Trusted Instant Messaging (TIM+)
Applicability Statement

DRAFT Standard for Trial Use v1.0 US Realm
July 14, 2020

Sponsored by:
DS2019_02 Trusted Instant Messaging Consensus Body

DISCLAIMER: DRAFT Standards are not approved standards under the DirectTrust Standards Operating Procedures. This draft is being published for the sole purpose of allowing for testing and initial feedback from companies who wish to test the technical requirements listed in the DRAFT Standard.

Table of Contents

Foreword

(This foreword is not part of this Standard)

DirectTrust Standards are designed to serve the public interest by facilitating interoperability, interchangeability and improvement of products. Existence of such Standards shall not in any respect preclude any member or non-member of DirectTrust from developing or selling products not conforming to such Standards.

Except as provided in this document, Standards are proposed or adopted by DirectTrust without regard to whether their proposal or adoption may in any way involve patents or intellectual property on articles, materials, or processes. By such action, DirectTrust does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting DirectTrust Standards, to parties manufacturing or selling products or services conforming to such Standards or to users of such products or services. Other DirectTrust rules respecting Standards where patents are involved are contained in DirectTrust Standards Development Operating Procedures and should be read in conjunction with these Guides. Furthermore, in all cases specific requirements and restraints expressed elsewhere in these Guides must govern.

Authors		
DS2019_02 Trusted Instant Messaging Consensus Body		
Content Contributors and Reviewers		
Members of DS2019_02		

Revision History

Document Version	Date	Description
Draft v1.0	July 14, 2020	Initial draft

		DISCLAIMER: Draft Standards are not approved standards under the DirectTrust Standards Operating Procedures. This draft is being published for the sole purpose of allowing for testing and initial feedback from companies who wish to test the technical requirements listed in the DRAFT STANDARD.

Introduction

Trusted Instant Messaging (TIM+) defines a protocol that facilitates real-time communication and incorporates secure messaging concepts to ensure information is transmitted securely between known, trusted entities both within and across enterprises. TIM+ will determine the availability or presence of trusted endpoints and support text-based communication and file transfers.

This document describes how to use RFC 6120 and associated RFCs and XEPs to securely route information over the Internet between edge clients through one or more TIM+ service providers in an active and real time modality. This document also provides a specification for federating secure and trusted connections between distinct TIM+ service providers. TIM+ combines best practices in security and privacy to achieve enterprise-grade, real time communication on behalf of the ultimate message originator or receiver.

This document is intended as a 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 secure instant communication (*e.g.,* healthcare).

Scope

This document describes how to use RFC 6120 and associated RFCs and XEPs to securely route information over the Internet between edge clients through one or more TIM+ service providers in an active and real time modality. This document also provides a specification for federating secure and trusted connections between distinct TIM+ service providers. TIM+ combines best practices in security and privacy to achieve enterprise-grade, real time communication on behalf of the ultimate message originator or receiver.

Normative References

The following standard contains provisions that, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards published by them.

RFC 1929	Leech, Username/Password Authentication for SOCKS V5, RFC 1929, March 1996
RFC 5246	Dierks & Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, August 2008
RFC 5280	Cooper et al., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008
RFC 6120	Saint-Andre, Extensible Messaging and Presence Protocol (XMPP): Core, RFC 6120, March 2011
RFC 6121	Saint-Andre, Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence, RFC 6121, March 2011
RFC 6122	Saint-Andre, Extensible Messaging and Presence Protocol (XMPP): Address Format, RFC 6122, March 2011
RFC 6125	Saint-Andre & Hodges, Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS), RFC 6125, March 2011
XEP 0013	Saint-Andre & Kaes, Flexible Offline Message Retrieval, XEP 0013, July 14 2005
XEP 0030	Hildebrand et al., Service Discovery, XEP 0030, October 3 2017
XEP 0045	Saint-Andre, Multi-User Chat, XEP 0045, May 15 2019

XEP 0047	Karneges & Saint-Andre, In-Band Bytestreams, XEP 0047, June 26 2012
XEP 0054	Saint-Andre, vcard-temp, XEP 0054, July 16 2008
XEP 0065	Smith et al., SOCKS5 Bytestreams, XEP 0065, September 19 2015
XEP 0071	Saint-Andre, XHTML-IM, XEP 0071, March 18 2018
XEP 0079	Miller & Saint-Andre, Advanced Message Processing, XEP 0079, November 30 2005
XEP 0085	Saint-Andre & Smith, Chat State Notifications, XEP 0085, September 23 2009
XEP 0095	Muldowney et al., Stream Initiation, XEP 0095, November 29 2017
XEP 0096	Muldowney et al., SI File Transfer, XEP 0096, November 29 2017
XEP 0115	Hildebrand et al., Entity Capabilities, XEP 0115, May 5 2020
XEP 0138	Hildebrand & Saint-Andre, Stream Compression, XEP 0138, May 27 2009
XEP 0160	Saint-Andre, Best Practices for Handling Offline Messages, XEP 0160, October 7 2016
XEP 0166	Ludwig et al., Jingle, XEP 0166, September 19 2018
XEP 0191	Saint-Andre, Blocking Command, XEP 0191, March 12 2015
XEP 0203	Saint-Andre, Delayed Delivery, XEP 0203, September 15 2009
XEP 0234	Saint-Andre & Stout, Jingle File Transfer, XEP 0234, June 19 2019
XEP 0237	Saint-Andre & Cridland, Roster Versioning, XEP 0237, February 8 2012
XEP 0260	Saint-Andre et al., Jingle SOCKS5 Bytestreams Transport Method, XEP 0260, May 15 2018
XEP 0261	Saint-Andre, Jingle In-Band Bytestreams Transport Method, XEP 0261, September 23 2011

Terms and Definitions

For the purposes of this Standard, the following definitions apply.

TBD

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

1 Domains and Endpoints

TIM+ domains are defined by a domain part as outlined in section 2.2 of RFC 6122 and identifies an organization that assigns TIM+ endpoints.

Example: samplepractice.org

TIM+ endpoints are defined by a local part and domain part as outlined in section 2.1 of RFC 6122 and identifies an entity that can be communicated with over the TIM+ protocol.

Example: provider@samplepractice.org

TIM+ endpoints are vouched for by the organization bound to the TIM+ domain.

TIM+ domains SHALL NOT use the following subdomains as they are reserved for TIM+ services:

- ftproxystream
- groupchat

1.1 Endpoint Identity

TIM+ endpoints are used for routing TIM+ messages between a source and destination and generally cannot be used to deterministically infer the identity of an entity bound to an endpoint. To associate an identity to an endpoint, TIM+ service providers SHALL assign attributes (or "claims") to an entity through the use of Vcards as defined in XEP 0054. Organizations bound to TIM+ domains must vouch for the claims for an entity. Required claims and the processes by which those claims are validated are a matter of local policy and are beyond the scope of this document.

Another TIM+ endpoint or other TIM+ service may retrieve the identity information of an entity using the TIM+ feature discovery protocol and the query protocol outlined in XEP 0054.

> **Practice Note**: Attributes in Vcards are public and discoverable by all TIM+ endpoints. XEP 0054 defines a privacy classification element, however there is no policy or technical implementation to enforce it. Required attributes in a Vcard are a matter of local policy, and care should be taken in determining what information should be included in a Vcard.

2 Endpoint Discovery and Routing

In many cases, it will be necessary for endpoints within one TIM+ service provider to communicate with endpoints hosted within another TIM+ service provider. To facilitate the discovery and routing paths of endpoints between discrete service providers, TIM+ service providers SHALL maintain and publish SRV records for the DNS domains that correspond to the TIM+ endpoints. These SRV records shall follow the semantics as defined in section 3.2 of RFC

6120 using the *xmpp-server* service type. A service provider SHALL publish one or more DNS A or AAAA records for each endpoint domain that it hosts where the name of the record corresponds to the fully qualified domain of the endpoint. Each A or AAAA record SHALL point to an IP address where the TIM+ services are hosted. In addition, a service provider SHALL follow the resolution rules as defined in RFC 6120 to determine the hosting server(s) of TIM+ endpoints belonging to a different service provider.

