Oklahoma State Bureau of Investigation

Management of Information Systems

Card Scan
Interface Specifications Document
Version 1.1

January 29, 2003

Table of Revisions

Release Date	Version ID	Notes, Comments, and References
August 2, 2000	Draft 1.0	Draft Release
September 19, 2000	Draft 2.0	Added multiple sections.
September 29, 2000	Version 1.0	Release Version
October 1, 2000	Version 1.0	Reformatted Document
January 29, 2003	Version 1.1	Added Section 3.11

Table of Contents

List of Figures

List of Tables

1.0 Introduction

This section provides the scope, purpose, background, and reference for the Oklahoma State Bureau of Investigation's (OSBI) card scan interface.

1.1 Scope

This document is the only document that defines the interface described herein. This document, once approved, shall be the defining control document and shall not be changed or modified without the express written consent of the OSBI, and notated in this document. **This document is to be used for law enforcement applications only.**

1.2 Purpose

This document defines the interface specifications for card scan station connection to the OSBI's Automated Fingerprint Identification System (AFIS).

1.3 Background

In the manual world of fingerprinting, cards must be physically transported and processed. This process causes substantial delays in the identification cycle. To improve the speed and accuracy of the fingerprint identification process and eliminate the need for contributing agencies to create and mail paper fingerprint cards to the OSBI for processing, the OSBI is purchasing a National Institute of Standards and Technology (NIST) compliant AFIS. This will allow any agency that wants to submit fingerprint data electronically via a card scan station to do so as long as the specifications in this document are followed.

1.4   References

OSBI Type-2 Record Specifications Version 3.6-4,
Revised July 1, 2002

WSQ Gray-scale Fingerprint Image Compression Specification,
February 16, 1993, IAFIS-IC-0110V2

American National Standards Institute (ANSI), Data Format for the Interchange of Fingerprint Information,
ANSI/NIST-ITL 1-2000

Transmission Control Protocol (TCP),
September 1, 1981, RFC 793 (Request for Comments – Proposed Standard)

Internet Protocol (IP),
September 1, 1981, RFC 791 (Requests for Comments – Proposed Standard)

Simple Mail Transfer Protocol (SMTP),
August 1, 1982, RFC 821 (Requests for Comments – Proposed Standard)

Point-to-Point Protocol (PPP),
July 1994, RFC 1661 (Requests for Comments – Proposed Standard)

Federal Bureau of Investigation (FBI), Electronic Fingerprint Transmission Specification,
January 1999, CJIS-RS-0010 (V6.2)

2.0 Description of Operational Concepts

This section describes the operational concepts for the submitting card scan station. The overall NIST based Internet communication is listed in Figure 1.0.

Figure 1.0

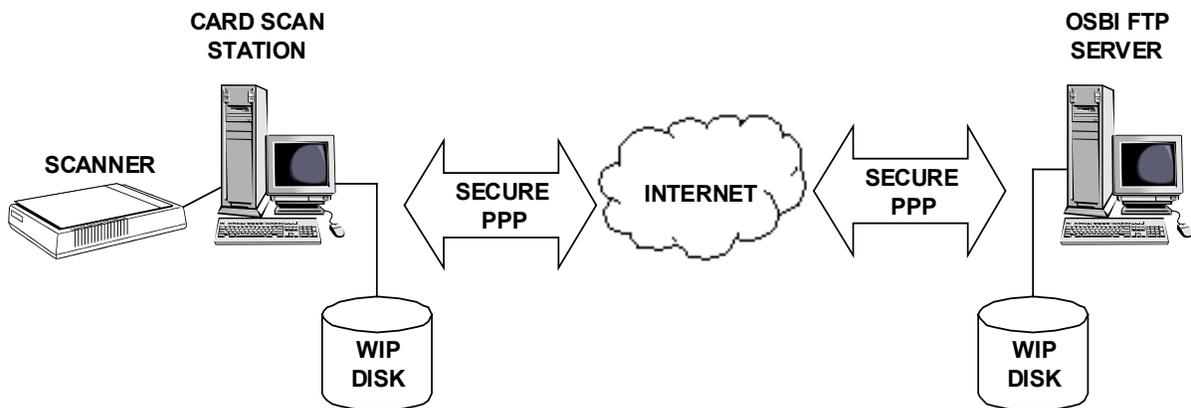AFIS NIST BASED INTERNET COMMUNICATIONS CONCEPT
Diagram 1.0
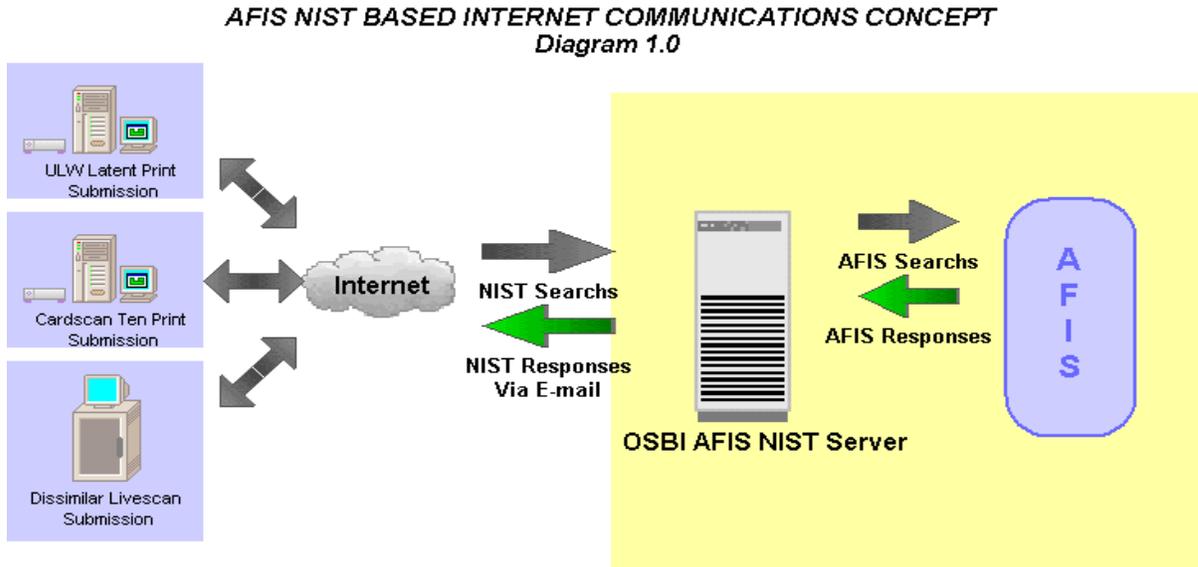
2.1 Card Scan Connectivity

