The Direct Project

Applicability Statement for Secure Health Transport

Version 1.2

3 August 2015

Contents

Status of this Specification

This document is PUBLISHED.

IPR Statement

By contributing to this specification, all contributors warrant that all applicable patent or other intellectual policy rights have been disclosed and that any of which contributors are aware of will be disclosed in accordance with the Direct Project IPR Policy.

Abstract

This document describes how to use SMTP, S/MIME, and X.509 certificates to securely transport health information over the Internet. Participants in exchange are identified using standard e-mail addresses associated with X.509 certificates. The data is packaged using standard MIME content types. Authentication and privacy are obtained by using Cryptographic Message Syntax (S/MIME), and confirmation delivery is accomplished using encrypted and signed Message Disposition Notification. Certificate discovery of endpoints is accomplished through the use of the DNS and LDAP. Advice is given for specific processing for ensuring security and trust validation on behalf of the ultimate message originator or receiver.

Introduction

Purpose

This document is intended as an applicability statement providing constrained conformance guidance on the interoperable use of a set of RFCs describing methods for achieving security, privacy, data integrity, authentication of sender and receiver, and confirmation of delivery consistent with the data transport needs for health information exchange. Unless explicitly stated otherwise within this document, RFCs noted in requirements apply in their entirety.

Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

An implementation is not compliant if it fails to satisfy one or more of the MUST or REQUIRED level requirements for the protocols it implements. An implementation that satisfies all the

MUST or REQUIRED level and all the SHOULD level requirements for its protocols is said to be "unconditionally compliant"; one that satisfies all the MUST level requirements but not all the SHOULD level requirements for its protocols is said to be "conditionally compliant."

Synopsis

This document describes the following REQUIRED capabilities of a Security/Trust Agent (STA), which is a Message Transfer Agent, Message Submission Agent or Message User Agent supporting security and trust for a transaction conforming to this specification:

- Use of Domain Names, Addresses, and Associated Certificates
- Signed and encrypted Internet Message Format documents
- Message Disposition Notification
- Trust Verification
- Certificate Discovery Through the DNS and LDAP

The scope of this specification is limited to the STA features that claim conformance to this applicability statement.

1.0 Domain Names, Addresses, and Associated Certificates

Direct Addresses consist of a Health Domain Name portion, which is a fully qualified domain name, and a Health Endpoint Name. For example: `johndoe@direct.sunnyfamilypractice.example.org`. Direct Addresses MUST be linked to an associated certificate that confirms the identity either of the domain name or of the full address.

The intent of a Direct Address is to provide a method of routing from an origination point to the addressed recipient, not to provide a single, definitive ID for the intended recipient. The same real-world person may have multiple Direct Addresses (e.g. one address for each practice location, multiple addresses for different processing purposes such as labs, routed to the EHR, vs unstructured messaging, routed to the secure messaging client and copied to the chart).

1.1 Health Domain Name

A Health Domain Name is a string conforming to the requirements of RFC 1034 and identifies the organization that assigns the Health Endpoint Names. Example:

direct.sunnyfamilypractice.example.org. A Health Domain Name MUST be a fully qualified domain name, and SHOULD be dedicated solely to the purposes of health information exchange.

Organizations that manage Health Domain Names MUST maintain DNS entries for the Health Domain Name, to include MX Resource Records to identify the SMTP server or servers for the domain.

1.2 Health Endpoint Name

A Health Endpoint Name is a string conforming to the local-part requirements of RFC 5322.

Health Endpoint Names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. Example: johndoe (referring to in individual), sunnyfamilypractice, memoriallab (referring to organizational inboxes), diseaseregistry (referring to a processing queue).

1.3 Formatting

A Direct Address may be formatted as an e-mail address by following the addr-spec requirements of RFC 5322, using the Health Domain Name for the domain, and the Health Endpoint Name for the local-part.

