



Electronic Fingerprint Submission (EFS) FINRA Certification Procedures

©2014 Financial Industry Regulatory Authority (FINRA). All rights reserved. Materials may not be reprinted or republished without the express permission of FINRA. This document contains FINRA Confidential and Proprietary information. FINRA provides this information to member firms only for the firms' internal assessment or use in configuring an electronic fingerprint system for submission of fingerprints from the firm to the FINRA Electronic Fingerprint Processing System. Any other use is strictly prohibited by FINRA. A firm's use of this document demonstrates its acknowledgement that this document contains FINRA Confidential and Proprietary information, agreement that the firm will not reprint, republish or otherwise disclose this information to any third party and its agreement that FINRA may protect its rights, including but not limited to intellectual property rights.

Table of Contents

Timeline for EFS Vendor and Firm Certification in Test Environment	2
FINRA Interface Guidelines	3
I. EFS Overview.....	3
II. Record Submission Requirements	3
III. Electronic Fingerprint System Certification.....	4
A. FINRA Fingerprint Imaging Requirements	5
B. FINRA Fingerprint Record Data Content Requirements	5
C. FINRA Fingerprint Record Formatting, Encryption and Transmission Requirements	6
IV. EFTS Formatting	6
V. S/MIME Encoding	10
A. S/MIME Terminology	10
B. S/MIME Process	10
C. S/MIME Software	11
VI. Record Retention	11

Timeline for EFS Vendor and Firm Certification in Test Environment

Step	Task	Actor	Notes
1	FINRA Certification Procedures sent to firm.	FINRA	Initial document
2	Forward certification documentation to selected vendor.	Firm	
3	Notify FINRA of selected vendor and provide the appropriate contact information.	Firm	Vendor will be certified along with firm following successful
4	Acquire and install EFS System, livescan or card scan configuration.	Firm	System must meet FINRA Interface Guidelines requirements.
5	Notify FINRA that the firm is ready to submit EFS fingerprint data in the test environment.	Firm	Contact the Gateway Call Center at (301) 869-6699
6	Firm returns signed copy of FINRA EFS User Agreement to FINRA.	Firm	
7	FINRA and firm exchange e-mail certificate information.	FINRA Firm	
8	FINRA provides firm with User Acceptance testing information, testing dates and test data.	FINRA	
9	Firm makes submissions to FINRA EFS test environment using test data.	Firm	
10	Submissions received into FINRA EFS test environment and reviewed for accuracy.	FINRA	
11	Firm and vendor receive notice of certification and date that firm may begin submitting EFS data to FINRA EFS production environment, which will update CRD.	FINRA	

FINRA Interface Guidelines For the Electronic Submission of Fingerprint Records

I. EFS Overview

The FINRA Electronic Fingerprint Processing (EFP) System facilitates the FBI's criminal background search process by: (1) enabling Electronic Fingerprint Submission (EFS) to FINRA via the Internet; (2) providing on-line validation and direct forwarding of records to the FBI Integrated Automated Fingerprint Identification System (IAFIS); and (3) supporting network communication of search results from the FBI. This document provides guidelines for configuring an *electronic fingerprint system* (a standard livescan or card scan fingerprinting system) for use by a firm to submit electronic fingerprints from the firm to the FINRA EFP System. Apart from the technical requirements contained in this document, FINRA requires firms (and their agents, such as service bureaus, as applicable) to complete and periodically update EFP System user agreements, and to agree to follow certain FINRA and EFP System terms and conditions. For more information on required agreements and terms and conditions, see the EFP System page on FINRA's web site at: www.finra.org

II. Record Submission Requirements

The FINRA EFP System provides the capability to receive and process electronically transmitted fingerprint records that are formatted in accordance with FINRA specifications. Any livescan or card scan system used to create and transmit fingerprint records to FINRA must be configured to:

- (1) Format each fingerprint record in accordance with the FINRA implementation of the FBI Electronic Fingerprint Transmission Specifications (FINRA-EFTS) version 6.2 or version 7.0. Details of the FINRA-EFTS formatting requirements are provided in Section IV.
- (2) Encode each fingerprint record into a secure S/MIME¹-encoded message and transmit the encoded message to FINRA EFP via the Internet. Details of S/MIME encoding are provided in Section V.

