DirectTrust Governmental Trust Anchor Bundle

Standard Operating Procedure

Change Control

Date	Version	Description of changes
1-February-2018	1.4	Clarification of terms and requirements
15-December-2016	1.3	Added requirement of HISPs already in the accredited trust anchor bundle to undergo HISP to HISP interop testing.
1-December-2016	1.2	Edits to correct name of DirectTrust-EHNAC Accreditation programs.
17-March-2016	1.1	Removing FIPS module information in attestation requirements.
4-February-2016	1.0	Final version approved by DirectTrust Trust Anchor Approval Committee and DirectTrust Policy Committee.
3-February-2016	0.4	Updated requirements on LoA3 authentication.
8-December-2015	0.3	Revised with suggestions and updated requirements from FHA.
5-November-2015	0.2	Draft after modifications by the Trust Anchor Approval Committee, beginning in September, 2015.
9-July-2015	0.1	Initial draft.

Scope

This document defines the process for including X.509 digital certificate trust anchors into the DirectTrust Governmental Trust Anchor Bundle for the purpose of enabling Direct Messaging between governmental agencies and the private sector. It also includes the full set of criteria for a trust anchor to be included in the bundle.

Value Proposition

There is mutual benefit for members of both governmental agencies at the federal or state levels and private sector health care organizations to exchange health information between the two communities via the Direct Messaging standard and protocols. DirectTrust members in the private sector already utilize the DirectTrust Accredited Trust Anchor Bundle to support exchange of Direct messages and attachments among their subscribers and end users. Several federal agencies have expressed interest in becoming members of the DirectTrust community, and they want to rely upon the DirectTrust Security and Trust Framework, accreditation programs, and trust bundle operations for the purpose of facilitating trusted relationships between themselves and private sector HISPs and their customers.

However, because these federal agencies generally require security and trust in identity policies and controls that are stronger than those supported by the DirectTrust framework and as asserted by inclusion in the DirectTrust Accredited Trust Anchor Bundle, there is a recognized need for a new trust bundle that captures these additional requirements. (As reference, see the relevant documents "Federal Health Architecture Directed Exchange Guidelines," May, 2015, and the "Federal Health Architecture Federal Directed Exchange Trust Framework," January, 2015.)

The key value proposition of the DirectTrust Governmental Trust Anchor Bundle is, therefore, to facilitate voluntary interoperable Direct Messaging exchange between governmental agencies and private sector members of the DirectTrust community. The DirectTrust Governmental Trust Anchor Bundle creates a single community of trust shared by participating governmental agencies and private sector provider organizations.

Roles

Roles for the DirectTrust Governmental Trust Anchor Bundle are inherited from the DirectTrust Accredited Trust Anchor Bundle and Trust Anchor Approval Committee charter documents.

Definitions

Term	Definition

FHA	The Federal Health Architecture (FHA) is an E-Government Line of Business (LoB) initiative designed to bring together the decision makers in federal health Internet technology (IT) for inter-agency collaboration -- resulting in effective health information exchange (HIE), enhanced interoperability among federal health IT systems and efficient coordination of shared services. FHA also supports federal agency adoption of nationally-recognized standards and policies for efficient, secure HIE.

Procedure

Trust Anchor Approval Committee Procedure

Approval committee procedures for the DirectTrust Governmental Trust Anchor bundle are inherited from the DirectTrust Accredited Trust Anchor bundle and Trust Anchor Approval Committee charter documents.

Trust Anchor Inclusion

The procedure for including Health Information Service Providers (HISP) trust anchors into the DirectTrust Governmental Trust Anchor Bundle includes the following high-level steps.

1. Trust anchor and required artifact submission
2. Baseline trust anchor approval
3. Validation of attestation
4. Interoperability testing
5. Final anchor approval
6. Trust bundle generation and publication

Step 1: Trust anchor and required artifact submission

After a HISP and the utilized Certificate Authority and Registration Authority entities have achieved DirectTrust-EHNAC Accreditation for HISPs, and the appropriate network fees as determined by DirectTrust have been paid, the HISP may apply for inclusion into the Governmental Trust Anchor Bundle.

