Trusted Email Services

Technical Standards for Trusted Email Services

Author	Version	Date	Comment
Neil Cook neil.cook@open-xchange.com	0.1	18-Nov-15	Initial Draft
Neil Cook neil.cook@open-xchange.com	0.2	23-Nov-15	Incorporated comments from Peter Hoebel, Pieter Lexis, Michiel Nuyts. Added Appendices and References.
Neil Cook neil.cook@open-xchange.com	0.3	8th Dec 15	Included comments from Kevin San Diego.
Peter Höbel peter.hoebel@open-xchange.com Neil Cook	0.4	16-Mar- 16	Changed hostnames from tes_member, tes_master to tes-member, tes-master. Added NIST standards reference.

Overview

Trusted Email Services (TES) is an initiative to help consumers and businesses to easily identify an Email provider which fulfills their trust, security and privacy needs.

Defining standards for security and privacy are extremely difficult to do in isolation. Email is an open standard implemented by thousands of service providers all over the world, with huge differences in the implementation of security and privacy standards. Only by working together can service providers, software developers and experts agree on a set of standards that consumers can trust to ensure their privacy and security.

Any service provider or software developer wishing to improve security and privacy for their own customers will benefit from participating in TES, and in doing so, improve those standards for all consumers.

By participating in TES, members will not only be able to participate in defining the standards to which all members will have to adhere, but they will also be able to participate in creating a network of trust that adds value to their own services by being greater than the sum of its parts.

Technical Standards

The Trusted Email Services initiative will initially cover several areas that each protect the privacy, security and integrity of the end-user email experience in different ways.

Trusted Transport

This is base level for any trusted email service to be certified as TES compliant, and thus for the service provider to be a certified TES member. Users need to be able to trust that their emails are not passing unencrypted and thus readable by anyone over the public internet.

Users whose email is hosted by a TES member can trust that when sending or receiving emails to/from an address hosted by another TES member, those emails will always be transported using highly secure encryption, and so cannot be easily read by criminals, governments, secret services or hackers. Users will always be informed when recipients are TES members when they are sending email. Users will always be informed when they receive emails that are not encrypted.

Trusted Authentication

Trusted Authentication is directly relevant to a Trusted Email Service, because without trusted authentication, user credentials can be compromised or stolen. Therefore these standards also cover mandatory standards for trusted authentication where they apply to email.

Trusted End-To-End Encryption

This is an optional certification for TES members. Users need to be able to trust that, when they desire it, nobody except the recipients of the email will be able to read the content.

Users whose email provider complies with this certification can trust that they have the ability to send encrypted emails that can only be read by the intended recipients. Users can enable or disable encryption at will, and are able to distinguish between emails that are encrypted vs unencrypted.

Trusted Mailbox

This is an optional certification for TES members. Users need to be able to trust that the contents of their mailbox are readable only by themselves, and not by any third-party.

Users whose email provider complies with this certification can trust that their mailbox is stored in an encrypted form at all times, and can only be accessed by themselves.

Note that the words MUST, MUST NOT, SHOULD, and SHOULD NOT are to be interpreted as defined in RFC2119 [RFC2119].

Trusted Transport Standards

Standards for Mail Submission

The following standards apply to submission of emails (i.e. emails sent from end-users of the service).

- Mail submission between the client and server MUST be encrypted with TLS.
- The submission MTA MUST support TLS 1.2 [RFC5246] or higher. It is recognized that some clients may not support TLS 1.2, and thus submission MAY take place over a TLS version of 1.1 or greater. The cipher suites advertised MUST NOT include the insecure cipher suites listed in "Standards for Mail Relay between TES Members" as well as the NIST standards for TLS cipher suites referenced in that section.
- For submission ports that are configured to rely on STARTTLS [RFC3207] for encryption, submission MTA MUST NOT advertise any authentication mechanisms until after STARTTLS has been successfully negotiated.
- Unauthenticated mail submission MUST be rejected by the MTA.

Standards for Mail Retrieval

The following standards apply to retrieval of emails:

- Mail retrieval (over any protocol, including HTTP, IMAP4 or POP3) MUST be secured with TLS.
- Mail retrieval servers (over any protocol, including HTTP, POP3 or IMAP4) MUST support TLS 1.2 [RFC5246] or higher. It is recognized that some clients may not support TLS 1.2, and thus retrieval MAY take place over a TLS version of 1.1 or greater. The cipher suites advertised MUST NOT include the insecure cipher suites listed in "Standards for Mail Relay between TES Members" as well as the NIST standards for TLS cipher suites referenced in that section.
- For retrieval protocols that are configured to rely on STARTTLS [RFC3207] for encryption, authentication MUST NOT be allowed until after STARTTLS has been successfully negotiated.