The EFTS record formatting, S/MIME encoding process and transaction formatting and transmission are performed automatically by the livescan or card scan system. Firms should require their vendor to configure the system for FINRA EFS compatibility during installation.

Each firm, prior to initiating EFS operations, must:

- (1) Obtain a certification from the vendor that its system meets FINRA's specified requirements and that the vendor has configured the system in accordance with FINRA's EFP configuration specifications. FINRA's technical requirements for livescan and card scan systems are provided in Section III.
- (2) Conduct a transmission test to verify the proper configuration of its installed system. In this test, the firm will send ten (10) electronic record submissions to FINRA's Test EFP Transaction Server and FINRA will verify the successful transmission and handling of each transaction.

A firm that has purchased and installed a livescan or card scan system and obtained certification from the vendor that the system meets FINRA technical requirements must then request a transmission test.

¹ S/MIME - Secure Multipurpose Internet Mail Extensions, a specification for formatting encrypted and unencrypted messages so that they can be sent over the Internet.

The FINRA EFP Coordinator will schedule a test with the firm and provide necessary test performance details (e.g., the Internet mail address of the EFP test server). The firm will be responsible for working with its vendor to resolve any problems identified during testing and for scheduling another transmission test if required. Upon successful completion of the transmission test, FINRA will provide an Internet mail address for the production EFP Transaction Server and authorize the firm to commence electronic submission of records.

III. Electronic Fingerprint System Certification

The special formatting and encoding required for transmission of fingerprint records should be configured and tested by the livescan or card scan vendor for each installation so that the formatting, encoding and submission process is fully automatic from the perspective of the user.

Before a firm may commence production fingerprint submission operations, however, all electronic fingerprint systems must be certified for compliance with FINRA's technical requirements and standards. ***FINRA will not accept electronic transmissions of ten-print fingerprint records originated by livescan or card scan systems that have not been certified by FINRA.***

From the perspective of a firm, the certification process has two elements:

- (1) **System Certification:** Each firm is responsible for requiring that its electronic fingerprint system vendor certify that any electronic fingerprint system to be used for EFS is fully compliant with FINRA's technical standards. Existing systems will have to be upgraded and certified by the vendor. Firms with new systems should ensure that the vendor meets system certification requirements.
- (2) **Installation Certification:** The installation certification test is essentially a transmission test, in which 10 fingerprint records are sent to FINRA EFP under a coordinated observation, in order to validate that the data content, data formatting, message encryption, and Internet transmission mechanisms have been configured correctly and the test is run successfully.

Any system used to digitize and transmit fingerprint records to FINRA must be compliant with FINRA functional and technical standards, including:

- (1) FINRA fingerprint imaging requirements;
- (2) FINRA data content requirements; and
- (3) FINRA record formatting, encryption and transmission requirements.

FINRA will utilize a self-certification process, in which each prospective vendor is required to implement, test and verify capabilities that satisfy FINRA-specific technical requirements. FINRA does not intend to perform technical tests other than transmission tests and periodic inspection and analysis of fingerprint record products.

Note that FINRA's acceptance of a vendor's compliance certification is not intended as an endorsement of a vendor's product, but will enable vendors to offer specific product configurations that have been tested and found to comply with FINRA technical requirements.

Technical Requirements for Electronic Fingerprint Systems

FINRA's technical requirements for livescan and card scan systems are as follows:

A. FINRA Fingerprint Imaging Requirements

(a)	The livescan system or the fingerprint card scanner incorporated into a card scan system must be FBI Certified and listed on the FBI Certified Products Web Site http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_cert as having been tested and found to be in compliance with the FBI IAFIS Image Quality Specifications (IQS), as specified in the FBI EFTS C.IIS-RS-0010 (V7) January 29, 1999 Appendix F.
(b)	The software used to compress fingerprint images must be a <i>Wavelet Scalar Quantization</i> (WSQ) compression method that is certified by the FBI for compliance with the FBI standard for compression of ten-print fingerprint images (IAFIS-IC-01 10 v.2, February 16, 1993, or latest version).
(c)	The maximum compression of ten-print fingerprint images must not exceed a WSQ compression ratio of 15:1.
(d)	Any missing rolled fingerprint must contain an annotation ('XX' for missing or bandaged; 'UP' for Unprintable) corresponding to the missing image.
(e)	A record containing no fingerprints (e.g., both hands amputated or bandaged) may not be submitted to FINRA via EFS and the vendor's electronic fingerprint system must enforce this prohibition.

