

# *Strong Authentication Technologies*

**A Primer**

**A WHITE PAPER  
BY ACCUDATA SYSTEMS**

By  
Jamie Bjerke, CISSP  
Steve Helms, CISSP

February 2003



13700 Veterans Memorial ♦ 281.440.7220 ♦ [www.accusys.com](http://www.accusys.com)

HOUSTON ♦ AUSTIN ♦ DALLAS

This page intentionally left blank.

## Table of Contents

<b>EXECUTIVE SUMMARY</b> .....	<b>5</b>
<b>ONE-TIME PASSWORDS</b> .....	<b>6</b>
<b>Asynchronous Example: S/KEY</b> .....	<b>6</b>
<b>Synchronous Example: RSA ACE/Server</b> .....	<b>7</b>
<b>The ACE/Server</b> .....	<b>7</b>
<b>The SecurID</b> .....	<b>7</b>
<b>DIGITAL SIGNATURES</b> .....	<b>8</b>
<b>Public-Key Cryptography System</b> .....	<b>8</b>
<b>Storing Digital Certificates</b> .....	<b>9</b>
<b>Common Uses</b> .....	<b>9</b>
<b>BIOMETRIC IDENTIFICATION</b> .....	<b>10</b>
<b>Only Three Unique Identifiers</b> .....	<b>10</b>
<b>Biometrics Challenges</b> .....	<b>10</b>
<b>Common Uses</b> .....	<b>11</b>
<b>RSA SECURID – OVERVIEW</b> .....	<b>12</b>
<b>How it works</b> .....	<b>12</b>
<b>Strengths</b> .....	<b>12</b>
<b>Possible Weaknesses</b> .....	<b>12</b>
<b>Ideal Situations</b> .....	<b>12</b>
<b>DIGITAL CERTIFICATES ON HARDWARE DEVICES</b> .....	<b>13</b>
<b>How it works</b> .....	<b>13</b>
<b>Strengths</b> .....	<b>13</b>
<b>Possible Weaknesses</b> .....	<b>13</b>
<b>Ideal Situations</b> .....	<b>13</b>
<b>DIGITAL CERTIFICATES ON PC</b> .....	<b>14</b>
<b>How it works</b> .....	<b>14</b>
<b>Strengths</b> .....	<b>14</b>
<b>Possible Weaknesses</b> .....	<b>14</b>
<b>Ideal Situations</b> .....	<b>14</b>
<b>BIOMETRICS – OVERVIEW CHART</b> .....	<b>15</b>
<b>How it works</b> .....	<b>15</b>
<b>Strengths</b> .....	<b>15</b>
<b>Possible Weaknesses</b> .....	<b>15</b>
<b>Ideal Situations</b> .....	<b>15</b>
<b>ABOUT THE AUTHORS</b> .....	<b>16</b>
<b>ABOUT ACCUDATA SYSTEMS</b> .....	<b>17</b>
<b>REFERENCES</b> .....	<b>18</b>

This page intentionally left blank.

“The concept of strong authentication encompasses the technologies, tools, and processes employed to securely authenticate users.”

## EXECUTIVE SUMMARY

**S**trong authentication, more commonly referred to as two-factor or multi-factor authentication, is a newly coined term in the IT security industry. The concept of strong authentication encompasses the technologies, tools, and processes employed to securely authenticate users. Strong authentication is generally accomplished in one of three ways:

One-time passwords

- Digital signatures
- Biometrics

These three technologies implement strong authentication by using something a user knows or something a user has or is.

The **something a user knows** component of strong authentication is often:

- A password
- A PIN number

The **something a user has or is** component of strong authentication is often a token such as:

- A smartcard or software package
- A digital signature

A digital signature is an electronic file stored on a computer or smartcard. When it is unlocked, via a password, it can be used as an electronic signature to uniquely identify a user. Biometrics are unique physical characteristics, such as a thumb print, iris or palm print, and are used to provide even stronger authentication because of their ability to identify individuals.

Where these three technologies are used to successfully authenticate users, the authentication system becomes considerably stronger than password only systems. Potential hackers need not only to know the password or PIN, but also to possess the token, digital certificate or physical characteristic of a user in order to penetrate the network.

