

Biometric Authentication System

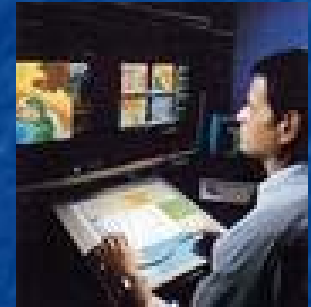
**Presented by Debra Lynn Shapiro
President
Integrated Technology Solutions, Inc**

May 19, 2002



Integrated Technology Solutions, Inc. (ITSI)

- Full service information technology and systems engineering firm specializing in information systems for:
 - Criminal Justice
 - Public Safety
 - Intelligent Transportation
- Supporting the Department of Justice, NIJ, and State and Local Public Safety agencies



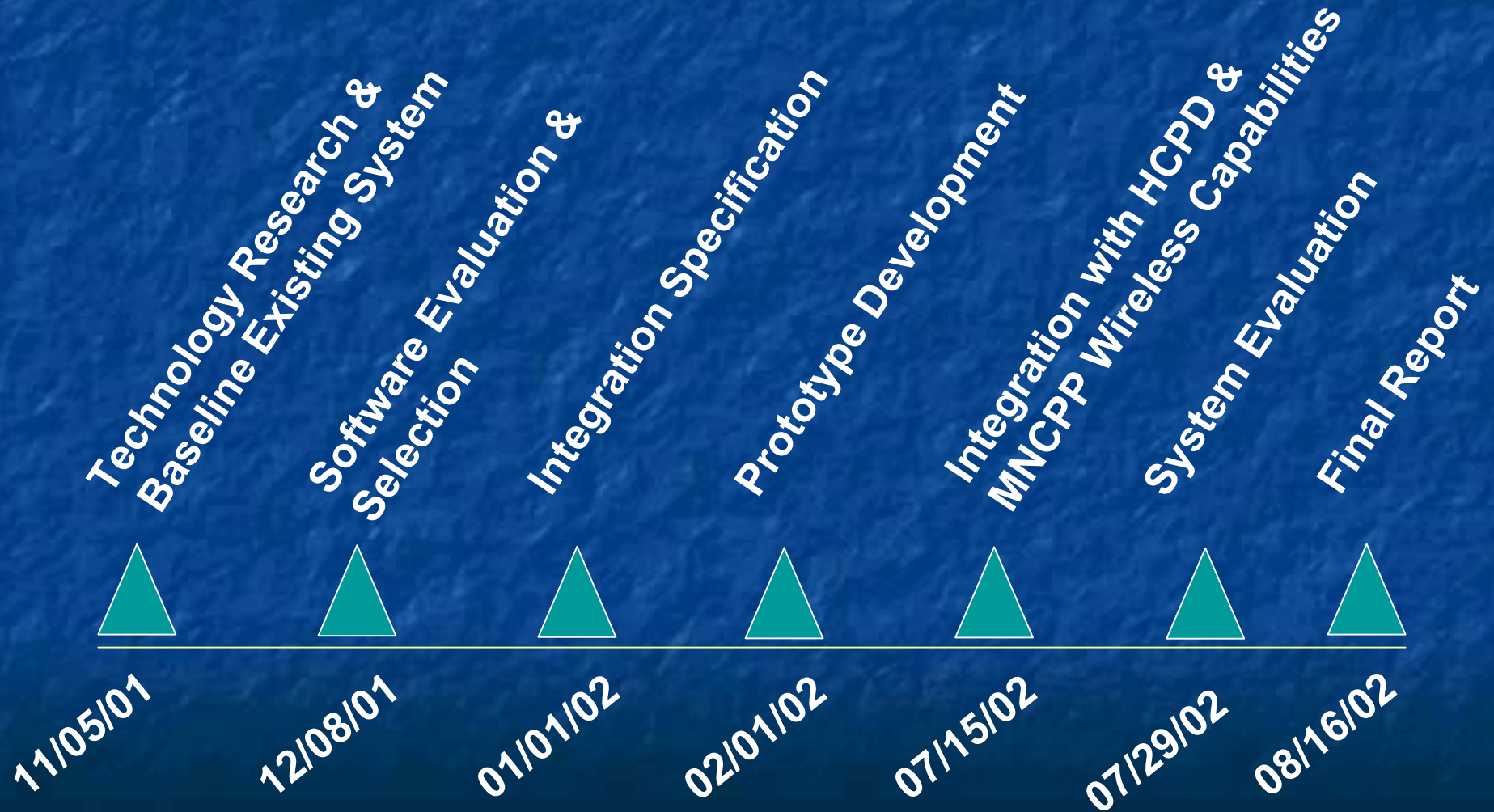
**The Right System Built
the Right Way**

