

ISCHEDULE

IETF 86 Orlando
March 2013
Cyrus Daboo

draft-desruisseaux-ischedule

OVERVIEW

- draft-desruisseaux-ischedule-04
- Sending iCalendar scheduling messages over HTTP.
- Server-to-server protocol as the calendar server is generating scheduling messages on behalf of calendar users.
- Scheduling messages cross domains and thus need strong security so that access control can be reliable.
- DKIM chosen as the security mechanism.

DKIM CHANGES # 1

- New header canonicalization method defined to cover only the headers relevant to iSchedule (not intending to define a "generic" DKIM-HTTP signature mechanism).
- Needed to cope with HTTP proxies/middle boxes that may concatenate multiple headers with the same name into one, or insert extra white space etc

DKIM CHANGES #2

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

DKIM CHANGES #3

- Stronger requirements about the signature.
 - Valid signature means the sender has authenticated and authorized the originating calendar user. The receiver can then use the originator identifier for access control purposes.
 - Invalid signature means the iSchedule message must be rejected.