DirectTrust Accredited Trust Anchor Bundle

Standard Operating Procedure

Change Control

Date	Version	Description of changes
13-December - 2018	1.9	Adding bundle interop testing for additional certificate profiles per anchor. Adding all ATAB members to the testing pool. Removal of Step 7a Change Org level certs to Domain Bound certs and Address level certs to Address Bound certs
1-February-2018	1.8.1	Inserted “any one of” under the section Removal from Trust Bundle
25-January-2018	1.8	Clarification of terms and requirements
9-August-2017	1.7.1	Removal of the word “administrative” under the section Removal from Trust Bundle
14-June-2017	1.7	Adding requirements of CP 1.3 after its go live date. Editing the DirectTrust accreditation program.
1-Dec-2016	1.6	Edits to correct name of DirectTrust-EHNAC Accreditation programs.
1-Sept-2016	1.5	Added requirements for post approval testing during initial interop testing for bundle admittance.
19-May-2016	1.4	Adding requirements for annual retesting.

		Added language concerning “in effect” timing of policy documents.
26-June-2015	1.3	Added requirements for category OID usage. Sunset the usage of CP 1.1
7-May-2015	1.2	Cleaned up language, grammar, spelling. Updated procedural language.
21-July-2014	1.1	Baseline approval requires signoff by two committee members to each line item in a checklist.
20-June-2014	1.0	Initial 1.0 release Updated submission procedure to reference new Trust Network Service website.
24-Apr-2014	0.9	Cleaned up language, grammar, and spelling.
17-Apr-2014	0.8	Formally defined the interoperability HISP pool. Modified the selection process of HISPs for interoperability testing to allow for HISPs to choose 5 of their own testing partners from the interoperability HISP pool.
10-Apr-2014	0.7	Included provisions for a HISP under review to request a new DirectTrust-EHNAC accredited HISP. Specified artifacts of proof for interoperability testing.
03-Apr-2014	0.6	Moved the anchor verification process to occur before the approval committee takes up the anchors. Moved the approval committee process into its own procedural section. Added interoperability testing requirements Added language to allow the approval committee to review baseline requirements after interoperability testing.

		Tightened and simplified language in the dispute resolution process to reference the Federated Services Agreement.
06-Mar-2014	0.5	Updated name of SOP to remove “Fully.” Added role of Applicant. Updated reference to the Federation Agreement to now reference the DirectTrust Federated Services Agreement. Added approval step for interoperability testing Added rules for final anchor and operational approval
19-Dec-2013	0.4	Updated the name of the bundle and federation agreement for fully accredited HISPs. Included the requirements for paying bundle administration fees. Categorizes bundle profile requirements by entity.
25-Nov-2013	0.3	Re-added the requirement of a signed federation agreement when available. Specified that non-self entity relationships will be verified via phone call to an authorized member of the CA and/or RA.
11-Nov-2013	0.2	Included bundle requirements discussed by the trust anchor bundle operations committee. Includes relationship validation, CP compliance, and removal of the federation agreement requirement, dispute resolution, and anchor removal.
10-Oct-2013	0.1	Initial draft.

Scope

This document defines the process for including X.509 digital certificate trust anchors into the DirectTrust Accredited Trust Anchor Bundle. It also includes the full set of criteria for a trust anchor to be included in the bundle.

Value Proposition

This DirectTrust Accredited Trust Anchor Bundle has as participants Health Information Service Providers (HISPs), Certificate Authorities (CAs), and Registration Authorities (RAs) that have achieved accreditation through the either the DirectTrust Accreditation Program or through DirectTrust-EHNAC Accreditation.

All participants in this bundle have not only successfully achieved DirectTrust Accreditation, but have also met the set of profiled requirements described by this document. This bundle assures that all anchors and associated end-entity certificates represented are in use by a DirectTrust Accredited HISP.

The key value proposition of the DirectTrust Accredited Trust Anchor Bundle is to facilitate interoperable Direct exchange between HISPs in a uniform and scalable manner that is consistent with industry best practices for security and trust, thereby avoiding the need for further one-off negotiations between relying parties who are participants in the bundle.