To support the discovery of group chat services, TIM+ service providers SHALL maintain and publish SRV records for the group chat subdomain as defined in section 3.2.4 of RFC 6120. The group chat subdomain is defined in section 9.1 of this document. The rules for publishing DNS A or AAAA records for the group chat subdomain are the same as the main TIM+ domain.

3 Domain Certificate Binding

Organizations bound to a TIM+ domain SHALL associate the domain name to an X.509 certificate as outlined in section 13.7 of RFC 6120 with the following requirements:

- The X.509 certificate SHALL include one and only one DNS-ID identifier type as defined by RFC 6125 where the dnsName is bound to the TIM+ domain name.
- The X.509 certificate SHALL include one and only one DNS-ID identifier type as defined by RFC 6125 where the dnsName is bound to the TIM+ domain's SOCKS5 file transfer proxy JID as outlined in section 10.1.2.1 of this document.
- The X.509 certificate SHALL include one and only one DNS-ID identifier type as defined by RFC 6125 where the dnsName is bound to the TIM+ group chat JID as outlined in section 9.1 of this document.
- The X.509 certificate SHALL include one and only one SRV-ID identifier type as defined by RFC 6125 where the service type is _xmpp-server and the name is bound to the TIM+ domain name.
- If a TIM+ service provider implements DNS SRV resolution for the purpose of client connections, then the X.509 certificate SHALL include one and only one SRV-ID identifier type as defined by RFC 6125 where the service type is _xmpp-client and the name is bound to the TIM+ domain name.
- The X.509 certificate CN attribute of the Subject Name field SHALL not be null.
- For backward compatibility for older implementations of RFC 6120, the certificate MAY include one and only one XmppAddr identifier type as defined by section 13.7.1.4 of RFC 6120.
- 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.
- The X.509 certificate SHALL NOT be self-signed.

An organization SHALL vouch for the identity of all TIM+ endpoints bound to the domain in the certificate. Procedures for validating identity are a matter of local policy and are beyond the scope of this document.

Certificates SHALL publish certificate status using CRLs and MAY also publish certificate status using OSCP.

4 Server Authentication and Trust

Server authentication and trust is the process by which one TIM+ service provider makes a connection to another TIM+ service provider and establishes a secure and validated communication link.

4.1 Trust Anchors

For each maintained TIM+ domain, A TIM+ provide SHALL 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 Trusted Connection Establishment

TIM+ requires the use of STARTTLS negotiation as outlined in section 5 of RFC 6120 and SHALL be advertised as mandatory to negotiate in order to establish and secure and trusted connection. The receiving service provider SHALL NOT advertise any other feature other than STARTTLS during the initial stream negotiation process.

The TLS negotiation follows the rules outlined in section 5.4.3.1 of RFC 6120 with the following requirements:

- The receiving entity SHALL present a certificate based on the domain part contained in the "to" attribute of the initial stream header.
- The initiating entity SHALL present a certificate based on the domain part contained in the "from" attribute of the initial stream header.
- Each entity SHALL validate the certificate presented by the counterparty as outlined in section 4.3 of this document.

TIM+ service providers SHALL support a minimum of TLS 1.2 for secure connections between TIM+ service providers; TLS versions prior to 1.2 SHALL NOT be used. TLS connection attempts that request versions lower than TLS 1.2 will be terminated with a "protocol_version" alert in accordance to Appendix E.1 of RFC 5246.

A service provider SHALL establish a discrete connection per TIM+ domain. Upon successful TLS negotiation, the connection will proceed as outlined in section 5.4.3.3 of RFC 6120.

4.2.1 Validity of Long-Lived Connections

Because TIM+ uses connections that can be persisted over long periods of time, it is possible that an entity's certificate may become invalid (in the context of a trusted connection) while the connection remains established. A TIM+ provider SHALL check the status of a long-lived connection as outlined in section 13.7.2.3 of RFC 6120 with the following requirements:

- Certificate status SHALL be checked according to the rules of certificate validation in section 4.3 of this document.
- A valid certificate chain SHALL be checked according to the rules of certificate validation in section 4.3 of this document.

The required interval for checking the status of long-lived connections is not specified and is a matter of local policy.

4.3 Certificate Validation

During the process of TLS negotiation, each service provider SHALL validate the counter party's TLS certificate in conformance to section 13.7.2 in RFC 6120 with the following requirements:

- The certificate chain only needs to be verified to a trust anchor in the service provider's trust anchor store. It does not need to validate the full certificate path to the root certificate. Discussion of certificate paths and path verification is referenced in section 6 of RFC 5280.
    - Service providers SHALL support certificate chain building use the Authority Information Access (AIA) extension (Section 4.2.2.1 of RFC 5280). Service providers MAY use other mechanisms to build a certificate chain, but if no certificate chain to a trust anchor can be built using an alternative mechanism, service providers SHALL attempt to do so using the AIA extension before concluding that a valid chain does not exist.
- Service providers SHALL support the ability to check certificate status using CRLs and MAY support OCSP as an alternative if a certificate publishes certificate status using OCSP.
- A TIM+ provider MAY also apply local policy to either reject or accept connections based on additional attributes and extensions within the certificate.

For the purpose of entity validation, a TIM+ provider will match its reference identifier to an identifier in the presented certificate following the rules outlined in section 13.7.2.1 of RFC 6120. The initiating entity will use the domain in the 'to' address of its initial stream header as its sole reference identifier. The receiving entity will use the domain in the 'from' address of the initial stream header as its sole reference identifier.

Note that a TIM+ domain's DNS SRV target name (*i.e.,* the host name of the receiving entity) is not used as part of the validation phase. Only a match of the reference identifier to a "presented identifier" in the counter party's certificate in accordance to section 6.4.1 or 6.4.2 or RFC 6125 is required. This is further illustrated in section 13.7.1.2.2 of RFC 6120.

5 Rosters and Presence

Although endpoints are addressable destinations that can be communicated with at virtually any time (even when the destination is not connected to the network), real time communication is most effective when both endpoints are available to send and receive messages. Therefore, it is desirable to be aware of the online status or *presence* of an endpoint. To facilitate managing the presence of endpoints, those endpoints are grouped and maintained in a *roster*.

5.1 Roster Management

Rosters are managed following the specifications outlined in section 2 of RFC 6121. The workflow for maintaining and displaying the roster in a client application is out of scope of this document, however, it is RECOMMENDED that an end user client not permanently hide entries in the roster or auto remove entries from the roster even if presence information has not been approved. This also implies that an entry may exist in the roster even if a presence request as described in section 5.2 of this document has either not been acted upon or has been denied.

TIM+ service providers MUST support roster versioning as defined by section 2.6 of RFC 6121.

5.2 Endpoint Presence

Presence subscription and presence information exchanges are outlined in section 3 and 4 of RFC 6121. An endpoint can receive presence information of a destination endpoint only if that destination endpoint approves a request for its presence status to be known (although communication can still occur regardless of the request status as mentioned in section 4.1 of RFC 6121). A TIM+ service provider MAY provide the ability for a presence subscription to be auto approved on behalf of a user, but it SHALL only provide the capability in accordance to section 3.1.3 of RFC 6121.

TIM+ service providers SHALL support the presence pre-approval capability as outlined in section 3.4 of RFC 6121.

There is the potential for use cases where a TIM+ user may wish to stay connected to a TIM+ service provider for the purposes of communicating with its contacts but may wish to appear offline. In this case, the user would broadcast the "unavailable" presence type and subsequently broadcast a different presence type when wishing to appear online again.

With each presence notification sent, a TIM+ endpoint SHALL include a capabilities element as outlined in XEP 0115. If a client's capabilities change during a presence session, the endpoint SHALL send a new presence message with the newly generated verification string.

5.3 Contact Privacy

TIM+ endpoints can control who can see their presence by approving or denying presence requests. However, endpoints cannot control who can send them presence requests (even after they may have denied permission several times) which could lead to frustrating scenarios. Additionally, denying the ability for a counterparty to receive presence information does not limit the counter party for sending messages if the counterparty knows the TIM+ endpoint address. To mitigate this situation, a TIM+ endpoint can add another TIM+ endpoint to a blocklist.

TIM+ service providers SHALL support blocklists as defined by XEP 0191. When an endpoint is added to a blocklist, a TIM+ service provider SHALL NOT cancel any existing subscriptions between the endpoints as described in section 4 of XEP 0191. This implements a "polite blocking" paradigm. A TIM+ service provider SHALL advertise support for blocklists using service discovery queries as outlined in section 3 of XEP 0191.

