Subject: NATE Procedure for Onboarding to a Trust Profile			**Procedure #**: 3.d.1
Status: Approved		**Approved/Authorized By**: NATE Board of Directors	
Date Approved: 10/29/2013	**Effective Date**: 10/29/2013	**Version**: 1.0	**Pages**: 11

I. Purpose

This Procedure defines the process for administering the NATE Trust Bundles that define membership in the NATE Trust Community and conformance to NATE Trust Profiles.

II. Responsibilities

A. Member State Representative:

- Inform the Trust Bundle Coordinator when an organization has been determined to meet all requirements of a NATE Trust Profile and request that they be added to the appropriate NATE Trust Bundle.

B. Trust Bundle Coordinator

- Maintain and publish all NATE Trust Bundles.
- Add new NATE-Qualified Entities to the NATE Trust Bundles corresponding to the appropriate NATE Trust Profile when requested by a Member State Representative.
- Remove organizations from a NATE Trust Bundle when requested by a Member State Representative.
- Inform all NATE-Qualified Entities and all Member State Representatives of changes to a NATE Trust Bundle.

C. NATE-Qualified Entity

- Work with the Trust Bundle Coordinator to incorporate the NATE Trust Certificate in the appropriate NATE Trust Bundle(s).
- Complete testing.
- Install or update NATE Trust Bundles, as appropriate, when alerted of updates by the Trust Bundle Coordinator.

III. Procedure

This procedure comprises two parts:

1. The procedure for adding a new member to a NATE Trust Bundle, and
2. The procedure for removing a member from a NATE Trust Bundle.

A NATE Trust Bundle comprises the technical component of membership in the NATE Trust Community for a specific NATE Trust Profile. Therefore, the procedures for adding members to and removing members from a NATE Trust Profile equates to the procedures for adding NATE Trust Certificates to and removing NATE Trust Certificates from a NATE Trust Bundle.

A. Adding a Member to a Trust Profile

Precondition: A candidate NATE-Qualified Entity has made application to a Member State to be added to a NATE Trust Profile, and has been vetted by the Member State Representative.

Post-condition: The new NATE-Qualified Entity has been added to the appropriate NATE Trust Bundle.

1. The Member State Representative determines that a candidate NATE-Qualified Entity has met the policy and process requirements for a NATE Trust Profile and that its NATE Trust Certificate should be added to the corresponding NATE Trust Bundle.

   Rationale – The Member State Representative has the sole authority to determine whether a candidate NATE-Qualified Entity meets the policy and process requirements of a NATE Trust Profile.

2. The Member State Representative identifies a single trust bundle point of contact (POC) within the candidate NATE-Qualified Entity for all communications regarding Trust Bundle management, along with an email address that is regularly monitored by that POC.

   Rationale – Notification of changes to each NATE Trust Bundle will be communicated through email. The name and contact information of the POC, including an email address, should be collected by the Member State Representative as part of the application process of a candidate NATE-Qualified Entity.

3. The Member State Representative identifies a single testing POC within the candidate NATE-Qualified Entity for testing, along with an email address that is regularly monitored by that POC and a Direct address.

   Rationale – Each candidate NATE-Qualified Entity is required to test with other NATE-Qualified Entities. The name and contact information of the POC, including an email

address and Direct address, should be collected by the Member State Representative as part of the application process of a candidate NATE-Qualified Entity.

4. The Member State Representative contacts the Trust Bundle Coordinator by email instructing the Coordinator to add the new NATE-Qualified Entity to the appropriate Trust Bundle, providing the contact information of the trust bundle and testing POCs.

   Rationale – It is desirable for NATE to define a single point of contact – the Trust Bundle Coordinator – to manage the process for Trust Bundle Administration.

5. The Trust Bundle Coordinator contacts the trust bundle POC of the new NATE-Qualified Entity via email requesting that the NATE Trust Certificate be provided by return email. If the organization maintains a staging/testing system as well as a production system, NATE Trust Certificates are requested for both.

