FIDO Metadata Service

Review Draft, January 05, 2026

This version:
https://fidoalliance.org/specs/mds/fido-metadata-service-v3.1.1-rd02-20260105

Issue Tracking:
GitHub

Editors:
Billy Jack (Microsoft)
Rolf Lindemann (Nok Nok Labs)

Former Editor:
Yuriy Ackermann (FIDO Alliance)

Abstract

The FIDO Authenticator Metadata Specification defines so-called "Authenticator Metadata" statements. The metadata statements contains the "Trust Anchor" required to validate the attestation object, and they also describe several other important characteristics of the authenticator. The metadata service described in this document defines a baseline method for relying parties to access the latest metadata statements.

Status of This Document

This section describes the status of this document at the time of its publication. Other documents may supersede this document. A list of current FIDO Alliance publications and the latest revision of this technical report can be found in the FIDO Alliance specifications index at https://fidoalliance.org/specifications/.

This document was published by the FIDO Alliance as a Review Draft Specification. This document is intended to become a FIDO Alliance Proposed Standard. If you wish to make comments regarding this document, please Contact Us. All comments are welcome.

This is a Review Draft Specification and is not intended to be a basis for any implementations as the Specification may change. Permission is hereby granted to use the Specification solely for the purpose of reviewing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this Specification for other uses must contact the FIDO Alliance to determine whether an appropriate license for such use is available.

Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The FIDO Alliance, Inc. and its Members and any other contributors to the Specification are not, and shall not be held, responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

THIS FIDO ALLIANCE SPECIFICATION IS PROVIDED “AS IS” AND WITHOUT ANY WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

1 Notation

1.1 Key Words

2 Overview
2.1 Scope
2.2 Detailed Architecture

3 Metadata Service Details
3.1 Metadata BLOB Format
3.1.1 Metadata BLOB Payload Entry dictionary
3.1.2 BiometricStatusReport dictionary
3.1.3 StatusReport dictionary
3.1.4 AuthenticatorStatus enum
3.1.4.1 Certification Related Statuses
3.1.4.2 Security Notification Statuses
3.1.4.3 Info Statuses
3.1.5 RogueListEntry dictionary
3.1.6 Metadata BLOB Payload dictionary
3.1.7 Metadata BLOB
3.1.7.1 Examples
3.2 Metadata BLOB object processing rules

4 Considerations

Index
Terms defined by this specification
Terms defined by reference

References
Normative References
Informative References

IDL Index

Issues Index

1. Notation§

Type names, attribute names and element names are written as `code`

String literals are enclosed in “”, e.g. “UAF-TLV”.

In formulas we use “|” to denote byte wise concatenation operations.

The notation `base64url(byte[8..64])` reads as 8-64 bytes of data encoded in base64url, "Base 64 Encoding with URL and Filename Safe Alphabet" [RFC4648] *without padding*.

Following [WebIDL-ED], dictionary members are optional unless they are explicitly marked as `required`.

WebIDL dictionary members MUST NOT have a value of null.

Unless otherwise specified, if a WebIDL dictionary member is DOMString, it MUST NOT be empty.

Unless otherwise specified, if a WebIDL dictionary member is a List, it MUST NOT be an empty list.

For definitions of terms, please refer to the FIDO Glossary[FIDOGlossary].

All diagrams, examples, notes in this specification are non-normative.

Note: Certain dictionary members need to be present in order to comply with FIDO requirements. Such members are marked in the WebIDL definitions found in this document, as `required`. The keyword `required` has been introduced by [WebIDL-ED], which is a work-in-progress. If you are using a WebIDL parser which implements [WebIDL], then you may remove the keyword `required` from your WebIDL and use other means to ensure those fields are present.

1.1. Key Words§

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

2. Overview§

This section is not normative.

[FIDOMetadataStatement] defines authenticator metadata statements.

These metadata statements contain the trust anchor required to verify the attestation object (more specifically the `KeyRegistrationData` object), and they also describe several other important characteristics of the authenticator, including supported authentication and registration assertion schemes, and key protection flags.

These characteristics can be used when defining policies about which authenticators are acceptable for registration or authentication.

The metadata service described in this document defines a baseline method for relying parties to access the latest metadata statements.

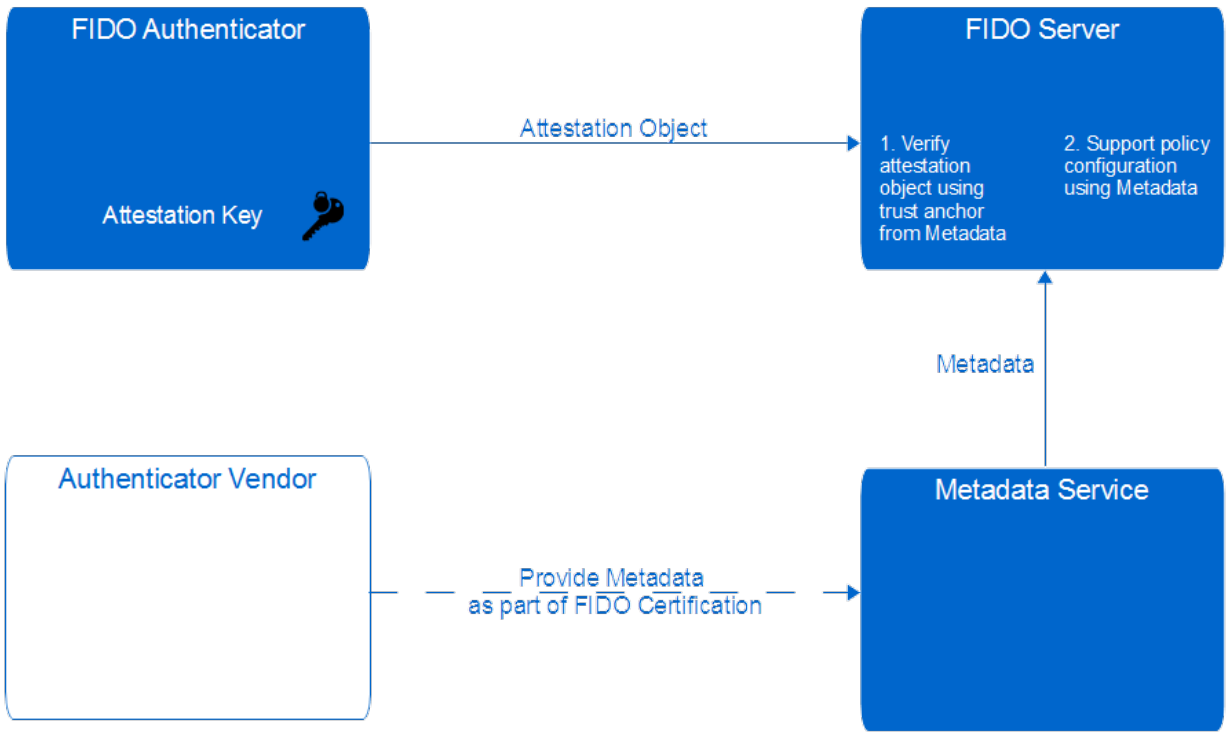

Figure 1 *FIDO Metadata Service Architecture Overview*

2.1. Scope§

This document describes the FIDO Metadata Service architecture in detail and it defines the structure and

interface to access this service. It also defines the flow of the metadata related messages and presents the rationale behind the design choices.

2.2. Detailed Architecture§

The metadata BLOB file contains a list of metadata statements related to the authenticators known to the FIDO Alliance (FIDO Authenticators).

The FIDO Server downloads the metadata BLOB file from a well-known FIDO URL and caches it locally.

The FIDO Server verifies the integrity and authenticity of this metadata BLOB file using the digital signature. It then iterates through the individual entries and parses the metadata statements related to authenticator models relevant to the relying party.

Individual metadata statements are included in the entry of the metadata BLOB file, and may be cached by the FIDO Server as required.

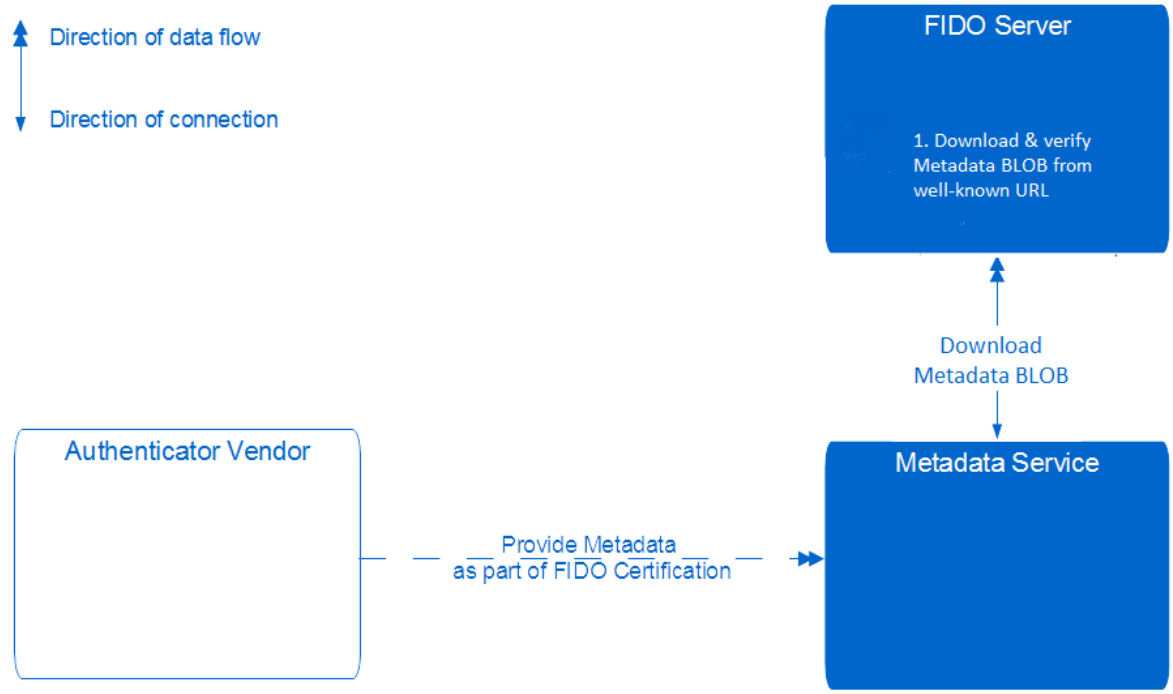

Figure 2 *FIDO Metadata Service Architecture*

> The single arrow indicates the direction of the network connection, the double arrow indicates the direction of the data flow.

> The metadata BLOB file is accessible at a well-known URL published by the FIDO Alliance.

> The relying party decides how frequently the metadata service is accessed to check for metadata BLOB updates.

3. Metadata Service Details§

This section is normative.

The relying party can decide whether it wants to use the metadata service and whether or not it wants to accept certain authenticators for registration or authentication.

The relying party could also obtain metadata directly from authenticator vendors or other trusted sources.

3.1. Metadata BLOB Format§

The metadata service makes the metadata BLOB object (see Metadata BLOB) accessible to FIDO Servers.

This object contains all metadata for each authenticator including the metadata statements defined in [FIDOMetadataStatement]. The BLOB object contains one signature.

