



**INTERNET SECURITY BLANKET**  
A SECURITY SOLUTIONS COMPANY

**ACUTRUST™ TECHNOLOGY**  
**WHITE PAPER**  
**MAY 2005**  
VERSION 2.0

**INSIDE**

- q OVERVIEW
- q USER EXPERIENCE
- q TECHNOLOGY

## Contents

Executive Summary .....	3
Overview.....	4
User Experience .....	6
User Participation .....	6
User Requirements .....	7
Service Provider Login.....	7
Technology .....	10
Token Generation .....	10
Data To Be Encoded.....	11
Token Display .....	11
Active User Name Identification.....	12
Passive User name Identification .....	12
Visual Element Construction.....	13
Conclusion .....	14
Company Information .....	15

## EXECUTIVE SUMMARY

In the physical world, you wouldn't hand over personal and financial information to strangers without proper verification. But in the virtual world, identities are hard to verify. How do you really know the Website you are logging into is really your service provider's Website?

The problem is the traditional one-way authentication username/password method. Knowing someone's username and password is enough information to access someone's account online. Phishing is a scam that tricks people into giving out personal information. Once the information is obtained, it is used for Identity Theft and unauthorized account access.

The solution is ACUTrust's™ authenticity technology. It combines username and password with an encrypted token. The encrypted token lets customers visually confirm the authenticity of a communication, Web Service, Website, Email, etc.

## OVERVIEW

The Internet era has opened up a new sales and services channel to all businesses. More than ever, companies are opening virtual doors to the Internet, and are allowing more online business transactions. Personal, financial, and confidential information is exchanged via the Internet at an increasing rate.

Unfortunately, scam artists are also looking to profit from the Internet. The Federal Trade Commission (FTC), "Consumer Sentinel ([www.consumer.gov/sentinel/](http://www.consumer.gov/sentinel/))" indicates that 39% of the fraud complaints filed were Identity Theft claims. Phishing, the latest online scam today, uses forged emails and fraudulent Websites to trick people into disclosing personal and financial information such as credit card numbers, social security numbers, bank account numbers, passwords, etc. Once this information is obtained, the fraudsters can use it to conduct illicit financial transactions.

The primary issue with online transactions is that you don't really know who you are dealing with over the Internet. In the traditional brick and mortar world, it is easy to know who you are dealing with. There is a physical building that you can see and people you can interact with face-to-face. On the Internet it is not so easy. Just about anyone with the right tools can create fraudulent Websites that look just like the real ones. How do you really know where you are on the Internet? Who can you trust on the Internet?

The root of the problem is the traditional one-way authentication username/password method. After entering the correct username/password, the Website verifies the users' identity but a customer has no way of knowing the identity of the Website. Many online scams use fraudulent Websites that look like the genuine

Website. The Websites are generally online an average of six days. When unsuspecting users login to the fraudulent Websites, the scam artists immediately capture the users' username and password. The login information is then used to gain access to legitimate online accounts.

The solution is ACUTrust's™ two-way authenticity technology. ACUTrust™ builds on the username/password method that users are familiar with and adds a token confirmation for the users to verify the identity of the Website. Customers are assured of the authenticity of a communication, Web Service, Website, etc.

## USER EXPERIENCE

The user experience is critical to the success of any business entity. When a service provider's user community does not feel safe, there are many negative effects for both the service provider and the user community.

By implementing ACUTrust™, the service provider shows that it recognizes the importance of data privacy and positive identification. ACUTrust™ is a simple to implement authenticity technology that allows a user to determine if they are accessing or interacting with their true service provider.

## USER PARTICIPATION

In the case of ACUTrust™, the user and the service provider must determine the identification information they plan to use. Many service providers collected identification information from their users during account setup. In fact, many service providers are already using some of this unique information (mother's maiden name, personal identification numbers, birth date, account number, and social security number, etc.) for user verification.