Standards for Mail Relay between TES Members

The following standards apply to mail relayed between members of the Trusted Email Service initiative. Some of the standards in this section are expected to be checked by sending/receiving MTAs, others will be checked by out-of-band certification.

- Sending MTAs (i.e. those MTAs relaying a message to another MTA) MUST use the TES membership lookup mechanism described in Appendix A to determine if the receiving MTA is a member of TES. If not, then the standards for mail relay between a TES member and a non-TES member apply.
- In the following standards, if the standard states that an MTA should refuse to relay an email, it is up to individual TES members whether such emails are

bounced immediately, or if they are queued (in order to give the receiving TES member to fix any configuration or other issues).

- Receiving MTAs MUST advertise STARTTLS, and support TLS 1.2 or greater.
- The sending MTA MUST refuse to relay email over the connection if the version of TLS negotiated over STARTTLS is less than 1.2.
- TES Members MUST publish TLSA [RFC6698] records in DNS for all receiving MTAs for all zones advertised as being a TES member.
- The sending MTA MUST use DANE [RFC6698] to verify the certificate of the receiving MTA. If the certificate cannot be verified using DANE, then the sending MTA MUST refuse to relay emails over that connection.
- The following is the minimum profile for TLSA keys and MTA certificates.
    1. MTA Certificate Key Length: 2048 Bit
    2. TLSA Hash Type: SHA256 or greater
    3. TLSA Usage: 2 or 3 only
    4. TLSA Selector: Any
- A prerequisite for DANE is a signed DNSSEC [RFC4034] zone. The following is the minimum profile for any zone advertised (using the mechanism described in Appendix A) as being a TES member:
    1. Zone Signing Key Length: 1024 Bit
    2. Key Signing Key Length: 2048 Bit
- All service provider elements involved in enforcing the standards in this document MUST be configured to use a DNSSEC validating resolver.
- Mail relayed between TES members must use cipher suites that provide forward secrecy. Email relayed between TES members MUST use one of the following key-exchange mechanisms:
    1. Diffie-Hellman (DHE-RSA, DHE-DSS)
    2. Elliptic Curve Diffie-Hellman (ECDHE-RSA, ECDHE-ECDSA)
- Mail relayed between TES members SHOULD comply to the NIST standards related to TLS cipher suites as described in http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295 with the following modifications:
    1. The publication of a Certification Revocation List (OCSP, CRL) is optional, because of performance and security issues.
    2. TLS compression shall not be enabled on TES server transports
    3. Diffie Hellman parameter size >= 2048 bit is required, 4096 bit is recommended
    4. Self-signed certificates are accepted because DANE ensures that we can trust these certificates.

- Mail relayed between TES members must not use cipher suites that have known vulnerabilities. Email relayed between TES members MUST NOT use cipher suites that use the following encryption mechanisms:
    1. RC4
    2. aNULL
    3. DES,
    4. 3DES,
    5. MD5,
    6. DES+MD5,
    7. EXP
    8. eNULL
    9. LOW
- The receiving MTA MUST add an X-header indicating that the message was received from a TES member. This obviously also implies that the mail was received over an encrypted transport complying with the standards defined above. If the message was not received from a TES member any existing header has to be removed.
- The receiving MTA MUST add an X-header containing the following:
    1. TLS version used for transport
    2. Cipher suites used for encryption
- Sending MTAs MUST sign mail with DKIM [RFC 6376] before it is relayed, and SHOULD publish DMARC [RFC 7489] records for their sending domains.
- Receiving MTAs MUST reject emails from TES members without DKIM signatures, or emails from TES members with invalid DKIM signatures, and SHOULD support DMARC validation for deciding what to do with unsigned emails or emails which fail verification.

Standards for Mail Relay between a TES Member and others

The following standards apply for mail relayed between a TES member and a non-TES member:

- Sending MTAs of TES Members MUST be configured with Opportunistic TLS, and must use DANE if TLSA records exist for the receiving domain.
- Receiving MTAs of TES Members MUST advertise STARTTLS and support TLS 1.2 or greater.
- Receiving MTAs of TES Members MUST NOT advertise the cipher suites with known vulnerabilities listed in “Standards for Mail Relay between TES Members”.
- Sending MTAs of TES Members MUST sign mail with DKIM before it is relayed, and SHOULD publish DMARC records for their sending domains.

