user being locked out of network resources than with event-synchronous or challenge-response (in all forms of two-factor authentication, the token is locked if a user enters a PIN incorrectly multiple times).

Portability

Time-synchronous hardware tokens are extremely portable because they are in no way tied to the user's desktop. You can also choose from any number of form factors that can be easily integrated into the user's arsenal of business tools, such as Palm devices and mobile phones.

The remainder of this paper explores some of the more compelling advantages of the RSA SecurID solution that demonstrate its superior overall value.

random number). The seed is embedded within a token and generates a new token code every 60 seconds. The "seed record" is housed within the RSA ACE/Server software and generates the same token code at the same time. When the user enters the passcode, the server validates that this code matches its records at that point in time. If the code matches, the user is authenticated and granted access to protected resources.

IT professionals cite time-synchronous authentication as more effective than challenge-response or event-synchronous authentication for many reasons, including the following:

Enhanced Security

The time-synchronous approach to two-factor authentication is inherently more secure than event-based or challenge response authentication. Time-synchronous technology is based on the token's secret seed, which is virtually hacker-proof. The other approaches are less sophisticated and prone to vulnerability.

Ease of Use

Time-synchronous authentication requires two simple steps. In contrast, challenge-response authentication involves five steps and event-synchronous involves three steps. As a result, fewer user errors occur with time-synchronous authentication.

Fewer Administrative Headaches

Because fewer keystrokes are required with time-synchronous authentication, there are fewer mistakes and

III. RSA SecurID Value Points

When you purchase any technology product, you expect much more for your money than simply a product that works. You expect a product that is manageable, a product that can scale with your company as it grows, a product that is interoperable with your existing network topology and, of course, great service. You also want to work with a company that has the experience and stability to be your technology partner, now and in the future. Your decision to purchase one product over another is based on much more than just the price. That is, you want a complete solution that will deliver substantial added value.

RSA SecurID authentication offers exactly that. When you purchase RSA SecurID authentication, you'll get added value in the following respects:

Flexible Solution for Multiple Applications

Whether your application is for enterprise, B2B, or B2C, RSA SecurID authentication can protect your network and the multiple applications on that network. RSA SecurID authentication is compatible out of the box with most network communication products available today, including remote access servers, firewalls, VPN, Web and wireless. That means it's easy for you to implement two-factor authentication. Equally important, you can quickly extend that protection to include other applications as the need arises. There are over 200 products from more than 150 vendors that are already RSA SecurID Ready. No other authentication product can ensure the same level of flexibility and investment protection.

RSA SecurID Authentication A Better Value for a Better ROI

Figure 2. Authentication Choices

Category	RSA Security	ActivCard	Secure Computing	Vasco
Hardware Token	✓	✓	✓	✓
Software token — PCs, mobile phones, PDAs	✓	—	✓	—
Stored-value smart card	✓	—	—	✓
Cryptographic smart card	✓	✓	—	✓
Digital Certificates	✓	✓	✓	✓
Biometrics	✓	✓	—	—

Authentication Choices

RSA Security offers a wide range of form factors — including a variety of hardware and software tokens. Equally important, RSA Security offers a host of other options should your authentication requirements evolve. Some of these options include smart cards, biometrics and even digital certificates (PKI). This is advantageous because you can choose the form factor that best fits your needs and the needs of your users. Such needs may include portability, deployment, cost and ease of use.

Management Software

RSA ACE/Server software, the power behind RSA SecurID authentication, helps you centrally manage a distributed deployment of RSA SecurID tokens, enforce security policy and maintain an audit trail of user access and administrative changes.

Seamless Deployment

RSA SecurID Web Express is a Web-based, self-service workflow product that enables you to easily and rapidly provision RSA SecurID hardware tokens and assign users to the RSA ACE/Server software. Users of RSA SecurID Web Express have lowered their deployment costs by over 50% and reduced their time spent deploying tokens by as much as 90%.

Database Replication

Database replication enables not only high performance authentication but also flexibility. By distributing multiple replicas (up to 10) across your network, users can authenticate locally, improving performance and reducing

long distance telecommunication costs. Replicated servers can also increase authentication performance by automatically routing authentication requests to the fastest performing server across the network. In addition, multiple replicas provide disaster recovery flexibility in the event of a site failure.

