SecurDigital©

SecurVoice© Privacy Edition
Banking & Financial Services

SecurVoice© Privacy Edition provides secure communications for Banking and Financial Services with an attractive new pricing model.

The Myth of Mobile Security

With the introduction of an iPhone app that lets you deposit a check by taking a picture of it, options for mobile banking are growing rapidly. And though you might think the boost in convenience comes at the expense of security, banking on your cell phone can actually be safer than using your PC if you take precautions.

Prior to **Secur**Voice©, you had three options for mobile banking: downloading a dedicated program for your cell phone, use your phone's browser to access a mobile version of your bank's site, or simply sending an SMS message.

The quality of downloadable apps vary, and downloadable apps and mobile sites both typically require logging in with the same user name and password you'd use on your PC. They also use simple encryption for communications to and from the bank. SMS messages are the least secure method of banking, as SMS doesn't normally allow for encryption. Well, times have changed and so has technology.

Safe Mobile Banking?

Using a PIN or a password to lock your phone is the first option, and it's a no-brainer--just knowing which bank you use can help a potential ID thief. Next are remote-wipe options that let you clear the contents of your phone if you should ever lose it. Some banks offer the feature for their downloadable apps. You can remote-wipe BlackBerrys and iPhones (if you pay for the MobileMe service), too, and some programs such as Kaspersky Mobile Security offer the feature for phones running Symbian OS or Windows Mobile. SMS messages are the least-secure option and possibly work if you notify your bank. Good recommendations; but not good enough.

Introducing **Secur**Voice© Privacy Edition

SecurDigital has upped the ante considerably here. In a sudden leap, this innovative new product has shaken off the complexity of unified communications and has taken the lead in terms of ease of use, security and interoperability. Starting with simple encryption techniques in a Java-based application, **Secur**Digital has introduced **Secur**Voice© Privacy Edition, a next-gen secure digital data transmission solution, which takes the focus away from hardware or firmware centric smart phone offerings and provides a Solution that is application platform, operating system, device and carrier independent.

SecurVoice© delivers encrypted voice, data or video transmission from any device to any device(s), with selectable encryption algorithms allowing any companies to literally "**Secur** their Communications".

SecurVoice© Product Overview

ONE-TOUCH SWITCHING BETWEEN PRIVACY AND STANDARD COMMUNICATIONS

WMS AND VOIP SECURE COMMUNICATION OPTION

INTUITIVE, USER-FRIENDLY INTERFACE

AVAILABLE TO PURCHASE AND DOWNLOAD ONLINE

SOFTWARE BASED SOLUTION – NOT HARDWARE

Technical Specifications

Encryption AES 128 bit
Private Key generation 128/128+ bit key
Voice Compression G723.1
Modems V.32, V.110
Compatible Networks GSM 850,900,1800 and 1900
Network Data Rate 9600 BPS, Asynchronous - Circuit Switched Data
Mobile Phones Supported Blackberry 8830, 96xx, Tour running OS version 4.5 and up
Mobile Phone Platforms in development Symbian, Brew, Window Mobile 6.5, iPhone, Google

Purchase Options

Single License (Hosted) starts at $19.95 a month Group and Corporate license (bundles)

Contact Information

Contact Sales at (203) 912-5532 or email sales@securdigital.com

Copyright 2009 **Secur**Digital, Inc. All Rights Reserved. (203) 912-5532. Email: sales@securdigital.com Online: www.securdigital.com
SecurVoice, the SecurVoice logo, and all other trademarks mentioned in this document are the property of their respective owners.

SecurDigital©

SecurVoice© Privacy Edition
Banking & Financial Services

SecurVoice© Encryption Process Overview

SecurVoice© Privacy Edition System has several modes of operation and utilizes AES encryption, the Advanced Encryption Standard.

What is Advanced Encryption Standard (AES)?

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) [PDF, 273K] on November 26, 2001 and is adopted as an encryption standard by the U.S. government.

The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plain text. AES is one of the most popular algorithms used in symmetric key cryptography.

