ADVANCED WIRELESS SECURITY USING BIOMETRIC ENCRYPTION FOR SENDER VALIDATION

Debra Lynn Shapiro*, David Swan, Matthew Heinrichs
Integrated Technology Solutions, Inc.
Suite 200, 8775 Cloudleap Ct, Columbia, MD 21045

Abstract

Digitized biometric finger print capture provides the basis for generating encryption keys to provide validation capabilities for wireless data transfers. The biometric supports decryption, validation of the sender, and control of the digital signature for signed documents.

1.0 Security for Wireless Transmissions is a Priority

The rapid improvement in wireless technologies has accelerated the ability to send text, voice, and video transmissions. As wireless traffic increases, so do concerns about security. The ability to capture or "sniff" transmissions from the airwaves is also rapidly evolving. The Army has special needs to be able to verify wireless communications under its IT/C4ISR initiatives. There are three aspects of secure transfers that must be addressed, protection of the information transmitted, verification that the information is correct, and validation that the message received was transmitted by the approved sender.

To date, the primary mode of security has been encryption. Many wireless services offer encryption capabilities to ensure the safety of the transfer. Much has been written lately about the strength of encryption and the level of protection it affords. The greater the number of bits in the encryption key, the higher the level of security for the message. Faster processors reduce the time that it takes to determine a key. In public key encryption, the replacement of a message becomes an even bigger risk. Verification and validation of messages is a critical part of secure wireless transfers. Integrated Technology Solutions, Inc, (ITSI) has developed the ability to encrypt, decrypt, and verify the sender using biometric fingerscan technologies.

2.0 Biometric Supported Encryption

The advances in biometric fingerprint scan technologies provide a solution to the problems of verification and validation as well as a greater level of encryption security. ITSI has developed middleware called **iSURE™**, which integrates today's technologies in biometric finger scan with encryption technology and incorporates security for electronic signatures. **iSURE™** provides both encryption and validation security for wireless and TCP/IP transfers of any information stored in a file, whether text, digitized voice, and digital video files using a biometric encryption key.

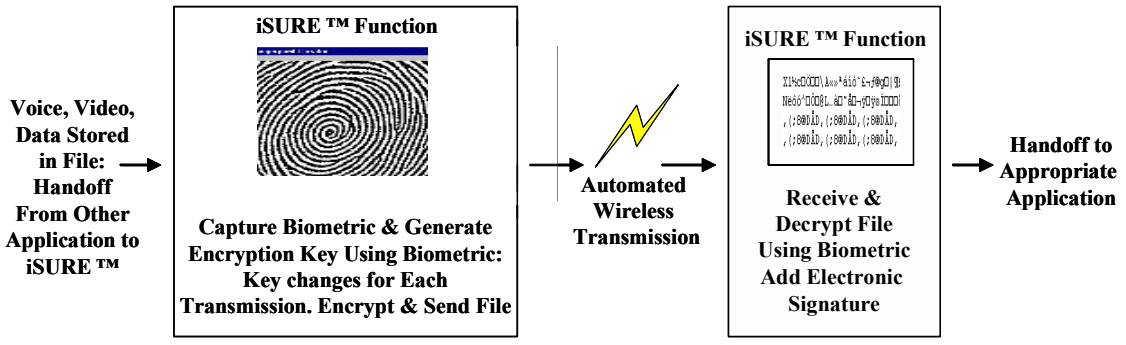

Figure 1.1 iSURE ™ is Interoperable with all Applications and Runs on Windows 9x, 2000 and XP

In addition, the system provides electronic signature management for validated files. Signatures are biometrically encrypted when stored and only valid file decryption allows the application of the signature. **iSURE ™** has been tested using RF, CDPD, and wireless and TCP/IP technologies. Successful decryption validates the identity of the sender and verifies that the message has not been replaced or modified.

3.0 iSURE ™ Middleware Architecture

ITSI completed extensive evaluation of biometric capture, encryption, and electronic signature capabilities prior to selecting the technologies that would be used in the system. Thirteen different encryption products were evaluated for effectiveness of the encryption algorithms, ease of use and speed of encryption. ITSI selected the Blowfish encryption process since it best met system requirements.

Research showed that Silanis Inc. provides the electronic signature algorithms for the majority of electronic signature capabilities currently on the market. ITSI has incorporated Silanis' electronic signature capabilities into **iSURE ™**. Electronic signatures are stored encrypted in the systems. When a report requires a signature, the system decrypts the report and the signature and affixes the signature in the proper location. Reports are not signed electronically until the sender has been validated.

ITSI reviewed the biometric finger scan products from ten different companies. We selected Identix's capabilities since they provided a mature development environment for biometric fingerscan technologies. We are currently using Identix PC Cards and Identix's Software Development Kit (SDK). ITSI has used the SDK to build the necessary software to manage the digitized print after capture. ITSI is moving forward to work with other fingerscan capabilities.

4.0 Support Environment

The Biometric Authentication System currently runs on Microsoft Windows NT, 2000, and XP platforms. It supports both Access and SQL Server databases, and in the near future, Oracle. Since the system uses a minimal number of tables, it is a simple process to incorporate those tables or field entries into an existing database.

Wireless capabilities in RF, CDPD, and wireless Ethernet are supported, as well as all wire based transfer mechanisms. The biometric fingerscan portion of the system is built using Java and electronic signature management has been developed using Visual Basic. The system has been developed to be interoperable with other Biometric capabilities if access to the biometric characteristics file is supported.

5.0 Biometric Authentication Applications

Enrollment in the system provides the information needed to support identity validation and secure transmission. Transmission of reports is not permitted unless the sender's identity is verified before transmission. This prevents one user from sending a report belonging to another user, thereby preventing access to an incorrect electronic signature.

The **iSURE ™** middleware is interoperable with many applications and can provide additional security for existing systems. **iSURE ™** benefits include:

- Biometric Encryption Key varies with each transmission providing multi-tiered security
- Electronic Signature is stored encrypted and can only be attached when sender is validated
- Notifies sender that transmission has been received
- Supports multiple wireless transmission protocols and TCP/IP
- No graphical images are kept so storage requirements are minimal
- Integrates with existing databases or can be delivered with internal database
- Interfaces with other record management systems, and voice or video management systems
- Encryption key is a standard 128 bits but easily increased to larger sizes
- Automated management of Microsoft Word 2000 documents
- Stores transmissions in encrypted or unencrypted form
- Interoperable with existing commercial technologies

The flexibility of **iSURE ™** is one of its greatest strengths. It works efficiently and effectively, automatically transmitting files as soon as the encryption is completed. The encryption has been developed to work quickly on laptops with slower processors and minimal storage. This system has been well optimized and thoroughly tested and is an effective means of adding security, verification, and validation to wireless transmissions.

Acknowledgements

The biometric authentication capabilities used in iSURE ™ were developed in partnership with the National Institute of Justice Agile Interoperability Program. (*iSure™ is a trademark of Integrated Technology Solutions, Inc.; Patent Pending)