To initiate the process, the HISP fills out and submits all requested materials to the DirectTrust Trust Network Services web site at http://services.directtrust.org/. Submitted materials include:

- All trust anchor files

- Sample end entity certificate(s) pairs chaining to each trust anchor. Each pair must consist of one certificate asserting the digital signature key usage attribute and the other asserting the key encipherment key usage attribute.
    - An example of each certificate type that will be issued by the trust anchor should be submitted. Certificates types include:
        - Org level certs
        - Address level certs
    - Example of Address level cert with validated National Provider Identifier (for NPI holders only). Both provider and organization NPIs are valid. HISPs are not required to deploy Address level certificates with validated NPI attributes in production, but MUST prove that they have the ability to do so in the correct format.
        - Attestation must be included in the HISP/CA/RA document profile outlining how the validation step requirements are met.
    - If the sample end entity certificates do not directly chain to the submitted anchors, all intermediate issuing certificates in the certificate chain between the anchors and end entity certificates must be submitted.
        - A list of all current intermediate CAs. This list must contain the common name of each intermediate CA.
    - All necessary certificates that build a path chain from the anchor up to a specific FBCA cross certificate. The format of the chain will be in the form of a PKCS7 container of certificates.

- HISP/CA/RA profile document. This includes attestation to additional HISP operational procedures enumerated in Step 2 and 3.

All required artifacts must be submitted no later than the end of business hours (EOB, 5 PM ET) two business days before the next Trust Anchor Approval Committee (TAAC) meeting in order to be placed on the next meeting's agenda. For example, if the approval committee meets on a Thursday, all artifacts must be submitted by EOB on the Tuesday prior to the meeting. At the discretion of the Trust Anchor Approval Committee, artifact corrections and/or addendums may be accepted after the submission deadline, but must be received by the Committee prior to the approval Committee meeting.

Step 2: Baseline Trust Anchor Approval Process and Criteria

After the anchors have been submitted, the Trust Anchor Approval Committee will review the HISP's documents and the submitted anchors for baseline approval. The committee will evaluate the HISP and the submitted trust anchor(s) for compliance against the trust bundle profile criteria. Approval criteria consists of the following:

<u>Requirements For All Entities</u>

- The HISP, the trust anchor's Certificate Authority, and Registration Authorities used to validate identities MUST be in compliance with all of the requirements of the DirectTrust Accredited Trust Bundle. This bundle inherits all requirements enumerated by the DirectTrust Accredited Trust Bundle. NOTE: Members of the Governmental Trust Bundle are not required to be a member of the Accredited Trust Bundle.

HISP Requirements

- HISP controlled private keys may be protected in 2 possible abstract designs:
  - Private keys may be stored and protected on a Federal Information Processing Standards (FIPS) 140 level 2 minimum cryptographic module.
  - Private keys may be stored outside of a cryptographic module, but must be protected with a secret key of appropriate strength stored on a FIPS 140 level 2 minimum cryptographic module.
- Cryptographic Operations:
  - All cryptographic functions that utilize the asymmetric private key MUST be performed on a FIPS 140 level 2 minimum cryptographic module, and the private key may only be decrypted and activated when loaded into the module. All other cryptographic operations may be performed on a FIPS 140 level 1 module or equivalent standards recognized by the community.

- Only 140-2 approved algorithms for Secure/Multipurpose Internet Mail Extensions (S/MIME) operations may be used.

- Authentication
  - Direct users of address bound certificate must have the capability to provide evidence of authentication level by the end of December 31, 2017. Certain federal agencies will require NIST LoA3 authentication.

All sent messages MUST be protected using message wrapping as required in the current version of the DirectTrust Health Information Service Provider (HISP) Policy. This requirement MUST be used for both organizational and address type certificates.

