SecurDigital©
Technical Synopsis Document

Effective January, 2010

This document provides a technical synopsis to engineers who are charged with evaluating the **Secur**Digital© System and includes a description of both how the system is designed and how it is being developed. As such, this specification is subject to change based on customer input in the development process, along with requirements generated by formal laboratory testing.

The system is designed for government and enterprise customers who require technology based on the GSA FIPS 140.2 Compliance Validation. The base **Secur**Digital© configuration is designed to meet this requirements, but is for the commercial marketplace Additional features (PKI, 3DES, VOIP) have been added to the product during development to resolve perceived commercial functional requirements, however, some of these such as PKI, cannot pass the GSA's FIPS 140.2 Compliance Validation. The FIPS compliant versions of the product will exclude these features in the build process.

Customers who require GSA's FIPS 140.2 Compliance Validation need to contact **Secur**Digital© and ask for SecurVoice©.

The **Secur**Digital© System has several modes of operation. There include one form of encryption, two forms of cryptographic key management supported and three forms of communications when operating as a voice device.

One forms of encryption.

1. AES: The **Advanced Encryption Standard (AES)** is an encryption standard adopted by many governments world-wide. Each AES cipher has a 128-bit block size.

Two forms of cryptographic key management.

1. Secret Key: This is the default, and for most customers the only supported service.
2. PKI: Offered as an extra service, the PKI system is less secure.

Three voice operating modes.

1. 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.
2. 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.
3. 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 SecurDigital© patent pending cryptographic key exchange system include:
    - Having the ability to easily manage hundreds or thousands of cryptographic keys in each phone in the fleet
    - The ability to instantly disable encryption on a lost phone
    - Activating encryption on a new phone
    - Creating domains of trust. This will allow multiple handsets attached to trusted servers to place encrypted calls without having to arrange a prior relationship.

SecurDigital©
Technical Synopsis Document

Effective January, 2010

Two forms of voice communications.

1. 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.
2. 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.

Supported Cell Phones

By client request the first supported device is the RIM Blackberry phone. In addition to the RIM Blackberry, **Secur**Digital© can operate on 90% of the mobile phone operating systems by supporting the following cell phone operating systems.

J2ME

Symbian (used in Euro, Middle East, Africa)

Brew

Microsoft Windows Mobile 5 and Windows CE

Linux

By implementing the **Secur**Digital© system at the application layer any handset make and model to can become secure. The only constraints are based on the handset processing power, amount of memory and the operating system. An 'open' approach also allows **Secur**Digital© to be mobile network agnostic. **Secur**Digital© calls can operate on any cell phone carrier that uses a supported phone. For example, one caller may be on Verizon and another caller on AT&T, Sprint, or US Cellular. Alternatively, one caller may be in Europe using on Vodafone while the other end of the call may be in the United States on Nextel. The **Secur**Digital© software is both carrier and operating system agnostic.

Placing a Call

The **Secur**Digital© software is always active. When the caller dials a number or accesses a number from the directory, the **Secur**Digital© software 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**Digital© 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**Digital© 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.

SecurDigital©
Technical Synopsis Document

Effective January, 2010

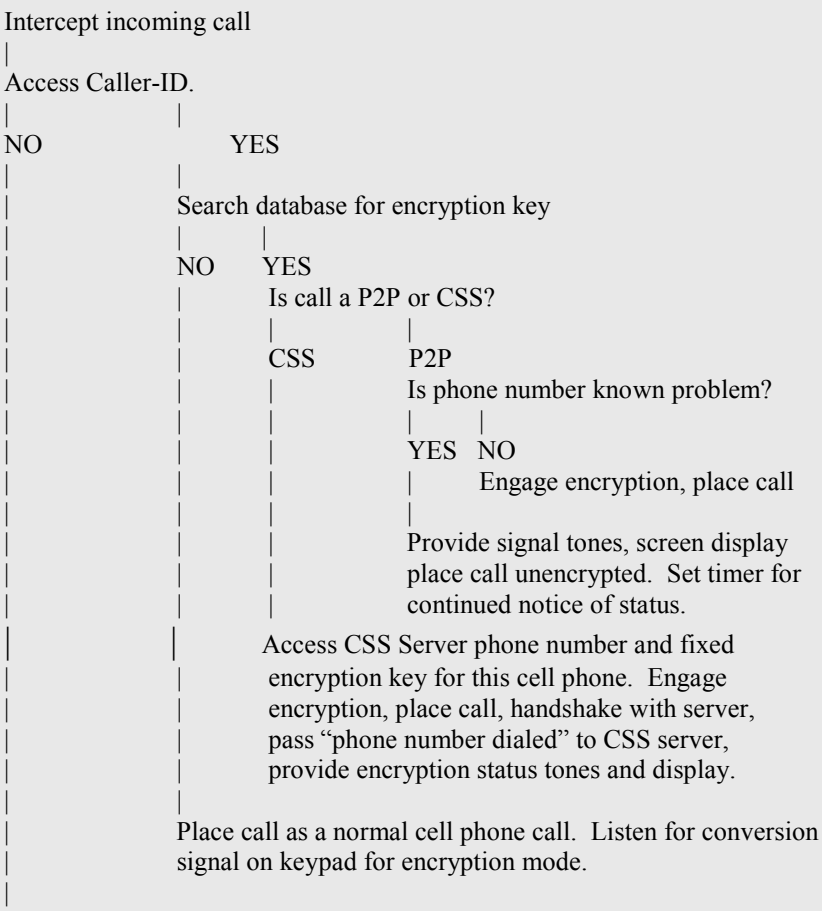
Receiving a Call

When a call is received, the **Secur**Digital© software intercepts the call and activates the ACCEPT key. The caller ID is examined by the software to determine if it is a known **Secur**Digital© 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 SecurDigital© 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.

Ongoing Unencrypted Call

If during an ongoing call the user presses the 9 key three times in quick succession then the call undergoes conversion to a crypto call. The user is requested to select a crypto key and the encryption functions are engaged.

Logic Flows for Incoming Call.



Logic Flow for Outgoing Call

Intercept outgoing call
|
Is the phone number flagged as a crypto call?
| |
| Yes ***(step 2)***
| Is the call a CSS call?
| | |
| | Yes
| | Dial the preprogrammed CSS phone number
| | Handshake and send the "desired number dialed"
| | Phone call continues
| No
| Must be a P2P call
| Place "dialed" number, handshake with the other P2P phone
| Phone call continues
No
Place call as a normal cell phone call
Listen for the signal to convert to a crypto call.
| |
| Signal received to convert
| restart logic flow at step 2
No conversion
Call continues as normal cell phone call

Logic Flow for Incoming "Call Waiting" Call

Version 1 of this software may disable call waiting to be implemented later. If so then call waiting must not be allowed to be processed in the cell phone.

Intercept incoming "call waiting" call.
Place current call "on hold" along with the in-use encryption key
Restart new call using Logic Flow for Incoming Call

Allow user to switch between multiple active calls insuring that the encryption key is switched as appropriate.

Logic Flow for Conversion of Standard Call to Encrypted Call

During unencrypted standard call listen for conversion signal (999 keypad)

Conversion signal received
|
Is call unencrypted
| |
| No, call is already encrypted. Ignore signal.
Is this a CSS call?
| |
| Yes, caller-id must be defective. Transmit cell phone number.
| Handshake and send the "desired number dialed". Phone call continues
No
Caller-id must be defective.