3.1.1. Metadata BLOB Payload Entry dictionary§

Represents the MetadataBLOBPayloadEntry

```
dictionary MetadataBLOBPayloadEntry {
    AAID                        aaid;
    AAGUID                      aaguid;
    DOMString[]                 attestationCertificateKeyIdentifiers;
    required MetadataStatement  metadataStatement;
    BiometricStatusReport[]     biometricStatusReports;
    required StatusReport[]     statusReports;
    required DOMString          timeOfLastStatusChange;
    DOMString                   rogueListURL;
    DOMString                   rogueListHash;
};
```

`aaid`, of type AAID
: The AAID of the authenticator this metadata BLOB payload entry relates to. See [UAFProtocol] for the definition of the AAID structure. This field MUST be set if the authenticator implements FIDO UAF.

NOTE: FIDO UAF authenticators support AAID, but they don't support AAGUID.

`aaguid`, of type AAGUID
: The Authenticator Attestation GUID. See [FIDOKeyAttestation] for the definition of the AAGUID structure. This field MUST be set if the authenticator implements FIDO2.

NOTE: FIDO2 authenticators support AAGUID, but they don't support AAID.

`attestationCertificateKeyIdentifiers`, of type DOMString[]
: A list of the attestation certificate public key identifiers encoded as hex string. This value MUST be calculated according to method 1 for computing the keyIdentifier as defined in [RFC5280] section 4.2.1.2.

- The hex string MUST NOT contain any non-hex characters (e.g. spaces).
- All hex letters MUST be lower case.
- This field MUST be set if neither `aaid` nor `aaguid` are set. Setting this field implies that the attestation certificate(s) are dedicated to a single authenticator model.

FIDO U2F authenticators do not support AAID nor AAGUID, but they use attestation certificates dedicated to a single authenticator model.

`metadataStatement`, of type MetadataStatement
: The metadataStatement JSON object as defined in [FIDOMetadataStatement].

`biometricStatusReports`, of type BiometricStatusReport[]
Status of the FIDO Biometric Certification of one or more biometric components of the Authenticator [FIDOBiometricsRequirements].

`statusReports`, of type StatusReport[]
An array of status reports applicable to this authenticator.

`timeOfLastStatusChange`, of type DOMString
ISO-8601 formatted date since when the status report array was set to the current value.

`rogueListURL`, of type DOMString
URL of a list of rogue (i.e. untrusted) individual authenticators.

`rogueListHash`, of type DOMString
`base64url(string[1..512])`

The hash value computed over the Base64url encoding of the UTF-8 representation of the JSON encoded rogueList available at `rogueListURL` (with type rogueListEntry[]). The hash algorithm related to the signature algorithm specified in the JWTHeader (see Metadata BLOB MUST be used.

This hash value MUST be present and non-empty whenever `rogueListURL` is present.

> This method of base64url-encoding the UTF-8 representation is also used by JWT [JWT] to avoid encoding ambiguities.

```
EXAMPLE 1
{
  "no": 1234,
  "nextUpdate": "2014-03-31",
  "entries": [
    {
      "aaid": "1234#5678",
      "metadataStatement": "Metadata Statement object as defined in Metadata Statement spec."
,
      "statusReports": [
        {
          "status": "FIDO_CERTIFIED",
          "effectiveDate": "2014-01-04"
        }
      ],
      "timeOfLastStatusChange": "2014-01-04"
    },
    {
      "attestationCertificateKeyIdentifiers": [
        "7c0903708b87115b0b422def3138c3c864e44573"
      ],
      "metadataStatement": "Metadata Statement object as defined in Metadata Statement spec."
,
      "statusReports": [
        {
          "status": "FIDO_CERTIFIED",
          "effectiveDate": "2014-01-07"
        },
        {
          "status": "UPDATE_AVAILABLE",
          "effectiveDate": "2014-02-19",
          "url": "https://example.com/update1234"
        }
      ],
      "timeOfLastStatusChange": "2014-02-19"
    }
  ]
}
```

3.1.2. BiometricStatusReport dictionary§

Contains the current `BiometricStatusReport` of one of the authenticator's biometric component.

```
dictionary BiometricStatusReport {
    required unsigned short certLevel;
    required DOMString      modality;
    DOMString               effectiveDate;
    DOMString               certificationDescriptor;
    DOMString               certificateNumber;
    DOMString               certificationPolicyVersion;
    DOMString               certificationRequirementsVersion;
};
```

`certLevel`, of type unsigned short
: Achieved level of the biometric certification of this biometric component of the authenticator [FIDOBiometrics Requirements].

`modality`, of type DOMString
: A *single* a single USER_VERIFY short form case-sensitive string name constant, representing biometric modality. See section "User Verification Methods" in [FIDORegistry] (e.g. "fingerprint_internal"). This value MUST NOT be empty and this value MUST correspond to one or more entries in field `userVerificationDetails` in the related Metadata Statement [FIDOMetadataStatement]. This value MUST represent a biometric modality.

For example use `USER_VERIFY_FINGERPRINT` for the fingerprint based biometric component. In this case the related Metadata Statement must also claim fingerprint as one of the user verification methods.

`effectiveDate`, of type DOMString
: ISO-8601 formatted date since when the `certLevel` achieved, if applicable. If no date is given, the status is assumed to be effective while present.

`certificationDescriptor`, of type DOMString
: Describes the externally visible aspects of the Biometric Certification evaluation.

For example it could state that the "biometric component is implemented OnChip - keeping biometric data inside the chip only.".

`certificateNumber`, of type DOMString
: The unique identifier for the issued Biometric Certification.

`certificationPolicyVersion`, of type DOMString
: The version of the Biometric Certification Policy the implementation is Certified to, e.g. "1.0.0".

`certificationRequirementsVersion`, of type DOMString
: The version of the Biometric Requirements [FIDOBiometricsRequirements] the implementation is certified to, e.g. "1.0.0".

3.1.3. StatusReport dictionary§

Contains an `AuthenticatorStatus` and additional data associated with it, if any.

New `StatusReport` entries will be added to report known issues present in firmware updates.

The latest `StatusReport` entry MUST reflect the "current" status. For example, if the latest entry has status `USER_VERIFICATION_BYPASS`, then it is recommended assuming an increased risk associated with all authenticators of this AAID; if the latest entry has status `UPDATE_AVAILABLE`, then the update is intended to address at least all previous issues *reported* in this StatusReport dictionary.

The certification of FIDO Authenticators does NOT cover the security characteristics of multi-device keys.

```
dictionary StatusReport {
    required AuthenticatorStatus status;
    DOMString                    effectiveDate;
    unsigned long                authenticatorVersion;
    DOMString                    batchCertificate;
    DOMString                    certificate;
    DOMString                    url;
    DOMString                    certificationDescriptor;
    DOMString                    certificateNumber;
    DOMString                    certificationPolicyVersion;
    DOMString[]                  certificationProfiles;
    DOMString                    certificationRequirementsVersion;
    DOMString                    sunsetDate;
    unsigned long                fipsRevision;
    unsigned long                fipsPhysicalSecurityLevel;
};
```

`status`, of type AuthenticatorStatus
Status of the authenticator. Additional fields MAY be set depending on this value.

`effectiveDate`, of type DOMString
ISO-8601 formatted date since when the status code was set, if applicable. If no date is given, the status is assumed to be effective while present.

`authenticatorVersion`, of type unsigned long
The authenticatorVersion (firmware version) that this status report relates to. In the case of FIDO_CERTIFIED* status values, the status applies to higher authenticatorVersions until there is a new statusReport.

For example, if the status would be USER_VERIFICATION_BYPASS, the authenticatorVersion indicates the vulnerable firmware version of the authenticator. Similarly, if the status would be UPDATE_AVAILABLE, the authenticatorVersion indicates the updated firmware version that is available now. If the status would be SELF_ASSERTION_SUBMITTED, the authenticatorVersion indicates the firmware version that the self assertion was based on.

The firmware version of the authenticator providing the attestation can be found in the attestation certificate in extension id-fido-gen-ce-fw-version (OID 1.3.6.1.4.1.45724.1.1.5).

`batchCertificate`, of type DOMString
Base64-encoded [RFC4648] (not base64url!) DER [ITU-X690-2008] PKIX certificate value related to the current status, if applicable.

As an example, this could be an Batch Attestation Certificate (see[FIDOMetadataStatement]) related to a set of compromised authenticators (USER_KEY_REMOTE_COMPROMISE).

`certificate`, of type DOMString
Base64-encoded [RFC4648] (not base64url!) DER [ITU-X690-2008] PKIX certificate value related to the current status, if applicable. This field will typically not be present if field `batchCertificate` is present.

As an example, this could be an Attestation Root Certificate (see[FIDOMetadataStatement]) related to a set of compromised authenticators (ATTESTATION_KEY_COMPROMISE).

`url`, of type DOMString
HTTPS URL where additional information may be found related to the current status, if applicable.

For example a link to a web page describing an available firmware update in the case of status `UPDATE_AVAILABLE`, or a link to a description of an identified issue in the case of status `USER_VERIFICATION_BYPASS`.

`certificationDescriptor`, of type DOMString
Describes the externally visible aspects of the Authenticator Certification evaluation.

For example it could state that the authenticator is a "SecurityKey based on a CC EAL 5 certified chip hardware".

`certificateNumber`, of type DOMString
The unique identifier for the issued Certification.

`certificationPolicyVersion`, of type DOMString
The version of the Authenticator Certification Policy the implementation is Certified to, e.g. "1.0.0".

`certificationProfiles`, of type DOMString[]
array of strings. Each entry represents a supported certification profile. The supported profiles are defined in the active version of the Authenticator Certification Policy document. At the time of writing this specification, the supported profiles are: "consumer" and "enterprise".

`certificationRequirementsVersion`, of type DOMString
The Document Version of the Authenticator Security Requirements (DV)[FIDOAuthenticatorSecurityRequirements] the implementation is certified to, e.g. "1.2.0".

`sunsetDate`, of type DOMString
ISO-8601 formatted date since when the status wil expire, if applicable. If no date is given, the status is assumed to not have a scheduled expiry.

`fipsRevision`, of type unsigned long
The revision number of the FIPS 140 specification, e.g. "3" in the case of FIPS 140-3. This entry MUST be present if and only if the status entry is one of FIPS140_CERTIFIED_L*.

`fipsPhysicalSecurityLevel`, of type unsigned long
In the case the status represents a FIPS certification, this field contains the "physical security level" of the FIPS certification. This entry MUST be present if and only if the status entry is one of FIPS140_CERTIFIED_L*. It MUST reflect the physical security level which might deviate from the overall level.

3.1.4. AuthenticatorStatus enum§

This enumeration describes the status of an authenticator model as identified by its AAID/AAGUID or attestationCertificateKeyIdentifiers and potentially some additional information (such as a specific attestation key).

```
enum AuthenticatorStatus {
    "NOT_FIDO_CERTIFIED",
    "FIDO_CERTIFIED",
    "USER_VERIFICATION_BYPASS",
    "ATTESTATION_KEY_COMPROMISE",
    "USER_KEY_REMOTE_COMPROMISE",
    "USER_KEY_PHYSICAL_COMPROMISE",
    "UPDATE_AVAILABLE",
    "RETIRED",
    "REVOKED",
    "SELF_ASSERTION_SUBMITTED",
    "FIDO_CERTIFIED_L1",
    "FIDO_CERTIFIED_L1plus",
    "FIDO_CERTIFIED_L2",
    "FIDO_CERTIFIED_L2plus",
    "FIDO_CERTIFIED_L3",
    "FIDO_CERTIFIED_L3plus",
    "FIPS140_CERTIFIED_L1",
    "FIPS140_CERTIFIED_L2",
    "FIPS140_CERTIFIED_L3",
    "FIPS140_CERTIFIED_L4"
};
```

3.1.4.1. Certification Related Statuses

> The certification of FIDO Authenticators does NOT cover the security characteristics of multi-device keys.