   Rationale – The presence of an organization's NATE Trust Certificate in a Trust Bundle is the sole technical indication of a NATE-Qualified Entity's membership in the NATE Trust Community and conformance with the policies and procedures of a NATE Trust Profile. Technical testing with other NATE-Qualified Entities will be accomplished using a staging Trust Bundle.

   Noteworthy: Since the NATE Trust Certificate is a public key, strong security is not required to transport it.

6. Each NATE Trust Certificate is inspected by the Trust Bundle Coordinator to verify conformance with requirements identified in NATE policies, if any. If defects are identified, the Trust Bundle Coordinator contacts the Member State Representative to report the failure and contacts the trust bundle POC to correct the defect(s) and resubmit the NATE Trust Certificate(s).

   Rationale – This may be the first technical check on meeting digital certificate requirements identified in policies and processes for a NATE Trust Profile, and issues should be reported to the Member State Representative. It is desirable to correct any defects before proceeding to technical testing.

   Noteworthy: A defect in the NATE Trust Certificate may indicate a deviation from policy and process requirements. The Member State Representative should determine whether failure at this step indicates that new NATE-Qualified Entity status should be revoked and this procedure should be halted.

7. The Trust Bundle Coordinator records the expiration of each NATE Trust Certificate and makes a note to remind the trust bundle POC of pending certificate expiration at least two weeks before any NATE Trust Certificate expires.

Rationale – Expired digital certificates cannot be used to enable secure exchange. Monitoring of certificate expiration should be part of standard Trust Bundle management.

Noteworthy: The NATE-Qualified Entity or its vendor should likewise monitor NATE Trust Certificate expiration dates.

8. The Trust Bundle Coordinator informs the trust bundle POC of successful verification, and adds the new staging/testing NATE Trust Certificate to the NATE Staging Trust Bundle. If no staging/testing NATE Trust Certificate is provided by the new NATE-Qualified Entity, the production NATE Trust Certificate is included instead.

   Rationale – Policies for NATE Trust Profiles require successful testing as part of the vetting process. Further testing with other NATE-Qualified Entities is required to verify that the Trust Bundle is functional and that the new NATE-Qualified Entity can interoperate with other NATE-Qualified Entities.

   Noteworthy: Production systems may have access to protected health information (PHI). Each organization should consider carefully what NATE Trust Certificates are included in the NATE Staging Trust Bundle.

9. The Trust Bundle Coordinator publishes the updated NATE Staging Trust Bundle.

   Noteworthy: NATE conforms to the *Implementation Guide for Direct Project Trust Bundle Distribution v1.0* for both content and transport of Trust Bundles. NATE also publishes a legacy format comprising NATE Trust Certificates in a ZIP compressed archive as an aid to organizations that have not yet implemented the standard. NATE may discontinue use of the legacy ZIP format at some future date.

10. The Trust Bundle Coordinator sends an email to the trust bundle POCs of all NATE-Qualified Entities, including the newly added organization, alerting them that the Staging Trust Bundle has been updated and testing may proceed.

    Rationale – NATE has elected to create such an out-of-band mechanism of alerting NATE-Qualified Entities of Trust Bundle updates to ensure that organizations that do not automatically update NATE Trust Bundles are alerted to the need for a manual update.

11. The Trust Bundle Coordinator sends testing POC contact information for all NATE-Qualified Entities in the Staging Trust Bundle to the testing POC of new NATE-Qualified Entity.

    Rationale – It is the responsibility of the new NATE-Qualified Entity to conduct testing before being added to a production Trust Bundle.

    Noteworthy: The Trust Bundle Coordinator must maintain a list of the testing POCs for all NATE-Qualified Entities.

12. The new NATE-Qualified Entity coordinates with other NATE-Qualified Entities to conduct testing with at least two NATE-Qualified Entities with vendors different than the new NATE-Qualified Entity.

    Rationale – Testing with other NATE-Qualified Entities that use different vendors and therefore, presumably, independent implementations provides a reasonable assurance that all standards have been implemented appropriately, and that the new NATE-Qualified Entity will be able to interoperate with most, if not all, other NATE-Qualified Entities.