This white paper focuses on defining these three technologies and discussing their common uses in the implementation of strong authentication systems.

“One-time password systems have found common usage in dial-in remote access, VPNs, and the remote management of sensitive systems or networks.”

## ONE-TIME PASSWORDS

A one-time password is just that, a password that is valid only one time for authenticating a user to a system. Technically, a one-time password system could be derived from a simple static password system by placing provisions on the system where, after authenticating each time, a user's account is disabled until a new password is configured.

Conceptually, this system works, but two major hurdles stand in the way of implementing it. First, many authentication systems do not offer the option of automatically disabling a user account upon authentication. Second, this model is not practical in the real world because users have to arrange to change their passwords each time they use them before authenticating again. Thankfully, specialized software packages have been developed to provide one-time passwords.

These packages offer various forms of one-time passwords. They are generally based on one of two concepts:

- Asynchronous or challenge-response mechanisms, such as S/KEY
- Synchronous or time-based systems, such as RSA's ACE/Server using SecurID.

### Asynchronous Example: S/KEY

S/KEY, one of the strong authentication pioneers, was developed at Bellcore, Bell's communications research arm, currently Telcordia. S/KEY relies on a secret password that both the user and authentication server know. This secret password is run through a message digest, or one-way hash function (by default MD4),  $n$  times, and the output is stored on the server.

When a user attempts to authenticate, the server sends a challenge which is  $n-1$ . The S/KEY client on the user's side prompts for the secret password and applies the hash function  $n-1$  times. The result is sent back to the server, which runs the hash on its corresponding secret password for the user and compares the result to the response sent from the user. If these match, the user is authenticated. The S/KEY system is quite clever in that the user's one-time password is never sent over the network; only the one-way hash function for the  $n-1$  iteration is sent.

Although one of the strong authentication pioneers, S/KEY has a few limitations worth mentioning.

- First, the system uses MD4 for the hash function, and weaknesses have been found with it. A stronger hash function would be SHA-1.
- Second, the  $n-1$  characteristic of S/KEY can also be a limiting factor. Once  $n-1$  reaches zero, the S/KEY system for that particular user must be reset with a new secret password. Since the secret password should never be sent over the network, this has to be set up manually on both the user and S/KEY server.
- Third, the challenge-response nature of S/KEY requires a client-side application to create the hash iterations, adding to the complexity of the system from a user perspective. Nonetheless, S/KEY has proved its value over the years and continues to be a viable strong authentication option.

## **Synchronous Example: RSA ACE/Server**

RSA's ACE/Server is one of the leading strong authentication products. The ACE product was originally developed by Security Dynamics and has since been purchased by RSA Security. This product comprises two primary components: the ACE/Server and the SecurID.

### **The ACE/Server**

The ACE/Server is the server-side component of this authentication product, containing the user accounts database as well as logging and reporting functions. The ACE/Server is the mechanism that decides if an authentication attempt is approved or disapproved.

### **The SecurID**

The SecurID hardware or software token is the client-side component that provides users with a one-time password, also known as a token-code.

Both the client-side and server-side components rely upon time, thus keeping the server clock accurate is key to success. By default, each client-side token-code is valid for sixty seconds and one authentication per sixty-second window. Thus, both the ACE/Server and the SecurID token must be time-synchronized. This is accomplished by synchronizing the ACE/Server with a time server. The SecurID hardware token has a built-in clock and is guaranteed for three to five years, depending on the token purchased. Each token-code is composed of a random six-digit number. When matched with the user's PIN, this combination is considered the one-time password or passcode.

This system is called synchronous because, unlike S/KEY, it does not require a challenge-response. The user simply enters his username and four- to eight-digit PIN, plus the one-time token code showing on the SecurID token, and sends the request to the ACE/Server. The ACE/Server then validates this username/PIN/plus token-code and either permits or denies the authentication attempt.

The ACE/Server system tends to be easier to use than others, requiring less administrative overhead for the server-side. To date, this system has not been cracked! It has been hailed as one of the more secure strong authentication systems in use today. However, it is worth mentioning that this system requires either a hardware or software token or device on the client-side to work properly, which does add to the complexity of the system.