> **Practice Note:** Although blocklists can be useful, they may also lead to undesired effects. Usage of blocklists that constitute undesired or potentially abuse behavior are matters of policy; TIM+ endpoints should use discretion when adding other endpoints to a blocklist.

6 Feature Discovery

RFC 6120, 6121, and supporting RFCs and XEPs describe a large number of features and capabilities that can be supported (many of which are optional). It is desirable for TIM+ service providers to be able to advertise their capabilities and for TIM+ clients to be able to dynamically discover these capabilities. TIM+ utilizes two specifications for feature and capability discovery:

- Stream negotiation
- Service Discovery

6.1 Stream Negotiation

Stream negotiation is outlined in section 4.3 of RFC 6120. During stream negotiation, a TIM+ server advertises a feature set that a client or another TIM+ server receives during the initial connection sequence. The feature set may change as certain features are negotiated, and some features may be required to negotiate (*e.g.,* STARTTLS).

The version number of the initiating entity SHALL be 1.0 in the initial stream and a TIM+ service provider's initial response stream SHALL also set the version number to 1.0. All mandatory to negotiate features SHALL be satisfied before the stream negotiation process is completed, and the stream negotiation process SHALL be completed before TIM+ messaging can proceed. The order that features are satisfied is not relevant, however additional features MAY be presented after preceding features have been satisfied.

6.2 Service Discovery

Service discovery is outlined in XEP 0030 and allows a TIM+ client or another TIM+ server to query for capabilities of a TIM+ provider. Additionally, it allows a TIM+ server to enumerate "items" associated with an endpoint which can be further traversed to discover more items or capabilities. For example, a TIM+ server may advertise a list of group chat rooms through a list of items, and a subsequent query against a specific chat room may enumerate attributes about the room.

Service discovery (or "disco") information *(i.e.*, queries using the http://jabber.org/protocol/disco#info namespace) queries where the to: address is a TIM+ domain SHALL contain an identity element with a category of *server,* a type of *im*, and name with an arbitrary name that describes the server. Information queries SHALL return one or more features, and features SHALL conform to and be listed in the feature registry and https://xmpp.org/registrar/disco-features.html. The http://jabber.org/protocol/disco#info feature SHALL be returned in the feature list.

To help alleviate network congestion with querying capabilities against large rosters (called a "disco flood"), a TIM+ service provider SHALL support capabilities discovery as outlined in XEP 0115.

6.3 Required Features

TIM+ service providers SHALL support the features outlined in the subsequent subsections.

6.3.1 Required Stream Negotiation Features

During the stream negotiation, a TIM+ provider SHALL support the following features.

- STARTTLS: The STARTTLS feature is mandatory to negotiate and SHALL be the only feature advertised after the initial opening stream is sent.
- SASL: The SASL feature is outlined in section 6 off RFC 6120 and is mandatory to negotiate. TIM+ service providers SHALL use the EXTERNAL mechanism as outlined in section 6.4.3 our RFC 6120 for server to server communication. Specifically, server to server communication will authenticate using mutual TLS and x509 certificates and validate certificate credentials as outlined in section 4 of this document.

If a TIM+ service provider supports TCP based client to server connections defined in RFC 6120, a TIM+ service provider SHALL support SASL SCRAM as an authentication mechanism as outlined in section 13.8.3 of RFC 6120.

A TIM+ service provider can support any type of client to server protocol including proprietary protocols not defined by a XEP or RFC, and authentication requirements are a matter for local policy and specific to the client to server protocol.

- Resource Binding: Resource binding is outlined in section 7 of RFC 6120 and mandatory to negotiate for client to server connections. Resource binding SHALL occur after STARTTLS negotiation and SASL negotiation for client to server connections.
- Compression: Compression is outlined in XEP 0138 and is not mandatory to negotiate. A TIM+ provider SHALL support zlib compression and MAY optionally support other compression algorithms defined in the stream compression methods registry found at https://xmpp.org/registrar/compress.html.
- Roster Versioning: Roster versioning is outlined in section 2.6 of RFC 6121 and is not mandatory to negotiate. Although also outlined in XEP 0237, XEP 0237 "has been incorporated into RFC 6121." However, XEP 0237 is a helpful reference and contains useful guidelines and examples.

A TIM+ service provider MAY support other features at stream negotiation time, however additional features SHALL NOT be mandatory to negotiate.

6.3.2 Required Service Discovery Features

A TIM+ provider SHALL support the following feature as part of a service discovery request. Different features will be available depending on the entity type that is queried and will be indicated below.

- Service Discovery: Service discovery is outlined in XEP 0030 and further detailed in section 6.2 of this document. Service discovery SHALL be returned as a supported feature for every service discovery query as defined in XEP 0030.
- Multiuser Chat (MUC): MUC is outlined in XEP 0045 and is further detailed in section 9 of this document. MUC support SHALL be returned as a supported feature via service discovery queries targeted as defined in section 6 of XEP 0045.
- Vcard: Vcards are outlined in XEP 0054 as a mechanism to query for identity claims of an endpoint. Each TIM+ endpoint SHALL have a Vcard associated with it. Required attributes for a Vcard are a matter of local policy and out of scope for this document. Vcard support SHALL be returned as a supported feature via service discovery queries targeted at TIM+ endpoints.
- Chat State Notifications: Chat state notification is outlined in XEP 0085 and support SHALL be returned as a supported feature via service discovery queries targeted at TIM+ endpoints
- Offline Storage: Offline storage is outlined in XEP 0160 and SHALL be returned as a supported feature via service discovery queries as defined in section 4 of XEP 0160.

- Jingle: Jingle is outlined in XEP 0166 and SHALL be returned as a supported feature via service discovery query as defined in section 11 of XEP 0166.
- Jingle File Transfer: Jingle file transfer is outlined in XEP 0234 and SHALL be returned as a supported feature via service discovery query as defined in section 11 of XEP 0234.
- Jingle SOCKS5 Bytestreams: Jingle SOCKS5 Bytestreams are outlined in XEP 0260 and SHALL be returned as a supported feature via service discovery query as defined in section 5 of XEP 0260.
- Jingle In-Band Bytestreams: Jingle In-Band Bytestreams are outlined in XEP 0261 and SHALL be returned as a supported feature via service discovery query as defined in section 4 of XEP 0261.
- Blocking Comment: The blocking command is outline in XEP 0191 and and SHALL be returned as a supported feature via service discovery query as defined in section 3 of XEP 0191.

6.3.3 Additional Required XEPs

A TIM+ provider SHALL support the following XEPs that are not dynamically discoverable but are used in the normal operation of a TIM+ server.

- Capability Discovery: Capability Discovery is outlined in XEP 0115 as a mechanism to alleviate “disco flood” when discovering capability information about a large collection of endpoints. TIM+ client SHALL broadcast capabilities as outlined section 5.2 of this document.
- Delayed Delivery: Delayed delivery is outlined XEP 0203 as a mechanism to timestamp messages that cannot be delivered at the time they were sent.

7 Chat

A key value proposition of TIM+ is the “user to user chat” which allows two TIM+ endpoints to communicate in bursts of interactive messages over a relatively short period of time. TIM+ also supports storing messages targeted to disconnected TIM+ endpoints that will be delivered the next time the target endpoint connects to a TIM+ service provider.

7.1 User to User Chat

Two TIM+ endpoints exchange messages with each other in one-to-one chat sessions as outlined in section 5.1 of RFC 6121. In the message exchange, the message “type” SHALL be set to “chat.”

If the initiating TIM+ endpoint does not share presence information at the time the chat is initiated with the destination endpoint, then the initiating entity of the chat SHALL send a directed presence message to the destination endpoint in accordance with section 4.6 of RFC 6121. If the receiving entity responds back to the initiating entity, then the receiving entity SHALL send a directed presence message to the initiating entity if the receiving entity does not already share presence information with the initiating entity. When the chat session is completed, a directed presence with a type of "unavailable" shall be sent from an entity to the counterpart entity if the entity does not share presence information with the counterpart entity.

In the scenario above, a receiving entity MAY choose not to respond to the initiating entity. In this case, no directed presence is sent to the initiating entity.