Roles

Trust Bundle Officer: Responsible for the executive decisions relating to trust bundles and trust anchors residing within a specific trust bundle. Decisions include, but are not limited to: approval of trust bundle profiles; approval of a trust anchor's inclusion within one of more or trust bundles, and approval of a trust anchor's removal or suspension within one of more trust bundles. Specific executive decisions may require the concomitant approval of an appropriate committee designated by DirectTrust. However, the trust bundle officer must ultimately sign off on all decisions covered by this role. This role is played by the DirectTrust CEO or a designee appointed by the DirectTrust CEO.

Trust Bundle Administrator: Responsible for the operational aspects of trust bundles. Responsibilities include, but are not limited to: verification of trust anchor integrity submitted by a HISP; maintaining a repository of approved trust anchors, and generation and publication of trust bundles. The administrator is also responsible for content generation and maintenance of the trust bundle web site.

Trust Anchor Approval Committee: The committee is a permanent Advisory Committee to the DirectTrust Board of Directors. Membership is defined in Trust Anchor Approval

Committee Charter. This Committee is responsible for evaluating the compliance criteria of a HISP submitting a trust anchor to one or more trust bundles. Evaluation includes validating that a HISP and its submitted trust anchor(s) meet all of the inclusion criteria of a trust community profile. The TAAC is also charged by the DirectTrust Board of Directors with assisting in policy breach identification, notification, and resolution; and to represent the Board when necessary on operational and accreditation matters relating to trust anchors.

Applicant: A DirectTrust accredited HISP submitting one or more trust anchors for consideration by the Trust Anchor Approval Committee.

Referenced Documents

Implementation Guide for Direct Project Trust Bundle Distribution

Definitions

Term	Definition
Trust Anchor	An X.509 certificate that is used to validate the first certificate in a sequence of certificates. The trust anchor public key is used to verify the signature on a certificate issued by a trust anchor CA. The security of the validation process depends upon the authenticity and integrity of the trust anchor. For trust anchors included in trust bundles managed by DirectTrust, the trust anchor MUST have the basic constraint attribute set to TRUE.
Trust Community:	Trust Communities are formed by organizations electing to follow a common set of policies and processes related to health information exchange. Examples of these policies include identity proofing policies, certificate management policies, and HIPAA compliance processes.
Trust Community Profile	A Trust Community can create multiple sets of policies and processes and enforce these sets of policies on selected organizations that wish to voluntarily conform to them. For example, a Trust Community could create a set of policies and processes that organizations agree to conform to support Direct exchange associated with use cases in which providers exchange personal health information during coordination and transitions of care and for referrals. If the policies and processes agreed to include the use of Direct exchange between providers and patients/consumers, a different profile might be created and used. These sets of policies and processes are called Trust Community Profiles and are intended to be transparent and open to public view. The word “Profile” indicates a distinct set of policies and processes.

Trust Bundle	A collection of X.509 digital certificate trust anchors that meet a common set of minimum policy requirements within a Trust Community Profile. Relying parties may include the trust anchors in the bundle into their Security and Trust Agent (STA) implementations (trust stores) with confidence that each trust anchor adheres to the policies set by the Trust Community managing the bundle.
Relying Party	An individual or entity that has received information that includes a Certificate and a digital signature verifiable with reference to a public key listed in the Certificate, and is in a position to rely on them for the purpose of Directed exchange.
Certificate Profile	Certificate profiles are defined and enumerated by the DirectTrust certificate profiles documents. Certificate profiles in the context of an anchor submission are enumerated by the subset of certificate profiles that describe end entity certificates. Certificate profiles are not sub-categorized beyond what is enumerated in the DirectTrust certificate policy documents. For example, in CP v1.3, the address certificate profile is not sub-categorized by patient and provider certificates.

Procedure

Trust Anchor Approval Committee Procedure

A quorum for the purposes of the Trust Anchor Approval Committee meeting consists of 50 percent or greater of the whole Committee. Assuming a quorum is achieved, the meeting will be conducted using parliamentary procedure rules.

Approval is achieved by a majority of affirmative votes of the members. Committee members MUST recuse themselves from voting if they are affiliated with any of the entities under consideration. If a committee member is recused, the number of required positive votes for approval is not reduced.

