Section	SubSection	Page	No	Description	Statu
1		2	1	Spec(T) **MUST** specify behavior for the following: 1. The manner in which users are authenticated 2. The mechanisms used to secure the communication among nodes within the Trust Domain 3. The mechanisms used to secure the communication between UAs and nodes within the Trust Domain 4. The manner used to determine which hosts are part of the Trust Domain 5. The default privacy handling when no Privacy header field is present 6. That nodes in the Trust Domain are compliant to SIP [1] 7. That nodes in the Trust Domain are compliant to this document 8. Privacy handling for identity as described in Section 7.	M

Section	SubSection	Page	No	Description	Statu
5		5	1	A proxy that is about to forward a message to a proxy server or UA that it does not trust **MUST** remove all the P-Asserted-Identity header field values if the user requested that this information be kept private.	M
5		5	2	When a proxy receives a message from a node it does not trust and it wishes to add a P-Asserted-Identity header field, the proxy**MUST** authenticate the originator of the message, and use the identity which results from this authentication to insert a P-Asserted-Identity header field into the message.	M
5		5	3	If the proxy received the message from an element that it does not trust and there is a P-Asserted-Identity header present which contains a SIP or SIPS URI, the proxy **MUST** replace that SIP or SIPS URI with a single SIP or SIPS URI or remove this header field.	M
5		5	4	Similarly, if the proxy received the message from an element that it does not trust and there is a P-Asserted-Identity header present which contains a tel URI, the proxy **MUST** replace that tel URI with a single tel URI or remove the header field.	M
5		6	5	If it does not trust the element, then the proxy**MUST** examine the Privacy header field (if present) to determine if the user requested that asserted identity information be kept private.	M

Section	SubSection	Page	No	Description	Statu
6		6	1	The proxy **MUST** remove the user-provided P-Preferred- Identity header from any message it forwards.	M
6		6	2	A user agent only sends a P-Preferred-Identity header field to proxy servers in a Trust Domain; user agents **MUST NOT** populate the P- Preferred-Identity header field in a message that is not sent directly to a proxy that is trusted by the user agent.	M

Section	SubSection	Page	No	Description	Statu
7		6	1	If this token is present, proxies **MUST** remove all the P-Asserted- Identity header fields before forwarding messages to elements that are not trusted.	M
7		6	2	If the Privacy header field value is set to "none" then the proxy **MUST NOT** remove the P-Asserted-Identity header fields.	M
7		6	3	This decision is a policy matter of the Trust Domain and **MUST** be specified in Spec(T)	M
7		6	4	It is **RECOMMENDED** that the P-Asserted-Identity header fields **SHOULD NOT** be removed unless local privacy policies prevent it, because removal may cause services based on Asserted Identity to fail.	R
7		6	5		S
7		7	6	It is therefore STRONGLY **RECOMMENDED** that all users have access to privacy services as described in this document.	R
7		7	7	If multiple P-Asserted-Identity header field values are present in a message, and privacy of the P-Asserted-Identity header field is requested, then all instances of the header field values **MUST** be removed before forwarding the request to an entity that is not trusted.	M

Section	SubSection	Page	No	Description	Statu
8		7	1	However, if a User Agent Server receives a message from a previous element that it does not trust, it **MUST NOT** use the P-Asserted- Identity header field in any way.	M
8		7	2	If a UA is part of the Trust Domain from which it received a message containing a P-Asserted-Identity header field, then it can use the value freely but it **MUST** ensure that it does not forward the information to any element that is not part of the Trust Domain, if the user has requested that asserted identity information be kept private.	M

Section	SubSection	Page	No	Description	Statu
9	9.1	8	1	A P-Asserted-Identity header field value**MUST** consist of exactly one name-addr or addr-spec.	M
9	9.1	8	2	If there is one value, it**MUST** be a sip, sips, or tel URI.	M
9	9.1	8	3	If there are two values, one value**MUST** be a sip or sips URI and the other MUST be a tel URI.	M
9	9.2	8	4	A P-Preferred-Identity header field value**MUST** consist of exactly one name-addr or addr-spec.	M
9	9.2	8	5	If there is one value, it**MUST** be a sip, sips, or tel URI.	M
9	9.2	8	6	If there are two values, one value**MUST** be a sip or sips URI and the other MUST be a tel URI.	M
9	9.3	9	7	Note that a user requesting multiple types of privacy**MUST** include all of the requested privacy types in its Privacy header field value.	M

Section	SubSection	Page	No	Description	Statu
11		13	1	The following specifications**MUST** be supported:	M
11		13	2	Users **MUST** be authenticated using SIP Digest Authentication.	M
11		13	3	Connections between nodes within the Trust Domain and between UAs and nodes in the Trust Domain**MUST** use TLS using a cipher suite of RSA_WITH_AES_128_CBC_SHA1.	M
11		13	4	Mutual authentication between nodes in the trust domain**MUST** be performed and confidentiality**MUST** be negotiated.	M
11		14	5	If no Privacy header field is present in a request, elements in this Trust Domain **MUST** act as if no privacy is requested.	M

Section	SubSection	Page	No	Description	Statu
12		14	1	When a trusted entity sends a message to any destination with that party's identity in a P-Asserted-Identity header field, the entity**MUST** take precautions to protect the identity information from eavesdropping and interception to protect the confidentiality and integrity of that identity information.	M