Certificate Authority Requirements

- Trust anchors submitted by HISPs for inclusion into the bundle MUST meet the following requirement:
  - The anchor MUST have a trust path through a cross certificate to the Federal Bridge Certificate Authority (FBCA) at FBCA medium or higher.

  - The anchor must not be the cross certificate.
  - No certificates in the trust path below the anchor may have cross certification.

- All end entity certificates must be issued at FBCA Medium or higher.

- All end entity certificates issued by the trust anchor (or sub anchors) MUST be in compliance with FIPS-186. Specifically, all certificates asserting the digitalSignature key usage bit must only be used for signature and verification purposes.
  - Practice Note: Legacy Direct dual use signing and encryption certificates do not meet the FIPS-186 requirement.

The baseline approval process includes a checklist of items that MUST be reviewed by the approval committee. Each item in the checklist MUST be reviewed and signed off by two members of the approval committee or the appropriate member of DirectTrust staff.

HISPs will be notified of their baseline approval status by the Approval Committee within 10 business days of trust anchor submission.

Step 3: Validation of Attestation

The TAAC will review the attestation statements in the submitted HISP/RA/CA profile document for compliance with the additional HISP requirements defined in section 2 of this document. Specifically, HISP attestation will be evaluated for compliance with the following requirements:

- Use of a certified FIPS 140 Level 2 cryptographic module for private key protection and for cryptographic operations when utilizing RSA private key material.

Attestation to FIPS requirements will be confirmed at the HISP's next DirectTrust-EHNAC Accreditation audit. At the time of writing, DirectTrust-EHNAC Accreditation does not audit these criteria (DirectTrust-EHNAC Accreditation will need to update its accreditation requirements to include these criteria). When DirectTrust-EHNAC Accreditation does audit FIPS criteria, validation of DirectTrust-EHNAC Accreditation will suffice for attestation.

HISPs will be required to submit compliance to FIPS requirements after each DirectTrust-EHNAC Accreditation audit to the trust bundle administrator. On DirectTrust-EHNAC Accreditation audit "off years" HISPs will be required to submit attestation of continuing FIPS compliance to the trust bundle administrator due on the anniversary of their DirectTrust-EHNAC Accreditation audit.

Step 4: Interoperability Testing

Any HISP that applies to the DirectTrust Governmental Trust Anchor Bundle that is not already a member of the DirectTrust Accredited Trust Anchor Bundle must successfully perform interoperability testing via the processes defined in the DirectTrust Accredited Trust Anchor Bundle standard operating procedure document. Interoperability testing for this requirement may not apply more restrictive than that of the Accredited Trust Anchor Bundle. In other words, more restrictive policies may not be applied for the purpose of interoperability testing. This requirement may change as more HISPs are included into the DirectTrust Governmental Trust Anchor Bundle.

Any HISP that applies to the DirectTrust Governmental Trust Anchor Bundle that is already a member of the DirectTrust Accredited Trust Anchor Bundle must successfully perform interoperability testing via the processes defined in the DirectTrust Accredited Trust Anchor Bundle standard operating procedure document except the number of HISPs will be reduced to 5 and successful testing against at least 4 HISP must be executed. All 5 tests HISPs will be selected by DirectTrust. The list may be biased but will be a diverse selection of HISPs testing the capability of the applicant's system with other HISP implementations.

All HISPs must perform additional interoperability testing against a DirectTrust control HISP to validate compliance with the HISP and CA requirements defined in section 2 of this document. Interoperability testing against the control HISP will consist of the same steps as those outlined in the DirectTrust Accredited Trust Anchor Bundle standard operating procedure document, but will validate the following additional criteria:

- Proper use of message wrapping for messages sent from the HISP under review.
- Validation of proper key usage. Specifically the process will validate the HISP under review:
    - Only signs messages with certificates that assert the digital signature key usage bit and only encrypt messages with certificates that assert the key encipherment key usage bit.
    - Uses a different key pair for encryption and digital signatures when single use certificates are utilized.
- Validation of use of approved algorithms for S/MIME operations.