A Committee member may delegate another Committee member as a proxy for the purposes of anchor approval voting. A single Committee member may possess two or more votes via proxy; however, a single Committee member may not possess a majority of votes. A delegating member assigns his or her proxy privilege by emailing their proxy nomination to the entire Committee list prior to the subsequent meeting. A proxy is only valid for the immediate subsequent meeting, and an email is required for each following meeting.

Trust Anchor Inclusion

The procedure for including HISP trust anchors into the DirectTrust Accredited Trust Anchor Bundle includes the following high-level steps.

1. Trust anchor and required artifact submission
2. Baseline trust anchor approval
3. Interoperability testing
4. Final anchor and operational approval
5. Handoff to trust bundle administrator
6. Trust anchor verification
7. Trust bundle generation and publication

Step 1: Trust anchor and required artifact submission

After a HISP has achieved DirectTrust Accreditation and the utilized CA and RA entities have achieved DirectTrust-EHNAC Accreditation, the HISP submits its trust anchor(s) for inclusion into the trust bundle by filling out and submitting 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) chaining to each trust anchor
        - An example of each certificate type that will be issued by the trust anchor should be submitted. Certificates types include:
            - Domain Bound certificates
            - Address Boundcertificates
    - 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.
- HISP/CA/RA profile spreadsheet
- Executed copy of the DirectTrust Federated Services Agreement from both the submitting HISP and the relied upon certificate authority. If the HISP and certificate authority represent the same entity, then only the single executed agreement is necessary.

DirectTrust reserves the right to require a method of submission of these documents, e.g. through a dedicated website upload process.

All required artifacts must be submitted no later than EOB two business days before the next Trust Anchor Approval Committee 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: Trust anchor verification

If trust anchors are submitted over a non-secure transport, out of band verification MUST be performed to ensure the integrity and validity of trust anchors. Verification in such cases is performed by the Trust Bundle Administrator via an over the phone verification with an authoritative member of the submitting HISP. The HISP member will verify the following attributes of the trust anchor(s):

- Trust anchor thumbprint
    - Thumbprint is the thumbprint attribute of the trust anchor
- Trust anchor subject (distinguished name) attributes
- Trust anchor issuer
- Trust anchor valid from and valid to dates

Although the trust anchor thumbprint is cryptographically sufficient for verification, the additional attributes are validated for additional assurance.

If the verification process is not successful due to inconsistencies in the artifacts submitted, the HISP will resubmit their artifacts to the designated submission location. Upon receipt, the Trust Bundle Administrator will discard the invalid trust anchor(s) and re-verify the new trust anchor(s). If the subsequent resubmission and verification are not successful, the Trust Bundle Administrator will engage the HISP submitter directly to facilitate alternative means of trust anchor submission.

Step 3: 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 have achieved DirectTrust Accreditation and/or DirectTrust-EHNAC accreditation.

  - The HISP, the trust anchor's Certificate Authority, and Registration Authorities used to validate identities MUST be listed as currently accredited entities on the DirectTrust web site. The previously mentioned website MUST be protected with an EV SSL certificate.

- The HISP, the trust anchor's Certificate Authority, and Registration Authorities used to validate identities MUST be in compliance with the most recently approved version of the DirectTrust HISP Policy. For the purposes of baseline approval, interoperability testing, and post approval testing, the approved HISP Policy goes into effect 90 days after approval by the DirectTrust Board of Directors. The most recently approved version of the HISP Policy also applies to existing entities in the bundle 90 days after approval by the DirectTrust Board of Directors. All anchors and end entity certificate MUST be in compliance with an active CP version.

HISP Requirements

- The HISP and the DirectTrust President and CEO MUST maintain an executed DirectTrust Federated Services Agreement.

- Required Network Services fees MUST be paid in full.

Certificate Authority Requirements

- The Certificate Authority, if a separate third party from the HISP, MUST have signed the DirectTrust Federated Services Agreement CA/RA Addendum.