NOT_FIDO_CERTIFIED

This authenticator is not FIDO certified.

> Applicable StatusReport fields are:
>
> - effectiveDate - When status was achieved
> - authenticatorVersion - The minimum applicable authenticator version.
> - url - To the authenticator page or additional information about the authenticator

SELF_ASSERTION_SUBMITTED

The authenticator vendor has completed and submitted the self-certification checklist to the FIDO Alliance. If this completed checklist is publicly available, the URL will be specified in url.

> Applicable StatusReport fields are:
>
> - effectiveDate - Date of incident being reported
> - authenticatorVersion - New authenticator version that is

FIDO_CERTIFIED

This authenticator has passed FIDO functional certification. This certification scheme is phased out and will be replaced by FIDO_CERTIFIED_L1.

> Applicable StatusReport fields are:
>
> - effectiveDate - When certification was issued
> - authenticatorVersion - The minimum version of the certified solution
> - certificationDescriptor - Authenticator Description. I.e. "Munikey 7c Black Edition"
> - certificateNumber - FIDO Alliance Certificate Number
> - certificationPolicyVersion - Authenticator Certification Policy
> - certificationProfiles - list of supported certification profiles
> - certificationRequirementsVersion - Security Requirements Version
> - url - URL to the certificate, or the news article about achievement of the certification.
>
> These fields are applicable to any of the FIDO_CERTIFIED_*.

FIDO_CERTIFIED_L1
The authenticator has passed FIDO Authenticator certification at level 1. This level is the more strict successor of FIDO_CERTIFIED.

FIDO_CERTIFIED_L1plus
The authenticator has passed FIDO Authenticator certification at level 1+. This level is the more than level 1.

FIDO_CERTIFIED_L2
The authenticator has passed FIDO Authenticator certification at level 2. This level is more strict than level 1+.

FIDO_CERTIFIED_L2plus
The authenticator has passed FIDO Authenticator certification at level 2+. This level is more strict than level 2.

FIDO_CERTIFIED_L3
The authenticator has passed FIDO Authenticator certification at level 3. This level is more strict than level 2+.

FIDO_CERTIFIED_L3plus
The authenticator has passed FIDO Authenticator certification at level 3+. This level is more strict than level 3.

FIPS140_CERTIFIED_L1
The authenticator has passed FIPS 140 certification at overall level 1.

> Applicable StatusReport fields are:
>
> - certificateNumber - certificate number as given in the FIPS certificate
> - url - URL to the FIPS certificate (e.g. https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/[nn])
> - sunsetDate - the sunset data as given in the FIPS certificate
> - fipsPhysicalSecurityLevel - the level of the physical security according to the FIPS certificate
>
> These fields are applicable to any of the FIPS140_CERTIFIED_*.

FIPS140_CERTIFIED_L2
The authenticator has passed FIPS 140 certification at overall level 2.

FIPS140_CERTIFIED_L3
The authenticator has passed FIPS 140 certification at overall level 3.

FIPS140_CERTIFIED_L4
The authenticator has passed FIPS 140 certification at overall level 4.

RETIRED
The authenticator vendor has decided to retire the product, that this authenticator should not be accepted any longer. For example if a prototype version of the authenticator was added to FIDO MDS and has now

been superseded by the final product, the entry for the prototype might be set to "retired".

> Applicable StatusReport fields are:

- effectiveDate - Date of retirement
- url - URL to the news/corporate article explaining the reason for retirement

REVOKED

The FIDO Alliance has determined that this authenticator should not be trusted for any reason. For example if it is known to be a fraudulent product or contain a deliberate backdoor. Relying parties SHOULD reject any future registration of this authenticator model.

> Applicable StatusReport fields are:

- effectiveDate - Date of incident being reported
- authenticatorVersion - New authenticator version that is
- url - URL to the news/corporate article explaining the reason for revocation

3.1.4.2. Security Notification Statuses

USER_VERIFICATION_BYPASS

Indicates that malware is able to bypass the user verification. This means that the authenticator could be used without the user's consent and potentially even without the user's knowledge.

> Applicable StatusReport fields are:

- effectiveDate - Date of incident being reported
- authenticatorVersion - Minimum affected authenticator version
- batchCertificate - Base64 DER-encoded PKIX certificate identifying the compromised batch attestation certificate related to the affected authenticators.
- certificate - Base64 DER-encoded PKIX certificate. Might not be present if batchCertificate is present. identifying the attestation root certificate related to the affected authenticators.
- url - URL to the news/corporate article explaining the incident

ATTESTATION_KEY_COMPROMISE

Indicates that an attestation key for this authenticator is known to be compromised. The relying party SHOULD check the certificate field and use it to identify the compromised authenticator batch. If neither the batchCertificate nor the certificate field are set, the relying party should reject all new registrations of the compromised authenticator. The Authenticator manufacturer should set the date to the date when compromise has occurred.

> Applicable StatusReport fields are:

- effectiveDate - Date of incident being reported
- authenticatorVersion - Minimum affected authenticator version
- batchCertificate - Base64 DER-encoded PKIX certificate identifying the compromised batch attestation certificate related to the affected authenticators.
- certificate - Base64 DER-encoded PKIX certificate. Might not be present if batchCertificate is present. identifying the attestation root certificate related to the affected authenticators.
- url - URL to the news/corporate article explaining the incident

USER_KEY_REMOTE_COMPROMISE

This authenticator has identified weaknesses that allow registered keys to be compromised and should not

be trusted. This would include both, e.g. weak entropy that causes predictable keys to be generated or side channels that allow keys or signatures to be forged, guessed or extracted.

> Applicable StatusReport fields are:

- effectiveDate - Date of incident being reported
- authenticatorVersion - Minimum affected authenticator version
- batchCertificate - Base64 DER-encoded PKIX certificate identifying the compromised batch attestation certificate related to the affected authenticators.
- certificate - Base64 DER-encoded PKIX certificate. Might not be present if batchCertificate is present. identifying the attestation root certificate related to the affected authenticators.
- url - URL to the news/corporate article explaining the incident

USER_KEY_PHYSICAL_COMPROMISE

This authenticator has known weaknesses in its key protection mechanism(s) that allow user keys to be extracted by an adversary in physical possession of the device.

> Applicable StatusReport fields are:

- effectiveDate - Date of incident being reported
- authenticatorVersion - Minimum affected authenticator version
- batchCertificate - Base64 DER-encoded PKIX certificate identifying the compromised batch attestation certificate related to the affected authenticators.
- certificate - Base64 DER-encoded PKIX certificate. Might not be present if batchCertificate is present. identifying the attestation root certificate related to the affected authenticators.
- url - URL to the news/corporate article explaining the incident

3.1.4.3. Info Statuses

UPDATE_AVAILABLE

A software or firmware update is available for the device. The Authenticator manufacturer should set the url to the URL where users can obtain an update and the date the update was published. When this status code is used, then the field authenticatorVersion in the authenticator Metadata Statement [FIDOMetadataStatement] MUST be updated, if the update fixes severe security issues, e.g. the ones reported by preceding StatusReport entries with status code USER_VERIFICATION_BYPASS, ATTESTATION_KEY_COMPROMISE, USER_KEY_REMOTE_COMPROMISE, USER_KEY_PHYSICAL_COMPROMISE, REVOKED. The Relying party MUST reject the Metadata Statement if the authenticatorVersion has not increased

> Applicable StatusReport fields are:

- effectiveDate - Date of incident being reported
- authenticatorVersion - New authenticator version that is available. MUST match authenticatorVersion in the metadata statement.
- url - URL to the page with the update info

> Relying parties might want to inform users about available firmware updates.

More values might be added in the future. FIDO Servers MUST silently ignore all unknown AuthenticatorStatus values.

3.1.5. RogueListEntry dictionary

Contains a list of individual authenticators known to be rogue.
New `RogueListEntry` entries will be added to report new individual authenticators known to be rogue.

Old `RogueListEntry` entries will be removed if the individual authenticator is known to not be rogue any longer.

```
dictionary RogueListEntry {
    required DOMString sk;
    required DOMString date;
};
```

`sk`, of type DOMString
Base64url encoding of the rogue authenticator's secret key (sk value, see[FIDOEcdaaAlgorithm], section ECDAA Attestation).

In order to revoke an individual authenticator, its secret key (sk) must be known.

`date`, of type DOMString
ISO-8601 formatted date since when this entry is effective.

```
EXAMPLE: ROGUELISTENTRY[] EXAMPLE
[
    { "sk": "MO-oaqbeJSSayzXaDUhh9LMKeT4Zio1bqn6W8kDaUfM",
      "date": "2016-06-07"},
    { "sk": "k96Npt4jJIq7NNoNSGH0swp5PhU6jVuyf5jyYNtxrNQ",
      "date": "2016-06-09"},
]
```

3.1.6. Metadata BLOB Payload dictionary

Represents the MetadataBLOBPayload

```
dictionary MetadataBLOBPayload {
    DOMString                          legalHeader;
    required Number                    no;
    required DOMString                 nextUpdate;
    required MetadataBLOBPayloadEntry[] entries;
};
```

`legalHeader`, of type DOMString
The legalHeader, which MUST be in each BLOB, is an indication of the acceptance of the relevant legal agreement for using the MDS. The FIDO Alliance's Blob will contain this legal header: "legalHeader": "Retrieval and use of this BLOB indicates acceptance of the appropriate agreement located at https://fidoalliance.org/metadata/metadata-legal-terms/"

`no`, of type Number
The serial number of this Metadata BLOB Payload. This serial number MUST be incremented whenever the contents of the BLOB changes. Serial numbers MUST be consecutive and strictly monotonic, i.e. the successor BLOB will have a `no` value exactly incremented by one.

`nextUpdate`, of type DOMString
ISO-8601 formatted date when the next update will be provided at latest.

> NOTE: The FIDO operational approach to publishing the FIDO Metadata has changed. Guidance on the download frequency and download approach is given in section Metadata BLOB Processing Rules. The use of the "nextUpdate" field is discouraged and the field will be removed in the future. FIDO servers should ensure this field is not required by their code.

`entries`, of type MetadataBLOBPayloadEntry[]
List of zero or more MetadataBLOBPayloadEntry objects.

> NOTE: The "issued at" claim (`iat`) is included in the JWT header according to [RFC7519].

3.1.7. Metadata BLOB

The metadata BLOB is a JSON Web Token (see [JWT] and [JWS]). It consists of three elements:

- 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 Metadata BLOB Payload (see example at the beginning of section Metadata BLOB Format>),
- and the base64url-encoded, also without padding, JWS Signature [JWS] computed over the to-be-signed payload using the Metadata BLOB signing key, i.e. `tbsPayload = EncodedJWTHeader | "." | EncodedMetadataBLOBPayload`

All three elements of the BLOB are concatenated by a period ("."): `MetadataBLOB = EncodedJWTHeader | "." | EncodedMetadataBLOBPayload | "." | EncodedJWSSignature`

The hash algorithm related to the signing algorithm specified in the JWT Header (e.g. SHA256 in the case of "ES256") MUST also be used to compute the hash of the metadata statements (see section Metadata BLOB Payload Entry Dictionary).