1.4 Associated X509 Certificates

The organization maintaining the Health Domain Name MUST also associate the Health Domain Name and/or Direct Address with one or more X.509 certificates. Such certificates MUST be assigned to at least one of two levels:

- Organizational Certificates, tied to the Health Domain Name
- Address Certificates, tied to each Direct Address

An organization that maintains Organizational Certificates MUST vouch for the identity of all Direct Addresses at the Health Domain Name tied to the certificate(s).

Certificates used as Organizational Certificates MUST be assigned to the Health Domain Name, by binding the Health Domain Name to the subjectAltName extension dNSName in the certificate.

Certificates used as Address Certificates MUST be assigned to the Direct Address, by binding the Direct Address to the subjectAltName extension rfc822Name.

The organization SHOULD publish the certificates for discovery by other implementations for the purposes of encryption and signature verification. To support universal certificate discovery, an organization that publishes certificates MAY do so using either DNS (see Section 5 of this applicability statement) or LDAP as described in the S&I Framework Certificate Discovery for Direct Project Implementation Guide.

Each STA MUST maintain a set of valid certificate and key pairs for each such Direct Address or Organization for the purposes of decryption and signature. The mechanism by which keys are managed and stored is implementation specific.

2.0 Signed and Encrypted Internet Message Format Documents

2.1 Health Content Containers

A Health Content Container (prior to signing and encrypting, as otherwise described in this document) SHALL be an Internet Message Format document conforming to RFC 5322.

The message body prior to signing and encrypting MUST be a valid MIME body. However, nothing in this specification obligates a specific address to handle all valid MIME bodies. Specific addressees MAY place additional constraints on the message body (for example, that it contain a specific healthcare format). Such addressees MUST provide appropriate error notification in response to inbound messages that do not conform to its specification. Where possible in such cases, it is RECOMMENDED that an address that is more permissive in the content types that it accepts be supplied. (For example, a specific address may expect to receive inbound HL7 laboratory result messages and a general purpose address exists that accepts PDF, TIFF, textual and other human readable representations of data.)

Sender addresses MAY send only a limited type or set of types of MIME bodies. The use of alternative human readable representations of structured content is RECOMMENDED as a matter of policy to enable wider understanding of the content. For example, a sender may send both a structured HL7 laboratory result message and the equivalent PDF representation of the same content, or may send an XML document with an included stylesheet allowing browser-based display).

Messages corresponding to the IHE XDM specification are RECOMMENDED if the sender has the ability to create such a message.

2.2 Message Headers

The following message headers documented in RFC 5322 are required:

Header	Content	Example
from	Source addressee as a Direct Address formatted as an e-mail address	smith@direct.sunnyfamilypractice.example.org
to	Destination addressee(s) as Direct Addresses formatted as an e-mail addresses	jones@direct.happyvalleypractice.example.org
orig-date	As per RFC 5322	Thu, 8 Apr 2010 16:00:19 -0400
message-id	As per RFC 5322.	<db00ed94-951b-4d47-8e86-585b31fe01bf@nhin.sunnyfamilypractice.example.org>

While common use in e-mail may have SMTP command arguments different from RFC 5322 headers, it is RECOMMENDED that the MAIL FROM SMTP command match the RFC 5322 from header. It is also RECOMMENDED that the RCPT TO command match the union of `to` and `cc`. It is RECOMMENDED that the `bcc` header not be used. A processing model that accepts data originated by e-mail clients is RECOMMENDED to handle `bcc` explicitly, but no guidance (beyond that provided by RFC 5322) is provided in this document for how that should be done.

Note that, unless prevented by policy, message headers may contain personally identifiable information (PII). Such information may be contained in Subject headings, Direct Addresses that reveal patient names, etc. See Section 6, Security Considerations.

2.3 Discovery of Recipient Certificates Prior to Sending

The STA MUST have a method for discovering the certificates of message recipients prior to sending a message in order to fulfill the encryption functions of S/MIME.

For universal digital certificate distribution, STAs MUST be able to discover certificates using both the DNS as specified in Section 5 of this applicability statement and LDAP as described by the S&I Framework Certificate Discovery for Direct Project Implementation Guide. STAs MAY support other certificate discovery methods in addition to DNS and LDAP, such as obtaining digital certificates from prior e-mail exchanges of S/MIME signed messages or through some other out-of-band and thus manual means.

