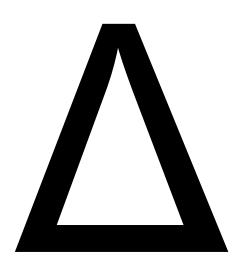
DISPATCH KSS: Amazon S3 Attachments

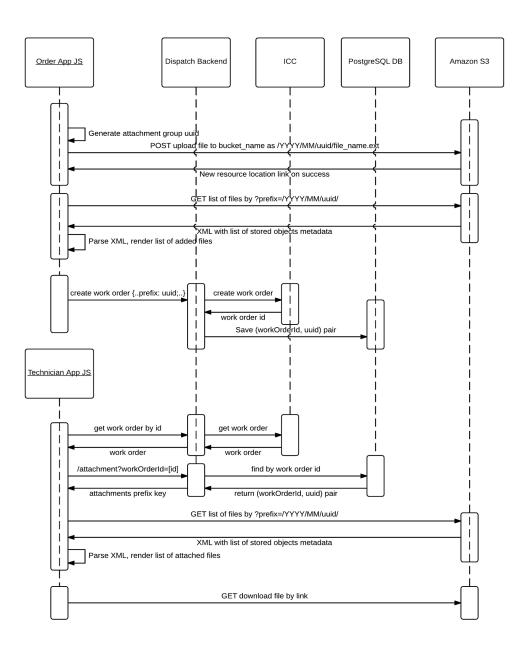


AGENDA

- Amazon S3:
 - Account
 - Bucket structure and config
 - REST API
- Attachments solution:
 - Architecture
 - Signing procedure
 - Postman requests demo
 - Ready parts demo

Signing

```
1. Canonical Request
                                "GET" | "PUT" | "POST" | ...
                                 URI-ENCODE(<resource>)
   HTTP Verb + "\n" +
                                Uri-Encode(<QueryParameter1>) + "=" + "Uri-Encode(<value>) + "&" +
   Canonical URI + "\n" +
                                Uri-Encode(<QueryParameter2>) + "=" + "Uri-Encode(<value>) + "&" +
                                                                                                   Sorted by
                                                                                                   QueryParameter
   Canonical Query String + "\n"
                                Uri-Encode(<QueryParameterN>) + "=" + "Uri-Encode(<value>)
                                 Lowercase(<HeaderName1>) + ":" +Trim(<value>) + "\n"
   Canonical Headers +\n"
                                                                                                   Sorted by
                                 Lowercase(<HeaderName2>) + ":" + Trim(<value>) + "\n"
                                                                                                   HeaderName
   Signed Headers + "\n"
                                 Lowercase(<HeaderNameN>) + ":" + Trim(<value>) + "\n"
   Hashed Payload
                                                                                                   Sorted by
                                 Lowercase(<HeaderName1>) + ";" + Lowercase (<HeaderName2>)
                                                                                                   HeaderName
                                + ";" + ... + Lowercase (< HeaderNameN>)
                                Hex(SHA256Hash(<payload>)
2. StringToSign
   "AWS4-HMAC-SHA256" + "\n" +
                                     Format ISO8601, e.g. "20130524T000000Z"
   TimeStamp + "\n" +
                                          "<yyyymmdd>/<AWS Region>/s3/aws4_request"
   Scope + "\n" +
                                          e.g., "20130524/us-east-1/s3/aws4_request"
   HEX(SHA256Hash(Canonical Request))
3. Signature
    DateKey
                         = HMAC-SHA256 ("AWS4" + "<SecretAccessKey>", "<yyyymmdd>")
    DateRegionKey
                         = HMAC-SHA256(<Hash1>, "<aws-region>"
    DateRegionServiceKey = HMAC-SHA256(<Hash2>, "<aws-service>"
                         = HMAC-SHA256(<Hash3>, "aws4_request")
    SigningKey
   signature = HMAC-SHA256 (SigningKey, StringToSign)
```



NEXT STEPS

- Support for different environments
- Signing endpoint
- Deletion of uploaded files
- Deletion of not used files