DirectTrust will generate the artifacts for the additional interoperability testing.

After interoperability testing is successfully completed, the HISP under review will submit their generated testing artifacts to the Trust Anchor Approval Committee for final approval. Artifacts will be emailed to the DirectTrust Administrator.

Step 5: Final Approval

Upon completion of interoperability testing, the Trust Anchor Approval Committee will review the submitted anchor(s) again for final approval. The committee will review the results of interoperability testing and determine if all criteria have been successfully met as defined by the interoperability testing measures. If it is determined that the criteria has not been met, then the HISP must continue interoperability testing until all issues are resolved.

The Committee also reserves the right to revaluate the criteria of baseline approval if additional issues are discovered during in the interoperability-testing phase. If baseline issues are found at this stage that result in a denial, then the HISP must go back through baseline approval and interoperability testing.

Step 6: Trust bundle generation and publication

Upon successful final anchor approval, the Trust Bundle Administrator will move the trust anchor(s) into the trust bundle anchor repository location. This repository location contains a collection of all approved trust anchors in the DirectTrust Governmental Trust Anchor Bundle, and is regularly renewed and updated.

The Trust Bundle Administrator will then generate a new trust bundle file that includes all existing and the newly approved trust anchors using the necessary tooling. The new trust bundle will use the identical file name of the existing bundle.

Before the new trust bundle is published to the publicly accessible URL, the existing trust bundle will be backed up into a trust bundle archive location. After the existing trust bundle has been archived, the new trust bundle will be moved to the trust bundle publication URL.

Lastly, the trust bundle details page will be updated with all required information including but not limited to:

- HISP name
- HISP ID
- Trust anchor(s) common name
- CA operator name
- RA operator name
- Trust anchor(s) compliance information
    - DirectTrust CP version compliance
    - CP URL and CPS URL
- Issued certificate types

Post Approval Operations

All anchors in the DirectTrust Governmental Trust Anchor Bundle must be validated daily (every 24 hours) as certificates the can create a valid chain to an FBCA cross certificate. Chaining requirements include but are not limited to:

- A cryptographically valid chain following the AIA extensions of each link in the chain from the submitted trust anchor to the Federal Common CA.
- At each certificate in the chain, the certificates must be validated against the certificate's CRL.
- Each certificate in the chain must have a valid not before and not after time range at the time the validation is performed.

If one or more anchor certificates fail this validation, a notification will be sent immediately to the DirectTrust Governmental Trust Anchor Bundle administrator. Upon notification, the administrator will take the following action:

- The DirectTrust Governmental Trust Anchor Bundle administrator will attempt to manually verify that the notification resulted from a valid failure condition.
- If the failure condition is verified, the DirectTrust Governmental Trust Anchor Bundle administrator will notify the affected HISP and CA parties.
- Upon sending the notification to the HISPs and CAs, the parties will have 1 full business day to take corrective action and notify the DirectTrust Governmental Trust Anchor Bundle administrator that the issue(s) has been resolved.
- The DirectTrust Governmental Trust Anchor Bundle administrator will validate that the failure condition has been resolved.
- If the failure condition has not been resolved within one full business day of the DirectTrust Governmental Trust Anchor Bundle administrator sending the initial notification to the HISP and CA parties, then the affected anchors will be removed from the bundle.

If anchors are removed from the bundle due to validation failures, the HISPs will be required to resubmit their anchors to the Trust Anchor Approval Committee to be re-included into the bundle, but will only need to demonstrate compliance with the Certificate Authority Requirements section of this document.

Disputes of Compliance

Over the course of the life of the DirectTrust Governmental Trust Anchor Bundle, disputes of an entity's compliance with either its accreditation responsibilities/status or requirements of this Standard Operating Procedure and bundle profile may occur. In such cases, any complaints or disputes will be referred to and managed according to the

dispute resolution process as specified in the DirectTrust Federated Services Agreement to which all participants in the Accredited Trust Anchor Bundle are signatories.