- Trust anchors and end entity certificates submitted by the HISPs must adhere to the most recent active DirectTrust X.509 Certificate Policy (CP) at the time of submission. Trust anchors are considered for compliance under one of the two following provisions:

  - Trust anchor(s) in compliance with any CP allowed by this profile and the HISP is its own CA. This case implies a 1-1 relationship between the CA and the HISP meaning that certificates are only issued to entities within the single HISP (i.e. the CA does not issue certificates to other HISPs).

- Trust anchor(s) in compliance with any CP allowed by this profile where the CA may issue to multiple HISPs. In this case, the trust anchor under consideration may only issue to HISPs that are DirectTrust Accredited.

- All subjects or organizational representatives of organizations using end entity certificates issued by the CA issuing the trust anchor (also any ISSOs where a HISP is used) MUST be identity proofed using at minimum DirectTrust LoA 3 or an equivalent identity proofing process.

- All end entity certificates issued by the trust anchor (or sub anchors) must express in the certificate policies extension an entity category policy OID defined under the 1.3.6.1.4.1.41179.2 OID arc. For all anchors existing in the bundle before this requirement becomes effective, all newly issued end entity certificates MUST contain the entity category policy OID starting October 1st, 2015 and all existing end entity certificates MUST contain the entity category policy OID by January 1st, 2016.

- All HISPs holding end entity certificates issued by the CA issuing the trust anchor must have fulfilled the requirement to sign the DirectTrust Federated Services Agreement, i.e. the CA issuing the trust anchor may only issue certificates to subjects or organizational representatives that are served by a HISP that has signed the DirectTrust Federated Services Agreement.

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.

NOTE: CP 1.3 specifies additional policy OIDs to assert additional attributes such as accreditation status and issuing LoA. However, this requires relying parties to be able to process the policy OIDs. At the time of writing, this functionality is not available in the majority of HISPs. Future versions of this SOP may allow for CP 1.3 compliant CAs to issue to HISPs at non-accreditation statuses and LoAs lower than DirectTrust LoA 3.

NOTE: End entity certificates issued before their associated CP version's end of life date are allowed to remain in circulation and considered to be in compliance (as long as they are in compliance with all other requirements of this bundle profile) until they expire. Any certificate issued after the applicable CP version's end of life date is considered to be out of compliance with this bundle profile.

Upon baseline approval or denial by the Committee, the original submitter will be sent an email indicating the results of the Committee's decision. For trust anchors that are denied, detailed information will be included indicating the reasons for denial. If multiple trust anchors were submitted, it is possible that some trust anchors may be approved while others are not. For trust anchors that are baseline approved, the anchors will move forward in the process to interoperability testing.

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

Step 4: Interoperability testing

Upon baseline trust anchor approval, HISPs must complete interoperability testing to prove a reasonable level of operational competency and compliance. The Security and Trust Compliance workgroup continuously operates a matrix of interoperability testing among members of the DirectTrust community, and an interoperability HISP pool of DirectTrust Accredited members that have successfully connected with 80% of the other members of the matrix will be created for the interoperability-validation phase herein described.

The HISP will provide a Direct address per submitted anchor and submitted end entity certificate profile whose end entity certificate chains to the anchor(s) under review to the Trust Bundle Administrator. This address should be an address within a production environment that will be utilized for sending and receiving test Direct messages with other members of the DirectTrust network. The HISP's trust anchor will be placed in a temporary validation trust bundle that can be consumed by the HISPs in the interoperability HISP pool during the testing phase. The HISP's anchor will be removed from the validation trust bundle after the testing phase has been completed.

Interoperability testing will consist of bidirectional exchange of messages between the HISP under review using one of the submitted Direct addresses (i.e. only one submitted end entity certificate profile will be used for this set of testing) and 10 other DirectTrust Accredited HISPs. The 10 HISPs will consist of:

- 5 HISPs selected from the interoperability HISP pool chosen by the HISP under review.
- 5 HISPs randomly selected from the interoperability HISP pool. The trust bundle administrator will execute this selection process.

Bidirectional exchange consists of the following criteria:

- Successful sending of a message from the HISP under review to the DirectTrust Accredited HISP.