13. The testing or trust bundle POC of the new NATE-Qualified Entity contacts the Trust Bundle Coordinator via email to confirm that testing is complete.

14. If the production NATE Trust Certificate of the new NATE-Qualified Entity was included in the NATE Staging Trust Bundle and the new NATE-Qualified Entity wishes to have it removed, the Trust Bundle Coordinator removes it, publishes the updated Trust Bundle, and sends an email to all the trust bundle POCs of all NATE-Qualified Entities, including the newly added organization, alerting them that the Staging Trust Bundle has been updated.

    Rationale – Production systems may have access to PHI. It is not desirable to continue to enable exchange between production systems and staging/testing systems that may have reduced security in place.

15. The Trust Bundle Coordinator adds the new production NATE Trust Certificate to the appropriate NATE Trust Bundle.

16. The Trust Bundle Coordinator publishes the updated NATE Trust Bundle.

    Noteworthy: NATE conforms to the *Implementation Guide for Direct Project Trust Bundle Distribution v1.0* for both content and transport of Trust Bundles. NATE also publishes a legacy format comprising NATE Trust Certificates in a ZIP compressed archive as an aid to organizations that have not yet implemented the standard. NATE may discontinue use of the legacy ZIP format at some future date.

17. The Trust Bundle Coordinator sends an email to the Board of Directors and the trust bundle POCs of all NATE-Qualified Entities that are members of the NATE Trust Profile, including the newly added organization, alerting them that the NATE Trust Bundle has been updated.

    Rationale – The *Implementation Guide for Direct Project Trust Bundle Distribution v1.0* does not call for any in-band or out-of-band notification of Trust Bundle changes, but instead places the responsibility for establishing the update schedule on the Trust Community member. Email will be used to contact the trust bundle POCs to ensure that all NATE-Qualified Entities update their trust stores promptly.

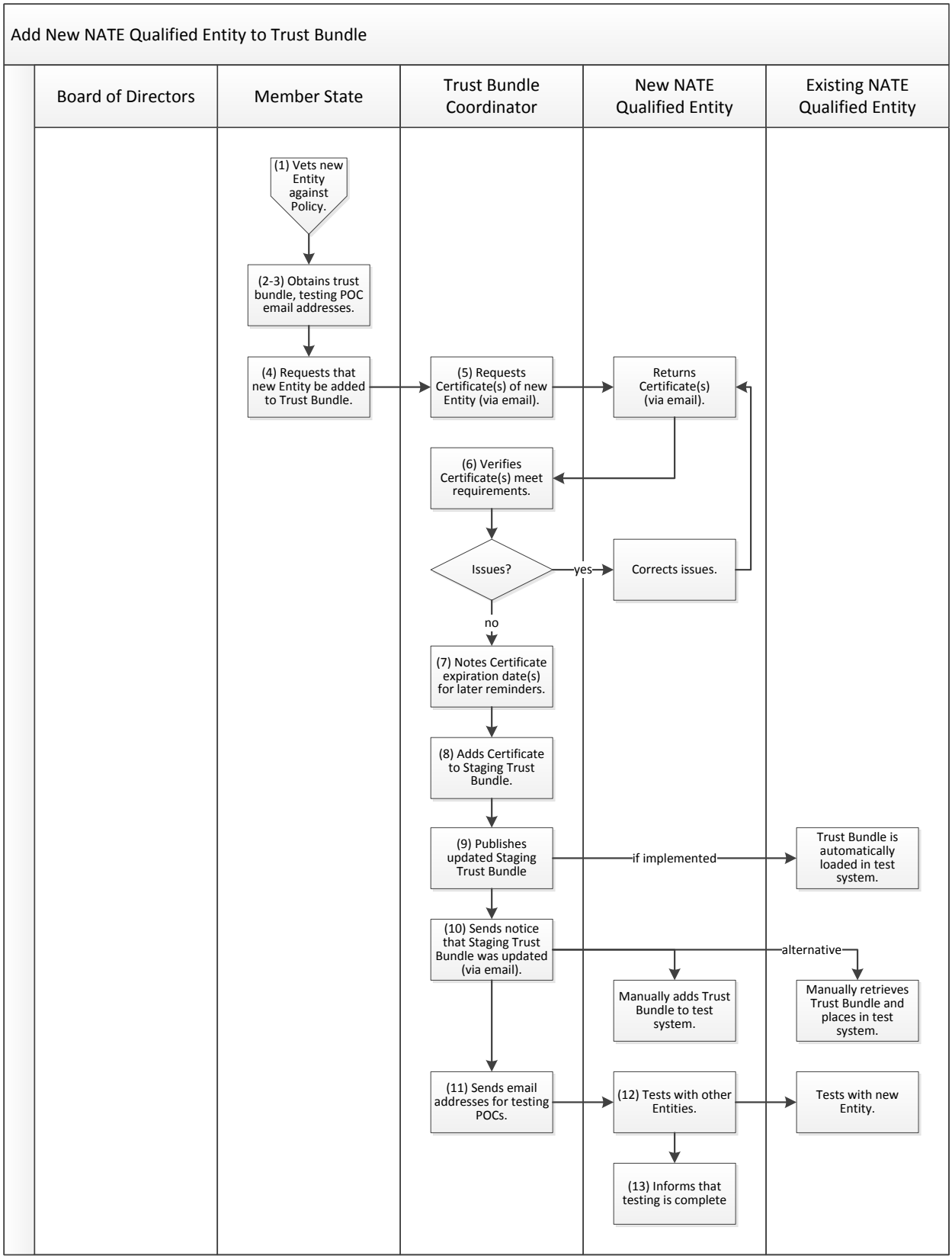
Noteworthy: The Board of Directors is alerted simply so they may monitor updates to NATE Trust Bundles. The Board of Directors might also alert Member States at its discretion.

