ISCHEDULE

Apps Area WG
IETF 86 Orlando
March 2013
Cyrus Daboo

draft-desruisseaux-ischedule

OVERVIEW

- iCalendar (RFC5545) is the IETF standard for calendar data interchange.

- iTIP (RFC5546) is the IETF standard for how iCalendar data is exchanged to allow scheduling between calendar users.

- iMIP (RFC6047) defines how scheduling occurs over email.

- CalDAV (RFC4791 & RFC6638) define a client-server protocol for calendaring and scheduling.

- Whilst iMIP is reasonable for "personal" scheduling, we want a more efficient, real time, server-to-server protocol for cross-domain scheduling.

KEY ELEMENTS

- Obviously we want full reuse of existing standards, i.e., we want the protocol to be based on iTIP and an existing transport protocol (HTTP was chosen).

- Calendar servers typically generate scheduling messages on behalf of the calendar users, so a "domain-level" security model is appropriate (DKIM was chosen).

- We want a protocol that can be implemented on top of any calendar system be it standards-based like CalDAV, or proprietary (e.g., Exchange, Google calendar etc).

- Needs to scale so that large calendar-in-the-cloud providers can connect to each other and deal with a high volume of scheduling requests.

- Strong authentication required from the outset to prevent any possibility of calendar "spam".

PROPOSED SOLUTION

- iSchedule service discovery via SRV record and .well-known resource.

- ITIP over HTTP (with SSL required) used for calendar data transport.

- DKIM used to sign and verify messages.

- Extensibility handled via a "capabilities" document returned from the .well-known resource.

PROPOSED SOLUTION

- Changes to core DKIM:

  - New header canonicalization method defined to cover only the headers relevant to iSchedule (not intending DKIM use to be a "generic" HTTP signature mechanism).

  - New public key lookup mechanism based on an HTTP well-known resource bootstrapped via a DNS record. Convenient for HTTP admins to manage the public keys rather than DNS admins. DNS admin still has to setup bootstrap record.

IMPLEMENTATIONS

- Work has been progressing in the Calendaring and Scheduling Consortium.

- Recent interoperability event had four independent implementations of iSchedule (C, Java, Python, PHP based).

- Each was able to exchange and verify iSchedule messages.

NEXT STEPS

- Want broader cross-area review of this work with the goal of standardizing it.

- Need to resolve IPR issues surrounding possible use of DKIM beyond the email application.