2.4 Signed and Encrypted Health Content Containers

STAs MUST support the creation and processing of signed and encrypted MIME entities. That is, they MUST be capable of creating and reading documents that are encrypted as EnvelopedData, as specified by RFC 5751, with media type application/pkcs7-mime (although STAs MUST be capable of also recognizing EnvelopedData with media type application/x-pkcs7-mime), where the encrypted content type is a multipart/signed document, where the first part is the secured Health Content Container document and the second part is the detached signature.

STAs MUST perform encryption/decryption and verification functions on the basis of the actual sender(s) and receiver(s) of the message (i.e., those who are or would be listed in an SMTP RCPT TO and MAIL FROM commands).

STAs MUST take responsibility for securing all sensitive data. Implementers of STAs should be aware that sensitive data might exist in RFC 5322 headers; associated risks are further discussed in Section 6.1. Sending STAs SHOULD therefore protect the outer, non-content-related message header fields by wrapping the message as specified in Section 3.1 of RFC 5751 (note that support for sending of unwrapped messages may be deprecated in future versions of this document).

2.5 Signatures

2.5.1 Detached Signatures

STAs MUST use detached signatures as specified by RFC 5751, and thus, while RFC 5751 defines multiple formats for signed messages, STAs MUST create and accept signed messages in the multipart/signed format as defined by RFC 5751, Section 3.4.3. In addition to the standard media type of application/pkcs7-signature required by RFC 5751 for the detached signature body part, to preserve interoperability with legacy systems, STAs also MUST be able to accept a media type of application/x-pkcs7-signature.

2.5.2 Certificates in Signatures

Signatures MUST include the signing certificate, following the requirements of RFC 5652.

2.5.3 Digest Generation and Verification

Message digests MUST be computed per RFC 5751, including the canonicalization described in Section 3.1.1 of that RFC.

2.6 Digest Algorithms

Sending and receiving STAs MUST support SHA-256. Sending STAs MUST NOT generate digital signatures using SHA-1, although receiving STAs SHOULD support SHA-1 for incoming messages for the purpose of providing backward compatibility (note that support for SHA-1 within future versions of this document may be further deprecated). STAs MUST NOT support less secure Digest Algorithms such as MD5.

STAs MAY support more secure Digest Algorithms, as listed as SHOULD+ in RFC 5751 section 2.1 but senders should be aware that receivers may not support more secure algorithms.

As security standards evolve, the list of MUST and MUST NOT algorithms is subject to change in future version of this specification. STAs are RECOMMENDED to support configurable or pluggable support for algorithms.

2.7 Encryption Algorithms

The STA MUST support the following Encryption Algorithms:

1. AES 128
2. AES 256

STAs MUST NOT support less secure Encryption Algorithms, including additional algorithms listed as SHOULD- in RFC 5751 section 2.7.

STAs MAY support more secure Encryption Algorithms, as listed as SHOULD+ in RFC 5751 section 2.7 but senders should be aware that receivers may not support more secure algorithms.

As security standards evolve, the list of MUST and MUST NOT algorithms is subject to change in future version of this specification. STAs are RECOMMENDED to support configurable or pluggable support for algorithms.

3.0 Mail System Reports

Mail system reports are messages that conform to the framework of the "multipart/report" content type defined in RFC 6522. Forms of mail system reports within the scope of this document include Message Disposition Notifications (“MDNs”) and Delivery Status Notifications (DSNs):

- MDNs sent by an STA MUST conform to RFC 3798 as clarified in Section 3.1.1 below.
- DSNs sent by an STA MUST conform to RFC 3464 as clarified in Section 3.1.2 below.

Mail system reports sent by an STA MUST implement the message security requirements in this document (that is, the mail system reports MUST be signed and encrypted, from the original message receiver to the original message sender). Particular mail system reports and circumstances under which they are required are specified in subsequent subsections.