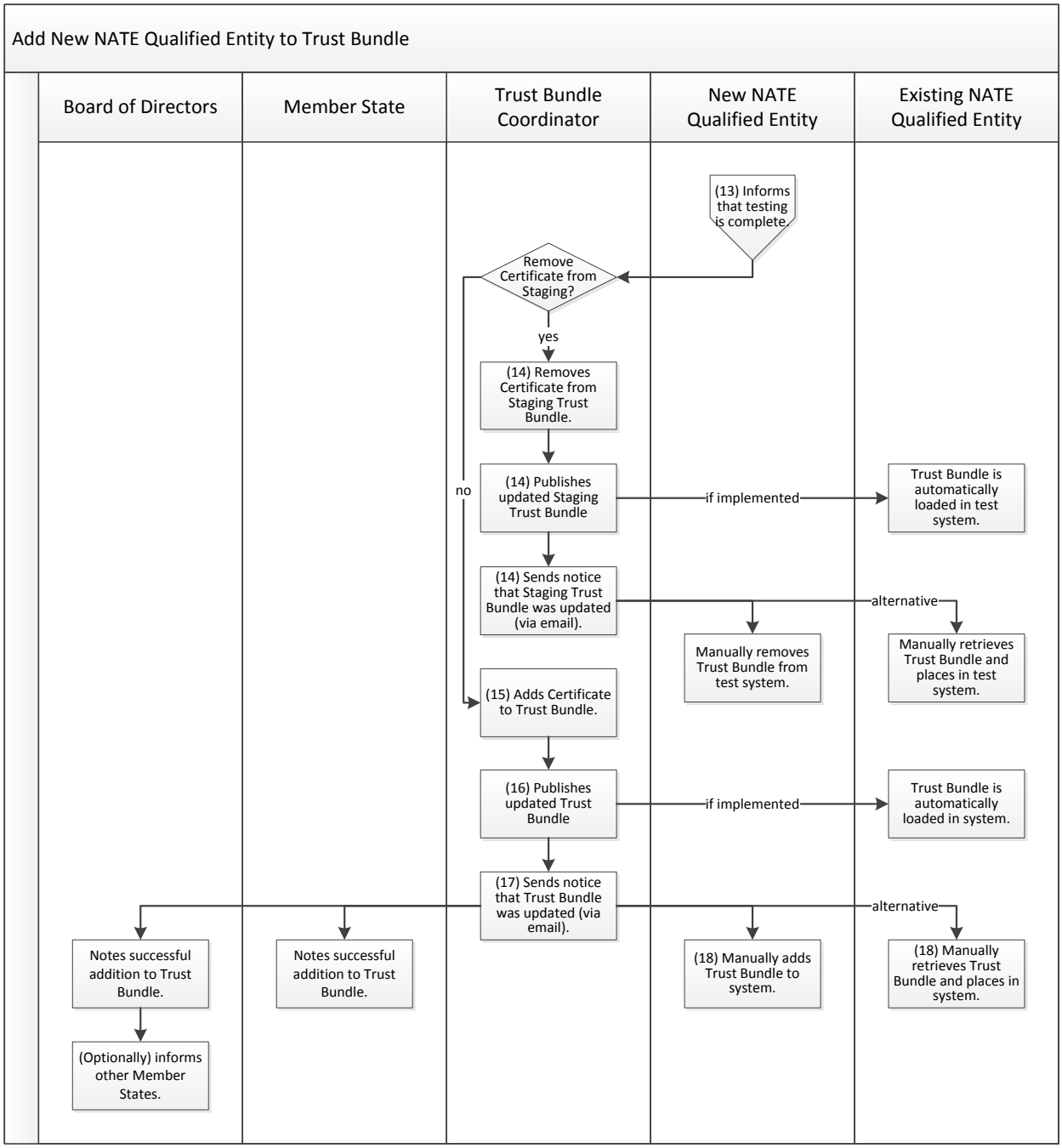
18. The trust bundle POCs of all NATE-Qualified Entities in the NATE Trust Profile download the updated Trust Bundle from the web service, and update their trust stores.