One-time password systems have found common usage in dial-in remote access, VPNs, and the remote management of sensitive systems or networks. Several security vendors offer integration with one-time passwords, including Cisco, Check Point, Symantec, and NAI. This is a proven technology that should remain viable in the foreseeable future.

“The use of Digital Signatures for strong authentication is gaining headway.”

## DIGITAL SIGNATURES

Conceptually, many people think of a digital signature as the scanned, digital equivalent of a standard handwritten signature. But it is not. Technically, it is much different. In fact, a digital signature is so complex that it cannot be discussed without first describing the components which are used to develop it.

RSA Security®, a global e-security leader, defines a digital signature as "the encryption of a message digest with a private key." We have already described a message digest which is a one-way hash function. A private key is the private component of a private-public key pair used in a system called public-key cryptography.

### Public-Key Cryptography System

When using a public-key cryptography system, each user has two keys – a public and a private – composed of a string of bits usually found in a file or stored on a smartcard.

- **The public key** is made public so that others can encrypt messages to the user and verify the user's identity when receiving a digital signature.
- **The private key** is kept safe and private and is used for decryption and digital signatures. The private key can be unlocked or made useable only with the user's secret password. The private key is never communicated over a network when decrypting or signing (authenticating).
- **A trusted third party**, known as a certificate authority or CA, issues and signs a digital certificate for each user, as well as verifies validity of digital certificates.

The process for authenticating using digital signatures is as follows:

1. The user's private key is unlocked with the secret password.
2. The user's digital certificate is run through a one-way hash
3. The resulting value is attached to the digital certificate, which is digitally signed using the private key.
4. The signed and hashed digital certificate, which represents the user's digital signature, is sent to the authenticating server or recipient.
5. The digital signature is verified with the user's public key.
6. The digital certificate is run through the hash and verified against the original hash sent by the user.
7. Finally, the user's digital certificate is validated with the CA and the user is successfully authenticated.

As you can see this is quite complicated. Fortunately, much of the complexity is handled by software and is transparent to the user. Further, many applications, such as VPN clients and web browsers, as well as many operating systems have implemented public-key cryptography within their software. Generally, the difficult part of implementing the use of digital signatures is setting up the PKI and CA infrastructure to support digital certificates and signatures.

## **Storing Digital Certificates**

Storing digital certificates in software (usually on a user's workstation) is considerably less secure than storing certificates on hardware devices such as smartcards. This is because a certificate on a networked workstation can be hacked and copied if the workstation is compromised. A certificate on a smartcard, on the other hand, is taken with the user and never stored on the workstation.

## **Common Uses**

Common uses for digital signatures include VPNs, email verification, and document signing. While the use of digital signatures is not as prevalent as the use of one-time passwords for strong authentication, they are gaining headway as major security software and operating system vendors, including Check Point and Microsoft, build PKI and public-key cryptography technologies into their products.

“Since biometric identification provides a very high degree of individual uniqueness, biometrics are generally considered strong authentication.”

## BIOMETRIC IDENTIFICATION

**B** iometric identification is the process of proving your identity via a physical measurement, such as fingerprint, facial recognition, iris scan, voice recognition, or other, in order to provide verification and identification services.

Biometrics alone generally are not considered to be two-factor authentication mechanisms. However, many biometric systems do provide the ability to require PINs or passwords in addition to physical characteristics as credentials for authentication.

Since biometric identification provides a very high degree of individual uniqueness (i.e. fingerprints are considered nearly 100% unique) with or without a PIN, they are generally considered strong authentication. Historically, biometric identification has been used for physical security. But in recent years, several vendors have started to implement biometric solutions for authentication to systems.

### Only Three Unique Identifiers

Of the many physical characteristics that are options for biometrics, only three are considered completely unique:

- Fingerprinting/finger images
- Iris scanning
- Retinal scanning

These identifiers provide the highest level of assurance in verification and identification of individuals. Hence, many manufacturers have focused development efforts around them.

Each of these options requires two devices to function– a biometric reader and an authentication server:

- **A biometric reader** is the input device responsible for scanning the user's biometric identifier (thumbprint, iris, etc.) and passing the results onto the server.
- **The authentication server** contains a user database with previously scanned or enrolled biometric data. The identification data is sent to the server and compared to that which is in the database to determine if the authentication attempt will be permitted or denied.

