

# JMAP extensions for S/ MIME signing and encryption

draft-ietf-jmap-smime-sender-extensions-04  
Alexey Melnikov <[alexey.melnikov@isode.com](mailto:alexey.melnikov@isode.com)>

# Summary

- Extra parameters to "Email/set" command (both optionals) to control S/MIME signing and/or encryption:
  - "smimeSign": true
  - "smimeEncrypt": true
- If both "smimeSign" and "smimeEncrypt" are set to true, the message is first signed and then the signed version is encrypted
- smimeSignOpaque (boolean) parameter controls how S/MIME signing is done. The default value is "true" (use application/pkcs7-mime container). "false" means use of multipart/signed media type.

# Recent Changes

- Extended Email/query operation to be able to find “all encrypted” or “all non encrypted” messages

# Two proposals

```
"Email/set", {  
  "accountId": "ue150411c",  
  "create": {
```

```
[...]
```

```
    "smimeSign": true,  
    "smimeEncrypt": true,  
    "bodyStructure": {  
      "type": "text/plain",  
      "partId": "bd48",  
      "header:Content-Language":
```

```
"en"},
```

```
•  
[...]
```

```
    "smimeOperations": [{  
      "operation": "sign",  
      "options": {  
        "opaque": false,  
        "headersToProtect":  
          "all"  
      }  
    },  
    {  
      "operation": "encrypt"    }  
  ],
```

# Comparison of 2 proposals

- draft-ietf-jmap-smime-sender-extensions-04:
  - pros: simple
  - cons: not extensible
- draft-melnikov-jmap-smime-sender-extensions-alt-01:
  - pros: flexible and extensible
  - cons: less simple