> **Practice note:** If an initiating entity sends a message to a receiving entity that does not share presence information, the receiving entity's TIM+ edge client might implement a type of "Opt In" feature that only displays messages from entities that he shares presence information with. In this case the message would be ignored by the edge client or simply not displayed. However, the receiving entity's TIM+ service provider will still send a successful delivery notification message to the initiating entity as outlined in section 8.2.1 of this document. In this case, the receiving entity's edge client SHOULD send an appropriate message indicating that the message was rejected. This rejected message SHALL NOT be a substitute for a positive or negative delivery notification as defined by section 8.2 of this document.

7.1.1 Chat Subjects and Threads

A message SHALL NOT include a subject however a message SHALL include a thread element as defined in section 5.2.5 of RFC 6121**.** The initial thread id of a user to user chat shall be created by the TIM+ endpoint that initiates the chat session, and the same thread id SHALL be present in each message exchanged by each endpoint throughout the duration of the chat session or until a TIM+ endpoint changes the context of the chat session. Chat session context is beyond the scope of this document but could be defined by additional implementation guides.

7.1.2 Extended Content

TIM+ implementations MAY contain extended content within a chat message as defined in section 8.4 of RFC 6120. The following sections enumerate requirements for the use of specific extended content name spaces. Extended content that is not enumerated in the following sections or incorporated by other sections of this document through the inclusion of RFCs, XEPs, or TIM+ implementation guides SHOULD NOT be used in user to user chat messages unless negotiated by the endpoints. Procedures for negotiating additional supported types of extended content between endpoints is beyond the scope of this document.

7.1.2.1 Alternate Message Body Representation

A TIM+ endpoint MAY support an alternative format of the message body using extended content that conforms to the XHTML-IM mark up as outlined in XEP 0071. If a TIM+ endpoint does support generating XHTML-IM content, then the content SHALL conform to the recommended profile outlined in section 7 of XEP 0071. If a TIM+ endpoint receives a message containing XHTLM-IM content and supports XEP 0071, then the client SHALL display the content in the XHTLM-IM element in favor of the general body element of the message. TIM+ endpoints that support XEP 0071 SHALL indicate support of the feature in service discovery requests (XEP 0030) as well as in entity capability requests (XEP 0115).

7.2 Off-Line Message Storage

User to user messages can be sent to a destination TIM+ endpoint even if the destination endpoint is not connected to a TIM+ service provider (NOTE: a destination with whose presence is “unavailable” does not necessarily indicate that the destination is not connected to a TIM+ service provider). In this case, messages targeted to disconnected endpoints SHALL be stored on the destination endpoint’s server as offline messages. A TIM+ service provider SHALL provide offline storage for messages with the type “chat” with the exception of transient messages (detailed in section 8) as outlined in XEP 0160. A TIM+ provider SHALL deliver all offline messages to a TIM+ endpoint after the endpoint has sent its initial presence broadcast message unless the TIM+ endpoint has decided to use XEP 0013 as described later in this section.

A TIM+ service provider MAY restrict the maximum amount of storage allocated to offline message storage, however the maximum storage size is a matter of local policy. If the maximum storage size has been exceeded, then a TIM+ service provider SHALL return an error of “service unavailable” to the sending TIM+ endpoint.

A TIM+ service provider MAY support “flexible offline message retrieval” as defined by XEP 0013, however it SHOULD be used by TIM+ endpoints only in specific circumstances where an endpoint would consider a flood of offline messages to be disruptive (for example, if a TIM+ endpoint had not connected to a server for several days or weeks and expects a high number of offline messages). If a TIM+ endpoint chooses to use XEP 0013, then it SHALL send a request for message headers before sending its initial presence broadcast message. If the request for headers is received by a TIM+ provider prior to a TIM+ endpoint sending its initial presence broadcast message, then the TIM+ provider SHALL NOT deliver messages to the endpoint using XEP 0160. This choice of delivery mechanisms is illustrated in section 3 of XEP 0013.

Favorability of XEP 0013 vs XEP 00160 has been debated for quite some time in the RFC 6120 community, and it has been noted that there is a possibility that XEP 0013 might be deprecated at some future time. The TIM+ specification recommends the use of XEP 0160 over XEP 0013.

A TIM+ service provider will time stamp offline messages as outlined by XEP 0203 using a textual delay reason of “Offline Storage.” The time stamp information will be present in messages delivered using both XEP 0160 and XEP 0013.

A TIM+ provider SHALL advertise support for offline storage using service discovery queries as outlined in section 4 of XEP 0160. If a TIM+ provider supports XEP 0013, then it SHALL advertise support using service discovery queries as outlined in section 6 of XEP 0013.

8 User to User Chat Notifications

User to user chat notifications are split into two categories: chat state notifications and message delivery notifications.

8.1 Chat State Notifications

Many modern instant messaging platforms provide real time feedback regarding the messaging activity of one endpoint to another endpoint. TIM+ endpoints SHALL send chat state notifications as outlined by XEP 0085 and SHALL only be required to send “active” and “composing” chat state messages. This requirement is true for both user to user chats and group chats. Chat state notification messages are transient and SHALL NOT be stored in off-line storage.

A TIM+ endpoint SHALL advertise support chat notification using service discovery queries as outlined in section 4 of XEP 0085. Because all TIM+ endpoints are required to send chat state notifications and contrary to section 5.1 of XEP 0085, it is not necessary to explicitly query an endpoint for chat state notification support.

8.2 Delivery Status Notifications

RFCs 6120 and 6121 cover many error conditions in which a chat message would not be delivered to a TIM+ destination, however these error conditions are not exhaustive. To create a deterministic delivery mechanism, TIM+ utilizes semantics defined in XEP-0079 to notify a TIM+ source endpoint about the delivery status of a user to user chat message. Because TIM+ does not implement the majority of the XEP-0079 specification, a TIM+ provider SHALL NOT advertise the use of XEP-0079 through any service discovery mechanism.

All non-transient user to user chat messages will result in either a delivery status notification, an off-line storage notification, or an error notification, and the delivery status notifications will be addressed to the TIM+ endpoint of the original message sender. User chat delivery notifications are considered to be transient messages however user chat delivery notification SHALL be stored offline in the event the recipient of the notification is not connected to a TIM+ provider and be delivered to the destination TIM+ endpoint as outlined in section 7.2 of this document.

> **Practice Note**: User chat status notifications are intended to provide feedback to the original message sender regarding the delivery status of a message. TIM+ workflows should provide an appropriate indication as to the delivery status of a message without impeding the use of the workflow.

8.2.1 Delivered Notification

Non transient user to user messages will result in a “deliver” notification being generated upon the recipient’s TIM+ service provider successfully delivering the message to the recipient’s TIM+ client. The format of the delivered notification SHALL be compliant with a notify result as described in section 3.4.4 of XEP 0079.

The deliver notification message stanza SHALL include the following attributes values:

- The id attribute of the message element SHALL be set to the id value of the original message.
- The status attribute of the amp element SHALL be set to a value of notify.
- The action attribute of the rule element SHALL be set to a value of notify.
- The condition attribute of the rule element SHALL be set to a value of deliver.
- The value attribute of the rule element SHALL be set to a value of direct.
-

8.2.2 Off-Line Storage Notification

In the event that a non-transient user to user message is successfully placed in offline storage, the TIM+ service provider placing the message into storage SHALL send a “stored” notification message. The format of the stored notification SHALL be compliant with a notify result as described in section 3.4.4 of XEP 0079.

The stored notification message stanza SHALL include the following attributes values:

- The id attribute of the message element SHALL be set to the id value of the original message.
- The status attribute of the amp element SHALL be set to a value of notify.
- The action attribute of the rule element SHALL be set to a value of notify.
- The condition attribute of the rule element SHALL be set to a value of deliver.
- The value attribute of the rule element SHALL be set to a value of stored.

At the time an offline message is delivered to the TIM+ destination endpoint by the use of either XEP 0013 or XEP 0160, a delivered notification SHALL be sent for each message delivered to the destination endpoint.