The Project Team

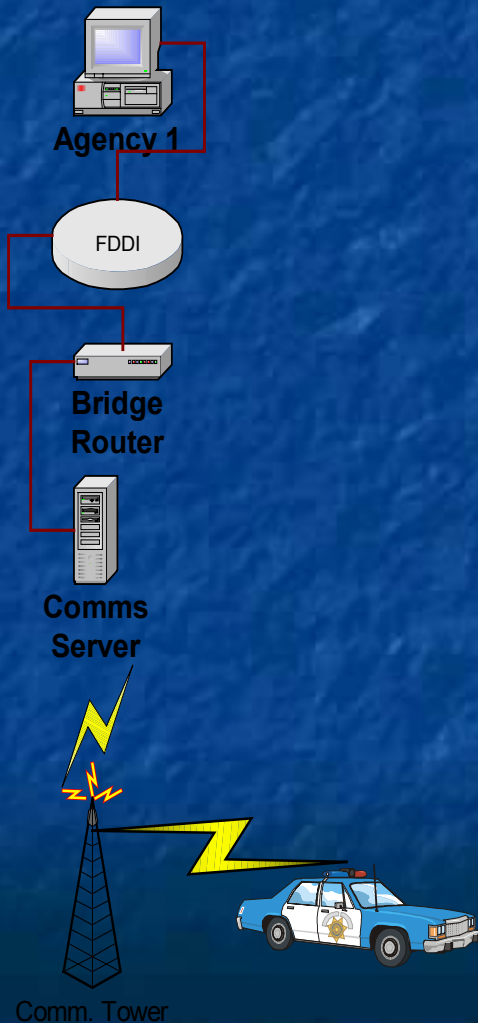
- ITSI
- National Institute of Justice
- Howard County Police Department, Howard County, MD
- Maryland National Capital Park Police



Project Schedule



The Security Challenge



- Wireless transfers of voice, data, and video in digital packets are becoming more prevalent
- Transfers are at risk from capture and replacement
 - New technologies are under development to "sniff" transmissions out of the airwaves
- Most, but not all, information is encrypted before transfer
- Misconception: Wireless transfer is safe because information is encrypted
 - Replacement of messages is a growing risk

The Authentication Need

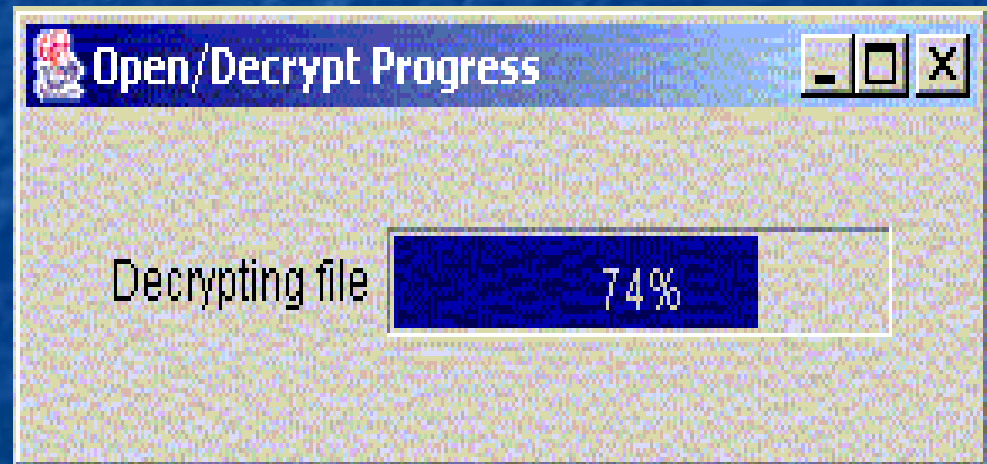
- Public Safety agencies, the Courts, and agencies involved in Homeland Security need the ability to validate the message at the receiving location
 - Is the sender a valid system user or someone who has inappropriately gained access?
 - Has the message been replaced with another?
 - Is there a way to validate the sender so an electronic signature can be used?