### Biometrics Challenges

Biometric systems tend to be less complex than other systems from a user perspective, but also present some unique and difficult hurdles.

First, biometrics requires the gathering and recording of individual human characteristics. Some individuals believe this is personal information. Some also may believe scanning devices can be hazardous to their health.

Second, discrepancies between the initial enrollment scan and subsequent reader scans can be an issue.


Unequal sensitivity levels and dirty or soiled readers, especially in the case of hand or thumbprint readers, often cause these discrepancies which in turn cause systems to incorrectly permit or deny access.

Sensitivity level settings can also be an issue when using biometric identification systems. If the system is set to too high a sensitivity level, false negatives will result, wrongly denying a user's authentication attempts. Conversely, setting the system sensitivity too low can result in false positives, which could allow an imposter to authenticate on another user's behalf. Neither condition is good. The goal in configuring sensitivity levels is to reach the crossover error rate (CER), the rate at which false negatives and false positives are equal. CER is often difficult to maintain given the ever-changing climate in many locations and reader-device cleanliness conditions.


### **Common Uses**

Biometric identification has yet to find many common uses outside of physical security measures. Advances continue to be made nonetheless in the area of system level biometric authentication. Several promising products from companies like Targus and SecuGen are on the market, trying to break into the strong authentication segment of the IT industry.


# RSA SecurID – OVERVIEW

Technology	How it works	Strengths	Possible Weaknesses	Ideal Situations
<p>One-time passwords (RSA SecurID)</p> 	<ul style="list-style-type: none"> <li>A random 6 digit code is displayed every 60 seconds.</li> <li>When logging in to a system (web server, VPN, etc) the user is required to enter a personal PIN and the 6 digits displayed to form a valid passcode.</li> <li>The authentication server verifies the passcode and access is either allowed or denied to the system.</li> </ul>	<ul style="list-style-type: none"> <li>The passcode cannot be used more than once.</li> <li>The physical token cannot be cloned and each has a unique serial number.</li> <li>Tokens require no other device to operate.</li> <li>Tokens can be easily disabled if lost or stolen.</li> <li>Users are not constrained to using only a single PC.</li> <li>Wide support for SecurID across multiple applications and security systems (firewalls, VPN, web servers, operating systems).</li> <li>Can be used in a hardware form (key fob, credit card) or software (PC, mobile phone, PDA).</li> <li>Nothing is left on a system once the user leaves. This is ideal for public systems or stations used by multiple individuals.</li> <li>Platform independent</li> <li>Key fobs fit easily on a key ring.</li> <li>Very mature technology</li> </ul>	<ul style="list-style-type: none"> <li>Authentication to every SecurID protected device is required.</li> <li>Token code may only be used once so users may have to wait till token code changes.</li> <li>Only good for authentication and not document signing.</li> <li>Must be replaced with the battery fails. (1-5 years depending on token).</li> <li>A token (hardware or software) is required for every user accessing a SecurID protected system.</li> <li>Users may potentially lose or forget tokens.</li> </ul>	<ul style="list-style-type: none"> <li>Mobile users that may use common access PCs, Internet café's, since no special hardware or software is required on the PC.</li> <li>Corporate RAS and VPN security.</li> <li>Intranet and extranet applications delivered via the web or a thin client (i.e. Citrix, etc).</li> </ul>