8.2.3 Delivery Failure Notification

RFCs 6120, 6121, and relevant XEPs dictate the generation and delivery of error conditions if a user to user chat message cannot be delivered to the TIM+ destination endpoint. Although the RFCs and XEPs are not exhaustive in the number of error conditions that can occur, they do cover a significant number of error scenarios. In the event that an error condition is not generated nor received by the original message TIM+ service provider, a delivered notification is not received, nor an offline storage notification is received within a given amount of time, then the original message TIM+ service provider SHALL generate a remote-server-timeout error message as outlined in section 8.3.3.17 of RFC 6120. The amount of time a TIM+ service provider should wait before generating a remote-server-timeout error is a matter of local policy.

9 Group Chat

Another key value proposition of TIM+ is the “group chat” which allows multiple TIM+ endpoints to communicate collaboratively inside a virtual room. Rooms have configurable attributes such as the maximum number of participants in a room.

A TIM+ service provider SHALL support group chats. The specifications for group chats are outlined in XEP 0045 and defines several options for room types, roles, affiliations, and other parameters specific to a room. TIM+ only implements a profiled subset of these options and defines default values for roles, affiliations, and room parameters.

The following subsections describe the profiled subset.

9.1 Service Discovery

A TIM+ service provider SHALL advertise support for group chats using service discovery queries as outlined in section 6.1 of XEP 0045. The JID of the group chat service returned by the “disco/items” query SHALL be groupchat.<healthcare organization domain>. For example, if the TIM+ healthcare organization domain is samplepractice.org, the JID of the chat service would be groupchat.samplepractice.org.

A TIM+ service provider SHALL advertise features supported by its group chat service as outlined in section 6.2 of XEP 0045. The identity element of the information/query response SHALL have the following value for its attributes:

- category: conference
- type: text
- name: TIM+ Group Chat Service

TIM+ rooms are hidden and SHALL NOT be discovered using room discovery as outlined in section 6.3 of XEP 0045. A “disco/items” query sent to the group chat service JID SHALL return and empty query element.

Example response:

```
<iq id=’qldkje4921’
   from=’prov@samplepractice.org’
   to=’samplepractice.org
   type=’result’ >
   <query xmlns=’http://jabber.org/protocol/disco#items’/>
</iq>
```

Because all TIM+ endpoints SHALL implement group chats, it is not necessary to send a disco/info request to a TIM+ endpoint to determine group chat capabilities. Group chat rooms are considered to be private, so any query to discover what rooms a TIM+ endpoint currently occupies or is affiliated with SHALL return an empty query element as outlined in section 6.7 of XEP 0045.

9.2 Group Chat Rooms

TIM+ group chats are ad-hoc dialogs between multiple participants and take place in temporary rooms meaning that the room is automatically destroyed when the last person exits the room. They are intended to be a private space for only those that have been invited to the conversation where each participant has an equal voice (*i.e.,* unmoderated). Although rooms allow for nicknames, they are not anonymous meaning that a room participant's real endpoint name is fully accessible.

9.2.1 Room Types

Section 4.2 of XEP 0045 defines several room types where a room may be of any combination of those types regardless if the combination is sensible or not. TIM+ rooms SHALL consist of the following type combination:

- Temporary
- Hidden
- Unmoderated
- Non-Anonymous
- Members-only
- Non-password protected

Practice note: Members-only rooms are considered rare according to section 7.8 of XEP 0045, however they are necessary to protect the privacy of rooms in the event another TIM+ endpoint is able to guess a room name and enter without having a member affiliation.

9.2.2 Room Roles

Every occupant within a room SHALL have a role of "participant" except the creator of the room who shall have a role of "moderator." All participants of a room SHALL have the ability to invite other occupants to the room. Occupants SHALL NOT have the ability to change roles within a room; room roles are static.

Practice note: The term "moderator" is defined in section 4.1 of XEP 0045, however a room moderator does not have the ability to remove occupants or grant and remove an occupant's voice. A moderator is a default assigned role to the room creator, but the moderator does not control the room.

9.2.3 Room Affiliations

Every occupant within a room SHALL have an affiliation of "member" except the creator of the room who shall have a role of "owner." Occupants SHALL NOT have the ability to change affiliations within a room; room affiliations are static. Room owners SHALL NOT have the ability to change the room configuration or destroy the room. Room configurations are static, and rooms are destroyed when the last occupant exits the room as described in section 9.2.4 of this document.

9.2.4 Room Creation

TIM+ rooms are on demand/instant rooms that are created using the process and protocol outlined in sections 10.1.1 and 10.1.2 of XEP 0045. TIM+ room names SHALL be random and globally unique. A TIM+ service provider SHALL automatically create a default configuration for a room, and room attributes are not configurable by a TIM+ endpoint. An attempt to request a room configuration form SHALL result in an error of "not-allowed". Room attributes are defined in section 16.5.3 of XEP 0045. To conform with room types outlined in section 9.2.1 of this document, the following attributes SHALL have the following values:

- roomconfig_persistentroom: ***0***
- roomconfig_membersonly: ***1***
- roomconfig_moderatedroom: ***0***
- roomconfig_passwordprotectedroom: ***0***
- roomconfig_publicroom: ***0***
- roomconfig_whois: ***anyone***

A TIM+ service provider SHALL also set default values for the following room parameters defined in section 16.5.3 of XEP 0045. Some default values are a matter of local policy while others have mandatory default values.

- maxhistory: set by local policy
- roomconfig_allowpm: ***none***
- roomconfig_allowinvites: ***anyone***
- roomconfig_enablelogging: set by local policy
- roomconfig_getmemberslist: ***anyone***
- roomconfig_changesubject: ***0***
- roomconfig_presencebroadcast: ***anyone***

The creator of a room SHALL also be assigned the role of moderator and an affiliation of owner. Once a room has been created, its attributes are static and cannot be changed by any occupant including the owner.

Room logging is a matter of local policy and the process for retrieving room logs is a matter of local implementation. If room logging is enabled, a TIM+ service provider SHALL warn occupants by including the status code "170" in the initial room presence message as outlined in section 7.2.12 of XEP 0045.

9.2.5 Room Destruction

TIM+ group chat rooms are temporary and are destroyed when the last occupant exits the room. A TIM+ service provider SHALL automatically destroy a group chat room when the last occupant exits the room.

9.3 Group Chat Room Participation

Participation in a group chat room is generally outlined in section 7 of XEP 0045. Because of the specificity of room types defined in section 9.2.1 of this document, not all rules in section 7 of XEP 0045 are applicable; only those rules applicable to TIM+ room types as outlined in section 9.2.1 of this document are relevant.

9.3.1 Room Invitations

TIM+ group chat rooms are members-only rooms and therefore require an invitation before an occupant can enter the room (except for the room owner who is automatically made a member at the time the room is successfully created). Potential group chat occupants SHALL be invited to a room using mediated invitations as described in section 7.8.2 of XEP 0045. Any existing occupant within a room SHALL be able to send a mediated invite. Upon sending an invitation, a TIM+ service provider SHALL automatically add the invitee to the room's members list. If the invitee declines the invitation (vs. ignoring the invitation), the invitee SHALL be removed from the room's members list.

TIM+ group chat rooms SHALL NOT support room registration as outlined in section 7.10 of XEP 0045.

9.3.2 Room Entrance

If a TIM+ endpoint wishes to enter a room after receiving an invitation, the endpoint SHALL send a presence stanza to the room as outlined in section 7.2.1 of XEP 0045. Although XEP 0045 allows for an endpoint to use virtually any nickname in the room, an endpoint SHOULD use a nickname that articulates the endpoint's real name. TIM+ group chat rooms SHALL NOT have reserved nicknames as outlined in 7.12 of XEP 0045, and reserved nickname lookup is not necessary. Rules for nickname anonymity are a matter of local policy. Room nicknames are not changeable once an endpoint becomes an occupant of a room, and any attempt for an occupant to change its nickname SHALL result in a <forbidden> error.

If a TIM+ service provider can successfully add the endpoint to the room and make the endpoint a room occupant, then the TIM+ service provider SHALL broadcast presence information outlined in section 7.2.2 of XEP 0045. The TIM+ service provider SHALL include each occupants' full JID in the presence messages as outlined in section 7.2.3 of XEP 0045.

TIM+ endpoints are denied entry into a group chat room under the following conditions:

- If a TIM+ endpoint attempts to enter a room that it was not invited to (*i.e.*, the endpoint is not on the members list), then the TIM+ service provider SHALL deny entrance as outlined in section 7.2.6 of XEP 0045.
- If a room already contains another TIM+ endpoint using the same nickname, then the TIM+ service provider shall deny entrance as outlined in section 7.2.8 of XEP 0045.
- If a room has reached its maximum number of occupants, then the TIM+ service provider SHALL deny entrance as outlined in section 7.2.9 of XEP 0045.