Authentication Has Other Justice Applications

- Transmission of Warrants from Court to Police Car
- Secure, controlled, integrated Case Management from arrest through parole
- Identification of probationers & parolees checking in at kiosks
- Anywhere positive identification is needed and wire connection is a challenge

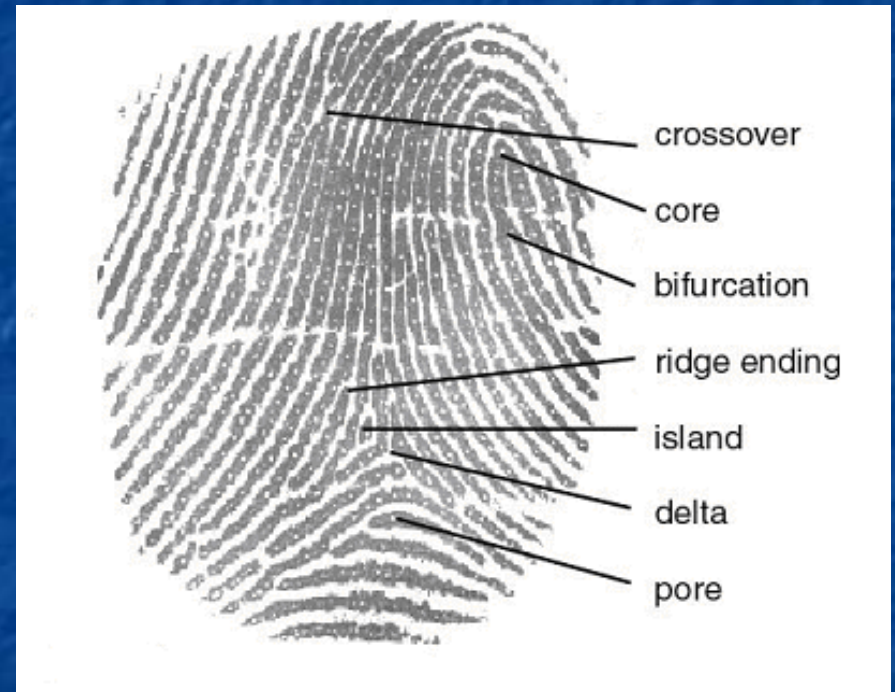
The Biometric Authentication Solution

- Biometric validation: Using an individual's unique characteristics to secure & validate wireless transmissions
 - Advances in biometric finger scan technologies and encryption make biometric validation possible
 - The biometric encryption key provides security and supports validation of the sender at the receiving site