Lightweight Directory Application Protocol (LDAP) Support

Lightweight Directory Application Protocol (LDAP) v3 support enables you to lower administration costs by centrally managing users from your existing LDAP repository (Active Directory, iPlanet or NDS eDirectory), while securely managing authentication information in the RSA ACE/Server software.

Service, Service, Service

Value added services for RSA SecurID authenticators include:

- Token programming: All RSA SecurID authenticators arrive to your end users pre-programmed and ready to use — no programming is required by your administrators.
- Token customization: RSA SecurID Select enables you to brand your RSA SecurID tokens with your company logo to enhance the visibility of your brand.
- 24/7 Worldwide Customer Support: RSA Security is renowned for its responsive customer service — something we've been doing for 20 years.
- Professional Services: the RSA Security Professional Services organization is comprised of industry experts to help you get the most out of your RSA SecurID implementation.

Complete e-Security Solution

RSA Security is more than a point product vendor — we aim to be your strategic e-security partner. We offer one stop shopping for a broad range of e-security needs — from two-factor authentication (RSA SecurID), to authorization (RSA ClearTrust), to digital certificates (RSA Keon), to security development tools (RSA BSAFE).

Experienced, Proven Company

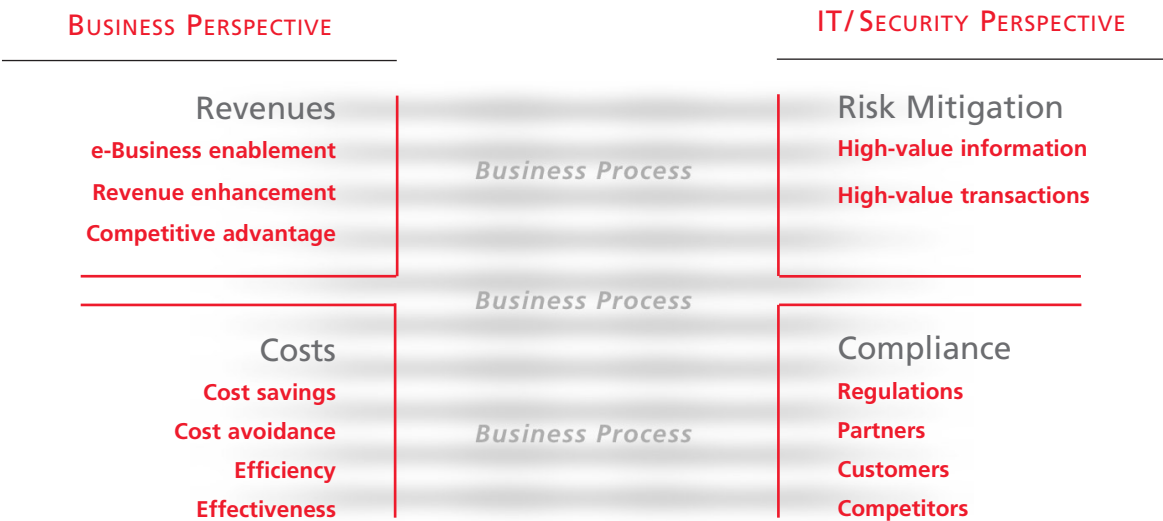
RSA Security has been securing the authenticity of people, devices and transactions for over 20 years. Our experienced staff of professionals has the breadth and expertise to provide you with top-notch service and the long-term vision that enables RSA Security to be your strategic e-security partner for years to come.

IV. The ROI of RSA SecurID Authentication

The return on investment (ROI) of your e-security solution can be broken down into four areas: mitigated risk, increased compliance, lower costs, and higher revenues. Because your RSA SecurID authentication solution helps you to mitigate e-security risk, comply with the security demands of customers and partners, reduce costs and increase revenues, your return on investment will be very high. If there's ever been a doubt, the following section can help you build an ironclad business case for your RSA SecurID implementation.

Figure 3 defines each of these segments.

Figure 3: e-Security ROI segments. Returns from e-security infrastructure are intertwined with returns from business process / applications



RSA SecurID Authentication A Better Value for a Better ROI

When determining the ROI of your security solution, you should consider the following:

Risk

- How important is the data that you're protecting?
- How valuable are your e-business transactions?
- Are you mitigating the risk of a security breach?