An STA MAY reflect the status indicated by a received mail system report in any appropriate way back to the original message sender (that is, the STA need not send the literal mail system report back to the sender if that is not workflow appropriate).

Note that a mail system report MUST NOT be sent in response to another mail system report nor in the situation where a message is not trust verified from the perspective of the receiver (because the reciprocal signature and encryption step for the mail system report will fail). Unencrypted mail system reports MUST NOT be sent back to the original message sender (to do so would create a means for an attacker to "sniff" for a valid address for later attack).

Additional and possibly multiple mail system reports beyond those specified MAY be sent in other situations (e.g., error notifications, read receipts, final delivery notifications, etc.).

3.1 Clarifications and Changes to RFCs Relevant to Mail System Reports

3.1.1 RFC 3798: Message Disposition Notification

The following clarifications and changes are applied in the use of RFC 3798 by this document:

```
disposition-type = "displayed"
                 / "processed"
                 / "failed"
                 / "dispatched"
```

Note that the production grammar for RFC 3798 removes the `processed`, `failed`, and `dispatched` values from the `disposition-type` definition, but refers to them in the RFC text.

The `disposition-type` of `processed` SHALL be interpreted as defined in Section 3.2.

The `disposition-types` of `displayed`, `failed`, and `dispatched` are as defined in RFC 3798. Other than as specified below, the role and use of such MDNs are outside the scope of this document.

When the `disposition-modifier` is `error`, the `error-field` MUST be provided. Multiline error messages MUST be conformant to RFC 5322. This MAY require normalization to break lines with a CRLF.

MDNs MUST implement the requirements in this document. This includes the requirements in Section 2.2, meaning that, contrary to RFC 3798, the envelope sender address (i.e., SMTP MAIL FROM) of an MDN SHOULD NOT be null (<>).

3.1.2 RFC 3464: An Extensible Message Format for Delivery Status Notifications

The following clarifications and changes are applied in the use of RFC 3464 by this document:

To enable a sending STA to correlate the DSN to the original message, a receiving STA MUST set a per-message extension field of `X-Original-Message-ID` with a value of the original message ID. If the `X-Original-Message-ID` is not present, for compatibility with legacy systems, a sending STA SHOULD use the value of the `In-Reply-To` field when available to correlate the DSN to the original message.

DSNs MUST implement the requirements in this document. This includes the requirements in Section 2.2, meaning that, contrary to RFC 3464, the envelope sender address (i.e., SMTP MAIL FROM) of a DSN SHOULD NOT be null (<>).

3.2 Processed Notifications

On successful receipt and trust verification of a message, an STA MUST promptly send an MDN with a `disposition-type` of `processed` (i.e., a `processed` MDN).

By sending a `processed` MDN, the receiving STA is asserting:

1. That bilateral message trust has been verified and the message digest has been validated
2. That the receiving STA has received the message and is taking responsibility to attempt further delivery of the message to the intended recipient

This obligation to confirm receipt overrides the specific requirements in RFC 3798 for disposition notification requests. That is, even if disposition notification was not specifically requested, the STA MUST confirm receipt with a `processed` MDN. If the `Disposition-Notification-To` header is not present, the `processed` MDN MUST be sent to the address or addresses indicated by the first available of the following fields:

- MAIL FROM SMTP command
- Sender header
- From header

Note that in a health care setting, many workflows require, by law or regulation, confirmation of receipt. Depending on the legal and regulatory framework and the level of confirmation required, `processed` MDNs might suffice for certain workflows. However, workflows requiring confirmation of actual successful or failed delivery to a final destination (for example, sending of laboratory results) MUST use additional mechanisms beyond the `processed` MDNs discussed in this document.

Because the STA's confirmation of receipt via a `processed` MDN could be used to indicate legal and regulatory compliance, it is RECOMMENDED that such confirmation be accompanied by appropriate audit logs.