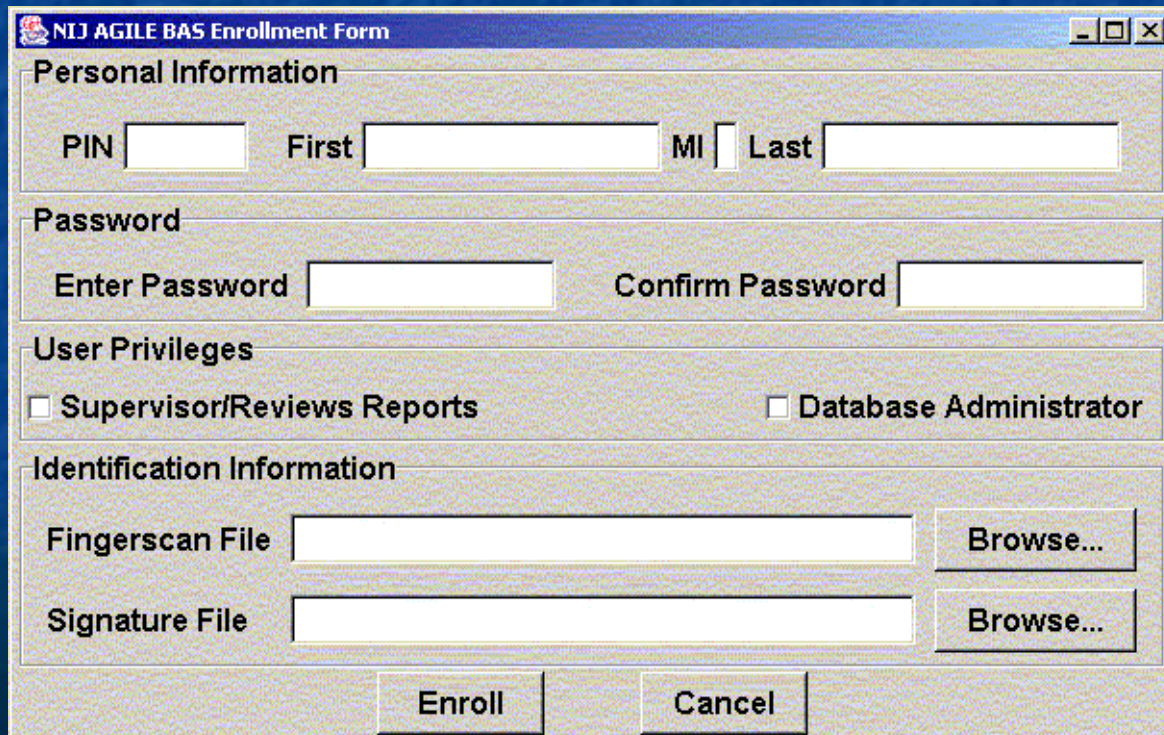
The Technical Challenge

- Biometric finger scan technologies do not provide precise, repeatable scans
- Prior attempts at encryption failed because inaccuracies in capture prevent development of a set key
- ITSI has developed an advanced process for managing the variability of the biometric finger scan after capture by commercial products



Biometric Finger Scan Encryption is Viable

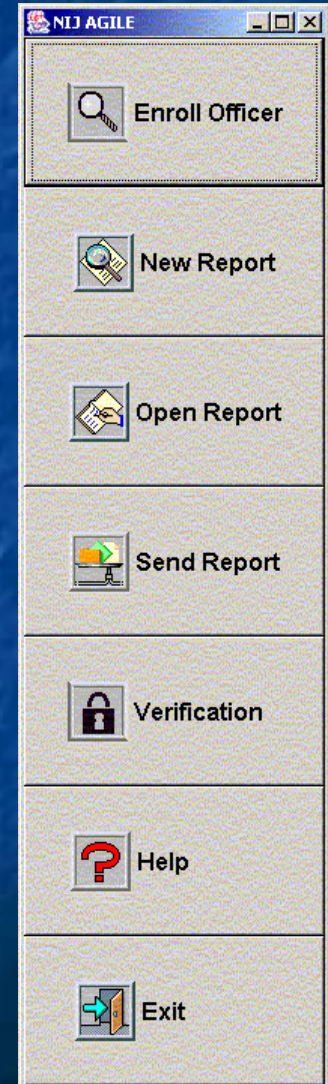
- ITSI has successfully enrolled users and encrypted and decrypted using a biometric encryption key based on the individual's finger scan



The screenshot shows a Windows-style application window titled "NJ AGILE BAS Enrollment Form". The form is divided into several sections:

