

metadata service

笔记本： FIDO

创建时间： 2015/10/23 9:25

更新时间： 2015/10/23 9:49

作者： yangzhou1989@gmail.com

3.1 Metadata TOC Format

NOTE

The metadata service makes the metadata TOC object (see [Metadata TOC](#)) accessible to FIDO Servers.

This object is a "table-of-contents" for metadata, as it includes the AAID, the download URL and the hash value of the individual metadata Statements. The TOC object contains one signature.

TOC文件中每个条目包含AAID，该条目所对应的metadata statement的下载URL，这个metadata statements的hash值：

Represents the MetadataTOCPayloadEntry

WebIDL

```
dictionary MetadataTOCPayloadEntry {  
    required AAID          aaid;  
    required DOMString     hash;  
    required DOMString     url;  
    required StatusReport[] statusReports;  
    required DOMString     timeOfLastStatusChange;  
};
```

Example:

EXAMPLE 1: UAF Metadata TOC Payload

```
{ "no": 1234, "next-update": "2014-03-31",  
  "entries": [  
    { "aaid": "1234#5678",  
      "hash": "90da8da6de23248abb34da0d4861f4b30a793e198a8d5baa7f98f260db71acd4",  
      "url": "https://fidoalliance.org/metadata/1234%x23abcd",  
      "statusReports": [  
        { status: "FIDO_CERTIFIED", effectiveDate: "2014-01-04" }  
      ],  
      "timeOfLastStatusChange": "2014-01-04"  
    },  
    { "aaid": "9876#4321",  
      "hash": "785d16df640fd7b50ed174cb5645cc0f1e72b7f19cf22959052dd20b9541c64d",  
      "url": "https://authnr-vendor-a.com/metadata/9876%x234321",  
      "statusReports": [  
        { status: "FIDO_CERTIFIED", effectiveDate: "2014-01-07" },  
        { status: "UPDATE_AVAILABLE", effectiveDate: "2014-03-08",  
          url: "https://example.com/update1234" }  
      ],  
      "timeOfLastStatusChange": "2014-02-19"  
    }  
  ]  
}
```

The character # is a reserved character and not allowed in URLs [RFC3986](#). As a consequence it has been replaced by its hex value %x23.

Metadata TOC is a JSON Web Token, 由3部分组成：

- The base64url encoding, without padding, of the UTF-8 encoded JWT Header (see example below),
- the base64url encoding, without padding, of the UTF-8 encoded UAF Metadata TOC Payload (see example at the beginning of section [Metadata TOC Format](#)),
- and the base64url-encoded, also without padding, JWS Signature [[JWS](#)] computed over the to-be-signed payload, i.e.

`tbsPayload = EncodedJWTHeader | "." | EncodedMetadataTOCPayload`

All three elements of the TOC are concatenated by a period ("."):

`MetadataTOC = EncodedJWTHeader | "." | EncodedMetadataTOCPayload | "." | EncodedJWSSignature`