    Rationale – This update adds the NATE Trust Certificate of the new NATE-Qualified Entity to the local trust store of each NATE-Qualified Entity, enabling trusted exchange and effectively adding the new organization to the NATE Trust Profile.

    Noteworthy: The *Implementation Guide for Direct Project Trust Bundle Distribution v1.0* has provisions for automated updates through periodic polling of each Trust Bundle. NATE-Qualified Entities may implement a manual process.

The following flow charts illustrate the Procedure for adding a new NATE-Qualified Entity to a Trust Bundle. Numbers within individual steps in the flow chart reference numbered steps in the above Procedure.


Add New NATE Qualified Entity to Trust Bundle
Board of Directors
Member State
Trust Bundle Coordinator
New NATE Qualified Entity
Existing NATE Qualified Entity
(1) Vets new Entity against Policy.
(2-3) Obtains trust bundle, testing POC email addresses.
(4) Requests that new Entity be added to Trust Bundle.
(5) Requests Certificate(s) of new Entity (via email).
Returns Certificate(s) (via email).
(6) Verifies Certificate(s) meet requirements.
Issues?
yes
Corrects issues.
no
(7) Notes Certificate expiration date(s) for later reminders.
(8) Adds Certificate to Staging Trust Bundle.
(9) Publishes updated Staging Trust Bundle
if implemented
Trust Bundle is automatically loaded in test system.
(10) Sends notice that Staging Trust Bundle was updated (via email).
alternative
Manually adds Trust Bundle to test system.
Manually retrieves Trust Bundle and places in test system.
(11) Sends email addresses for testing POCs.
(12) Tests with other Entities.
Tests with new Entity.
(13) Informs that testing is complete