End-User Presentation of Transport Security

The following standards apply to an end-user facing mail applications controlled by a TES member:

- TES members providing webmail or dedicated applications (desktop or mobile) for users to access their mailboxes MUST:
    1. Make it visible to the user which mails have been received over unencrypted links versus mails which have been received over encrypted links (this includes not only mail received from a TES member but also any mail received over a connection secured with TLS 1.2 or greater).
    2. Make it visible to a user when sending an email whether the recipient(s) are members of TES, i.e. that the email is guaranteed to be sent securely.

Trusted Authentication Standards

For an email service to be trusted, it must maintain minimum standards for authentication to reduce the potential for account compromise, password brute forcing etc. The following standards apply:

- Passwords MUST NOT be stored in plaintext.
- When passwords are created either automatically or by users, they MUST be verified against a password strength policy. That policy MUST be published by the email service provider.
- If hash functions are used to protect passwords, the hash function MUST NOT be MD5. The SHA1 hash function SHOULD NOT be used. Salted hashes SHOULD be used.
- Two-Factor authentication provides valuable protection against account compromise, and so a form of Two-Factor Authentication MUST be provided to users. This may be mandatory or optional to users.
- TES Members SHOULD provide TOTP compliant Two-Factor Authentication [RFC6238].

Trusted End-To-End Encryption Standards

End-To-End encryption is extremely important to a trusted email service, as it guarantees that the email can only be read by the intended recipients. End-To-End encryption is already possible using device-level software (such as plugins to mail applications or browser extensions), however this software is extremely difficult for naïve users to install and configure correctly, (For example see https://www.usenix.org/events/sec99/full_papers/whitten/whitten.pdf*).*

The TES standards specified here therefore concentrate on ensuring that certified members provide a straightforward way to perform end-to-end encryption, concentrating on the following problems:

- Generating private/public key pairs
- Discovering and Publishing public keys
- Using an open encryption standard: OpenPGP [RFC4880]

End-User Presentation of End-To-End Encryption

End-to-End encryption should be visible to and controllable by the end-user, thus the following standards apply:

- End-Users MUST be given a way to setup (or renew) end-to-end encryption by generating a public/private OpenPGP key pair:
    1. If the service provider has a webmail Application, this MUST offer key generation.
    2. Otherwise the service provider MUST offer an alternative method to generate a key pair, e.g. by sending a suitably crafted email.
- End-Users MUST be given a way to download their private and/or public keys, over HTTPS, using the standards specified below for webmail.
- End-Users MUST be given a way to upload OpenPGP public/private key pairs, or only a public key, over HTTPS, using the standards specified below for webmail.
- End-Users MUST be given the option to encrypt emails from either:
    1. A webmail Interface and native mail applications, if they exist.
    2. If not, via a suitably crafted email, e.g. by adding [ENCRYPT] to the Subject, or adding an X-Header
- Any provided webmail application MUST enable access only via HTTPS, and not HTTP. The following standards apply to the cipher suites provided by the webserver:
    1. The webserver MUST advertise cipher suites that provide forward secrecy as specified in “Standards for Mail Relay between TES Members”.

2. The webserver MUST NOT advertise cipher suites that have known vulnerabilities as specified in “Standards for Mail Relay between TES Members”.
3. The webserver MUST add HPKP and HSTS headers to any response.

Private Key Security

For any end-user who chooses to allow their service provider to generate a key-pair, or any user who uploads a key-pair to their service provider, the service provider must secure the private key to the best of their ability. The following standards apply:

- When generating keys, the service provider MUST ensure keys comply with the following:
    1. Key Length: 2048 Bit for RSA
    2. Key Length: 4096 Bit for Diffie-Hellman
- Private keys MUST be stored encrypted, either:
    1. With a passphrase supplied by the end-user. This passphrase MAY be the same as the email account password.

       And/or
    2. With a master key supplied by the service provider.
- Service Providers MAY choose to store a copy of the private key encrypted with a master key to enable recovery of the private key if a user forgets their password, or to provide a backdoor for government agencies. If so, the service provider MUST:
    1. Give end-users the ability to opt-out (at any time), i.e. using only a passphrase known to the user to decrypt the private key.
    2. Provide transparency about the fact that their private key is accessible to the service provider and any authorized third-parties to any users whose private key is stored in this way.

Content Encryption

The TES standards cover end-to-end encryption where the encryption is performed by the service provider on behalf of the user (if the users wished to perform the encryption themselves, this is already possible as discussed earlier). The standards in this section apply to the encryption performed by the service provider:

- Encryption MUST use OpenPGP. The following algorithms and ciphers MUST NOT be used:
    1. To be filled in.
- When the end-user indicates that encryption is required, the service provider MUST encrypt at the following service elements:

1. Webmail or Native Application submitting using HTTPS [RFC2818]: The web server application MUST perform the encryption.
2. Native Application submitting mail using SMTP: The native application OR the submitting MTA may perform the encryption.
3. SMTP: If this option is supported, and the user crafts an email in a manner that indicates they wish it to be encrypted, the MTA MUST perform the encryption.