3.3 Failure Notifications

A receiving STA MAY inform sending STAs of failure conditions by sending a failure notification in one of the following forms:

- An MDN with a `disposition-type` of `failed` (i.e., a `failed` MDN), or
- A Delivery Status Notification (DSN) with an action-value of `failed` (i.e., a `failed` DSN).

An STA MAY provide text explaining the failure condition:

- In the `failure-field` of a `failed` MDN, or
- As a comment to the `status-field` of a `failed` DSN.

When providing such text, in the interests of interoperability, it is RECOMMENDED that the text supply clear, human-comprehendible information describing the context of the condition, such as cause of failure and any remedial actions that might be taken by the original sender. An STA SHOULD format the provided text as per the guidance in section 3.1.1 of this document related to text provided in the `error-field`.

Note that a failure notification does not pre-empt conformance of the requirements in section 3.2. In other words, a failure notification can only be sent by a receiving STA if it has also sent a `processed` MDN.

4.0 Trust Verification

An STA verifies trust in a sender or recipient by verifying the trust and validity of the associated certificate.

STAs MUST check the following conditions for certificate validity:

1. Has not expired
2. Has a valid signature with a valid message digest
3. Has not been revoked
4. Binding to the expected entity
5. Has a trusted certificate path

The methods for verifying expiration and signature validity are well-characterized and not further specified in this document.

The STA MUST have a method for discovering certificate status, which is strongly RECOMMENDED to include OCSP and retrieval and storage of CRLs. Issuers of certificates used in Direct SHOULD publish certificate status for discovery by STAs; at a minimum this MUST include regular publication of CRLs.

Verification of binding to the expected entity and trust in the certificate path is further described below.

4.1 Verification of Certificate-Entity Binding

For the purposes of encryption or signature verification, the STA MUST verify the address or domain that an X.509 certificate is purported to be issued to by following the guidance in sections 4.1.2.6 and 4.2.1.6 of RFC 5280 and the subsections below. Any X.509 certificate extensions or attributes not detailed in that guidance, as well as the semantics of multiple subject alternative names within a certificate, are outside the scope of subject verification under this applicability statement, but may be in scope for particular policy domains.

4.1.1 Subject Verification for Direct Address-Bound Certificates

The following conditions MUST be true for a Direct Address-Bound Certificate:

1. The subjectAltName extension contains an rfc822Name with a value that matches the Direct Address using a case-insensitive comparison. This obligation to use a case-insensitive comparison overrides any specific requirements in RFC 5280 to match `local-parts` exactly.
2. If the Subject Distinguished Name contains an emailAddress legacy attribute, then its value matches the Direct Address using a case-insensitive comparison. Note that, in this case, the presence of the emailAddress legacy attribute, while permitted, is deprecated by RFC 5280.

4.1.2 Subject Verification for Organizationally-Bound Certificates

The following conditions MUST be true for an Organizationally-Bound Certificate:

- The subjectAltName extension contains a dNSName with a value that matches the Direct Address' Health Internet Domain.

4.1.3 Additional Extension Verification

Certificates may contain usage extensions that place restrictions on how the certificate key may be used. S/MIME implementations may also require that certificates be issued specifically to secure e-mail.

STAs MAY by policy enforce either restriction (or any other more restrictive policy) but need not. STAs MAY support any valid, non-expired, non-revoked and trusted certificate.

4.2 Certificate Paths and Trust

4.2.1 Trust Anchors

Each STA MUST, for each address or organization, be able to discover a set of trusted anchor certificates (trust anchors, as defined in RFC 5280, section 6). The mechanism by which that association is performed and by which trust anchors are selected and maintained is a critical matter of policy that is not defined in this document.

4.2.2 Certificate Paths

The STA MUST verify the certificate path for each certificate (both those tied to receivers and those tied to senders on receipt).

Discussion of certificate paths and path verification is found in RFC 5280, Section 6. The certificate chain of a given leaf certificate MUST include a trust anchor that is trusted by the STA.