The card scan station will connect to the OSBI File Transfer Protocol (FTP) server through a secure Internet Point-to-Point Protocol (PPP) connection. See Figure 2.0 below.
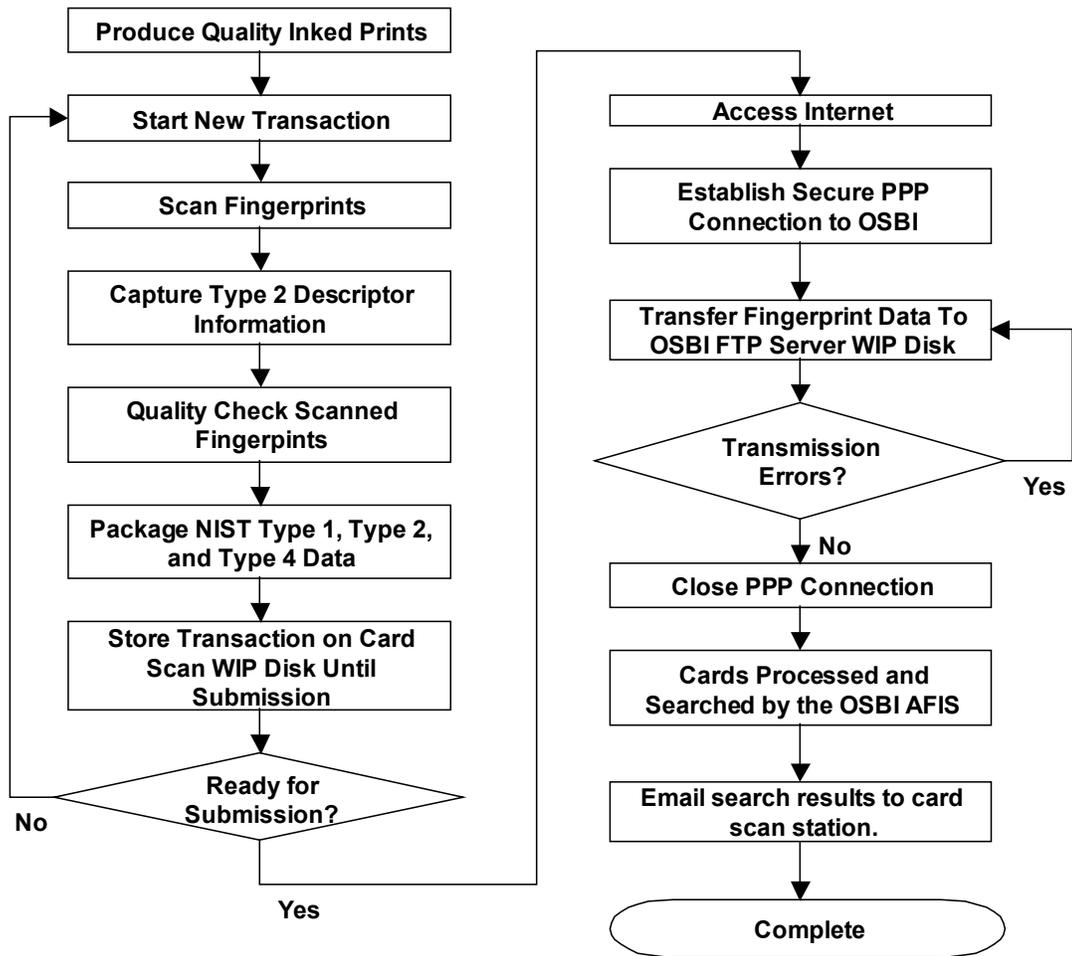
Figure 2.0

2.2 Card Scan Data Flow Diagram

Figure 3.0 below shows a high-level data flow diagram for the card scan station.