Voice communication Modes

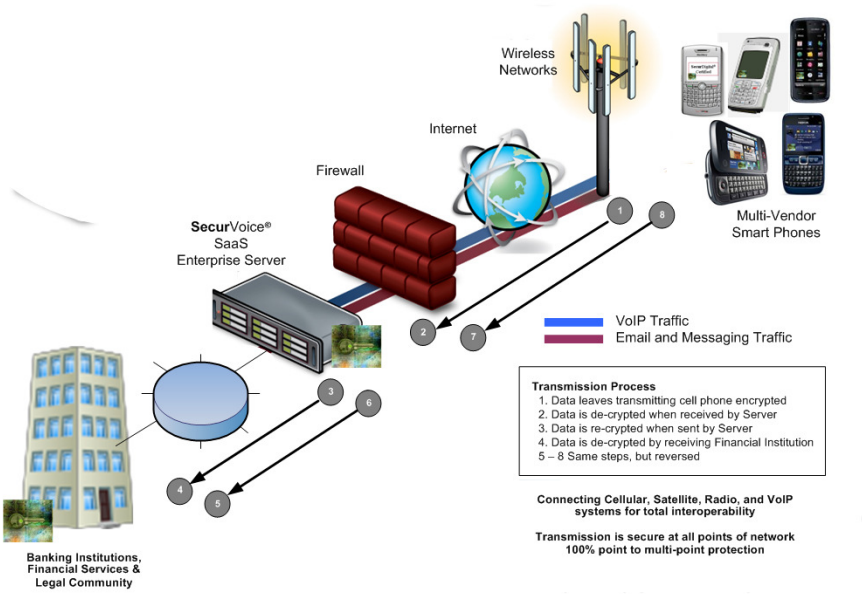
In the clear (CSS): These are normal cell phone calls. These calls are protected by whatever means is provided as a default by your cell phone carrier.

Phone to Phone (P2P): P2P calls are made directly from one cell phone to another cell phone without the use of a server and they are secure.

Phone to Server (P2S): P2S calls route from the phone to the enterprise server that contains the key management system. The benefits of using the **Secur**Voice© patent pending cryptographic key exchange system include:

Normal Voice calls: On phones that allow the voice stream to be captured for encryption, then normal voice cell phone operation is the preferred default.

VoIP calls: On phones that do not allow access to the voice stream VOIP feature is added to the phone and transmits the encrypted voice as a digital stream.



Placing a Secure Call and Transactions

SecurVoice© software is always active. When the caller dials a number or accesses a number from the directory, **Secur**Voice© intercepts the number and activates the SEND command. If the number is flagged as having a cryptographic key associated with it, then the call is automatically dialed as a **Secur**Voice© call. There is no reason to provide the customer with an option to disable the encryption for that call since all phone numbers associated with crypto keys are to be placed as **Secur**Voice© calls.

If the phone number is not flagged, the cell phone system operates normally and the call is placed unencrypted. If the number to be called is flagged, the system retrieves the cryptokey and activates. Once activated the system makes the decision to conduct the call as either a CSS or a P2P call. If the call is a P2P call, the call is encrypted unless the recipient is flagged as a "problem number". In this case, the call begins as a standard unencrypted call, alerting the caller to provide an opportunity to convert to encrypted mode.

Receiving a Secure Call

When a call is received, **Secur**Voice© intercepts the call and activates the ACCEPT key. The caller ID is examined by the software to determine if it is a known **Secur**Voice© device. The caller ID number is used as an index to retrieve the cryptographic key. If the phone number displayed is flagged as a problem number but caller-ID is received then the Problem Number routines are ignored. If the caller-ID is not present, then the call is handled as a normal phone call with the exception that the user can activate the **Secur**Voice© feature upon selection of a valid crypto key. Note that there can be a race condition where the caller-ID number is not available when the call signal is received. Mobile networks always send called-ID, but in rare circumstances caller-ID is not sent. If caller-ID is not sent, the call is dealt with as a normal, unencrypted call.

Copyright 2009 **Secur**Digital, Inc. All Rights Reserved. (203) 912-5532. Email: sales@securdigital.com Online: www.securdigital.com
SecurVoice, the SecurVoice logo, and all other trademarks mentioned in this document are the property of their respective owners.