9.3.3 Room Discussion History

Upon completion of sending presence information for a group chat room, a TIM+ service provider SHALL send a room's discussion history as outlined by section 7.2.13 of XEP 0045 and based on the room's default setting. Each message in the discussion history SHALL include the full JID of the original sender of the message.

A TIM+ endpoint MAY additionally control the amount of discussion history received upon room entrance by including a <history> element in its initial room presence message as outlined in section 7.2.14 of XEP 0045.

TIM+ group chat rooms SHALL NOT have associated subjects, therefore a TIM+ service provider SHALL send an empty room subject messages following the room discussion history as outlined in section 7.2.15 of XEP 0045.

9.3.4 Room Presence Status

Similar to a TIM+ endpoint broadcasting its presence status to subscribed parties, a TIM+ endpoint SHALL send its presence status to all group chat rooms that it is an occupant of as outlined in section 7.7 of XEP 0045. A TIM+ service provider SHALL broadcast the presence status change to all room occupants as lined in the same section (7.7).

9.3.5 Room Messaging

A TIM+ service provider SHALL support sending group chat messages to all occupants within a room as outlined in section 7.4 of XEP 0045. Because rooms are unmoderated, all occupants are granted a "voice" within the room. A TIM+ endpoint SHALL include an id attribute in the message element of the group chat message, and a TIM+ service provider SHALL reflect the same message id that was generated by the TIM+ endpoint in the message that is delivered to the occupants.

As detailed in section 3 of XEP 0160, group chat messages SHALL NOT be stored offline for later delivery.

A TIM+ service provider SHALL NOT support private messaging outlined 7.5 of XEP 0045. Private messaging through a group chat room is useful when the bare or full JIDs of the occupants are not available (due to room configuration) and initiating a user to user chat is problematic. TIM+ rooms do not hide the full JIDs of room occupants, so user to user chats are easy to initiate. Private messages are effectively user to user chats, and private messages lower the quality of service relative to user to user chats due to the lack of offline storage and delivery notifications.

9.3.5.1 Group Chat State Notifications

Group chat state notifications use the same rules as user to user chat state notification outlined in section 8.1 of this document. Group chat state notifications SHALL be sent to the room and delivered to all room occupants in the same method group chat messages are sent.

9.3.5.2 Group Chat Delivery Status Notifications

Group chat delivery status notifications use the same rules as user to user delivery status notifications outlined in section 8.2of this document with the exception that group chat messages SHALL NOT create Offline Storage notification messages.

A TIM+ service provider SHALL send a delivery notification per room occupant. The delivery notification messages SHALL use the same attributes as those describes in section 8.2 of this document with the following exceptions:

- The from attribute of the message element SHALL be set to JID of the original recipient. Because room nicknames are ephemeral and are only relevant for the duration of a room, the original recipient's JID is used to unambiguously identify the endpoint.
- The to attribute of the amp element SHALL be the JID of the original recipient of the message. Because room nicknames are ephemeral and are only relevant for the duration of a room, the original recipient's JID is used to unambiguously identify the endpoint.
- The from attribute of the amp element SHALL be the JID of the original sender of the message.

Identical to section 8.2.3 of this document, a remote-server-timeout error message will be generated if no positive or negative notification message is received within a given amount of time.

> **Practice Note:** Delivery notifications in a group setting can result in a large amount of notifications being delivered to the message sender, and it may not be practical to display delivery notifications messages within a TIM+ enabled workflow. Delivery notifications for group chats are generally intended to be used as a tracking and potentially an auditing mechanism for TIM+ enabled applications.

9.3.6 Room Exit

To exit a group chat room, a TIM+ endpoint SHALL send a presence stanza of unavailable as outlined in section 7.14 of XEP 0045. A TIM+ service provider SHALL then send subsequent unavailable presence stanzas outlined in the same section (7.14). Upon exit of the last occupant of the room, the TIM+ service provider SHALL destroy the room.

10 File Transfer

RFC 6120 implementations have commonly used XEPs 0095 and 0096 to negotiate stream connections and transfer files between endpoints, however these XEPs have been deprecated in favor of the Jingle protocol defined by XEP 0166. XEP 0096 (SI File Transfer) is the only protocol that utilizes the stream initiation and negotiation capabilities defined in XEP 0095 while Jingle is the stream negotiation mechanism utilized by several stream-based protocols such as file transfers and voice and video streams. Because Jingle supports the negotiation of multiple stream protocols, it is advantageous to use a single specification for the initiation and negotiation and various TIM+ stream-based modalities.

10.1 File Transfer Protocol

TIM+ service providers and endpoints SHALL support file transfers. The TIM+ file transfer negotiation protocol is outlined in XEP 0234. Although XEP 0234 allows any endpoint to either offer a file or request a file, TIM+ only defines the "File Offer" use case described in section 4.1 of XEP 0234 where a TIM+ endpoint takes on the initiator role content sender and Jingle session columns. The file transfer process begins with the negotiation of a session as outlined in section 6.1 of XEP 0234.

A TIM+ provider SHALL advertise support for file transfers using service discovery queries as outlined in section 11 of XEP 0234. In addition, A TIM+ provider SHALL advertise support for the SOCKS5 and In-Band Bytestream transport mechanisms as outlined in section 5 of XEP 0260 and section 4 of XEP 261 respectively.

10.1.1 Application Format

The application format section of the request (*i.e.*, the "description" XML element) SHALL contain the following elements:

- Date
- Description
- Media Type
- Name
- Size
- Hash or Hash Used
  i) The hash algorithm SHALL be sha-256.
  ii) The hash value MAY be sent at a later time if it is not known at the time the file transfer session is initiated. In this case, the hash value in the session-initiate message is empty, the application formation section uses the "Hash Used" element instead of a "Hash" element. In this case, the sender SHALL also send a subsequent "session-info" message once the hash value has been calculated as described in section 8.2 of XEP 0234.

The application format section of the request SHALL NOT include a range element as range transfers are not supported by TIM+.

A TIM+ endpoint MAY send multiple files per session by adding multiple "content" elements in the session-initiate method.

10.1.2 Transports

TIM+ file transfers SHALL support Jingle SOCKS5 and Jingle In-Band Bytestream as transport mechanisms as defined by XEPs 0260 and 0261 respectively. TIM+ endpoints SHALL attempt to initiate the session using Jingle SOCKS5 first, and use Jingle In-Band Bytestreams if a SOCKS5 session cannot be established or fails. Falling back to Jingle In-Band Bytestreams are negotiated using the same stream id as the SOCKS5 stream by use of the "transport-replace" message.