B. FINRA Fingerprint Record Data Content Requirements

(a)	<p>The electronic fingerprint system must provide interactive data entry controls that ensure data quality and reduce data entry errors, including:</p> <ol style="list-style-type: none"> 1. Entry of NCIC/FINRA codes and standard information from code/information tables. NCIC standard code tables include Gender, Race, Hair Color, Eye Color, Place of Birth/Citizenship. 2. Automated validity checking to detect and flag incorrect entries. Validity checking must be performed with respect to EFTS standard data definitions and FINRA data definition restrictions identified in Tables 4-1 and 4-2. 3. Interactive validation of bar code numbers.
(b)	<p>The electronic fingerprint system should provide maintainable tables for installation-specific standard information including branch office addresses and transaction codes. The data entry controls should enable:</p> <ol style="list-style-type: none"> 1. Easy selection of any table value for inclusion in a fingerprint record. 2. Designation of a default selection from the table of installation-specific entries for each table-supported field. Default values should be automatically entered in each electronic fingerprint record, but must be able to be overwritten by an operator selection or entry of another value.
(c)	The electronic fingerprint system must provide for automatic or interactive recording of the date that the fingerprints were taken and include this "date fingerprinted" information in the EFTS-formatted record.
(d)	The electronic fingerprint system must provide for the input of all FBI-required record information as defined in the EFTS and for all FINRA additional information, as identified in Section 4, Table 4-2.

C. FINRA Fingerprint Record Formatting, Encryption and Transmission Requirements

(a)	The electronic fingerprint system must format fingerprint records in accordance with the FBI EFTS, version 6.2 or version 7, and in accordance with FINRA- specific restrictions and extensions of the EFTS standard. FINRA-EFTS specifications are provided in Section IV of this document.
(b)	<p>Each electronic fingerprint system must be configured with FINRA-compatible security certificates, including:</p> <ul style="list-style-type: none"> - Fingerprint System’s Root Certificate (obtained from Symantec) - Digital Certificate for the Firm (obtained from Symantec) - Digital Certificate for FINRA (provided by FINRA) - Software to send S/MIME messages (available through Cogent)
(c)	The electronic fingerprint system must provide a capability to provide automatic S/MIME certificate verification and message encoding for secure transmission of transactions. The system’s S/MIME implementation must be fully compatible with FINRA’s Triple-DES encryption standard and message security configuration, as described in Section V of this document.
(d)	<p>Each electronic fingerprint system must provide a standard <i>Simple Mail Transfer Protocol</i> (SMTP) formatting and transmission capability to connect with and transmit fingerprint records to the FINRA Transaction Server. The transmission software must be configured to ensure that each Internet mail transaction message contains the following:</p> <p style="margin-left: 40px;">Date: The date and time the message was sent From: The mail address of the sender To: The mail address of the FINRA Transaction Server Subject: FINRA Ten-print Submission</p>

IV. EFTS Formatting

All electronic fingerprint records must be submitted to FINRA as *Non-Federal Applicant User Fee* (NFUF) transactions, and the transactions must be compliant with the FBI’s EFTS version 6.2 or version 7.0. The current version of the FBI EFTS document, which defines standard data elements and format requirements for properly formatting a fingerprint record for transmission, is available from the FBI and may be accessed and downloaded via the following link: <https://www.fbibiospecs.org/docs/efts71.pdf>. In the FINRA EFS implementation, specific contents or content restrictions are required for some of the standard EFTS data fields and additional data requirements have been defined in the FINRA-EFTS specification.