For received messages, the message signature MUST contain the signing certificate and implementations MUST construct and verify the full certificate path of the signing certificate. When sending, implementations MUST construct and verify the full certificate path for receivers. Implementations MUST support certificate chain building using the Authority Information Access (AIA) extension (RFC 5280, Section 4.2.2.1). Implementations MAY use other mechanisms to build a certificate chain, but if no certificate chain to a trusted anchor can be built using alternative mechanisms, implementations MUST attempt to do so using the AIA extension before concluding no valid chain exists.

A certificate that appears in any certificate path of length greater than one MUST contain an AIA extension. At a minimum, the AIA extension MUST include an HTTP URI pointing to one or more certificates issued to the Issuer of that certificate, as specified in RFC 5280 Section 4.2.2.1.

4.2.3 Certificate Trust

Normative discussion of certificate path verification is found in RFC 5280, Section 6.

Each implementation MUST maintain an association with a supported address (sender or recipient) and a collection of Trusted Anchors. The address trusts any valid leaf certificate whose certificate chain contains at least one certificate from the address's Anchor list.

To determine if a leaf certificate is trusted:

1. Build a certificate chain for the leaf certificate (see above).
2. If the chain cannot be built, reject leaf certificate as un-trusted.
3. Traverse up the chain, starting at the bottom. For each certificate:
    1. If the certificate is invalid, then reject leaf certificate as un-trusted
    2. If an entry in the certificate chain is found in the Trusted Anchor list the leaf certificate is trusted.
    3. If the entire trust chain contains zero trusted anchors, the leaf certificate is un-trusted.

STAs MAY store self-signed certificates in the collection of Trusted Anchors (but is NOT REQUIRED to do so, and may be prohibited by policy from doing so). Self-signed certificates have a certificate chain of length 1. Consequently, a trusted self-signed leaf certificate must also be a trusted anchor.

4.3 Communication of Verification Failures

An STA MUST appropriately communicate and log trust verification failures through appropriate mechanisms.

5.0 Certificate Discovery and Verification Through the DNS

This section assumes familiarity with the DNS protocol and DNS Servers. It describes how to use the DNS capabilities described in RFC 4398 in this context.

As noted, STAs MUST be able to discover certificates using both the DNS as specified in this section and LDAP as described by the S&I Framework Certificate Discovery for Direct Project Implementation Guide. To achieve universal certificate discovery, STAs MAY elect to publish certificates in the DNS or using LDAP through the capabilities detailed in this section and in the S&I Framework Certificate Discovery for Direct Project Implementation Guide respectively.

DNS Resource Records are associated with a domain – which serves as the record's primary key. RFC 4398 provides multiple mechanisms to associate a domain name to a certificate record.

5.1 Direct Address-Bound Certificates To Domain Name

To associate DNS CERT records with e-mail addresses, the Direct Address MUST be formatted as a domain name.

```
cert-domain-name = health-endpoint-name '.' health-domain-name
```

That is, the DNS cert domain name is constructed by replacing the '@' in the e-mail address with '.'

For example: `bob@direct.example.org` becomes `bob.direct.example.org`

Note that in rare cases, a dotted last name may be confused with a subdomain. For example `bob.smith@example.org` and `bob@smith.example.org` may be confused. For organizations using CERT records for multiple purposes for the same domain name, the use of fully qualified domain names with special purpose subdomains is RECOMMENDED. For example, organizations should distinguish `bob.smith@mail.example.org` and `bob.smith@direct.example.org` to limit this issue.

5.2 Organizationally-Bound Certificates

STAs SHOULD retrieve organizational certificates if no more specific certificate is found for the address, unless prevented from doing so by policy.

Organizational level certificates are stored under the `health-domain-name` for the address.

For example: `bob@direct.example.org` may have an organizational level certificate stored under `direct.example.org`

5.3 Resource Record Format

RFC 4398 prescribes the DNS CERT record format. To store certificates in conformance with this specification, CERT records MUST be provided as follows:

1. Certificate Type: 16 bit number field set to 1 [X509] or 4 [IPKIX]
2. Certificate: If type X509, MUST be the Base64 encoded DER representation of the X.509 Certificate, if type IPKIX, MUST be a URL whose resource is the DER representation of the certificate in accordance with RFC 2585

The value of other CERT RR attributes is not defined in this specification.

