

OPES Policy Considerations

Web Services? Work Flow?

IESG Considerations

What is the authorization model? Implication on policy model?

Policy authorization...Client/Origin requesting services

Called service authorization...Client/Origin or intermediate requesting services or both?

Authentication?

No policy distribution architecture? I.e., no control channel?

IAB Considerations

(2.1) One-party consent: An OPES framework standardized in the IETF must require that the use of any OPES service be explicitly authorized by one of the application-layer end-hosts (that is, either the content provider or the client).

May need to weed out any references to intermediary-specified rules...are interactions between origin & client rules still possible

(2.2) IP-layer communications: For an OPES framework standardized in the IETF, the OPES intermediary must be explicitly addressed at the IP layer by the end user.

N/A

(3.1) Notification: The overall OPES framework needs to assist content providers in detecting and responding to client-centric actions by OPES intermediaries that are deemed inappropriate by the content provider.

Need rules for specifying tracing and notification and architecture/protocols for retrieval (both rule owner and, as appropriate, other party)

(3.2) Notification: The overall OPES framework should assist end users in detecting the behavior of OPES intermediaries,

potentially allowing them to identify imperfect or compromised intermediaries.

Need rules for specifying tracing and notification and architecture/protocols for retrieval (both rule owner and, as appropriate, other party)

(3.3) Non-blocking: If there exists a "non-OPES" version of content available from the content provider, the OPES architecture must not prevent users from retrieving this "non-OPES" version from the content provider.

Need rules for specifying tracing and notification and architecture/protocols for retrieval

(4.1) URI resolution: OPES documentation must be clear in describing these services as being applied to the result of URI resolution, not as URI resolution itself.

N/A

(4.2) Reference validity: All proposed services must define their impact on inter- and intra-document reference validity.

N/A

(4.3) Any services that cannot be achieved while respecting the above two considerations may be reviewed as potential requirements for Internet application addressing architecture extensions, but must not be undertaken as ad hoc fixes.

N/A

(5.1) Privacy: The overall OPES framework must provide for mechanisms for end users to determine the privacy policies of OPES intermediaries.

N/A