Upon the outcome of the dispute resolution process or at the direction of the DirectTrust Board of Directors or its designee, the Trust Anchor Approval Committee will re-evaluate the status of an entity's inclusion in the trust bundle. Such outcomes may result in the removal of an anchor from the trust bundle.

Removal From Trust Bundle

Trust anchors will be removed from the Governmental Trust Bundle under any one of the following conditions:

- An entity no longer holds DirectTrust Accreditation for HISPs status.
- An entity does not successfully complete ongoing interoperability testing.
- An entity is no longer party to a valid Federated Services Agreement.
- The outcome of the dispute resolution process indicates that an entity is not in compliance with the requirements of this bundle.
- Action by the DirectTrust Board of Directors.
- An anchor is out of compliance with the post approval operations requirements.

Appendix 1 – FHA To Bundle Requirements Matrix

FHA Requirement	Bundle Requirement
Policy calling for the elimination of Dual-Use certs by end of 2015.	Use of end entity certificate(s) pairs chaining to each trust anchor. Each pair must consist of one certificate asserting the digital signature key usage attribute and the other asserting the key encipherment key usage attribute. All end entity certificates issued by the trust anchor (or sub anchors) MUST be in compliance with FIPS-186. Specifically, all certificates asserting the digitalSignature key usage bit must only be used for signature and verification purposes.
Requires a BAA with HISP and supported entities.	Required by the HISP Policy Document v1.0 and DirectTrust-EHNAC Accreditation.
The organization or individual to whom a domain or address bound certificate is issued must be identity proofed at Federal Bridge Medium assurance or higher.	The DirectTrust Governmental Trust Bundle requires that all persons be identity proofed at FBCA medium or higher.
Messages using domain bound certificates MUST use message wrapping.	**All** sent messages MUST be protected using message wrapping as required in the DirectTrust Health Information Service Provider (HISP) Policy v 1.0.
Certificates MUST be issued by an FBCA cross certified certificate authority at FBCA medium or higher.	The anchor MUST have a trust path through a cross certificate to the Federal Bridge Certificate Authority (FBCA) at FBCA medium or higher.
Strong private key protection.	HISP controlled private keys may be protected in 2 possible abstract designs: • Private keys may be stored and protected on a Federal Information Processing Standards (FIPS) 140 level 2 minimum cryptographic module.

	• Private keys may be stored outside of a cryptographic module, but must be protected with a secret key of appropriate strength stored on a FIPS 140 level 2 minimum cryptographic module. • All cryptographic functions that utilize the asymmetric private key MUST be performed on a FIPS 140 level 2 minimum cryptographic module, and the private key may only be decrypted and activated when loaded into the module.
Authentication	End users must be authenticated to the edge system using multifactor authentication. • Direct users of address bound certificate must have the capability to provide evidence of authentication level by the end of December 31, 2017. Certain federal agencies will require NIST LAO3 authentication.

Appendix 2 – NPI Validation Steps

When an applicant requests that an NPI be included in a Direct certificate, the following steps will be taken to validate it appropriateness:

1. A look up of the claimed number in the NPI Registry (currently NPPES) to confirm it exists and is associated with the applicant by ensuring full name and address details in the Registry match the applicant's current details to be validated as part of the Direct certificate issuance.

    a. If there is no match of data, request that the data in the Registry be updated to match current name and address as verified by ID Proofing process. NOTE: Certificate cannot be issued unless there is an exact match.

    b. Matching details also requires that NPI Type i.e. Individual (1) or Organization (2), be appropriate in context of the requested certificate in terms of the Direct address that the NPI is being bound to in the certificate.

2. The RA will verify control of the claimed NPI details by the applicant before the Direct certificate is issued. The following example (or a comparable process) is acceptable for this purpose: RA shall send an authentication code to a registered address in the Registry which the administrator must demonstrate possession back to the RA before the Direct certificate is approved for issuance.