The JWT Header SHALL include the "iat" ("issued at") claim as specified in [RFC7519].

3.1.7.1. Examples

This section is not normative.

EXAMPLE: ENCODED METADATA BLOB

```
ewoJImxlZ2FsSGVhZGVyIjogIlJldHJpZXZhbCBhbmQgdXNlIG9mIHRoaXMgQkxPQiBpbmRpY2F0ZXMg
YWNjZXB0YW5jZSBvZiB0aGUgYXBwcm9wcmlhdGUgYWdyZWVtZW50IGxvY2F0ZWQgYXQgaHR0cHM6Ly9m
aWRvYWxsaWFuY2Uub3JnL21ldGFkYXRhL21ldGFkYXRhLWxlZ2FsLXRlcm1zLyIsCgkibm8iOiAxNSwK
CSJuZXh0VXBkYXRlIjogIjIwMjAtMDMtMzAiLAoJImVudHJpZXMiOiBbewoJCQkiYWFpZCI6ICIxMjM0
IzU2NzgiLAoJCQkibWV0YWRhdGFTdGF0ZW1lbnQiOiB7CgkJCQkibGVnYWxIZWFkZXIiOiAiaHR0cHM6
Ly9maWRvYWxsaWFuY2Uub3JnL21ldGFkYXRhL21ldGFkYXRhLXN0YXRlbWVudC1sZWdhbC1oZWFkZXIv
IiwKCQkJCSJkZXNjcmlwdGlvbiI6ICJGSURPIEFsbGlhbmNlIFNhbXBsZSBVQUYgQXV0aGVudGljYXRv
ciIsCgkJCQkiYWFpZCI6ICIxMjM0IzU2NzgiLAoJCQkJImFsdGVybmF0aXZlRGVzY3JpcHRpb25zIjog
ewoJCQkJCSJydS1SVSI6ICLQn9GA0LjQvNC10YAgVUFGINCw0YPRgtC10L3RgtC40YTQuNC60LDRgtC-
0YDQsCDQvtGCIEZJRE8gQWxsaWFuY2UiLAoJCQkJCSJmci1GUiI6ICJFeGVtcGxlIFVBRiBhdXRoZW50
aWNhdG9yIGRlIEZJRE8gQWxsaWFuY2UiCgkJCQl9LAoJCQkJImF1dGhlbnRpY2F0b3JWZXJzaW9uIjog
MiwKCQkJCSJwcm90b2NvbEZhbWlseSI6ICJ1YWYiLAoJCQkJInNjaGVtYSI6IDMsCgkJCQkidXB2Ijog
W3sKCQkJCQkJIm1ham9yIjogMSwKCQkJCQkJIm1pbm9yIjogMAoJCQkJCX0sCgkJCQkJewoJCQkJCQki
bWFqb3IiOiAxLAoJCQkJCQkibWlub3IiOiAxCgkJCQkJfQoJCQkJXSwKCQkJCSJhdXRoZW50aWNhdGlv
bkFsZ29yaXRobXMiOiBbInNlY3AyNTZyMV9lY2RzYV9zaGEyNTZfcmF3Il0sCgkJCQkicHVibGljS2V5
QWxnQW5kRW5jb2RpbmdzIjogWyJlY2NfeDk2Ml9yYXciXSwKCQkJCSJhdHRlc3RhdGlvblR5cGVzIjog
WyJiYXNpY19mdWxsIl0sCgkJCQkidXNlclZlcmlmaWNhdGlvbkRldGFpbHMiOiBbCgkJCQkJW3sKCQkJ
CQkJInVzZXJWZXJpZmljYXRpb25NZXRob2QiOiAiZmluZ2VycHJpbnRfaW50ZXJuYWwiLAoJCQkJCQki
YmFEZXNjIjogewoJCQkJCQkJInNlbGZBdHRlc3RlZEZBUiI6IDAuMDAwMDIsCgkJCQkJCQkibWF4UmV0
cmllcyI6IDUsCgkJCQkJCQkiYmxvY2tTbG93ZG93biI6IDMwLAoJCQkJCQkJIm1heFRlbXBsYXRlcyI6
IDUKCQkJCQkJfQoJCQkJCX1dCgkJCQldLAoJCQkJImtleVByb3RlY3Rpb24iOiBbImhhcmR3YXJlIiwg
InRlZSJdLAoJCQkJImlzS2V5UmVzdHJpY3RlZCI6IHRydWUsCgkJCQkibWF0Y2hlclByb3RlY3Rpb24i
```

OiBbInRlZSJdLAoJCQkJImNyeXB0b1N0cmVuZ3RoIjogMTI4LAoJCQkJImF0dGFjaG1lbnRIaW50Ijog
WyJpbnRlcm5hbCJdLAoJCQkJInRjRGlzcGxheSI6IFsiYW55IiwgInRlZSJdLAoJCQkJInRjRGlzcGxh
eUNvbnRlbnRUeXBlIjogImltYWdlL3BuZyIsCgkJCQkidGNEaXNwbGF5UE5HQ2hhcmFjdGVyaXN0aWNz
IjogW3sKCQkJCQkid2lkdGgiOiAzMjAsCgkJCQkJImhlaWdodCI6IDQ4MCwKCQkJCQkiYml0RGVwdGgi
OiAxNiwKCQkJCQkiY29sb3JUeXBlIjogMiwKCQkJCQkiY29tcHJlc3Npb24iOiAwLAoJCQkJCSJmaWx0
ZXIiOiAwLAoJCQkJCSJpbnRlcmxhY2UiOiAwCgkJCQl9XSwKCQkJCSJhdHRlc3RhdGlvblJvb3RDZXJ0
aWZpY2F0ZXMiOiBbCgkJCQkJIk1JSUNNQ1ENQWVPZ0F3SUJBZ0lKQU91ZXh2VTNPeTJ3TUFvR0NDcUdT
TTQ5QkFNQ01Ic3hJREFlQmdOVkJBTU1GMU5oYlhCc1pTQkJkSFJsYzNSaGRHbHZiaUJTYjI5ME1SWXdG
QVlEVlFRS0RBMUdTVVJQSUVGc2JHbGhibU5sTVJFd0R3WURWUVFMREFoVlFVVWdWRmRmRITERFU01CQUdB
MVVFQnd3SlVHRnNieUJCYkhSdk1Rc3dDUVlEVlFRSURBSkRRVEVMTUFrR0ExVUVCaE1DVlZNd0hoY05N
VFF3TmpFNE1UQXpNek15V2hjTk5ERXhNVEF6TVRNek16TXlXakI3TVNBd0hnWURWUVFEREJkVFlXMXdi
R1VnUVhSMFpYTjBZWFJwYjI0Z1VtOXZkREVXTUJRR0ExVUVDZ3dOUmtsRVR5QkJiR3hwWVc1alpURVJN
QThHQTFVRUN3d0lWVUZHSUZSWFJ5d3hFakFRQmdOVkJBY01DVkJoYkc4Z1FXeDBiekVMTUFrR0ExVUVD
QXdDUTBFeEN6QUpCZ05WQkFZVEFsVlRNRmt3RXdZSEtvWkl6ajBDQVFZSUtvWkl6ajBEQVFjRFFnQUVI
OGh2MkQwSFhhNTkvQm1wUTdSWmVoTC9GTUd6RmQxUUJnOXZBVXBPWjNham51UTk0UFI3YU16SDMzblVT
QnI4ZkhZZRHJxT0JiNThweEdxSEppSeVgvNk5RTUU0d0hRWURWUjBPQkJZRUZQb0hBM0NMaHhGYkMwSXQ3
ekU0dzhoazVFSi9NQjhHQTFVZEl3UVlNQmFBRlBvSEEzQ0xoeEZiQzBJdDd6RTR3OGhrNUVKL01Bd0dB
MVVkRXdRRk1BTUJBZjh3Q2dZSUtvWkl6ajBFQXdJRFNBQXdSUUloQUowNlFTWHQ5aWhJYkVLVLWUtJanNQ
a3JpVmRMSWd0ZnNiRFN1N0VySmZ6cjRBaUJxb1lDWmYwK3pJNTVhUWVBSGpJekE5WG02M3JydUF4Qlo5
cHM5ejJYTmxRPT0iCgkJCQldLAoJCQkJImljb24iOiAiZGF0YTppbWFnZS9wbmc7YmFzZTY0LGlWQk9S
dzBLR2dvQUFBQU5TVWhFVWdBQUFFOEFBQUF2Q0FZQUFBQ2l3SmZjQUFBQUFYTlNSMElBcnM0YzZRQUFB
QVJuUVUxQkFBQ3hqd3Y4WVFVQUFBQUpjRWhaY3dBQURzUUFBQTdEQWNkdFFHUUFBQWFoU1VSQlZHaEQ3
WnI1YnhSbEdNZjllLelRCOEFNL1lFaEUyVzdwUVpjV0tLQmNsU3BIQVRsRUxBUkUkU3a05FQ0NBM0ZrV0sw
Q0tLU0NNRGSXNLQmNNVkNEV0dORVNkQVlpZHdnZ2dKQmlSaU1oRmMvNHd5ODg4NHp1OU5kbG5HVGZaSlAy
bjNuTysrODg5MzNmdmVCQngrUHFDDekprVFV2QmJJMbXBVRVRd2QlRJbXBjQ1NadlhMQ2RYOVIwNVNrMTli
YjVhdGY1OTlmRysyVFExcTQ3YVAxTExWYTlTSXlWTlVpOElpOGQ1a0dUc2kzME5GdjdhaTluN1Fa
UE13YmR5czJlclUyWE1xVWR5OCtaY2pGaGUlOM1JVZDNhMThuRjBmVWxvdlorMENNUeldwZDJW
aitlT20xYkV5eTZEeDRpNXBVTUdXdmVvNTA2cTIyN2R0dVdCSXVmZnI2b1dwVjBGUE5MaG93MTc1MU5t
MjFMdlBIM3JWdFdqZno2NkxmcmWw4dFg3RlJsOVlGlGU1hzbVNzZWI5Y2VPR2JZazdNTlVjR1pFbkFFpzYkn1
OXJmUVVVhYVYvSk1YOXNZZHpEQ2ZCrWkhtVFpnOXg3YkxxIY01uVGhiMTZlSittVmZZRZmRHTh5YVVaUU5H
NjRpWForMC9rcTZ1T1pGTzBRdGF0ZFdLZlhuUlE5OUJqOTFSNU9JRm5rNTRqTjBta1VpcWxxPM1hEVytN
bCs5OG1LQjZ0VzdyV3BaY1BjKzB6ZzR0THJZbFVjODZFNmVHRGpTRXViVnBjdXNlYXJmZ0lZZR1JrNmJy
aFpWci9KY0h6b29NNzU1MGplZExFeFeG9wV2NBcGkyWlVxaHU3Skx2clZzZUVU4MXprek9QZWVtTVJZZlZ1
UXNYN1BiaURRRWRWTVKdlpvbmZ0SysxVlk4SDl1dHg1MzBoMG9iK2ptdUlxajZvdWFFZGtVlblcvV2xZanA4
Y3diTW02ODJ0UHdxVzFSNHRqLzJTSDEzSVJKWWw0bW9adlhwaWVNxRHI3ZFh0UUh4YS9QSzMvK0JXc0x0sx
ZFRnSHU2Vjh0UUozYndGa3dRdnJnJVT1E1MHMxxcjNsZXZtOHpaY3ExNytCQmF3N0o0bEVLNXF6a1l1YXJ
OUE4cDdQM0d6REEsrbmQzRFFvdys2VUM4U1Z2ODJpdXYzO0ltN050OVVYVh0VjFDVnE2Umd3NHNBrc21iZGkz
YnUyRGU3NWZZZhQkJ4Y3FmdnFZQclVqRlF0RlVFEyMmxtZFZWVlQ2OHJUSktGNURuUuU21VamdkcWc0bVNTOXBt
c2ZZESlIzRzZUb0gwaVc5YVYY3TFdMSFlYS2xzVER0MExxUQXRrWUlhYW1wMVFqVnYrK3V5R1V4VmRKMERO
VlhhTbStiMXFSeHBsODRkZGZZMUxwMU8vZDY5dHNvZDB2czVoR3JlOXh1OG8rZnBpMUjFjR2hOVEQ2WjU3
QzlLTVdYZWZKZE9aOTRiYjlvcWQxUk9uUzdkxSVRUekhpbpU1xaXZiTzRnMERkVnlrM1dRRmhCenRRMzZZ
S05kTkMjE8zYWNTNmZEWkZnS2FVTHNMSFNnA1cmRybGlCcXA4OWNKVjMvbTdUdUdnMWcmtqR2ZONGNIwa1Bv
Wm4zVnUp1SU9ybloyMnlQMWZ0dlV4K081Z1NxZWJWTWl0ZeNlBN1WU5WaHE3VFdiRGlMVnZZsanBsTGxvcDZD
TFhQKzJxdzJHTElMLzF2aW1JJU2RNQmd6U29GWnl1NlRxZXhZZCtqenhhnc1BhVjlNlCQ3FlZS9OallrNnY2bEs5
Y3dpWFVWMVUR0ZjFIRHBNM2I1OTJ5N2gzVGh4NW96SzY5SExwVVd1UXhdhcVM1Y3YyYnNE3Y2ViOGVmVllsh
UmVQM2lGVTh6jFrblN3WlhITW1uQ2pZME9nYWxvN1VRZlNDZTTNxUVFyMkgvWEZQN3NzWHHg0NVlsOTFC
eWVDZXA0bW9ab0grMWZHM3hENHRUN3g0a3d5ajhudI5ZXYyNlYwQjZkKzdINHpLdnVkQUg1MzdGanF5
ek9IZEpuSEV1em1YcS9XanhPYnZOTWJ2N2N25oeXdzWDJhVnnNXdEM4KzQ4YUxxYXBFN3A1d0taaTBBMkFR
UlY1bnZSNEUrdUpjK2I2MWtBcHFFJbnhCZ21kLzRWNVFQL210MThIREM3c1JJZnRtZXU1bG1oVjBybi9B
TFgyMzJicWQ0QkZuRHg3VmkxY1dTMmnVmZjBJYkI0N3FleHhtVWo5UXV0WWp1cGQzdFlENmFiV0JCTXJo
K2FwTmJPS3JORjErdWdDVTRyaVhHZndNNUFB0VmlhdmhVM1lNT0FBbnVVYi9SMDdMMHlPU2VPYWRFODhB
cHNYRkdmZjJMueW5obEpnTTBTxQ1U2dk45RXpnbnB2SEJGGVXlpVnJhZVBpd0o1M0RGNVpUWm5vbUVUOZzg1
a05VZDJvSmkyV3ByNE99tbWtmTjR4NHpIIzmlWRmM4RHY4Tnp1aE5xT2lkWVdHdkE2REd1ZVp3Tzc4QUFR
bjZjaUVrNitydzVWY3ZqdnFOOFRFlQT29JVXdhS1NocnhBdVhMbGtINGFZZUdUdmTVlEYzEwV0Y1VGEzMWhQ
Sk9mY1VoclUvSmxJTmk2YzZlbFFJZZEJwbzYrK1lmang2MWxHTmZSbTRTRFNyaFqM0ZvR0h1akRTQk5h
cllVVZ01MeU1zektwYjd0WHBvSGZQczhoM1dwMUx6TmZZOazU0WHhDMXdER1lVtWXpYWWVmaDZ6L2NLdFZt
NEVVCeGE5VlFHRHpZcjNNclVNUmpIRUtrazd6YUZLWVFBMmhHUVUxeis4NU5GV3BYRHJejN2eDEwR3F4
UTZCemVOYmdCazVuOGs0bmViUmgrazFoV2Z2V4VEYwRDFFeVdVczVuditkZ1FxS2F4enVDZEUwaXNIbDAy
TlE4YWgwbVhyMTJMMYTNtMGY5d2lrOSt3TE5UUTVUVkVOZ0NUNUG84eWkzMU9meG1GUNlBXb3FHOStEWnVrWW5h
NTZtU1p0NVdXU3k1cVZBMXJ3VXlKcVhhbG56a2lhS9nSFNEN1JrVHlpaG9nQUFBQUJKUlU1RXJrSmdn
Zz09IgoJCQl9LAoJCQkic3RhdHVzUmVwb3J0cyI6IFt7CgkJCQkic3RhdHVzIjogIkZJRE9fQ0VSVElG
SUVEIiwKCQkJCSJlZmZlY3RpdmVEYXRlIjogIjIwMTQtMDEtMDQiCgkJCX1dLAoJCQkidGltZU9mTGFz
dFN0YXR1c0NoYW5nZSI6ICIyMDE0LTAxLTA0IgoJCX0sCgkJewoJCQkiYWFndWlkIjogIjAxMzJkMTEw