Compliance

- How important is secure e-business and trust between partners and customers?
- Have your customers or business partners mandated improvements to your security infrastructure?
- Have you lost customers because you failed to meet their security requirements?
- Are there regulations (governmental or other) to which you must adhere?

Costs

- What are the long-term savings associated with your e-business initiative?
- What long-term costs will you avoid by deploying secure e-business applications?
- How much more efficient and effective will your employees be?

Revenues

- Will this solution now enable you to conduct high-value electronic transactions with confidence?
- Will this security solution give you the confidence to conduct e-business with your existing customers and partners?
- Will you be able to reach new customers and partners with secure e-business applications?
- Will the solution improve customer satisfaction and thereby increase revenues?
- Will increased revenues provide you with a competitive advantage?

It's easy to see how RSA SecurID authentication mitigates the risk of malicious breaches. That in and of itself is a great return on your investment. However, RSA SecurID authentication also delivers returns in the areas of compliance, costs and revenues. Figure 4 shows some of the different value points of RSA SecurID authentication classified in the four ROI segments they satisfy.

CareWeb at Beth Israel Deaconess Medical Center

When Boston's Beth Israel and Deaconess Hospitals merged, they soon realized that they needed a way to offer doctors quick, easy access to medical records from both hospitals. They came up with the notion of CareWeb — an intranet providing a consolidated view of the individual systems of the merged hospitals. The hospital needed a network it could guarantee would be safe from break-ins. Without an airtight security solution, the project would never have gotten off the ground.

"By using RSA SecurID authentication, we know exactly who is accessing the system and know what information they are looking at. It's not just a guess based on a static password that could have been easily compromised."

Dr. John Halamka,
Executive Director,
CareGroup Center for Quality and Value

RSA SecurID Authentication A Better Value for a Better ROI

Figure 4. ROI of RSA SecurID Authentication

Key	
✓ Risk: helps to mitigate risks	× Risk: Does not help to mitigate risks
✓ Compliance: enables compliance with customers and/or partners	× Compliance: Does not enable compliance with customers and/or partners
✓ Costs: helps to reduce and/or avoid costs	× Costs: Does not help to reduce and/or avoid costs
✓ Revenues: enhances revenues by enabling more effective e-business	× Revenues: Does not enhance revenues

RSA SecurID Value Points	ROI Segment Satisfied	ROI Impact Statement
Flexible solution for multiple applications	✓ Risk × Compliance ✓ Costs ✓ Revenues	<i>Because RSA SecurID works seamlessly with so many network communications products, you can use the same server and tokens to protect multiple applications.</i>
Authentication choices	× Risk ✓ Compliance ✓ Costs ✓ Revenues	<i>RSA SecurID offers a full range of authentication choices. You can choose a host device (such as a PDA) that your users already have to reduce deployment costs.</i>
Management software	✓ Risk ✓ Compliance ✓ Costs ✓ Revenues	<i>The RSA ACE/Server enables you to enforce your own security policy, limiting the risk of exposing high value information to malicious intrusion.</i>
Seamless token deployment	✓ Risk ✓ Compliance ✓ Costs ✓ Revenues	<i>By automating the deployment of tokens, RSA SecurID Web Express allows you to lower your deployment costs and reduce your time spent deploying tokens.</i>
Database replication	✓ Risk ✓ Compliance ✓ Costs ✓ Revenues	<i>With database replication, you are assured the performance and fail-over recovery you need for 100% uptime in your authentication services.</i>
LDAP support	✓ Risk ✓ Compliance ✓ Costs ✓ Revenues	<i>RSA SecurID LDAP support enables you to enter user data only once and automate any later modifications — significantly reducing administrative costs.</i>