## DIGITAL CERTIFICATES ON HARDWARE DEVICES

Technology	How it works	Strengths	Possible Weaknesses	Ideal Situations
<p><b>Digital Certificates</b> (stored on hardware device)</p> 	<ul style="list-style-type: none"> <li>• Certificates are a public key and private key encryption.</li> <li>• The user's private key is stored on a smartcard or a USB token.</li> <li>• Users must place the smartcard in a reader or the USB token into a USB port in order to login to the system.</li> <li>• The user is prompted to enter a secret PIN to unlock the private key on the hardware device.</li> <li>• Data to be read by the user is encrypted with the user's public key so the private key can decrypt it.</li> <li>• The private key is used to encrypt data that is digitally signed by the user.</li> <li>• The USB token or smartcard is left plugged in for the duration of the session.</li> <li>• Once removed, the user is logged out or the computer is locked until the device and PIN are reentered.</li> </ul>	<ul style="list-style-type: none"> <li>• It is a unique physical device that cannot be cloned.</li> <li>• The certificate can be easily revoked if the device is lost.</li> <li>• The PIN locks the private key providing non-repudiation.</li> <li>• Can be used to enable reduced sign-on for multiple applications.</li> <li>• Often used to encrypt data as well as authenticate users.</li> <li>• Workstations are locked when the device is removed.</li> <li>• USB tokens require no special reader to be installed.</li> <li>• USB Tokens fit easily on key rings.</li> <li>• Smart cards are credit card sized so can be carried in a wallet or purse.</li> </ul>	<ul style="list-style-type: none"> <li>• Smartcards must be used with a compatible reader and operating system.</li> <li>• USB tokens require special drivers and operating system support.</li> <li>• Due to operating system hardware requirements and drivers, the devices are not as portable as some solutions.</li> <li>• Difficult to support external users where the companies IT department has no control over the remote PCs and operating system.</li> <li>• Smartcard format may be cost prohibitive unless used in conjunction with building access or photo IDs.</li> <li>• There are notable costs to support end users.</li> <li>• Logistics of deploying these devices must be carefully planned.</li> </ul>	<ul style="list-style-type: none"> <li>• Corporate networks where IT staff have full control over desktop systems and can configure them properly.</li> <li>• Remote VPN access for internal users.</li> <li>• Use of smartcards as building entry, photo ID, and network access.</li> <li>• Reduced sign-on to corporate applications or web-based applications.</li> </ul>

## DIGITAL CERTIFICATES ON PC

Technology	How it works	Strengths	Possible Weaknesses	Ideal Situations
<p><b>Digital Certificates</b> (stored on PC)</p> 	<ul style="list-style-type: none"> <li>The same as other digital certificates except the certificate is stored on the hard drive of a PC.</li> </ul>	<ul style="list-style-type: none"> <li>Less expensive than smartcards and USB tokens.</li> <li>No extra hardware requirements.</li> <li>Compatible with most operating systems.</li> <li>Typically there is no additional software to install.</li> <li>Deployment can be simplified and streamlined.</li> </ul>	<ul style="list-style-type: none"> <li>The private key is stored on a PC hard drive and is easy to duplicate and distribute.</li> <li>The PIN used to protect the key is a weak password and can be attacked by password cracking programs.</li> <li>There is limited mobility for users since the certificate is tied to a specific PC.</li> <li>Accountability of users is weakened due to the fact the private key can be used in multiple locations/PCs.</li> <li>The non-repudiation of the digital credentials is much weaker than other alternatives.</li> </ul>	<ul style="list-style-type: none"> <li>Intranet/Extranet deployments where the security requirements are not very high.</li> <li>Low risk applications such as e-commerce or other medium security online transactions.</li> </ul>

## BIOMETRICS – OVERVIEW CHART

Technology	How it works	Strengths	Possible Weaknesses	Ideal Situations
<p><b>Biometrics</b></p>  	<ul style="list-style-type: none"> <li>• Users identify themselves with a physical characteristic such as a fingerprint, retinal scan, voiceprint, or other personal characteristic.</li> <li>• Special hardware readers are required.</li> <li>• When users log in, the information collected by the reader is compared to data stored on an authentication server. If there is a match the user is authenticated.</li> </ul>	<ul style="list-style-type: none"> <li>• The non-repudiation of biometrics is very high since users each of unique traits.</li> <li>• It is highly portable and goes everywhere with the user.</li> <li>• Training is simple.</li> <li>• Some systems can both identify and authenticate users in one operation.</li> </ul>	<ul style="list-style-type: none"> <li>• Special hardware readers are required and may prevent user mobility.</li> <li>• Enrollment process to collect the initial biometrics can be time consuming.</li> <li>• Reliability and accuracy of different biometric systems have slowed the growth of this type of authentication.</li> <li>• Users may not be comfortable giving personal information for computer access.</li> <li>• Since biometrics are not one-time, there is a potential for replay attacks.</li> <li>• It is not possible to disable the credential of the user if there is a compromise other than removing the information from the authentication server.</li> <li>• The cost of reliable readers.</li> </ul>	<ul style="list-style-type: none"> <li>• Reduced/simplified sign-on to corporate LANs.</li> <li>• Areas where non-repudiation of information is critical such as financial, medical, government, and military environments.</li> </ul>