LWJmNGUtNDIwOC1hNDAzLWFiNGY1ZjEyZWZlNSIsCgkJCSJtZXRhZGF0YVN0YXRlbWVudCI6IHsKCQkJ
CSJsZWdhbEhlYWRlciI6ICJodHRwczovL2ZpZG9hbGxpYW5jZS5vcmcvbWV0YWRhdGEvbWV0YWRhdGEt
c3RhdGVtZW50LWxlZ2FsLWhlYWRlci8iLAoJCQkJImRlc2NyaXB0aW9uIjogIkZJRE8gQWxsaWFuY2Ug
U2FtcGxlIEZJRE8yIEF1dGhlbnRpY2F0b3IiLAoJCQkJImFhZ3VpZCI6ICIwMTMyZDExMC1iZjRlLTQy
MDgtYTQwMy1hYjRmNWYxMmVmZTUiLAoJCQkJImFsdGVybmF0aXZlRGVzY3JpcHRpb25zIjogewoJCQkJ
CSJydS1SVSI6ICLQn9GA0LjQvNC10YAgRklETzIg0LDRg9GC0LXQvdGC0LjRhNC40LrQsNGC0L7RgNCw
INC-0YIgRklETyBBbGxpYW5jZSIsCgkJCQkJImZyLUZSIjogIkV4ZW1wbGUgRklETzIgYXV0aGVudGlj
YXRvciBkZSBGSURPIEFsbGlhbmNlIiwKCQkJCQkiemgtQ04iOiAi5L6G6IeqRklETyBBbGxpYW5jZeea
hOekuuS-i0ZJRE8y6Lqr5Lu96amX6K2J5ZmoIgoJCQkJfSwKCQkJCSJwcm90b2NvbEZhbWlseSI6ICJm
aWRvMiIsCgkJCQkic2NoZW1hIjogMywKCQkJCSJhdXRoZW50aWNhdG9yVmVyc2lvbiI6IDUsCgkJCQki
dXB2IjogW3sKCQkJCQkibWFqb3IiOiAxLAoJCQkJCSJtaW5vciI6IDAKCQkJCX1dLAoJCQkJImF1dGhl
bnRpY2F0aW9uQWxnb3JpdGhtcyI6IFsic2VjcDI1NnIxX2VjZHNhX3NoYTI1Nl9yYXciLCAicnNhc3Nh
X3BrY3N2MTVfc2hhMjU2X3JhdyJdLAoJCQkJInB1YmxpY0tleUFsZ0FuZEVuY29kaW5ncyI6IFsiY29z
ZSJdLAoJCQkJImF0dGVzdGF0aW9uVHlwZXMiOiBbImJhc2ljX2Z1bGwiXSwKCQkJCSJ1c2VyVmVyaWZp
Y2F0aW9uRGV0YWlscyI6IFsKCQkJCQlbewoJCQkJCQkidXNlclZlcmlmaWNhdGlvbk1ldGhvZCI6ICJu
b25lIgoJCQkJCX1dLAoJCQkJCVt7CgkJCQkJSJ1c2VyVmVyaWZpY2F0aW9uTWV0aG9kIjogInByZXNl
bmNlX2ludGVybmFsIgoJCQkJCX1dLAoJCQkJCVt7CgkJCQkJSJ1c2VyVmVyaWZpY2F0aW9uTWV0aG9k
IjogInBhc3Njb2RlX2V4dGVybmFsIiwKCQkJCQkJImNhRGVzYyI6IHsKCQkJCQkJSJiYXNlIjogMTAs
CgkJCQkJCkibWluTGVuZ3RoIjogNAoJCQkJCl9CgkJCQkJfV0sCgkJCQkJW3sKCQkJCQkJSJ1c2VyVm
VmVyaWZpY2F0aW9uTWV0aG9kIjogInBhc3Njb2RlX2V4dGVybmFsIiwKCQkJCQkJSJjYURlc2MiOiB7
CgkJCQkJCQkJImJhc2UiOiAxMCwKCQkJCQkJCQkibWluTGVuZ3RoIjogNAoJCQkJCQkJfQoJCQkJCQl9
LAoJCQkJCQl7CgkJCQkJCQkidXNlclZlcmlmaWNhdGlvbk1ldGhvZCI6ICJwcmVzZW5jZV9pbnRlcm5h
bCIKCQkJCQkJfQoJCQkJCV0KCQkJCV0sCgkJCQkia2V5UHJvdGVjdGlvbiI6IFsiaGFyZHdhcmUiLCAi
c2VjdXJlX2VsZW1lbnQiXSwKCQkJCSJtYXRjaGVyUHJvdGVjdGlvbiI6IFsib25fY2hpcCJdLAoJCQkJ
ImNyeXB0b1N0cmVuZ3RoIjogMTI4LAoJCQkJImF0dGFjaG1lbnRIaW50IjogWyJleHRlcm5hbCIsICJ3
aXJlZCIsICJ3aXJlbGVzcyIsICJuZmMiXSwKCQkJCSJ0Y0Rpc3BsYXkiOiBbXSwKCQkJCSJhdHRlc3Rh
dGlvblJvb3RDZXJ0aWZpY2F0ZXMiOiBbCgkJCQkIk1JSUNQVENDQWVPZ0F3SUJBZ0lKQU91ZXh2VTNP
eTJ3TUFvR0NDcUdTTTQ5QkFNQ01Ic3hJREFlQmdOVkJBTU1GMU5oYlhCc1pTQkJkSFJsYzNSaGRHbHZi
aUJTYjI5ME1SWXdGQVlEVlFRS0RBMUdTVVJQSUVGc2JHbGhibU5sTVJFd0R3WURWUVFMREFoVlFVWWdW
RmRITERFU01CQUdBMVVFQnd3SlVHRnNieUJCYkhSdk1Rc3dDUVlEVlFSURBSkRRVEVMTUFrR0ExVUVC
aE1DVlZNd0hoY05NVFF3TmpFNE1UTXpNek15V2hjTk5ERXhNVEF6TVRNek16TXlXakI3TVNBd0hnWURW
UVFEREJkVFlXMXdiR1VnUVhSMFpYTjBZWFJwYjI0Z1VtOXZkREVXTUJRR0ExVUVDZ3dOUmtsRVR5QkJi
R3hwWVc1alpURVJNQThHQTFVRUN3d0lWUZHSUZSWFJ5d3hFakFRQmdOVkJBY01DVkJoYkc4Z1FXeDBi
ekVMTUFrR0ExVUVDQXdDUTBFeEN6QUpCZ05WQkFZVEFsVlRNRmt3RXdZSEtvWkl6ajBDQVFZSUtvWkl6
ajBEQVFjRFFnQUVIOGh2MkQwSFhhNTkvQm1wUTdSWmVoTC9GTUd6RmQxUUJnOXZBVXBPWjNham51UTk0
UFI3YU16SDMzblVTQnI4ZkhZRHJxT0JiNThweEdxSEpSeVgvNk5RTUU0d0hRWURWUjBPQkJZRUZQb0hB
M0NMaHhGYkMwSXQ3ekU0dzhoazVFSi9NQjhHQTFVZEl3UVlNQmFBRlBvSEEzQ0xoeEZiQzBJdDd6RTR3
OGhrNUVKL01Bd0dBMVVkRXdRRk1BTUJBZjh3Q2dZSUtvWkl6ajBFQXdJRFNBQXdSUUloQUowNlFTWHQ5
aWhJYkVLWUtJanNQa3JpVmRMSWd0ZnNiRFN1N0VySmZ6cjRBaUJxb1lDWmYwK3pJNTVhUWVBSGpJekE5
WG02M3JydUF4Qlo5cHM5ejJYTmxRPT0iCgkJCQldLAoJCQkJImljb24iOiAiZGF0YTppbWFnZS9wbmc7
YmFzZTY0LGlWQk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFFOEFBQUF2Q0FZQUFBQ2l3SmZjQUFBQUFYTlNS
MElBcnM0YzZRQUFBQVJuUVUxQkFBQ3hqd3Y4WVFVQUFBQUpjRWhaY3dBQURzTUFBQTdEQWNkdnFHUUFB
QWFoU1VSQlZHaEQ3WnI1YnhSbEdNZjlLelRCOEFNL1lFaEUyVzdwUVpjV0tLQmNsU3BIQVRsRUxBUkU3
a05FQ0NBM0ZrV0swQ0tLU0NGSXNLQmNnVkNEV0dORVNkQVlpZHdnZ2dKQmlSaU1oRmMvNHd5ODg4NHp1
OU5kbG5HVGZaSlAybjNuTysrODg5MzNmdmVCQngrUHFDekprVFV2QmJMbXBVRFd2QlRJbXBjQ1NadlhM
Q2RYOVIwNVNrMTliYjVhdGY1OTlmRysvZXJBNTQxcTQ3YVAxTExWYTlTSXlWTlVpOElpOGQ1a0dUc2kz
ME5GdjdhaTluN1FaUE13YmR5czJlclUyWE1xVWR5OCtaY2FObUdpbUU4eVhOM1JVZDNhMThuRjBmVWxv
dlorMENUeldwZDJWaitlT20xYkV5eTZEeDRpNXBVTUdXdmVvNTA2cTIyN2R0dVdCSXVmZnI2b1dwVjBG
UE5MaG93MTc1MU5tMjFMdlBIM3JWdFdqZno2NkxmcWw4dFg3RlJsOVlGU1hzbVNzZWI5Y2VPR2JZazdN
TlVjR1BnOFpzYk1lOXJmUVVhYVYvSk1YOXNxZHpEQ1N2cDBrWkhtVFpnOXg3YkxIY01uVGhiMTZlSitt
VmZRcTh5YVVaUU5HNjRpWForMC9rcTZ1T1pGTzBRdGF0ZFdLZlhuUlE5OUJqOTFSNU9JRm5rNTRqTjBt
a1VpcWxPM1hEVytNbCs5OG1LQjZ0VzdyV3BaY1BjKzB6ZzR0THJZbFVjODZFNmVHRGpJTXViVnBjdXNl
YXJmZ0lZR1JrNmJyaFpWci9KY0h6b29MNzU1MGplZExFeG9wV2NBcGkyWlVxaHU3Skx2clZzUVU4MXpr
ek9QZWVtTVJZdlZ1UXNYN1BiaURRWTVKdlpvbmZ0SysxVlk4SDl1dHg1MzBoMG9iK2ptUllxajZvdWFZ
dkVlblcvV2xZanA4Y3diTW02ODJ0UHdxVzFSNHRqLzJTSDEzSVJKWWw0bW9adlhwaVNxRHI3ZFh0UUh4
YS9QSzMvK0JXc0sxZFRnSHU2Vjh0UUozYndGa3dwRnJVT1E1MHMxcjNsZXZtOHpaY3ExNytCQmF3N0s4
bEVLNXF6a1llYXJrOUE4cDdQM0d6REsrbmQzRFFvdys2VUM4U1ZOODJpdXYzOGltN050YVh0VjFDVnE2
Umd3NHBrc21iZGkzYnUyRGU3WWZhQkJ4Y3FmdnFQclVqRlFOVFEyMmxmZFVWVlQ2OHJUSktGNURuU21V
amdkcWc0bVNTOXBtc2ZESlIzRzZUb0gwaVc5YVY3TFdMSFlYS2xsVER0MExUQXRrWUlhYW1wMVFqVnYr
K3V5R1V4VmRKMEROVlhTbStiMXFSeHBsODRkZGZYMUxwMU8vZDY5dHNvZDB2czVoR3JlOXh1OG8rZnBM
UjFjR2hOVEQ2WjU3QzlLTVdYZWZKZE9aOTRiYjlvcWQxUk9uUzdxSVRUekhpbU1xaXZiTzNnMERkVnlr
M1dRQmhCenRLMzVZS05kT25jOE8zYWNTNmZEWkZnS2FYTHNFSnA1cmRybGlCcXA4OWNKY3MvbTdUdnMw
cmtqR2ZQNGIwa1BvWm4zVUp1SU9vblovMnlQMWZtdlV4K081Z1NxZWlWMW0relN1WU5WaHE3VEdiRGlM

```
VnZsanBsTGxvcDZDTFhQKzJxdHZHTElMLzF2aW1JU2RNQmd6U29GWnl1NlRxZCtqenhnc1BhVjlCQ3Fl
ZS9OallrNnY2bEs5Y3dpVWMvU1R0ZjFIRHBNM2I1OTJ5N2gzVGh4NW96SzY5SExwWVd1QXdhcVM1Y3Yy
NnE3Y2ViOGVmVllhUmVQM2lGVTh6ajFrblN3WlhITW1uQ2pZME9nYWxvN1VRZlNDTTNxUVFyMkgvWEZQ
N3NzWHg0NVlsOTFCeWVDZXA0bW9ab0grMWZHM3hENHRUN3g4a3d5ajhud2I5ZXYyNlYwQjZkKzdINHpL
dnVkQUg1MzdGanF5ek9IZEpuSEV1em1YcS9XanhPYnZOTWJ2N25oeXdzWDJhVnNXdEM4KzQ4YUxlYXBF