10.1.2.1 Jingle SOCKS5 Transport

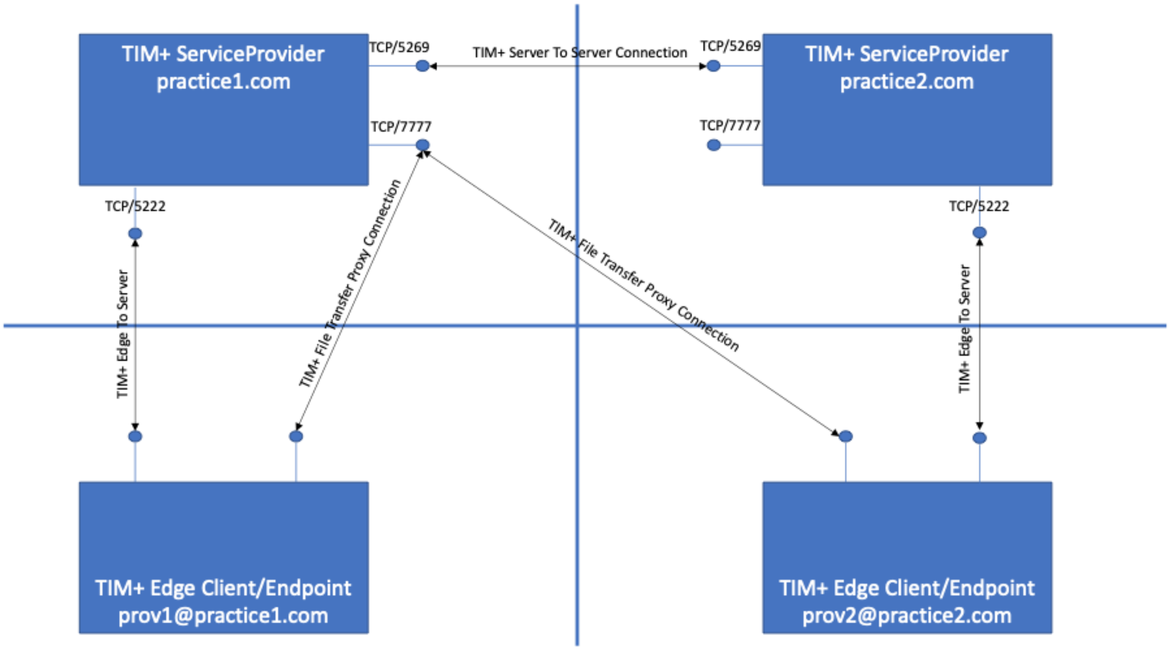
TIM+ service providers and endpoints SHALL support file transfers using the Jingle SOCKS5 transport as defined by XEP 0260 and further described by XEP 0065 (XEP 0260 defers many of the implementation details to XEP 0065), however TIM+ service providers SHALL only offer proxied connections as direct connections between TIM+ endpoints are inherently insecure. A TIM+ service provider SHALL deploy at least one proxy service for the purpose of SOCKS5 file transfers on TCP port 7777.

Proxy servers are discovered by TIM+ endpoints as described in section 4 of XEP 0065. The JID of the proxy service returned in the "disco/items" request SHALL be ftproxystream.<health

organization domain>. For example, if the TIM+ healthcare organization domain is samplepractice.org, the JID would be ftproxystream.samplepractice.org. A proxy server MAY support more than one network connection endpoint, and SHOULD make at least one network connection available on the public internet.

Once the proxy server(s) and corresponding network address information for the initiating TIM+ endpoint have been discovered, the TIM+ endpoints will negotiate a SOCKS5 proxy connection in accordance to section 2 of XEP 0260. The receiving TIM+ endpoint (*i.e.,* responder) SHALL only include transport candidates that were sent by the initiating TIM+ endpoint in the session-accept message; a responder SHALL NOT add additional candidates to the session-accept message.

The following diagram illustrates the connection points between the TIM+ endpoints and the service providers. In this diagram, the endpoint prov1@practice1.com offers to send a file to the endpoint prov2@practice2.com. Note that because prov1 is offering the file to prov2, prov1's proxy server is the proxy server used to moderate the transport of the file.



10.1.2.1.1 Jingle SOCKS5 Transport Security

XEPs 0260 and 0065 do not define security requirements for proxied connections. In order to secure the proxy connection, TIM+ endpoints SHALL authenticate to the SOCKS5 proxy server and establish an encrypted connection.

TIM+ SOCKS5 proxy servers SHALL support authentication using the username/password method as outlined in RFC1929 over an encrypted TLS connection. TIM+ SOCKS5 proxy servers SHALL support a minimum of TLS 1.2 for secure connections; TLS versions prior to 1.2 SHALL

NOT be used.   TLS connection attempts that request versions lower than TLS 1.2 will be terminated with a “protocol_version” alert in accordance to Appendix E.1 of RFC 5246.

A TIM+ proxy server shall use the Service Name Indication (SNI) TLS extension to indicate the certificate to be returned in the Server Hello message. The SNI name SHALL be the JID of the proxy service returned in the “disco/items” request. A TIM+ endpoint SHALL initiate a TLS connection to the proxy server, SHALL use the JID as its reference identifier, and SHALL match its reference identifier to an identifier in the presented proxy server’s certificate following the rules outlined in section 13.7.2.1 of RFC 6120.

> **Practice Note:** The certificate presented SHOULD be the same certificate used for TIM+ server to server connections as the certificate SHALL contain a DNS-ID identifier containing the proxy server’s JID.

TIM+ SOCKS5 proxy servers SHALL support a one time username and password that TIM+ endpoints can use to authenticate to the proxy server. A one time username and password can be obtained by sending an Info/Query get message to the JID of the proxy server with a single <credRequest> child element qualified by the ‘http://standards.directtrust.org/DS2019-02/filetransfer/proxy/auth#onetimeup’ namespace. The namespace identifies this transaction type to be a request for a one time credential to the proxy server.

Example:

```
<iq id=’csdke4023’
  to=’ftproxystream.samplepractice.org’
  type:’get’>
  <credRequest xmlns='http://standards.directtrust.org/DS2019-
02/filetransfer/proxy/auth#onetimeup' />
</iq>
```

The TIM+ service provider SHALL respond with an Info/Query result message with the following information in the <credRequest> element.

- Credentials: Contains the credentials to authenticate to the proxy server. The credentials element contains the following attributes:
  - Subject: The one time username used for authenticating to the proxy server.
  - Secret: The one time password used for authentication to the proxy server.
- CA: A pem representation of the proxy server’s certificate used to sign its TLS certificate. This certificate will be used later to validate the TLS connection to the proxy server. The representation of the certificate SHALL be a base64 encoding of the DER encoded format of the certificate. This is effectively a PEM representation of the certificate without the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- tags.

Example response to the previous query:

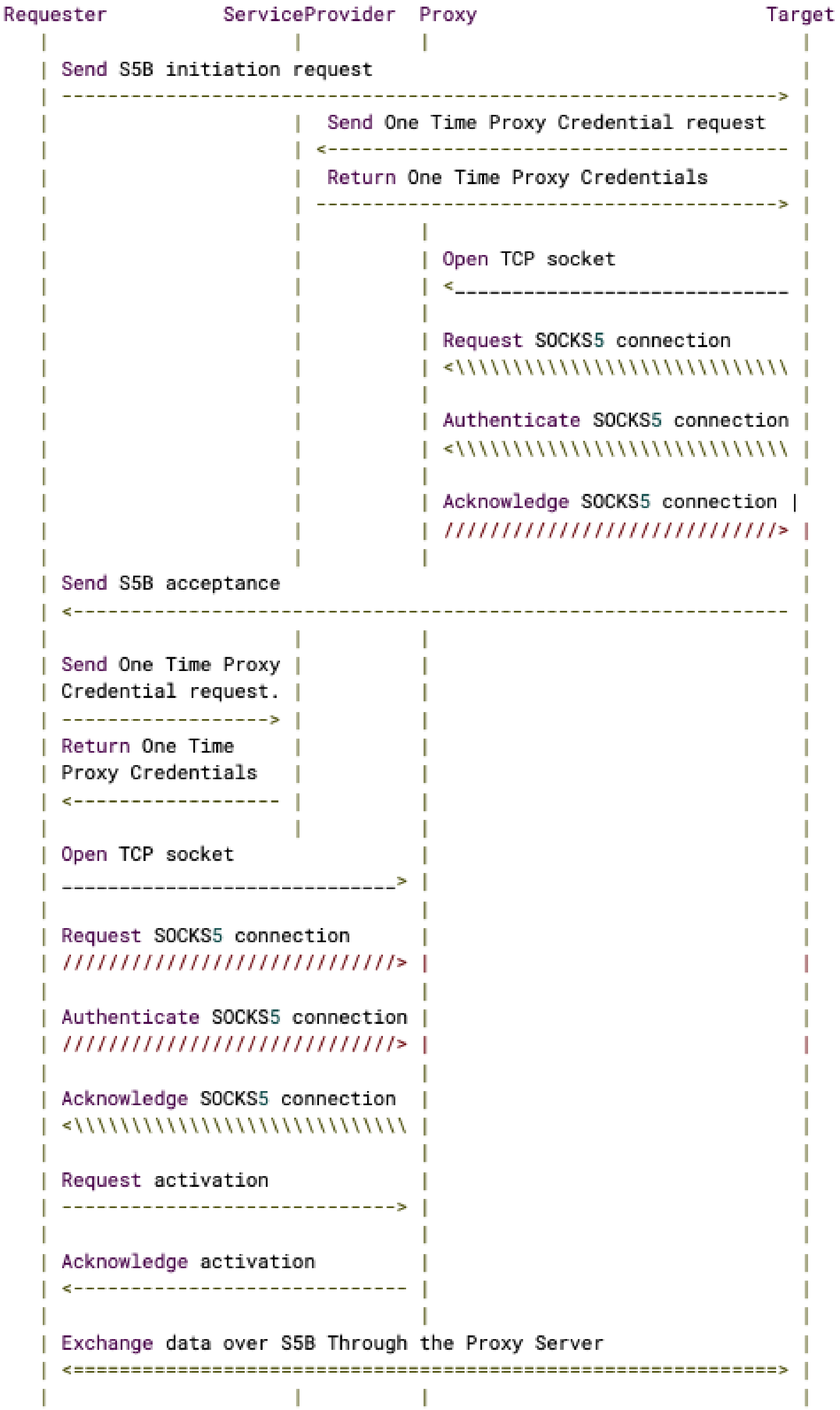
```
<iq id=’csdke4023’
  from=’ftproxystream.samplepractice.org’
  to=’sampledoc@samplepractice.org
  type=’result’>
  <credRequest xmlns='http://standards.directtrust.org/DS2019-
02/filetransfer/proxy/auth#onetimeup' >
     <credentials subject=’eickdlwiejed’
                  secret=’8dk3mdl302d9j3sksp3ksl3’ />
   <ca>
MIIDMTCCAhmgAwIBAgIUPOWXkDAcZ9AjqPMQBaotdRtJKlkwDQYJKoZIhvcNAQELBQA
wETEPMA0GA1UEAxMGcm9vdENBMB4XDTE4MTAwODIwMzAxNFoXDTE5MTAwODIwMz
AxNFowETEPMA0GA1UEAxMGcm9vdENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC
gKCAQEAqEIHGn3X5zIfH7kNT0J8aloM8BOGYYozIEksLJhjy3ZJJTJeScxIEv/U3sw2iTf1X2Sk
wUPkd/5T0GdTJe+5JY5oJFNOJlaO+8pcJ/UctrDuG3AeeIdR3ZmupyCrbcD+rRfhMaykFBHY
zhpsqAuVdWAvG2995mqFyzBVnRjK98Dz5e3txCgfhlcLkM3xg01uZUEjmp+QSNqg+dE5ka
fxil/GfaP6i7TLbmIfg5vGYjcK0ws1HsI7M4VTrOime/dDQP7pVuN/7vml4jQtDxrbET7nQWsk
na35ztzagGU9qIwpPM8t3+U8b8ASTYxc3Tp6oMpBiAv5Le1mWWRzwfSaRQIDAQABo4GA
MH4wHQYDVR0OBBYEFOXjuomG9Ud4GPTNjSJBaxhf2mNLMEwGA1UdIwRFMEOAFOXju
omG9Ud4GPTNjSJBaxhf2mNLoRWkEzARMQ8wDQYDVQQDEwZyb290Q0GCFDzll5AwHGf
QI6jzEAWqLXUbSSpZMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBA
EJ9+njsPiIZh5MSUpJX+doHbIUU+2KPe9hMTYiIlh2NJrzPMtTO+kRlWInscQMorQ3/sGUP/
oj4lBYdxpg+WcKicn5uYJsCMk8GaW+bfw6t6HTEw/hEHJersgtMuMUv2IecyZbwdR0grxM
GMpq60tvd9YiIi5ZVRa5cHqTryGqAA/6W8SNy/BXeuHRac0tGhszTCjceSttRJgTNb1i/J2f74
HRoe0TQKrZ2W7kGOuUiPSWn9ziVjKwnXJKZw2FyHPtpnQhKCaVFs95LB5hRRfgz3E36YJS
Xj4PLCMqsONNL3wW/HUhAwXopVgwKOJSYQYnt8mqFqWFAeiZ8QMiW4lM=
    </ca>
  <credRequest >
</iq>
```

The credentials SHALL allow a TIM+ endpoint to authenticate to the proxy server one time and before the credentials reach an expiration time. If the SOCKS5 connection is broken, then the TIM+ endpoint will need to request new credentials.

The length of the credential’s expiration time is a matter of local policy but is recommended to be a short time period (possibly no longer than one minute or less). TIM+ service providers SHOULD implement good security practices in terms of credentials character sets, length, and randomness. The username SHALL be unique for the duration that the credentials are not expired and the password SHALL use entropy of no less than 128bits.

To ensure validity of the proxy server connection, a TIM+ endpoint SHALL ensure that the proxy server’s TLS certificate chains to the certificate returned in the CA element of the Info/Query result message.

The data flow diagram below is a modification of the diagram from section 6.2 of XEP 0065 with the additional credential request and authentication steps.



```
Requester          ServiceProvider  Proxy                         Target
   |                     |          |                                 |
   | Send S5B initiation request                                      |
   | ---------------------------------------------------------------> |
   |                     |  Send One Time Proxy Credential request    |
   |                     | <----------------------------------------- |
   |                     |  Return One Time Proxy Credentials         |
   |                     | -----------------------------------------> |
   |                     |          |                                 |
   |                     |          | Open TCP socket                 |
   |                     |          | <______________________________ |
   |                     |          |                                 |
   |                     |          | Request SOCKS5 connection       |
   |                     |          | <\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ |
   |                     |          |                                 |
   |                     |          | Authenticate SOCKS5 connection  |
   |                     |          | <\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ |
   |                     |          |                                 |
   |                     |          | Acknowledge SOCKS5 connection |
   |                     |          | //////////////////////////////> |
   |                     |          |                                 |
   | Send S5B acceptance                                              |
   | <--------------------------------------------------------------- |
   |                     |          |                                 |
   | Send One Time Proxy |          |                                 |
   | Credential request. |          |                                 |
   | ------------------> |          |                                 |
   | Return One Time     |          |                                 |
   | Proxy Credentials   |          |                                 |
   | <------------------ |          |                                 |
   |                     |          |                                 |
   | Open TCP socket                |                                 |
   | _____________________________> |                                 |
   |                                |                                 |
   | Request SOCKS5 connection      |                                 |
   | /////////////////////////////> |                                 |
   |                                |                                 |
   | Authenticate SOCKS5 connection |                                 |
   | /////////////////////////////> |                                 |
   |                                |                                 |
   | Acknowledge SOCKS5 connection  |                                 |
   | <\\\\\\\\\\\\\\\\\\\\\\\\\\\\\ |                                 |
   |                                |                                 |
   | Request activation             |                                 |
   | -----------------------------> |                                 |
   |                                |                                 |
   | Acknowledge activation         |                                 |
   | <----------------------------- |                                 |
   |                                |                                 |
   | Exchange data over S5B Through the Proxy Server                  |
   | <==============================================================> |
   |                     |          |                                 |
```

10.1.2.2 Jingle In-Band ByteStream Transport

TIM+ service providers and endpoints SHALL support file transfers using the Jingle In-Band ByteStream transport as defined by XEP 0261 and further described by XEP 0047 (XEP 0261 defers many of the implementation details to XEP 0047). Due to its inherent slow performance and high usage of bandwidth, it SHALL be used only as a fallback method if the SOCKS5 file transport fails. The fallback protocol is described in section 3 of XEP 0260.

Because In-Band ByteStreams occur over already secured connections between TIM+ endpoints and TIM+ service providers, this transport protocol is inherently secure and does not need any additional layer of security defined.

11 Security Considerations

Assuming the implementation of good security principles that apply to all operating environments and the proper configuration of clients and servers to correctly implement this specification, this section discusses specific risks and mitigations related to the implementation of this specification.

11.1 Summary of Risk and Mitigation

The following are some common risks to all deployment models that need to be considered at the operational level above and beyond that implementers familiarize themselves with the underlying technologies in this specification and perform their own independent risk analysis.

1. When stanzas are sent from server to server, DNS can be spoofed to return an attacker's IP addresses rather than the correct ones. This could cause stanzas to be sent to an attacker's system.

    - TIM+ requires the use of mutual TLS for server to server communication. The connection initiator is required to validate the connection target's TLS certificate as described in section 4.3 of this document. Proper protection of the connection target's private key will ensure that only a legitimate owner of the private key will be able to successfully establish a TLS connection.

2. The private key for a TIM+ service provider may have been compromised.

    - Section 4.3 requires a TIM+ service provider to check certificate status with the issuer to confirm that the other party's certificate has not been revoked.