Add New NATE Qualified Entity to Trust Bundle
Board of Directors
Member State
Trust Bundle Coordinator
New NATE Qualified Entity
Existing NATE Qualified Entity
(13) Informs that testing is complete.
Remove Certificate from Staging?
yes
no
(14) Removes Certificate from Staging Trust Bundle.
(14) Publishes updated Staging Trust Bundle
if implemented
Trust Bundle is automatically loaded in test system.
(14) Sends notice that Staging Trust Bundle was updated (via email).
alternative
Manually removes Trust Bundle from test system.
Manually retrieves Trust Bundle and places in test system.
(15) Adds Certificate to Trust Bundle.
(16) Publishes updated Trust Bundle
if implemented
Trust Bundle is automatically loaded in system.
(17) Sends notice that Trust Bundle was updated (via email).
alternative
Notes successful addition to Trust Bundle.
Notes successful addition to Trust Bundle.
(18) Manually adds Trust Bundle to system.
(18) Manually retrieves Trust Bundle and places in system.
(Optionally) informs other Member States.

B. Removing a Member from a Trust Profile

Precondition: A Member State has determined that a NATE-Qualified Entity should be removed from a NATE Trust Bundle, or a NATE-Qualified Entity has determined that it no longer wishes to participate in a NATE Trust Profile.

Post-condition: The NATE-Qualified Entity has been removed from the appropriate NATE Trust Bundle.

1. The Member State Representative determines that a NATE-Qualified Entity no longer meets the policy and process requirements for a NATE Trust Profile or, for some other reason, should be removed from a NATE Trust Bundle, or a NATE-Qualified Entity may wish to be removed.

   Rationale – The Member State Representative has the sole authority to determine whether an organization should be removed from a NATE Trust Bundle due to non-conformance with policies and processes required for a NATE Trust Profile.

   Noteworthy: A NATE-Qualified Entity may no longer wish to participate in a NATE Trust Profile. While a NATE-Qualified Entity may simply remove a NATE Trust Bundle from its trust store to disable exchange, it may also wish to be removed so its nonparticipation is made clear to other NATE-Qualified Entities.

2. The Member State Representative or a representative of the NATE-Qualified Entity contacts the Trust Bundle Coordinator by email instructing the Coordinator to remove the organization from the appropriate NATE Trust Bundle.

   Rationale – It is desirable for NATE to define a single point of contact – the Trust Bundle Coordinator – to manage the process for Trust Community Administration.

3. The Trust Bundle Coordinator removes the NATE Trust Certificate for the removed organization from the appropriate NATE Trust Bundle.

4. The Trust Bundle Coordinator publishes the updated NATE Trust Bundle.

5. The Trust Bundle Coordinator sends an email to the Board of Directors and the trust bundle POCs of all NATE-Qualified Entities that are members of the NATE Trust Profile alerting them that the NATE Trust Bundle has been updated.

   Rationale – The *Implementation Guide for Direct Project Trust Bundle Distribution v1.0* does not call for any in-band or out-of-band notification of Trust Bundle changes, but instead places the responsibility for establishing the update schedule on the Trust Community member. Email will be used to contact the trust bundle POCs to ensure that all NATE-Qualified Entities update their trust stores promptly.