Figure 3.0

2.3 Card Scan Data Flow Narrative

Below is a narrative description of the high-level card scan data flow diagram (Figure 3.0).

1) Produce quality inked prints.

2) Start a new transaction on the Card Scan Workstation .

3) Scan fingerprints using *FBI/IQS Appendix F* certified scanner.

4) Key enter all Type 2 information as specified by the *OSBI Type-2 Record Specifications* Version 3.2.

5) Visually check the quality of scanned images.

6) Package NIST Type 1, Type 2, and Type 4 records.

7) Store all transactions on Work In Progress (WIP) disk until submission.

8) When ready to submit data, access the Internet.

9) Once connected to the Internet establish a secure PPP connection to the OSBI.

10) Transfer all fingerprint data to the OSBI using FTP protocol.

11) If there were any errors during transmission resend all data until successful.

12) After successful transmission close PPP connection.

13) Cards processed at the OSBI and AFIS database searched.

14) Search results emailed back to card scan station.

3.0 Specifications

This section defines the specifications for the submitting card scan station.

3.1 FBI Certified Card Scan

The card scan station must be *FBI/IQS (Appendix G)* certified.

3.2 FBI Certified Scanner

The card scan station scanner must be *FBI/IQS (Appendix F)* certified.

3.3 EFTS Compliant

All Card Scan stations must be able to meet the FBI's *Electronic Fingerprint Transmission Specifications (EFTS) V6.2* and above in order to be able to submit data to the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

3.4 Descriptor Data

All descriptor data must be formatted according to the *OSBI Type-2 Record Specifications* before being submitted from the card scan station to the OSBI.

3.5 Fingerprint Image Transmission

All fingerprint images transmitted from the card scan station must be NIST Type-4 high-resolution grayscale records as described in the *ANSI/NIST-ITL 1-2000* standard in section 11.

3.6 Data Transfer Protocol

TCP/IP and FTP will be the protocols used for all file transfer, and network communications between the card scan station and the OSBI.

3.7 Email Transfer Protocol

SMTP (Simple Mail Transfer Protocol) will be the protocol used for all email exchange between the card scan station and the OSBI.

3.8 Valid Email Account

A valid email account will have to be set up on the card scan station and the OSBI will have to be notified of the account name in order to exchange notifications and administrative email messages between the card scan station and the OSBI.

3.9 Internet Access

All agencies wanting to submit fingerprints via card scan stations must have Internet access with the ability to run secure PPP and FTP protocols for transmission of fingerprint information.

3.10 Fingerprint Image Compression/Decompression

The Wavelet Scalar Quantization (WSQ) compression/decompression algorithm will be used for all gray-scale fingerprint images transferred to and from the OSBI. For information regarding the WSQ algorithm refer to the *Wavelet Scalar Quantization Grayscale Fingerprint Image Compression Specification*, dated February 16, 1993.

3.11 Types of Transactions

This section describes the types of transactions that can be submitted from a card scan to the OSBI. The particular type of transaction is identified in the Type Of Transaction (TOT) Field in the Type-1 record that is used with each transaction. For further information about a Type-1 record refer to the *American National Standards Institute (ANSI), Data Format for the Interchange of Fingerprint Information,* ANSI/NIST-ITL 1-2000. Table 1 lists the types of transactions that are accepted by the OSBI.

Table 1

Type of Transactions	Description
CRCS	Criminal Card Scan

4.0   Glossary of Terms

WSQ	-	Wavelet Scalar Quantization
NIST	-	National Institute of Standards and Technology
TCP/IP	-	Transmission Control Protocol / Internet Protocol
OSBI	-	Oklahoma State Bureau of Investigation
ASCII	-	American Standard for Computer Information Interchange
AFIS	-	Automated Fingerprint Identification System
IQS	-	Image Quality Specification
SMTP	-	Simple Mail Transfer Protocol
EFTS	-	Electronic Fingerprint Transmission Specifications
FBI	-	Federal Bureau of Investigation
IAFIS	-	Integrated Automated Fingerprint Identification Specifications
FTP	-	File Transfer Protocol
PPP	-	Point-to-Point Protocol

5.0   OSBI Technical Contact Information

OSBI Management of Information Systems
6600 North Harvey
Oklahoma City, Oklahoma 73116
Phone: (405) 879-2972 Fax: (405) 879-2542
Toll Free 1-800-522-8017