N3A1d0taaTBBMkFRUlY1bnZSNEUrdUpjK2I2MWtBcHFJbnhCZ21kLzRWNVFQL210MThIREM3c1JIZnRt
ZXU1bG1oVjBybi9BTFgyMzJicWQ0QkZuRHg3VmkxY1dTMnVmZjBJYkI0N3FleHhtVWo5UXV0WWp1cGQz
dFlENmFiV0JCTXJoK2FwTmJPS3JORjErdWdDYTRyaVhHZndNUFB0VmlhdmhVM1lNT0FBbnVVYi9SMDdM
MHlPU2VPYWRFODhBcHNYRkdmZjMweW5obEpnTTUxQ1U2dk45RXpnbnB2SEJGVXlpVnJhZVBpd0o1M0RG
NVpUWm5vbUVOZzg1a05VZDJvSmkyV3ByNE9tbWtmTjR4NHpIZmlWRmM4RHY4Tnp1aE5xT2lkaWxHdkE2
REd1ZVp3Tzc4QUFRbjZjaUVrNitydzVWY3ZqdnFORFlQT29JVXdhS1NocnhBdVhMbGtINGFZdUdmTVlE
YzEwV0Y1VGEzMWhQSk9mY1VoclUvSmxJTmk2YzZlbFJZZEJwbzYrK1lmang2MWxHTmZSbTRNRDVySjFq
M0ZvR0huakRTQk5hcllVZ01MeU1zektwYjd0WHBvSGZQczhoM1dwMUx6TmZOazU0WHhDMXdER1VtWXpY
WWVmaDZ6L2NLdFZtNEVCeGE5VlFHRHpZcjNMclVNUmpIRUtrazd6YUZLWVFBMmhHUVUxeis4NU5GV3BY
RHJrejN2eDEwR3F4UTZCemVOYm9CazVuOGs0bmViUmgrazFoV2Z4VEYwRDFFeVdVczVuditkZ1FxS2F4
enVDZEUwaXNIbDAyTlE4YWgwbVhyMTJMYTNtMGY5d2lrOSt3TE5UTVkvODZNUG84eWkzMU9meG1UNlBX
b3FHOStEWnVrWW5hNTZtU1p0NVdXU3k1cVZBMXJ3VXlKcVhBbG56a2lhaS9nSFNEN1JrVHlpaG9nQUFB
QUJKUlU1RXJrSmdnZz09IiwKCQkJCSJzdXBwb3J0ZWRFeHRlbnNpb25zIjogW3sKCQkJCQkJImlkIjog
ImhtYWMtc2VjcmV0IiwKCQkJCQkJImZhaWxfaWZfdW5rbm93biI6IGZhbHNlCgkJCQkJfSwKCQkJCQl7
CgkJCQkJSJpZCI6ICJjcmVkUHJvdGVjdCIsCgkJCQkJSJmYWlsX2lmX3Vua25vd24iOiBmYWxzZQoJ
CQkJCX0KCQkJCV0sCgkJCQkiYXV0aGVudGljYXRvckdldEluZm8iOiB7CgkJCQkJInZlcnNpb25zIjog
WyJVMkZfVjIiLCAiRklET18yXzAiXSwKCQkJCQkiZXh0ZW5zaW9ucyI6IFsiY3JlZFByb3RlY3QiLCAi
aG1hYy1zZWNyZXQiXSwKCQkJCQkiYWFndWlkIjogIjAxMzJkMTEwYmY0ZTQyMDhhNDAzYWI0ZjVmMTJl
ZmU1IiwKCQkJCQkib3B0aW9ucyI6IHsKCQkJCQkJInBsYXQiOiAiZmFsc2UiLAoJCQkJCQkicmsiOiAi
dHJ1ZSIsCgkJCQkJCSJjbGllbnRQaW4iOiAidHJ1ZSIsCgkJCQkJCSJ1cCI6ICJ0cnVlIiwKCQkJCQkJ
InV2IjogInRydWUiLAoJCQkJCQkidXZUb2tlbiI6ICJmYWxzZSIsCgkJCQkJCSJjb25maWciOiAiZmFs
c2UiCgkJCQkJfSwKCQkJCQkibWF4TXNnU2l6ZSI6IDEyMDAsCgkJCQkJInBpblV2QXV0aFByb3RvY29s
cyI6IFsxXSwKCQkJCQkibWF4Q3JlZGVudGlhbENvdW50SW5MaXN0IjogMTYsCgkJCQkJIm1heENyZWRl
bnRpYWxZExlbmd0aCI6IDEyOCwKCQkJCQkidHJhbnNwb3J0cyI6IFsidXNiIiwgIm5mYyJdLAoJCQkJ
CSJhbGdvcml0aG1zIjogW3sKCQkJCQkJCSJ0eXBlIjogInB1YmxpYy1rZXkiLAoJCQkJCQkJImFsZyI6
IC03CgkJCQkJCX0sCgkJCQkJCXsKCQkJCQkJCSJ0eXBlIjogInB1YmxpYy1rZXkiLAoJCQkJCQkJImFs
ZyI6IC0yNTcKCQkJCQkJfQoJCQkJCV0sCgkJCQkJIm1heEF1dGhlbnRpY2F0b3JDb25maWdMZW5ndGgi
OiAxMDI0LAoJCQkJCSJkZWZhdWx0Q3JlZFByb3RlY3QiOiAyLAoJCQkJCSJmaXJtd2FyZVZlcnNpb24i
OiA1CgkJCQl9CgkJCX0sCgkJCSJzdGF0dXNSZXBvcnRzIjogW3sKCQkJCQkic3RhdHVzIjogIkZJRE9f
Q0VSVElGSUVEIiwKCQkJCQkiZWZmZWN0aXZlRGF0ZSI6ICIyMDE5LTAxLTA0IgoJCQkJfSwKCQkJCQkJ
CQkic3RhdHVzIjogIkZJRE9fQ0VSVElGSUVEX0wxIiwKCQkJCQkiZWZmZWN0aXZlRGF0ZSI6ICIy
MDIwLTExLTE5IiwKCQkJCQkiY2VydGlmaWNhdGlvbkRlc2NyaXB0b3IiOiAiRklETyBBbGxpYW5jZSBT
YW1wbGUgRklETzIgQXV0aGVudGljYXRvciIsCgkJCQkJImNlcnRpZmljYXRlTnVtYmVyIjogIkZJRE8y
MTAwMDIwMTUxMjIxMDAxIiwKCQkJCQkiY2VydGlmaWNhdGlvblBvbGljeVZlcnNpb24iOiAiMS4wLjEi
LAoJCQkJCSJjZXJ0aWZpY2F0aW9uUmVxdWlyZW1lbnRzVmVyc2lvbiI6ICIxLjAuMSIKCQkJCX0KCQkJ
XSwKCQkJInRpbWVPZkxhc3RTdGF0dXNDaGFuZ2UiOiAiMjAxOS0wMS0wNCIKCQl9CgldCn0
```

```
EXAMPLE: JWT HEADER
{
  "alg": "ES256",
  "typ": "JWT",
  "iat": 1743490805,
  "x5c": [
    "MIICZTCCAgugAwIBAgIBATAKBggqhkjOPQQDAjCBozEnMCUGA1UEAwweRVhBTVBM
    RSBNRFMzIFRFU1QgSU5URVJNRURJQVRFMSIwIAYJKoZIhvcNAQkBFhNleGFtcGxl
    QGV4YW1wbGUuY29tMRQwEgYDVQQKDAtFeGFtcGxlIE9SRzEQMA4GA1UECwwHRXhh
    bXBsZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1ZMRIwEAYDVQQHDAlXYWtlZmll
    bGQwHhcNMjEwNDE5MTEzNTA3WhcNMzEwNDE3MTEzNTA3WjCBpTEpMCcGA1UEAwwg
    RVhBTVBMRSBNRFMzIFNJR05JTkcgQ0VSVElGSUNBVEUxIjAgBgkqhkiG9w0BCQEW
    E2V4YW1wbGVAZXhhbXBsZS5jb20xFDASBgNVBAoMC0V4YW1wbGUgT1JHMRAwDgYD
    VQQLDAdFeGFtcGxlMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTVkxEjAQBgNVBAcM
    CVdha2VmaWVsZDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABNQJs6wTqixc+S+V
    DAajFlPNat10KEWJE5jcWOvm6qpO9SDAAMZvb4HHrvs+P5YRpHrSlUPdvK+uEQbd
    Wg31P9ujLDAqMAkGA1UdEwQCMAAwHQYDVR0OBBYEFLqsapcXV4ZoVHAnRpPZwQe7
    Yy20MAoGCCqGSM49BAMCA0gAMEUCIQC67za8EIuyRiKgNDXIP1s1aLr3jzH9WVXf
    Hx4bJ+zCsgIgG/tVButOJUU+vvoHIo/otAUAcH5bNHP3uIziDS+PTUc=",
    "MIIEHzCCAgegAwIBAgIBAjANBgkqhkiG9w0BAQsFADCBmzEfMB0GA1UEAwwWRVhB
    TVBMRSBNRFMzIFRFU1QgUk9PVDEiMCAGCSqGSIb3DQEJARYTZXhhbXBsZUBleGFt
    cGxlLmNvbTEUMBIGA1UECgwLRXhhbXBsZSBPUkcxEDAOBgNVBAsMB0V4YW1wbGUx
    CzAJBgNVBAYTAlVTMQswCQYDVQQIDAJNWTESMBAGA1UEBwwJV2FrZWZpZWxkMB4X
    DTIxMDQxOTExMzUwN1oXDTQ4MDkwNDExMzUwN1owgaMxJzAlBgNVBAMMHkVYQU1Q
    TEUgTURTMyBURVNUIElOVEVSTUVESUFURTEiMCAGCSqGSIb3DQEJARYTZXhhbXBs
    ZUBleGFtcGxlLmNvbTEUMBIGA1UECgwLRXhhbXBsZSBPUkcxEDAOBgNVBAsMB0V4
    YW1wbGUxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJNWTESMBAGA1UEBwwJV2FrZWZp
    ZWxkMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAENGumBbYnFQnTjP1RSfc70hsh
    gbiI1ZtpwQ5n6xRLA/Wq0PSCfLl5qQ+r7dlcK1d3r3vLa+vm6G6vKHGCPEeUzqMv
    MC0wDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUNk6F4RJnGGVFe+0/cbZwfrZd7ZUw
    DQYJKoZIhvcNAQELBQADggIBACnp1fm0FKlWmUtTplLuYg7mps4xP/COu8dnb38u
    1nMDVuOT4+CZaiM9AGz313GD22hjLGrmPuYn86wGOKI3HOrEpsGdMmfy7tTmKX/e
    M/eS3FEDXZnE82Pn5oFIyBT/f8sGuXyOsFZqWBvVdBIIDldCpD4mxMQZZOZtTrlv
    3WvBQMC/dsicOxe3QKXvWHi6Qb/Rhuaip3rPmwMf+4JpnJO+JMPqAaU1cAH8HVsf
    rLAMoKs148j2+cvbpaWmsT5rIoH/ezVrPaG/MOiIgq79w/efuvSi5AX8J+kDoLSE
    f3d5wOgkJYAqUqcRxXTEEtKIzDM6hzaBQFiAWvTn9IlVWgntQamSXvH+txaTF9iE
    lHxUf5INYFVciCpztSrydeHv/OCNRf7/LVricMSlo8Rh+O3yP9V+2uNf3X8sQJNt
    ufrQNaqq18wiXliTLufSn02/g+mkhIUiNKfTOJpvCjKeCnCFcxQU2/XT3Kh3G8gD
    JwsO6EVRjMUJt4AYKze/hEUCwF55IF2m3jHIoCu8jVfj24CeEX5dnfvSr+SVvN5Q
    B0uZ05M4rmyZXyqBm0zK3fR+iE0/ZpInuwLC7X+W82zXlnMkplI3Q+Jxd7jfQ15S
    YNE2K6rvRIT01w0P9ZqyDF7knGKpRlp7Oqxd37bD/VUbWpQ7gIAfsJNH5KBLowHJ
    FFjW"
  ]
}
```