RSA SecurID Authentication A Better Value for a Better ROI

RSA SecurID Value Points	ROI Segment Satisfied	ROI Impact Statement
Token programming services	<ul style="list-style-type: none"> ✓ Risk ✓ Compliance ✓ Costs ✓ Revenues 	<i>RSA SecurID tokens are delivered to you preprogrammed, which means you don't need resources to program tokens at the time of deployment or throughout their life cycle.</i>
Token customization services	<ul style="list-style-type: none"> ✗ Risk ✓ Compliance ✓ Costs ✓ Revenues 	<i>RSA SecurID Select allows you to incorporate your brand onto your tokens, which effectively puts your brand in every user's pocket — thereby increasing brand awareness.</i>
24x7 customer support	<ul style="list-style-type: none"> ✓ Risk ✗ Compliance ✓ Costs ✓ Revenues 	<i>RSA Security offers 24x7 customer support. That means you never have to deal with the risk associated with downtime of your authentication services.</i>
Professional services	<ul style="list-style-type: none"> ✓ Risk ✗ Compliance ✓ Costs ✓ Revenues 	<i>RSA Security Professional Services organization helps you stretch your resources and ensures that you get the most out of your RSA SecurID solution.</i>
Complete e-security solution	<ul style="list-style-type: none"> ✓ Risk ✓ Compliance ✓ Costs ✓ Revenues 	<i>RSA Security offers a full suite of e-security solutions from which to choose, enabling you to comply with any and all e-security requirements or regulations.</i>
Experienced, proven company	<ul style="list-style-type: none"> ✓ Risk ✗ Compliance ✓ Costs ✓ Revenues 	<i>RSA Security has been in the business for over 20 years — experience that we've used to build the best e-security solutions to protect your valuable resources from intrusion.</i>

Cable & Wireless

Having noticed a significant trend within the remote access market towards outsourcing, CWC developed a managed remote access solution for its customer base, Cable & Wireless Secure Dial Service. During the development phase of Secure Dial, customer feedback indicated that increased security was a must — and in some cases RSA Security was specifically named as a preferred supplier. CWC then set about evaluating the various manufacturers of network and data security solutions, and measured them on the following criteria: future product development strategy; technical support; how the product fit the existing technical infrastructure; and branding.

"RSA Security emerged as best of breed for several key reasons. RSA Security was a well-established company with a solid customer base, and its products were well advanced in the development cycle, ensuring that any potential problems had already been ironed out. We could see how the product had already evolved and were confident that this development had also built our confidence in the product's reliability and performance. It proved very straightforward to integrate the RSA Security products into our existing platform and they were fully compatible with all the other components of the service."

Lance Spencer
Managing Director, IP and Customer Solutions
Cable & Wireless



V. Investment Protection

One of the most important value points of RSA SecurID authentication is investment protection. That is, should you decide in the future to enhance your security infrastructure with a VPN and/or digital certificates, or enable your remote users to access confidential corporate data via a wireless device and/or the Internet, RSA SecurID authentication can always be used to verify the identity of the person accessing your network. All of this can be accomplished using the same authentication server and the same authenticators. This represents a tremendous cost savings since the authentication infrastructure is already in place. In addition, you won't have to do any custom coding because RSA SecurID technology is interoperable with all the major network communications products on the market. No matter what product you end up with, you just plug it in and activate the authentication option. Bottom line: RSA SecurID authentication enables you to build upon your current security investment now and in the future.

5.1 Securing VPNs

According to TeleChoice, Inc., "...a successful VPN begins with a well-defined security policy. Don't skimp in this area ... It may add to your overall costs, but it's well worth it in the long run." The experts agree that for a VPN to be effective, it must be combined with a strong authentication solution. The private tunnel through the public Internet may be encrypted and protected with firewalls — but that's not enough protection. You still need to know the identity of the user at the other end of the tunnel and you cannot know this with certainty without strong authentication. Two-factor authentication — something you know combined with something you have — establishes trust between you and your employees, partners, and customers. Once you have trust, you've built the foundation for effective e-business. Additionally, you need to make sure you have the most robust network security solution in the market — RSA SecurID authentication.

RSA SecurID Authentication A Better Value for a Better ROI

5.2 Securing Wireless Access

The 2000 Network World 500 survey indicates that almost 75% of hand held devices will be tied to enterprise networks within the next 12 months. The survey goes on to say that security for stored and transmitted data is the top concern of 80% of the IT professionals interviewed. This proves that as the use of wireless devices to access network applications becomes more pervasive, the need for strong authentication becomes even more important. RSA SecurID two-factor authentication is an effective, easy way to secure wireless Web or wireless LAN access to your valuable company information and provides sure proof of identity for a secure wireless transaction.

5.3 Securing Web Applications

Today, organizations worldwide are taking advantage of Web technology by setting up intranet and extranet applications to expedite business processes, to build stronger relationships with employees, customers and business partners, to lower the cost of doing business and, ultimately, to gain competitive advantage.