## ABOUT THE AUTHORS

**Jamie Bjerke** is a Senior Technology Consultant at Accudata Systems, Inc. (ASI), located in Houston, TX. Jamie's focus is delivering security services to ASI clients. Prior to joining ASI, Jamie worked as a security engineer at GTE Internetworking/BBN Technologies where he served as the technical lead in security assessments, network/security design, firewall/VPN/IDS engineering and implementation for the \$4 billion NASA contract called CSOC. Jamie worked extensively with complex Internet connection design and implementation aspects of the contract.

Jamie's earlier security work included technical team leader for Exxon's External Connections team of security engineers. This team was responsible for global external connection standards and practices concerning third party network connections to Exxon, including internet connectivity. While at Exxon, Jamie also served as a technical team lead for Exxon's global remote access infrastructure, as well as an engineer in the global data networking group.

**Steve Helms** is a Senior Security Engineer at Accudata Systems, Inc. (ASI) located in Houston, TX. Steve's focus is delivering security services to ASI clients. Prior to joining ASI, Steve worked as a senior security consultant for ThruPoint, Inc.

Steve has deployed many Check Point firewalls; performed security assessments using various commercial and public domain tools, designed carrier class networks, tested various networking products in labs for usability, features, and performance; and designed and implemented secure infrastructures for a wide range of clients.

## ABOUT ACCUDATA SYSTEMS

**A**ccudata Systems, Inc. is a professional IT consulting and system integration firm that provides strategic, tactical and operational services and solutions to Fortune 1000, middle market, and emerging companies. Accudata Systems has been building integrated networks for more than two decades, helping clients create a computing environment that maximizes their investment in Information Technology. Founded in 1982, Accudata Systems has grown over the past twenty years until today it offers a full range of IT services and solutions throughout Texas and the southwest.

We offer:

- Strategic consulting, project design and implementation, and support services
- Best-of-breed integrated solutions through strategic partnerships with industry leading hardware and software manufacturers
- Staffed with unmatched technical know-how

### A History of Client Satisfaction

While many companies claim their goal is a mutually beneficial partnering relationship with their customers, Accudata Systems' long-term client relationships prove it. Many of our customers have been with us for more than 15 years.

- Seven of the top ten largest Houston companies are clients.
- We work in a broad array of industries including energy, manufacturing, telecommunications, health care, engineering and construction, government, as well as financial, legal and other professional services.
- We have an unwavering commitment to client satisfaction at all levels.
- Strong relationships with premier industry partners enhance our service and support capabilities.
- Our regional geographic focus ensures the necessary resources to support our clients.

### A Reputation for Quality

From strategic planning to incident support, Accudata Systems has been providing a comprehensive array of IT solutions for more than twenty years and has established a reputation for service quality. Our goal is to continue to provide our clients with the solutions they need to maximize the value of their IT infrastructure.

- Strategic Planning
- IT Governance and Process Improvement
- Technology Assessments
- Security Management Consulting
- Full Lifecycle Project Planning and Implementation
- Infrastructure Upgrades and Platform Migrations
- Rapid Technology Deployment
- Technology Procurement
- Licensing Subscription and Renewal Management
- 24 X 7 Support

## REFERENCES

- EECSNet S/KEY  
[http://www.ece.northwestern.edu/CSEL/skey/skey\\_eecs.html](http://www.ece.northwestern.edu/CSEL/skey/skey_eecs.html)
- FreeBSD Handbook [http://www.freebsd.org/doc/en\\_US.ISO88591/books/handbook/skey.html](http://www.freebsd.org/doc/en_US.ISO88591/books/handbook/skey.html)
- RSA Security FAQ  
<http://www.rsasecurity.com/rsalabs/faq/index.html>
- Entrust Whitepapers  
<http://www.entrust.com/resources/whitepapers.htm>



Accudata Systems, Inc.  
13700 Veterans Memorial, Suite 280  
Houston, TX 77014  
281.440.7220 800.246.4908  
[www.accudatasystems.com](http://www.accudatasystems.com)