In order to produce the tbsPayload, we first need the base64url-encoded (without padding) JWT Header:

```
EXAMPLE: ENCODED JWT HEADER
ew0KICAiYWxnIjogIkVTMjU2IiwNCiAgInR5cCI6ICJKV1QiLA0KICAiaWF0IjogMTc0MzQ5MDgwNSwN
CiAgIng1YyI6IFsNCiAgICAiTUlJQ1pUQ0NBZ3VnQXdJQkFnSUJBVEFLQmdncWhrak9QUVFEQWpDQm96
RW5NQ1VHQTFVRUF3d2VSVmhCVFZCTQ0KICAgIFJTQk5SRk16SUZSRlUxUWdTVTVVUlZKTlJVUkpRVlJG
TVNJd0lBWUpLb1pJaHZjTkFRa0JGaE5sZUdGdGNHeGwNCiAgICBRR1Y0WVcxd2JHVXVZMjl0TVJRd0Vn
WURWUVFLREF0RmVHRnRjR3hsSUU5U1J6RVFNQTRHQTFVRUN3d0hSWGhoDQogICAgYlhCc1pURUxNQWtH
QTFVRUJoTUNWVk14Q3pBSkJnTlZCQWdNQWsxWk1SSXdFQVlEVlFRSERBbFhZV3RsWm1sbA0KICAgIGJH
UXdIaGNOTWpFd05ERTVNVEV6TlRBM1doY05NekV3TkRFM01URXpOVEEzV2pDQnBURXBNQ2NHQTFVRUF3
d2cNCiAgICBSVmhCVFZCTVJTQk5SRk16SUZOSlIwNUpUa2NnUTBWU1ZFbEdTVU5CVkVVeElqQWdCZ2tx
aGtpRzl3MEJDUUVXDQogICAgRTJWNFlXMXdiR1ZBWlhoaGJYQnNaUzVqYjIweEZEQVNCZ05WQkFvTUMw
VjRZVzF3YkdVZ1QxSkhNUkF3RGdZRA0KICAgIFZRUUxEQWRGZUdGdGNHeGxNUXN3Q1FZRFZRUUdFd0pW
VXpFTE1Ba0dBMVVFQ0F3Q1RWa3hFakFRQmdOVkJBY00NCiAgICBDVmRoYTJWbWFXVnNaREJaTUJNR0J5
cUdTTTQ5QWdFR0NDcUdTTTQ5QXdFSEEwSUFCTlFKczZ3VHFpeGMrUytWDQogICAgREFhakZsUE5hdDEw
S0VXSkU1amNXT3ZtNnFwTzlTREFBTVp2YjRISHJ2cytQNVlScEhyU2xVUGR2Syt1RVFiZA0KICAgIFdn
MzFQOXVqTERBcU1Ba0dBMVVkRXdRQ01BQXdIUVlEVlIwT0JCWUVGTHFzYXBjWFY0Wm9WSEFuUnBQWndR
ZTcNCiAgICBZeTIwTUFvR0NDcUdTTTQ5QkFNQ0EwZ0FNRVVDSVFDNjd6YThFSXV5UmlLZ05EWElQMXMx
YUxyM2p6SDlXVlhmDQogICAgSHg0YkorekNzZ0lnRy90VkJ1dE9KVVUrdnZvSElvL290QVVBY0g1Yk5I
UDN1SXppRFMrUFRVYz0iLA0KICAgICJNSUlFSHpDQ0FnZWdBd0lCQWdJQkFqQU5CZ2txaGtpRzl3MEJB
UXNGQURDQm16RWZNQjBHQTFVRUF3d1dSVmhCDQogICAgVFZCTVJTQk5SRk16SUZSRlUxUWdVazlQVkRF
aU1DQUdDU3FHU0liM0RRRUpBUllUWlhoaGJYQnNaVUJsZUdGdA0KICAgIGNHeGxMbU52YlRFVU1CSUdB
MVVFQ2d3TFJYaGhiWEJzWlNCUFVrY3hFREFPQmdOVkJBc01CMFY0WVcxd2JHVXgNCiAgICBDekFKQmdO
VkJBWVRBbFZUTVFzd0NRWURWUVFJREFKTldURVNNQkFHQTFVRUJ3d0pWMkZyWldacFpXeGtNQjRYDQog
ICAgRFRJeE1EUXhPVEV4TXpVd04xb1hEVFE0TURrd05ERXhNelV3TjFvd2dhTXhKekFsQmdOVkJBTU1I
a1ZZUVUxUQ0KICAgIFRFVWdUVVJUTXlCVVJWTlVJRWxPVkVWU1RVVkVTVUZVUlRFaU1DQUdDU3FHU0li
M0RRRUpBUllUWlhoaGJYQnNaVUJsZUdGdGNHeGxMbU52YlRFVU1CSUdBMVVFQ2d3TFJYaGhi
WEJzWlNCUFVrY3hFREFPQmdOVkJBc01CMFY0DQogICAgWVcxd2JHVXhDekFKQmdOVkJBWVRBbFZUTVFz
d0NRWURWUVFJREFKTldURVNNQkFHQTFVRUJ3d0pWMkZyWldacA0KICAgIFpXeGtNRmt3RXdZSEtvWkl6
ajBDQVFZSUtvWkl6ajBEQVFjRFFnQUVOR3VtQmJZbkZRblRqUDFSU2ZjNzBoc2gNCiAgICBnYmlJMVp0
cHdRNW42eFJMQS9XcTBQU0NmTGw1cVErcjdkbGNLMWQzcjN2TGErdm02RzZ2S0hHQ1BFZVV6cU12DQog
ICAgTUMwd0RBWURWUjBUQkFVd0F3RUIvekFkQmdOVkhRNEVGZ1FVTms2RjRSSm5HR1ZGZSswL2NiWndm
clpkN1pVdw0KICAgIERRWUpLb1pJaHZjTkFRUxCUUFEZ2dJQkFDbnAxZm0wRktsV21VdFRwbEx1WWc3
bXBzNHhQL0NPdThkbmIzOHUNCiAgICAxbk1EVnVPVDQrQ1phaU05QUd6MzEzR0QyMmhqTEdybVB1WW44
NndHT0tJM0hPckVwc0dkTW1meTd0VG1LWC9lDQogICAgTS9lUzNGRURYWm5FODJQbjVvRkl5QlQvZjhz
R3VYeU9zRlpxV0J2VmRCSUlEbGRDcEQ0bXhNUVpaT1p0VHJsdg0KICAgIDNXdkJRTUMvZHNpY094ZTNR
S1h2V0hpNlFiL1JodWFpcDNyUG13TWYrNEpwbkpPK0pNUHFBYVUxY0FIOEhWc2YNCiAgICBByTEFNb0tz
MTQ4ajIrY3ZicGFXbXNUNXJJb0gvZXpWclBhRy9NT2lJZ3E3OXcvZWZ1dlNpNUFYOEora0RvTFNFDQog
ICAgZjNkNXdPZ2tKWUFxVXFjUnhYVEVFdEtJekRNNmh6YUJRRmlBV3ZUbjlJbFZXZ250UWFtU1h2SCt0
eGFURjlpRQ0KICAgIGxIeFVmNUlOWUZWY2lDcHp0U3J5ZGVIdi9PQ05SZjcvTFZyaWNNU2xvOFJoK08z
eVA5VisydU5mM1g4c1FKTnQNCiAgICB1ZnJRTmFxcTE4d2lYbGlUTHVmU24wMi9nK21raElVaU5LZlRP
SnB2Q2pLZUNuQ0ZjeFFVMi9YVDNLaDNHOGdEDQogICAgSndzTzZFVlJqTVVKdDRBWUt6ZS9oRVVDd0Y1
NUlGMm0zakhJb0N1OGpWZmoyNENlRVg1ZG5mdlNyK1NWdk41UQ0KICAgIEIwdVowNU00cm15Wlh5cUJt
MHpLM2ZSK2lFMC9acEludXdMQzdYK1c4MnpYbG5Na3BsSTNRK0p4ZDdqZlExNVMNCiAgICBZTkUySzZy
dlJJVDAxdzBQOVpxeURGN2tuR0twUmxwN09xeGQzN2JEL1ZVYldwUTdnSUFmc0pOSDVLQkxvd0hKDQog
ICAgRkZqVyINCiAgXQ0KfQ
```