These qualities make the Web an attractive medium for delivering information. Yet conducting business on the Web often results in a "hostile network environment" in which you cannot set or control security policy. Moreover, you must be concerned with inherent security threats, such as unauthorized user access, data tampering and eavesdropping. Under these conditions, a strong network security solution is essential — one that transparently and automatically controls who gets access to corporate intranets and extranets as well as what they are authorized to access once they've been authenticated.

RSA Security provides the industry's leading integrated authentication, encryption and access control solution. RSA SecurID authentication provides the strong authentication you need to validate the identity of your users. Equally important, RSA ClearTrust® authorization provides the user privilege management capabilities that allow you to control what resources authenticated users are able to access.

5.4 Securing Digital Certificates

If you have committed to PKI, you may still need two-factor authentication to protect user certificates. RSA SecurID authentication binds a user's physical identity to his digital identity, so you know beyond a shadow of a doubt that the user is who he says he is.

RSA Keon products deliver the core PKI security benefits of authentication, confidentiality, data integrity and non-repudiation that enable secure e-business. These PKI services are built on unique private encryption keys and user credentials. Once the user is authenticated with an RSA SecurID authenticator, the digital credentials can be used for encrypting local files, establishing secure encrypted sessions between the user and a number of applications, and providing secure access to multiple applications. For even more security, you should consider using the RSA SecurID smart card solution. In this scenario, the user's keys are generated and stored on the card so it is virtually impossible for an imposter to access the user's digital identity.

Lufthansa German Airlines

Lufthansa German Airlines selected RSA SecurID authentication technology to establish and help secure a Web-based scheduling system to manage Lufthansa's flight information and schedules. Working together, RSA Security and Lufthansa created Lufthansa Crew Remote Access, a Web-based flight management system that is designed to allow the airline's 15,000 flight personnel to remotely access critical, detailed and sensitive flight information and schedules in a secure environment that is based on RSA SecurID authentication technology. To use the Lufthansa Crew Remote Access system, flight personnel use RSA SecurID authenticators to access the Web site from any PC with Virtual Private Network (VPN) access. Once on the system, they are prompted for the time-sensitive security passcode displayed on their RSA SecurID authenticator which is then authenticated with the RSA ACE/Server® software on the Lufthansa system. This provides a two-factor authentication solution that is designed to protect the network and the data integrity. The RSA ACE/Server software manages the system and records all users' access attempts.

"The system is very easy to both access and use, as well as saving time all-round. The ability to get accurate, up-to-date information from home or on the move makes flight preparations more manageable and relaxed."

Werner Bieske
Information & Communications Manager
Lufthansa



Lufthansa

VI. Conclusion

The value of RSA SecurID technology is unsurpassed by any other authentication vendor. The combination of industry leading technology, multiple authentication choices, top-notch service & support and seamless interoperability provides enterprise, B2B and B2C applications with the most return on their e-security investment. You know it's time to strengthen the protection of your valuable data and transactions. But don't settle for just any authentication token. Invest in RSA SecurID technology — a proven authentication solution that will protect your digital assets and deliver consistent returns on your investment, year after year.

About RSA Security

RSA Security, The Most Trusted Name in e-Security,[™] helps organizations build secure, trusted foundations for e-business through its RSA SecurID two-factor authentication, RSA ClearTrust[®] authorization, RSA BSAFE[®] encryption and RSA Keon[®] digital certificate management product families. With approximately one billion RSA BSAFE-enabled applications in use worldwide, more than ten million RSA SecurID authentication users and almost 20 years of industry experience, RSA Security has the proven leadership and innovative technology to address the changing security needs of e-business and bring trust to the online economy. RSA Security can be reached at www.rsasecurity.com.



RSA Security Inc.
20 Crosby Drive
Bedford, MA 01730 USA
Tel (US) 1 877 RSA 4900, +1 781 301 5000
Fax +1 781 301 5170

www.rsasecurity.com

RSA Security Ireland Limited
Bay 127, Shannon Free Zone
Shannon, County Clare, Ireland
Tel +353 61 72 5100
Fax +353 61 72 5110

www.rsasecurity.ie

©2001 RSA Security Inc. All rights reserved.

ACE/Server, BSAFE, ClearTrust, Keon, SecurID, RSA and RSA Security are registered trademarks and *The Most Trusted Name in e-Security* is a trademark of RSA Security Inc. All other trademarks are the property of their respective owners.