

Authernative Granted U.S. Patent on Key Conversion Method for Communication Session Encryption and Authentication System

REDWOOD CITY, Calif. – Nov. 26 (SEND2PRESS NEWSWIRE) – Authernative, Inc., the developer of innovative user authentication and identity management technologies, announced today that the United States Patent & Trademark Office has granted the company its patent for a key conversion method.



Send2Press Newswire

The newly issued patent number US 7,299,356 titled “Key conversion method for communication session encryption and authentication system” describes a new encryption key management system integrated into an interactive mutual authentication protocol that accomplishes mutual authentication through a secure exchange of session-only random symmetric encryption keys without allowing authentication credentials to cross non-trusted communication media.

Security of key distribution is enabled with a new Key Conversion Array (KCA(TM)) technology. It embraces sequential random number generators seeded with authentication credentials and arrays of veiling random bits and/or bytes. Furthermore, these veiling bits and/or bytes are replaced at certain session-only random positions in KCA with disassembled symmetric key’s bits and/or bytes. Key scrambling process of replacing veiling bits and/or bytes inside KCA with the actual key’s bits and/or bytes is reversed at the receiving end with a reciprocal key reengineering process according to one of patented Bit-Veil-Unveil (BitVU(TM)), Byte-Veil-Unveil (ByteVU(TM)), and Bit-Byte-Veil-Unveil (BBVU(TM)) algorithms.

The patented technology provides secure mutual authentication and session-only random symmetric key distribution in client-server architecture, which eliminates asymmetric key usage and overcomes certain weaknesses and difficulties in implementation, administration, maintenance, and cost containment of public key infrastructure (PKI), Kerberos, and some other commercially available authentication and key distribution systems and protocols. Key Conversion Array technology allows for security scalable with CPU power and network bandwidth, while KCA is highly resilient against communication session eavesdropping attacks, replay man-in-the-middle attacks, online and offline computer-processing attacks, and session hijacking/phishing attacks.

KCA(TM) technology extends the end-to-end security capabilities of Authernative(R) AuthGuard(R) user authentication solution. AuthGuard(R) performs strong user authentication and client-server mutual authentication during the authentication stage of the communication session. The secure session-only symmetric random encryption key distribution having occurred during this stage can protect secure content delivery between client and server during the post-authentication stage of the same communication session.

The rise and sophistication of online attacks, tools and strategies to steal authentication credentials and sensitive data are rapidly growing. According to the September 17, 2007, Internet Security Threat Report released by Symantec Corp, cyber criminals are increasingly becoming more professional – even commercial – in the development, distribution and use of malicious code and services. Authernative's Key Conversion Array technology gives end-users higher security and confidence when conducting Web-based transactions.

This patent issuance is a significant validation of the company's intellectual property and business strategy to protect user access and security of proprietary or sensitive data, which is essential to successfully conducting electronic business on a global basis. The company also currently holds more than 28 issued and pending US and foreign patents relating to the front- and back-end of authentication and encryption key management technologies.

Authernative has been expending the vision of AuthGuard(R) and the addition of the Key Conversion Array patented technology is a significant milestone, allowing for new product lines, including secure content delivery, single sign-on, and federated identity.

About Authernative:

Authernative provides innovative patented software security solutions offering identity and access management capabilities including authentication, authorization, administration, and auditing. The company's products are used to prevent unauthorized access to confidential data, protected resources, and financial transactions. They allow businesses to lower the cost of providing, deploying and managing user authentication for enabling e-commerce and addressing regulatory compliance requirements.

More information: www.authernative.com.

News issued by: Authernative, Inc.

The logo for Authernative, featuring the word "authernative" in a bold, blue, sans-serif font with a registered trademark symbol (®) to its upper right. Below the main text, the tagline "THE AUTHENTICATION ALTERNATIVE" is written in a smaller, blue, all-caps, sans-serif font. The entire logo is centered within a white rectangular area that has a thin black border.

authernative®
THE AUTHENTICATION ALTERNATIVE

Send2Press Newswire

Original Image: http://Send2Press.com/wire/images/07-1126-Autherntv_72dpi.jpg

#

Original Story ID: (3472) :: 2007-11-1126-003

Original Keywords: Authernative Inc, AuthGuard user authentication, Bit-Veil-Unveil, BitVU, KCA technology, Key Conversion Array technology, Bit-Byte-Veil-Unveil algorithms, BBVU, patent number US 7,299,356, Key conversion method for communication session encryption and authentication system Authernative, Inc.