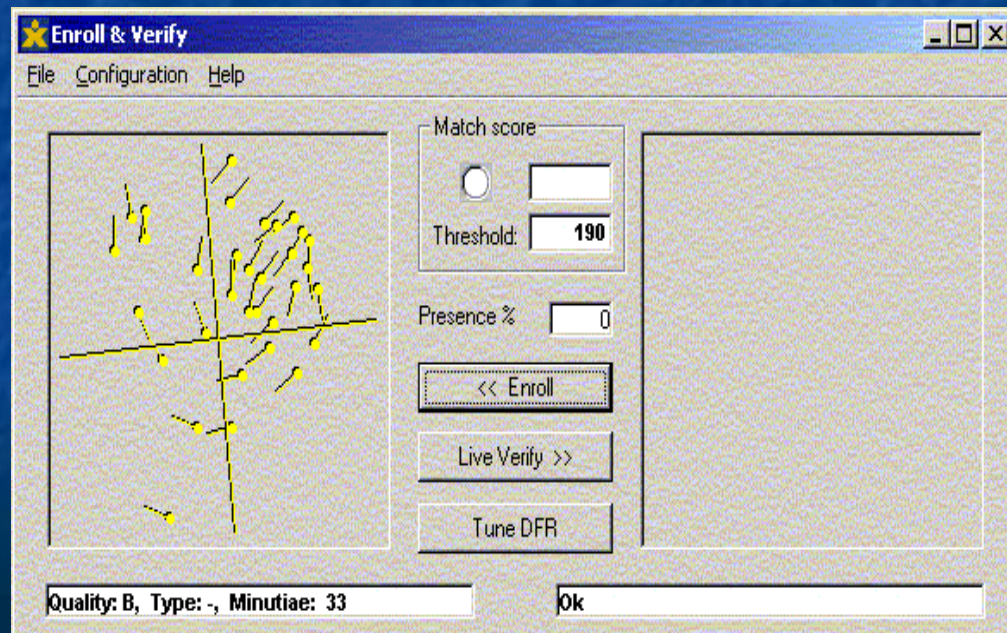
- Personal Information:** Contains input fields for "PIN", "First", "MI", and "Last".
- Password:** Contains input fields for "Enter Password" and "Confirm Password".
- User Privileges:** Contains two checkboxes: "Supervisor/Reviews Reports" and "Database Administrator".
- Identification Information:** Contains input fields for "Fingerscan File" and "Signature File", each with a "Browse..." button.

At the bottom of the form are two buttons: "Enroll" and "Cancel".



Putting Technology into Practice

- The system being developed supports secure and validated wireless transmission of police reports
- The system being demonstrated today integrates Identix's finger scan capabilities, Blow Fish Encryption, and Silanis Electronic Signature System, Microsoft Word with ITSI's algorithms and application code



ITSI's Middleware Is Interoperable with Multiple Commercial Technologies

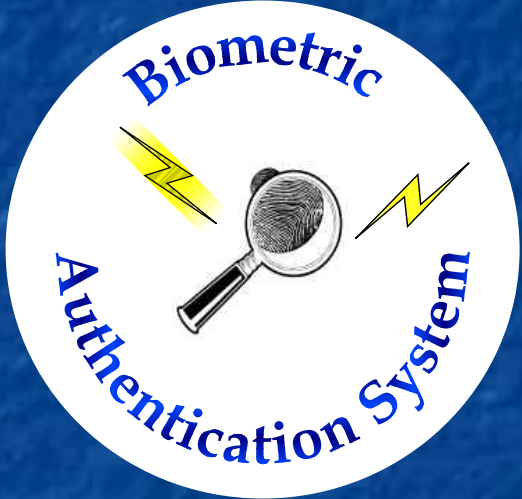
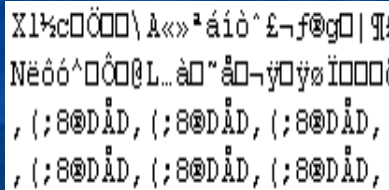
Commercial
Finger Scan
Capture
Product