- Service Providers SHOULD give users the option to use OpenPGP inline formatting, but the default MUST be OpenPGP MIME.
- The service element performing the encryption MUST use the mechanism described in Appendix B to retrieve a public key for the recipient. If found, that key MUST be used to encrypt the message. Public keyservers MUST NOT be used to lookup keys for mail relay between TES members.
  If a public key is not found using the described mechanism, then either:
  a. The user MUST be informed that the message cannot be encrypted, giving the user the option to cancel sending the message or continues to send the mail in plaintext.

     Or

  b. The content MUST be encrypted using an alternative mechanism. For example, the message could be encrypted using symmetric encryption, and a message sent with a link and a password (however the transport MUST be encrypted).
- Service elements performing encryption MAY cache retrieved public keys for a period of time, but MUST NOT store them permanently.
- The maximum cache time for retrieved public keys MUST be no longer than 7 days.

Public Key Publication Standards

A reliable mechanism to publish and discover public keys is vital to any functioning end-to-end encryption standard.

- Service Providers MUST provide a publicly accessible keyserver, supporting HKP over HTTPS [draft-shaw-openpgp-hkp-00] for each domain advertised as being a TES member. Each domain MUST publish a SRV record for the keyserver(s).
- Keyservers MUST be configured to disable:
  1. POST requests to the keyserver from the Internet
  2. Wildcard search requests to the keyserver from the Internet

  Thus making keyservers publicly “readonly”.

- When an end-user generates/replaces a public/private keypair, or uploads a new public key, the service provider MUST upload the public key to the keyserver infrastructure, replacing any existing key for that end-user for the purposes of lookup by email address over HKP, thus making it the only key available for public lookups by email address. Previously uploaded keys MUST still be available to lookup by keyid.
- Service Providers generating public/private key pairs on behalf of a user MUST generate a revocation certificate at the same time, in case the user forgets their passphrase. If/when a user generates a new key pair, then the service provider MUST upload to the public keyserver either the previously generated revocation certificate (if the user has forgotten their passphrase) with a generic reason, or a newly generated revocation certificate (if the user remembers their passphrase) with the "key is superseded" reason for the old key at the same time as the new public key is uploaded.
- Service providers MUST allow users who are maintaining their own keys to upload a revocation certificate for their key.

Trusted Mailbox Standards

At-Rest encryption of mailboxes is important to users who are concerned that the confidential contents of their mailbox may be available to hackers, or persons of malicious intent. This section addresses that concern by defining standards for the encryption of mailbox data, and applies to any service provider who hosts email mailboxes for end-users.

- Service Providers MUST provide an option for users to enable encryption of their stored mailbox data.
- Encryption of the mailbox data MUST be using the OpenPGP public key of the end-user. The end-user MUST be given the opportunity to generate/upload a key pair as specified in “End-User Presentation of End-To-End Encryption”. This key pair MAY be the same as the one used for end-to-end encryption, but the service provider MUST allow a different key pair to be generated for this purpose if requested by the end-user.
- The private key must be secured according to the standards as specified in “Private Key Security”, with a further restriction that any passphrase used to encrypt the private key MUST be the same as the account passphrase, otherwise the server would not be able to decrypt the mailbox when the user accessed it over standard protocols such as IMAP.
- The service element responsible for encrypting/decrypting the mailstore is dependent on the service provider’s mail storage software.

Appendix A – Using DNS to Publish and Lookup TES Membership for Mail Domains

Overview

A fundamental problem in any service designed to enforce standards between members is that of determining who is a member. In the case of TES, the standards require certain behaviors based on membership, therefore any lookup mechanism must be dynamic. Additionally, since the only information provided is an email address, some way of mapping the domain of the email address to the entity that is responsible for that domain is required, in order to determine if that entity is a member.

Happily, DNS is an extremely flexible mechanism to implement such lookups, and by making use of DNSSEC, the integrity of the data in DNS can be assured. This appendix describes the DNS lookup mechanism for query whether an email address domain belongs to an entity with membership of TES.