FINRA data requirements for the standard EFTS fields are defined in Table 4-1. The additional FINRA-EFTS data fields required to support EFS are listed in Table 4-2.

Table 4-1. Data Content Definitions for Standard EFTS Fields

Standard Data Element	Data Element Field	Content Specification
1.04 – TOT	Type of Transaction	'NFUF' ("Non-Federal User Fee")
1.07 – DAI	Destination Agency Identifier	'DCSEC000Z'
1.08 – ORI	Originating Agency Identifier	'DCSEC000Z'
1.09 – TCN	Transaction Control Number	29-digits, alphanumeric. 'FINRA' + Barcode + Date/Time Stamp > The letters 'FINRA' + Barcode = Bar code labels must be requested from FINRA. + Date/Time Stamp: YYYYMMDDhhmmss YYYY = Four-digit Year MM = Twodigit Month DD = Two-digit Day hh = Two-digit Hour; 24-hour format mm = Two-digit Minute ss = Two-digit Second <i>Example: NASD012376523420030208101 512</i>
1.10 – TCR	Transaction Control Reference (TCR)	Leave blank for new submissions. Optional* for resubmissions. <i>*FINRA will record the TCR returned by the FBI and will enter the TCR for resubmissions.</i>
2.005 – RET	Retention Code	'N'
2.016 – SOC	Social Security Number	9 digits; no separators (hyphens, spaces) <i>Non-mandatory field - if supplied, 1 entry only is allowed. This is an FINRA restriction of the standard EFTS definition.</i>
2.027 – HGT	Height (feet and inches)	3 digits (Feet + Inches) Example '502' = 5 feet 2 inches
2.029 – WGT	Weight (pounds)	3 digits (Pounds)
2.031 – EYE	Eye Color	3-character standard NCIC code <i>FINRA EFP does not accept Unknown ('XXX') as an allowed eye color code. All other NCIC eye color codes are acceptable.</i>
2.043 – TSR	Type of Search Requested	'P'
2.073 – CRI	Controlling Agency Identifier	'DCSEC000Z'
2.084 – AMP	Amputation Code	2 characters: 'XX' (amputated or bandaged) 'UP' (unprintable) Note that records for individuals, who have all ten fingers amputated, bandaged, or unprintable, may not be sent via electronic submission. FINRA has a separate process for these cases. Fingerprint systems should be configured to enforce this prohibition and to ensure that any record containing missing images includes an associated annotation code.

Electronic Fingerprint Submission Certification Procedures

In addition to the standard EFTS fields, FINRA has specified the following Mandatory and Optional additional data elements in each fingerprint record.

Table 4-2. FINRA-Required Additional EFTS Fields

FINRA Data Element Tag	Data Element Field	Content / Format Specification	Mandatory / Optional
2.901	Bar Code Number	10-digit numeric; 1 occurrence <i>Bar code labels must be requested from</i>	Mandatory
2.902	Applicant CRD Number	8-characters; 1 occurrence	Optional <i>Leave blank if no CRD # assigned yet.</i>
2.903	Firm CRD Number	8-characters; 1 occurrence	Mandatory
2.904	Last Name	50-characters; 1 occurrence Alpha plus special characters: <space>, <dash>, <ampersand>	Mandatory
2.905	First Name	50-characters; 1 occurrence Alpha plus special characters: <space>, <dash>, <ampersand>	Mandatory
2.906	Middle Name	50-characters; 1 occurrence Alpha plus special characters: <space>, <dash>, <ampersand>	Optional
2.907	Firm Name	128-characters; 1 occurrence Alpha plus special characters: <space>, <dash>, <ampersand>	Mandatory
2.908	Firm Street Address 1	50-characters; 1 occurrence Alphanumeric plus special characters	Mandatory
2.909	Firm Street Address 2	50-characters; 1 occurrence Alphanumeric plus special characters	Optional
2.910	Firm City	40-characters; 1 occurrence Alpha plus special characters <space>, <dash>, <ampersand>	Mandatory
2.911	Firm State	2-characters; 1 occurrence <i>Standard NCIC Code</i>	Optional
2.912	Firm Country	2-characters; 1 occurrence <i>Standard NCIC Code</i>	Mandatory

2.913	Firm Postal Code	11-characters; 1 occurrence	Optional
-------	------------------	-----------------------------	----------

V. S/MIME Encoding

S/MIME encoding is a form of encryption that is required to protect confidential personal information contained in fingerprint records when the records are transmitted over the Internet. The S/MIME encoding process is performed automatically by the electronic fingerprint system prior to transmission.