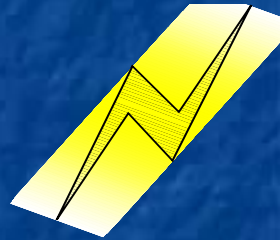
Electronic
Signature
Capability



Encryption



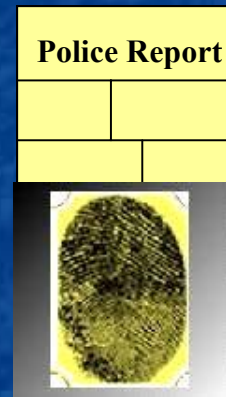
Biometric Authentication System: Report Generation and Transmission



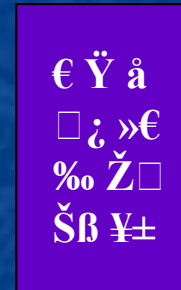
**Officer in the field
creates police report
or other file. No
signature is provided.**



**Officer validates using
biometric finger scan &
requests transmission
of the report**

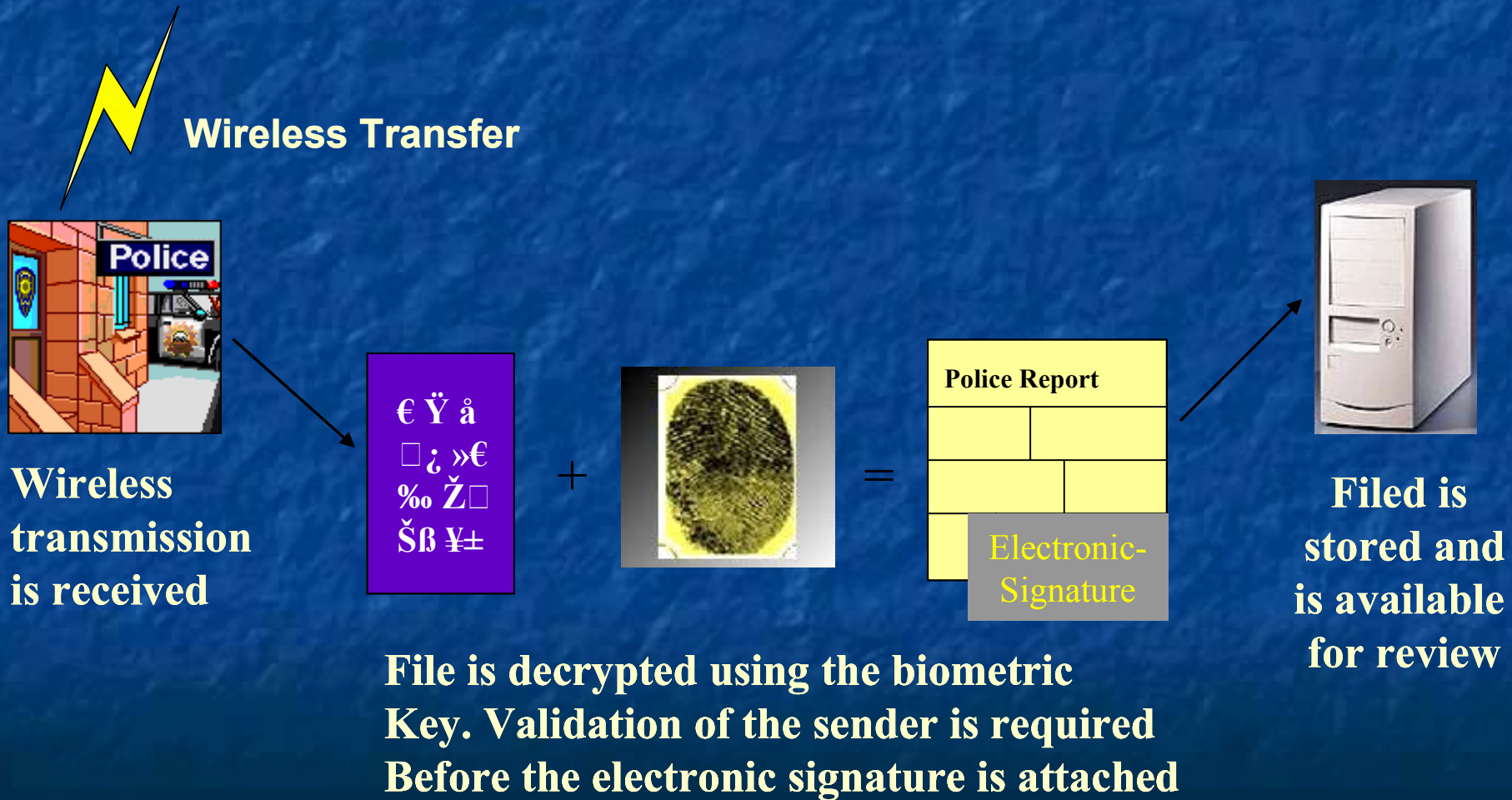


**Report is encrypted
using the biometric
encryption key**



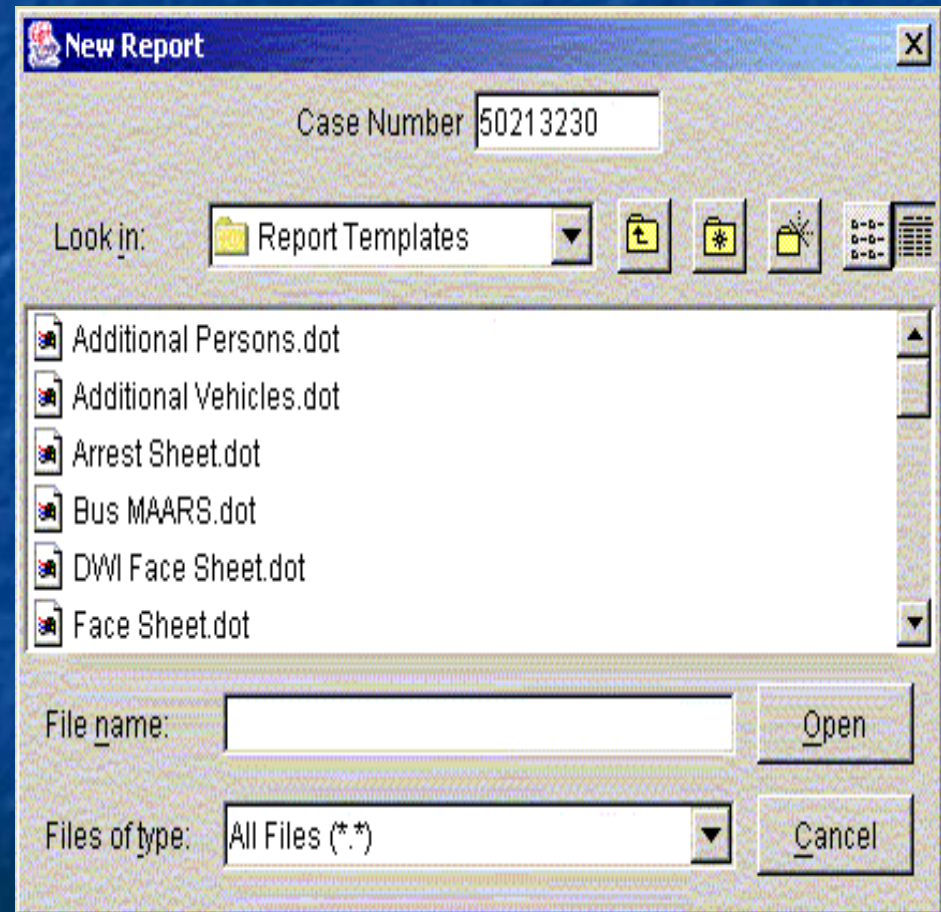
**Report is
sent via
RF, CDPD,
Or Wireless
Ethernet**