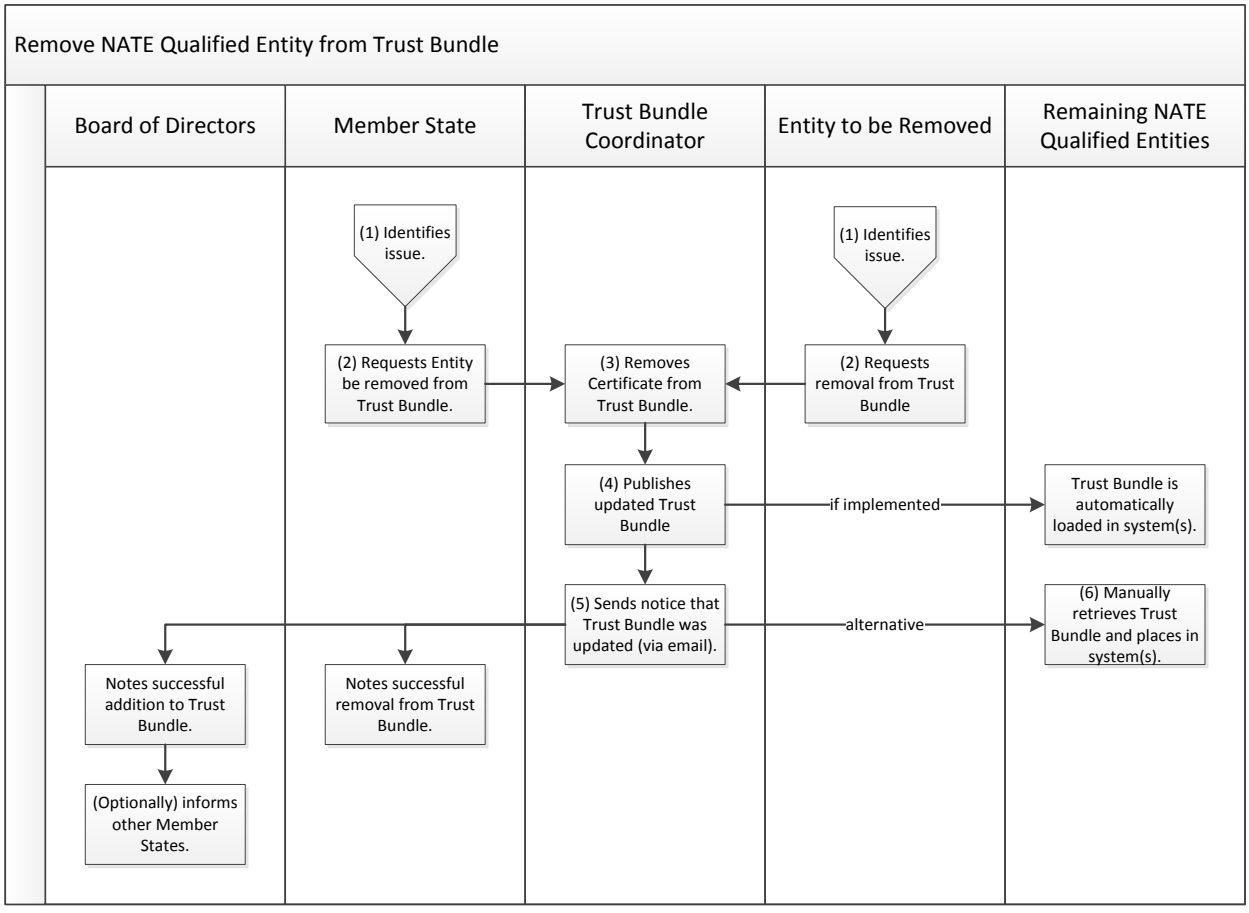
Noteworthy: The Board of Directors is alerted simply so they may monitor updates to NATE Trust Bundles. The Board of Directors might also alert Member States at its discretion.

6. The trust bundle POCs of all NATE-Qualified Entities in the NATE Trust Profile download the updated Trust Bundle from the web service, and update the trust stores.

   Rationale – This update removes the NATE Trust Certificate of the removed organization from the local trust store of each NATE-Qualified Entity, disabling exchange and effectively removing the organization to the NATE Trust Profile.

   Noteworthy: The *Implementation Guide for Direct Project Trust Bundle Distribution v1.0* has provisions for automated updates through periodic polling of each Trust Bundle. NATE-Qualified Entities may implement a manual process.

The following flow chart illustrates the Procedure for removing an existing NATE-Qualified Entity from a Trust Bundle. Numbers within individual steps in the flow chart reference numbered steps in the above Procedure.



IV. References

Implementation Guide for Direct Project Trust Bundle Distribution v1.0, which can be found at http://wiki.directproject.org/Trust+Bundle+Sub+Work+Group.

V. Related Forms

None.

VI. Version History

	Date	Author	Comment
1.0	10/29/2013	Aaron Seib	Approved Version