## USER REQUIREMENTS

Implementing ACUTrust™ requires little participation from the user. It does not require hardware or software beyond a preferred interface, making it an ideal solution for the service provider.

## SERVICE PROVIDER LOGIN

Any business that allows access to users' private information is required by law to protect that non-public private information.

The Website example below illustrates one of the many uses for ACUTrust™. Prior to implementing ACUTrust™ in a Web environment, the user will receive the service provider's existing login page.

Once ACUTrust™ is implemented, the user will receive an interface similar to Figure 1 asking only for the user's ID.

Figure 1



Please Enter  
User Name:

Pressing the submit button will verify the user, then invoke a database call to retrieve information to be included in the encryption token. The encrypted token is then displayed as shown in Figure 2, asking for the user's password/pass-phrase and containing an encrypted token.

Figure 2



The screenshot shows a blue rectangular form. At the top left, it says "Please Enter". To the right of this text is a rectangular area filled with a random pattern of black, white, and red pixels (a captcha). Below the captcha, the text "Passphrase:" is followed by a white rectangular input field that is currently empty. At the bottom right of the form is a grey button with the word "Submit" written on it.

As the user enters a password/pass-phrase, the encrypting token starts decrypting in real time. As seen in Figure 3, the user will notice animation of the encrypted token right before their eyes.

Figure 3



The screenshot shows the same blue rectangular form as in Figure 2. The "Please Enter" text and the captcha image are still present. The "Passphrase:" text is followed by a white rectangular input field that now contains seven asterisks ("\*\*\*\*\*"). The "Submit" button remains at the bottom right.

Providing the correct password/pass-phrase established by the service provider and the user will decrypt the encrypted token as seen in Figure 4. An incorrect password/pass-phrase will animate the encrypted token, but it will not correctly decrypt the non-public private information.

Figure 4



Finally, once the Website has been identified, the user can enter their password and submit it for system access as seen in Figure 5.

Figure 5



## TECHNOLOGY

ACUTrust™ leverages an encrypted token-based system to allow the authenticity of an electronic communication to be verified. ACUTrust™ presents the token to the user in a format that is easy to interpret (i.e. visual display, sound).

ACUTrust™ is comprised of two separate parts: the token generation and the token display process. The identification of the user is determined through an active or passive method. Next, the token generation process is used to create the encrypted token used by the token display process.

## TOKEN GENERATION

The first step of the token generation process uses the identification of the user to query a data repository. The repository contains the information used to create the unique security token, and the encryption key for the security token.

The information from the data repository is then passed to a security token generator. The token generator combines this user data with other data acquired by the system. The combined data helps the user determine the authenticity of the token, and prevents a third party from intercepting and relaying the token without the user's knowledge. Once all the data is gathered, it is converted into a token specific and appropriate to the communication medium and encrypted using appropriately strong encryption techniques. The token is then packaged with the necessary token display code and formatted for delivery. The

complete package and formatted token is then delivered to the user.

When ACUTrust™ is used to protect HTML documents, one way the security token can be delivered to users is in the form of a client-side scripting variable. The variable is of arbitrary length, and represents the encrypted data that is to be presented to the user.

### DATA TO BE ENCODED

The information to be encoded into the token is arbitrary, but should be specific, unique and identifying information to the user. Some examples of information that can be encoded are: a time stamp, a piece of user specific or identifying information, information that identifies the accessing machine, or any shared secret between the two parties.

### TOKEN DISPLAY

ACUTrust™ uses client-side processing to present the authenticity token to the user in a format that is easy for them to recognize, but difficult for a machine to perform data interpretation. The token could be displayed in any audio, visual, etc. format that the user has specified.

## ACTIVE USER NAME IDENTIFICATION

In order to implement ACUTrust™ for environments that are required to verify the authenticity of a Website, or other environments that require an active login process, it requires that the user login process be separated into two separate steps.