Report Receipt, Validation and Electronic Signature



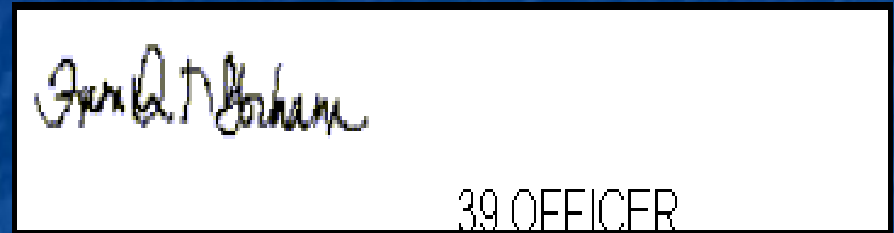
Report Access is Controlled

- In the field, only the owner may access his or her reports
- The sender must complete finger scan prior to the generation of the biometric encryption key
- Validation of the sender is done before each wireless transmission – the sender must be the owner of the document
- Implementation of biometric login can be managed by the system

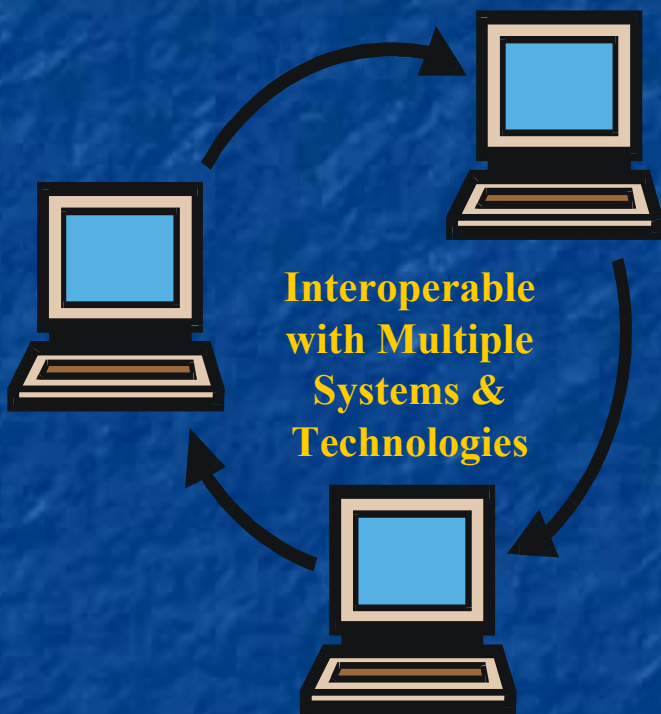


Electronic Signature Management

- Reports are transmitted without signature
- Signature is attached at the receiving site. Signature can be added only if report successfully decrypts, validating the users identity.
- The signature is stored as an encrypted file so it cannot be used on non-validated



Supports Multiple Environments



- Interoperable with report management systems and Microsoft Word
- Operating system independent
- Interoperable with any finger scan capability that supports access to the minutiae file
- Interoperable with any digital signature software

Current Activities

- Integrating validation capability with tool bar buttons
- Implementing sergeant review capabilities according to HCPD review processes
- Finalizing system test procedures
- Completing system documentation
- Working with Maryland National Capital Park Police to test CDPD transmission

Prototype System Demonstration

- Using Howard County Maryland Police Reports in Microsoft Word template format
 - Open a new police report
 - Save the police report with case number
 - Fill in report information
 - Close report
 - Request transmission of report
 - Send encrypted report using wireless internet

Prototype Demonstration Continued

- The server machine will receive the encrypted report
- An acknowledgement of report receipt will be transmitted to sender
- Report will be decrypted using biometric key
- Successful decryption validates the senders identity
- The electronic signature is attached after the file has been decrypted
- Files are saved for review by the sergeant

Biometric Authentication System Demonstration

Integrated Technology Solutions, Inc.
8775 Cloudleap Court
Columbia, MD 21045
410-772-3900
mgorham@itsi-inc.com