A. S/MIME Terminology

Digital Certificate: A “*Certificate*” is a binary data file that can absolutely identify the sender of a message such as an SMTP e-mail message, which is transmitted over a public or private network. Digital Certificates contain public and private keys and are usually purchased and controlled by third-party vendors, such as Entrust. Digital Certificates have a lifetime of 365 days from creation date, and must be renewed annually by their user.

Certificate Authority (CA): A “*Certificate Authority*” or “*Root Certificate*” is a digital certificate from a third-party vendor, such as Entrust, that can be used to validate any digital certificates issued by the same vendor and used on another system.

B. S/MIME Process

The S/MIME encoding process involves a series of steps that are required to establish message security for each message transmission. The steps in the process involving the originating electronic fingerprint system (the “sender”) and the FINRA EFP system (the “recipient”) are listed below:

- 1) The sender creates a standard e-mail message containing the EFTS-formatted fingerprint record.
- 2) The message is “signed” or converted into a pkcs#7-formatted (Public-Key Cryptography Standards) message blob using the sender’s digital certificate. This step allows the recipient to know and verify the sender’s identity.
- 3) The sender validates the local copy of the recipient’s digital certificate using the root certificate.
- 4) After successful validation of the recipient’s digital certificate, the sender uses it to encrypt the signed message blob using a private key and then encrypts the private key using the recipient’s public key. The encryption methods currently supported in the S/MIME standard include DES, Triple-DES, and RC2. **FINRA will implement Triple-DES encryption.**
- 5) The newly signed and encrypted message blob is attached to a new SMTP message, which is sent to the recipient.
- 6) The recipient retrieves the message from its server via POP3. The recipient checks for a certificate on its system matching the Internet mail address of the sender and attempts to validate that certificate using the root certificate.
- 7) If the sender’s certificate exists and is valid, the recipient decrypts the included private key using its own public key. It then uses the decrypted private key to decrypt the remaining message blob. The recipient now has the signed message

blob.

- 8) The recipient extracts the original message from the signed message blob using the sender's digital certificate. In the case of FINRA, the server would now have the sender's EFTS file to process.

C. S/MIME Software

Electronic fingerprint system vendors may obtain specific implementation details and/or a copy of FINRA's S/MIME software from FINRA's EFP vendor, Cogent Systems. For information, contact Tim Biggs (jennyhu@cogentsystems.com).

VI. Record Retention

Broker-dealers are required to maintain certain records pursuant to the Securities Exchange Act of 1934 (Exchange Act) and the rules thereunder. In particular, Exchange Act Section 17(f)(2) and Rule 17 f-2 thereunder identify specific information broker-dealers must maintain in connection with the processing of fingerprint cards. Under Exchange Act Rule 17f-2(d)(1), a broker-dealer must maintain the processed fingerprint card or a substitute record if the card is not returned after processing, in addition to any information received from the Attorney General or its designee with respect to that processing (i.e., the disposition and details of the fingerprint check). The "substitute record" must contain:

- (1) name of the person whose fingerprint card was submitted to the Attorney General of the United States;
- (2) the name of the member of a national securities exchange, broker, dealer, registered transfer agent or registered clearing agency that submitted the fingerprint card;
- (3) the name of the person or organization that rolled the fingerprints;
- (4) the date on which the fingerprints were rolled; and
- (5) the date the fingerprint card was submitted to the Attorney General of the United States.

FINRA is identifying the requirements and specific data elements here in the event a broker-dealer wishes to satisfy these requirements through its electronic fingerprint system (by capturing the information through its electronic fingerprint system functionality), rather than through traditional imaging or other reproduction of the cards or information. Each broker-dealer is responsible for meeting applicable record retention requirements.