5.3.1 Non-Normative Examples

The following CERT record contains the X509 Certificate for bob@direct.example.org

```
bob.direct.example.org. IN CERT 1 0 5 (
MIIDfzCCAuigAwIBAgIKcYxqqAAA
AAAAFzANBgkqhkiG9w0BAQUFADAV
MRMwEQYDVQQDEwpVTS1BTUFMR0Ex
MB4XDTEwMDYwMTE3NTM1NVoXDTEx
MDYwMTE4MDM1NVowgY0xCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJXQTEQ
MA4GA1UEBxMHUmVkbW9uZDEMMAoG
… Removed for Brevity …
)
```

The following CERT record contains an organizational level X509 Certificate for bob@direct.example.org

```
direct.example.org. IN CERT 1 0 5 (
MIIDfzCCAuigAwIBAgIKcYxqqAAA
AAAAFzANBgkqhkiG9w0BAQUFADAV
MRMwEQYDVQQDEwpVTS1BTUFMR0Ex
MB4XDTEwMDYwMTE3NTM1NVoXDTEx
MDYwMTE4MDM1NVowgY0xCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJXQTEQ
MA4GA1UEBxMHUmVkbW9uZDEMMAoG
… Removed for Brevity …
)
```

5.4 Use of TCP

The DNS protocol can run on either UDP or TCP. Both methods use Port 53. STAs should be aware that certificate records are likely to overflow UDP buffer limits and will need to upgrade to TCP or use TCP by default.

6.0 Security Considerations

Given the Protections specified, the Direct Project has executed Risk Assessments of some Deployment Architectures. These Risk Assessments include some residual risks that should be handled in the deployment or operational environment. These Risk Assessments followed a Threat Model Process

- Threat Model - SMTP with Full Service HISPs

    - Such as using the Service Model STA
- Threat Model - Simple SMTP
    - Full Service e-Mail Client,
    - Full Service Web Portal, or
    - where S/MIME is integrated into the EHR or PHR

S/MIME protects the message content end-to-end, that is the message can only be decrypted by the party holding the private key corresponding to the public certificate used for encryption. Therefore encrypted messages can travel in the wild without risk to the contents.

6.1 Summary of Risk and Mitigation

There are some common risks to all deployment models that need to be considered at the operational level.

- The security and trust features provided by the STA are only as secure as the operational environment of the STA. Implementers must apply appropriate security measures to protect the STA from well known risks, such as risk of untrusted code. Such security measures MUST be applied to the code and to critical aspects of the data associated with the STA, including private keys, trust anchors, and other configurations. The operation of the STA must occur within a high trust environment.
- Exposure of TO/FROM routing information (network, wireless, internet mailstop). Exposing that the addressee identified in the TO is having a private conversation with the addressee identified by the FROM. Where the conversation is provider-to-provider; there is no knowledge of the topic of the conversation, it could be about a golf game. Where the conversation is provider-to-patient; there is knowledge of types of conversations (e.g. where the provider is a specialist)
    - Each Recipient is in control of who they provide their endpoint address to, and each Sender is in control of who they communicate with.
    - Care should be taken when issuing Direct Project endpoint addresses to limit the exposure of sensitive information in an address itself
- The user may accidentally send sensitive content without security.
    - The 'service model STA' deployment model is designed to intercept all traffic and encrypt or reject it.
    - Some e-Mail clients can be configured to only send using S/MIME and will thus refuse to send to an address that can't be secured
    - Use of Integrated EHR/PHR with the e-mail infrastructure means user does not have access to e-Mail User Interface
    - Use of "Data Loss Prevention" systems to detect and block sensitive information from leaving an organization (see: Gartner report)
    - User training and inspection of audit logs and sent traffic/folder could detect violations of policy