Publishing DNS Records to indicate TES Membership

Domain-Level Records

For each mail domain (e.g. example.com) that is hosted by a TES member (e.g. myisp.net), the following CNAME record must be created:

```
tes-master.example.com    CNAME myisp.net.
```

The CNAME can point to any domain or subdomain under the control of the TES Member, as long as all hosted domains have a tes-master CNAME pointing to the same domain. For example the following CNAME would be equally valid:

```
tes-master.example.com    CNAME tes.myisp.net.
```

Entity-Level Records

TES members must create an entity-level record for each mail domain that they host, which validates that those domains do indeed belong to the TES member that they claim to belong to via the CNAME record.

For example, using the first example above:

```
example.com.tes-member.myisp.net. TXT "TES Mail Domain"
```

Using the second example we would have:

```
example.com.tes-member.tes.myisp.net. TXT "TES Mail
Domain"
```

TES Membership Records

Having established that a domain belongs to a particular entity, all that is required is to establish whether that entity is a member of TES. This is achieved

by the TES organization creating the following DNS record (using the first example above):

```
myisp.net.tes-member.trusted-email-services.com. TXT "TES
Mail Domain"
```

Using the second example, the record would instead be:

```
tes.myisp.net.tes-member.trusted-email-services.com. TXT
"TES Mail Domain"
```

Verifying TES Membership using DNS

To verify a sender or recipient of a mail on the mail client, the following steps are required (assuming the email address user@company.de, managed by the entity example-isp.de):

1. Do a DNS lookup for the CNAME RR for `tes-master.company.de`.

   The data field of the result contains the managing domain, in this example example-isp.de. If no CNAME is found, the domain is assumed to be outside of TES, otherwise the next step is taken.

2. Then the mail domain is validated by doing a DNS lookup for a TXT record with the name `company.de.tes-member.example-isp.de.`

   If a TXT RR found, the next step is taken. The validation fails if no record is found and the domain is assumed to be outside of TES.

3. Finally a DNS TXT record lookup is performed to: `example-isp.de.tes-member.trusted-email-service.com`.

   If that lookup succeeds, then the managing domain is validated and the domain is assumed to be a participant in TES. Otherwise the domain is assumed to be outside of TES.

Appendix B – Using DNS to locate HKP Compliant Keyservers for a Domain

The IETF draft "draft-shaw-openpgp-hkp-00" [draft-shaw-openpgp-hkp-00] proposes a mechanism for using DNS to lookup the responsible keyserver for a given address. That mechanism is reproduced here to avoid readers having to read that draft.

The mechanism proposed is very simple, and makes use of DNS SRV records, as specified in this extract from the draft:

A far more flexible scheme for listing multiple HKP keyservers in DNS is the use of DNS SRV records as specified in RFC-2782 [RFC2782].DNS SRV allows for different priorities and weights to be applied to each HKP keyserver in the list, which allows an administrator much more control over how clients will contact the servers. The SRV symbolic service name for HKP keyservers is "hkp". For example, the SRV record for HKP keyservers in domain "example.com" would be "_hkp._tcp.example.com".

SRV records contain the port that the target server runs on, so SRV can also be used to automatically discover the proper port for contacting a HKP keyserver.

An additional use of SRV records is when a client needs to locate a specified key by email address. For example, a client trying to locate a key for isabella@silvie.example.com could consult "_hkp._tcp.silvie.example.com".

References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5246] T. Dierks, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, August 2008

[RFC3207] P. Hoffman, “SMTP Service Extension for Secure SMTP over Transport Layer Security”, RFC 3207, February 2002.

[RFC6698] P. Hoffman, J, Schlyter, “The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA”, RFC 6698, August 2012.

[RFC4034] R. Arends et al, “Resource Records for the DNS Security Extensions”, RFC 4034, March 2005.

[RFC6376] D. Crocker, T. Hansen, M. Kucherawy, “DomainKeys Identified Mail (DKIM) Signatures”, RFC 6376, September 2011.

[RFC7489] M. Kucherawy, E. Zwicky, “Domain-based Message Authentication, Reporting, and Conformance (DMARC)”, RFC 7489, March 2015.

[RFC6238] D. M’Raihi et al, “TOTP: Time-Based One-Time Password Algorithm”, RFC 6238, May 2011.

[RFC4880] J. Callas, et al, “OpenPGP Message Format”, RFC 4880, November 2007

[RFC2818] E. Rescorla, “HTTP Over TLS”, RFC 2818, May 2000

[RFC2782] A. Gulbrandsen et al, “A DNS RR for specifying the location of services (DNS SRV)”, RFC 2782, February 2000

[draft-shaw-openpgp-hkp-00.txt] D. Shaw, “The OpenPGP HTTP Keyserver Protocol (HKP)”, Internet Draft (expired September 2003)