    - The message must be received and security and trust validated by the receiving HISP.
    - The receiving HISP must send back an MDN process message to the HISP under review.
    - The MDN processed message must be successfully received and security and trust validated by the HISP under review.
- Successful receipt of a message from the DirectTrust Accredited HISP to the HISP under review.
    - The message must be received and security and trust validated by the HISP under review.
    - The HISP under review must send back an MDN process message to the DirectTrust Accredited HISP.

The HISP under review must successfully complete bidirectional exchange with a minimum of 8 of the 10 DirectTrust Accredited HISPs, for an interoperability score of 80 percent or higher.

In addition, the HISP under review must successfully pass the tests required in the post approval section of this document using an address bound to a certificate from each submitted end entity certificate profile. NOTE: Performing the post approval tests does not remove the HISP's responsibility for performing the tests on its anniversary as described in the post approval testing section of this document.

If a HISP submits for approval any additional end entity certificate profiles under a currently approved anchor, the HISP will only be required to perform and successfully pass the tests required in the post approval section of this document using an address that is bound to a certificate that implements the end entity certificates profile(s) under review.

The HISP under review must compile artifacts from tests against each DirectTrust Accredited HISP as proof of successful bi-directional exchange as well as the post approval testing artifacts. Because retrieving artifacts from remote systems may be difficult, time consuming, and in some cases impractical, this required list is comprised of only artifacts that are in direct control of the HISP under review. These include:

Sending Messages:

- Proof of a message successfully sent from the HISP under review. This includes proof of security and trust validation.
- Proof of a receipt of the MDN processed message. This includes proof of security and trust validation and MUST show a correlation to the message ID of the originally sent message.

Receiving Messages:

- Proof of a message successfully received from the DirectTrust Accredited HISP. This includes proof of security and trust validation.
- Proof an MDN processed message successfully sent from the HISP under review. This includes proof of security and trust validation and MUST show a correlation to the message ID of the received message.

The medium, format, and contents of the artifacts are not specified, however they must deterministically demonstrate that the above stated criteria have been met.

In the event of an unsuccessful bidirectional exchange between the HISP under review and a DirectTrust Accredited HISP, the two parties should attempt to resolved interoperability issues and attempt a subsequent exchange. If interoperability issues cannot be resolved, the HISP under review may submit a request to the trust bundle administrator to replace the DirectTrust Accredited HISP with a different DirectTrust Accredited HISP. The request will be reviewed by the Trust Anchor Approval Committee and be either approved or denied at its discretion. If the committee approves the request, then a new DirectTrust Accredited HISP will be selected to replace the previous HISP. The HISP under review may only request at most 2 replacements during the duration of the approval process.

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

Step 5: Final anchor 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 have not been met, then the HISP must continue interoperability testing until all issues are resolved.

The Committee also reserves the right to reevaluate 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 Accredited 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 Testing

Over time, DirectTrust policies and industry standards continue to evolve in the pursuit of improved security, trust, and robustness. It imperative that HISPs in the Accredited Trust Anchor Bundle remain in compliance with the latest policies and standards. For these reasons, HISPs must complete ongoing interoperability testing to ensure that they remain in compliance with the Accredited Trust Anchor Bundle requirements.

Ongoing interoperability testing will be performed every two years on the "off years" of the HISP's DirectTrust recertification and will be completed during the anniversary month of the HISPs DirectTrust Accreditation. Testing will be executed against a DirectTrust test HISP and facilitated by the DirectTrust Trust Bundle administrator or designated DirectTrust representative, and the resulting test artifacts will be reviewed by the DirectTrust Trust Anchor Approval Committee. If the testing is not determined to be successful by the committee, the HISP under test will be notified of the deficiencies and be given 60 days to rectify all issues. On or before the 60 day period has expired, the HISP must perform the testing again, and the testing must then be deemed successful by the Trust Anchor Approval Committee. If the second testing attempted is not approved, the committee will determine appropriate action which may include

removal from the trust bundle. If the HISP is removed from the bundle, they will not be re-included until testing is completed again and approved by the Trust Anchor Approval Committee.

Disputes of Compliance

Over the course of the life of the DirectTrust Accredited 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 Accredited 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.