- The user may send the content securely but accidentally send sensitive content in the email "subject" field. Although S/MIME protects well the content of a message, it does not protect the subject or other email header values. The recommendation is for sending STAs to perform message wrapping (see Section 2.4) and/or have a blank or non-descriptive subject to prevent this.
  - Use of Integrated EHR/PHR with the e-mail infrastructure means user does not have access to e-Mail User Interface
  - Use of "Data Loss Prevention" systems to detect and block sensitive information from leaving an organization (see: Gartner report)
  - User training and inspection of audit logs and sent traffic/folder could detect violations of policy
  - The use of TLS (through RFC 3207) can mitigate this risk to the extent that the point-to-point connection is controlled. TLS can only protect point-to-point, and thus would require that all pathways along the communications are similarly protected.
- DNS can be spoofed to return an attacker's IP addresses rather than the correct ones. This could cause messages to be sent to an attacker's system.
  - TLS can be used at the SMTP level conforming to RFC 3207. This would add another layer of authentication that must be passed, but also adds to complexity of configurations. TLS is only guaranteed to the first point. This is an important step, but there may be other SMTP mail servers in the path.
  - S/MIME protects the content, and mitigations to protect the headers will also mitigate against this threat
- A method for certificate discovery (such as embedded certificates in a signature or the use of the DNS as described in this document) may be spoofed or attacked to return an attacker's certificate rather than the correct ones
  - Certificate verification must be used to ensure the received certificate was assigned to the correct entity by a certification authority trusted by the STA
- The methods for ensuring the correct identity of sender and receiver are only as strong as the methods for certificate issuance, identity assurance, and authentication in operational use
  - Methods for evaluating trust anchors must ensure common floor definitions of certificate issuance policy, including associated mechanisms for identity assurance and operational control and authentication to the issued certificates after issuance
- The private key for the other party in a transaction may have been compromised.
  - An STA should check certificate status with the issuer to confirm that the other party's certificate has not been revoked.
  - Implementers should note that an undetermined certificate status is not equivalent to “not revoked”. Treating them the same carries risk.

7.0 Examples

This section is non-normative.

8.0 Authors

Umesh Madan
Sean Nolan
Arien Malec

9.0 References

9.1 Normative References

RFC 1034	Mockapetris, Domain names – concepts and facilities. RFC 1034, November 1987
RFC 1035	Mockapetris , Domain names - implementation and specification. RFC 1035, November 1987
RFC 2045	Freed, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, RFC 2045, November 1996
RFC 2119	Bradner, Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, March 1997
RFC 2585	Housley & Hoffman, PKIX Operational Protocols: FTP and HTTP, RFC 2585, May 1999
RFC 3207	Hoffman, SMTP Service Extension for Secure SMTP over Transport Layer Security, RFC 3207, February 2002
RFC 3464	Moore & Vaudreuil, An Extensible Message Format for Delivery Status Notifications, RFC 3464, January 2003
RFC 3798	Hansen & Vaudreuil, Message Disposition Notification, RFC 3798, May 2004
RFC 4034	Arends et al., Resource Records for the DNS Security Extensions, RFC 4034, March 2005
RFC 4398	Josefsson, Storing Certificates in the Domain Name System (DNS), RFC 4398, March 2006
RFC 5280	Cooper et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008

RFC 5322	Resnick, Internet Message Format RFC 5322, October 2008
RFC 5652	Housley, Cryptographic Message Syntax, RFC 5652, September 2009
RFC 5751	Ramsdell and Turner, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, RFC 5751, January 2010
RFC 6522	Kucherawy & Cloudmark, The Multipart/Report Media Type for the Reporting of Mail System Administrative Messages, RFC 6522, January 2012
XDM	Integrating the Healthcare Enterprise, Cross-Enterprise Document Media Interchange (XDM) Integration Profile, ITI TF-1, August 2010 Integrating the Healthcare Enterprise, Distribute Document Set on Media, ITI TF-2b, August 2010 Integrating the Healthcare Enterprise, XDS Metadata, ITI TF-3, August 2010

10.0 Copyright