The separation of the steps allows the site to pull the user specific information from a repository that will be encoded and encrypted into the ACUTrust™ authenticity token. The separation also allows the encryption key to be determined that is used to encrypt the token. Once the encrypted token is generated, it is incorporated into the password/pass-phrase authentication step.

During the Active login phase, as the password/pass-phrase is typed, real time decoding of the token takes place. If the incomplete or incorrect password/pass-phrase is entered into the system, the token is displayed to the user in some unrecognizable form. Once the correct password/pass-phrase is entered, the token is correctly displayed revealing the identifying information to the user. The identifying information may be modulated in different ways as to make the data recognizable to a person, but difficult for a machine to recognize.

## PASSIVE USER NAME IDENTIFICATION

When ACUTrust™ is used to authenticate one-way communications such as email, instant messages, Web Services, or other electronic document sending mechanism, only the password/pass-phrase step of authentication is needed. The user's name can be presumed and the token can be generated for the specific user credentials of the user.

## VISUAL ELEMENT CONSTRUCTION

A method that can be employed to visually display the security token to a user is to use JavaScript, VBScript, JAVA Applet, or any other client-side active processing.

## CONCLUSION

With Internet related crime on the rise, the users' confidential data is at risk. Service providers can either choose to ignore the threat or implement technology to curb the threat. Legal action taken by users against service providers confers a hint of what a blind eye would bring.

ACUTrust™ is a straightforward two-way authenticity technology that leverages existing infrastructure. It is simple to implement, and it allows a user to determine if they are accessing or interacting with their true service provider.

Many service providers have already collected the identifying information (mother's maiden name, PIN, birth date, etc.) they need to implement ACUTrust™. In fact, many service providers use this information today.

Implementing ACUTrust™ requires minimum change for the service provider or the user using secure Website services. However, the login process flow is slightly different. ACUTrust™ is a revolutionary authenticity technology that can restore users' confidence in their service provider's communication methods. The user community is clamoring for help, and service providers can provide help with minimum effort using ACUTrust™ Technology.

## COMPANY INFORMATION

Internet Security Blanket Corporation (ISBlanket<sup>SM</sup>) was founded in 2001 and is a premier provider of security solutions. Our experience ranges from small companies with less than 50 people to Fortune 500 companies with 100,000+ employees.

ISBlanket's<sup>SM</sup> sole focus is information and network security. Our engineers have over 20 years experience in helping customers with security solutions. In addition to our experience, our staff currently holds the following security certifications: CISSP, GCFW, and GSEC.

We believe that maintaining proper security is a continual process. We work closely with our customers to keep them up-to-date with latest security news and methodologies. We employ NSA (National Security Agency) methodologies in all of our security services. This ensures that our customers are receiving information/services that are consistent with industry standards.

ISBlanket's<sup>SM</sup> customer exposure includes companies in the financial, insurance, government, manufacturing, and educational sectors. Also, for more information about ISBlanket<sup>SM</sup>, please visit our Website at <http://www.isblanket.com>.

The information in this document is subject to change without notice and must not be construed as a commitment on the part of Internet Security Blanket Corporation (ISBlanket<sup>SM</sup>). ISBlanket<sup>SM</sup> assumes no responsibility for any errors that may appear in this document. ISBlanket<sup>SM</sup>, ACUTrust™ and the ISBlanket<sup>SM</sup>, ACUTrust™ logo are U.S. registered trademarks, trademarks, or servicemarks of ISBlanket<sup>SM</sup>. Other brands and products are trademarks of their respective holders. Copyright 2005 ISBlanket<sup>SM</sup>. All rights reserved.

Internet Security Blanket Corporation  
Post Office Box 390841  
Snellville, Georgia 30047  
Phone: (888) 264-3110  
Email: [sales@isblanket.com](mailto:sales@isblanket.com)  
Web: [www.isblanket.com](http://www.isblanket.com)