then we have to append a period (".") and the base64url encoding of the `EncodedMetadataBLOBPayload` (taken from the example in section Metadata BLOB Format):

```
EXAMPLE: TBSPAYLOAD
ew0KICAiYWxnIjogIkVTMjU2IiwNCiAgInR5cCI6ICJKV1QiLA0KICAiaWF0IjogMTc0MzQ5MDgwNSwN
CiAgIng1YyI6IFsNCiAgICAiTUlJQ1pUQ0NBZ3VnQXdJQkFnSUJBVEFLQmdncWhrak9QUVFEQWpDQm96
RW5NQ1VHQTFVRUF3d2VSVmhCVFZCTQ0KICAgIFJTQk5SRk16SUZSRlUxUWdTVTVVUlZKTlJVUkpRVlJG
TVNJd0lBWUpLb1pJaHZjTkFRa0JGaE5sZUdGdGNHeGwNCiAgICBRR1Y0WVcxd2JHVXVZMjl0TVJRd0Vn
WURWUVFLREF0RmVHRnRjR3hsSUU5U1J6RVFNQTRHQTFVRUN3d0hSWGhoDQogICAgYlhCc1pURUxNQWtH
QTFVRUJoTUNWVk14Q3pBSkJnTlZCQWdNQWsxWk1SSXdFQVlEVlFRSERBbFhZV3RsWm1sbA0KICAgIGJH
UXdIaGNOTWpFd05ERTVNVEV6TlRBM1doY05NekV3TkRFM01URXpOVEEzV2pDQnBURXBNQ2NHQTFVRUF3
d2cNCiAgICBSVmhCVFZCTVJTQk5SRk16SUZOSlIwNUpUa2NnUTBWU1ZFbEdTVU5CVkVVeElqQWdCZ2tx
aGtpRzl3MEJDUUVXDQogICAgRTJWNFlXMXdiR1ZBWlhoaGJYQnNaVUJsZUdGdGNHeGxNUXN3Q1FZRFZRUUdFd0pW
VXpFTE1Ba0dBMVVFQ0F3Q1RWa3hFakFRQmdOVkJBY00NCiAgICBDVmRoYTJWbWFXVnNaREJaTUJNR0J5
cUdTTTQ5QWdFR0NDcUdTTTQ5QXdFSEEwSUFCTlFKczZ3VHFpeGMrUytWDQogICAgREFhakZsUE5hdDEw
S0VXSkU1amNXT3ZtNnFwTzlTREFBTVp2YjRISHJ2cytQNVlScEhyU2xVUGR2Syt1RVFiZA0KICAgIFdn
```

```
MzFQOXVqTERBcU1Ba0dBMVVkRXdRQ01BQXdIUVlEVlIwT0JCWUVGTHFzYXBjWFY0Wm9WSEFuUnBQWndR
ZTcNCiAgICBZeTIwTUFvR0NDcUdTTTQ5QkFNQ0EwZ0FNRVVDSVFDNjd6YThFSXV5UmlLZ05EWElQMXMx
YUxyM2p6SDlXVlhmDQogICAgSHg0YkorekNzZ0lnRy90VkJ1dE9KVVUrdnZvSElvL290QVVBY0g1Yk5I
UDN1SXppRFMrUFRVYz0iLA0KICAgICJNSUlFSHpDQ0FnZWdBd0lCQWdJQkFqQU5CZ2txaGtpRzl3MEJB
UXNGQURDQm16RWZNQjBHQTFVRUF3d1dSVmhCDQogICAgVFZCTVJTQk5SRk16SUZSRlUxUWdVazlQVkRF
aU1DQUdDU3FHU0liM0RRRUpBUllUWlhoaGJYQnNaVUJsZUdGdA0KICAgIGNHeGxMbU52YlRFVU1CSUdB
MVVFQ2d3TFJYaGhiWEJzWlNCUFVrY3hFREFPQmdOVkJBc01CMFY0WVcxd2JHVXgNCiAgICBDekFKQmdO
VkJBWVRBbFZUTVFzd0NRWURWUVFJREFKTldURVNNQkFHQTFVRUJ3d0pWMkZyWldacFpXeGtNQjRYDQog
ICAgRFRJeE1EUXhPVEV4TXpVd04xb1hEVFE0TURrd05ERXhNelV3TjFvd2dhTXhKekFsQmdOVkJBTU1I
a1ZZUVUxUQ0KICAgIFRFVWdUVVJUTXlCVVJWTlVJRWxPVkVWU1RVVkVTVUZVUlRFaU1DQUdDU3FHU0li
M0RRRUpBUllUWlhoaGJYQnMNCiAgICBaVUJsZUdGdGNHeGxMbU52YlRFVU1CSUdBMVVFQ2d3TFJYaGhi
WEJzWlNCUFVrY3hFREFPQmdOVkJBc01CMFY0DQogICAgWVcxd2JHVXhDekFKQmdOVkJBWVRBbFZUTVFz
d0NRWURWUVFJREFKTldURVNNQkFHQTFVRUJ3d0pWMkZyWldacA0KICAgIFpXeGtNRmt3RXdZSEtvWkl6
ajBDQVFZSUtvWkl6ajBEQVFjRFFnQUVOR3VtQmJZbkZRblRqUDFSU2ZjNzBoc2gNCiAgICBnYmlJMVp0
cHdRNW42eFJMQS9XcTBQU0NmTGw1cVErcjdkbGNLMWQzcjN2TGErdm02RzZ2S0hHQ1BFZVV6cU12DQog
ICAgTUMwd0RBWURWUjBUQkFVd0F3RUIvekFkQmdOVkhRNEVGZ1FVTms2RjRSSm5HR1ZGZSswL2NiWndm
clpkN1pVdw0KICAgIERRWUpLb1pJaHZjTkFRRUxCUUFEZ2dJQkFDbnAxZm0wRktsV21VdFRwbEx1WWc3
bXBzNHhQL0NPdThkbmIzOHUNCiAgICAxbk1EVnVPVDQrQ1phaU05QUd6MzEzR0QyMmhqTEdybVB1WW44
NndHT0tJM0hPckVwc0dkTW1meTd0VG1LWC9lDQogICAgTS9lUzNGRURYWm5FODJQbjVvRkl5QlQvZjhz
R3VYeU9zRlpxV0J2VmRCSUlEbGRDcEQ0bXhNUVpaT1p0VHJsdg0KICAgIDNXdkJRTUMvZHNpY094ZTNR
S1h2V0hpNlFiL1JodWFpcDNyUG13TWYrNEpwbkpPK0pNUHFBYVUxY0FIOEhWc2YNCiAgICByTEFNb0tz
MTQ4ajIrY3ZicGFXbXNUNXJJb0gvZXpWclBhRy9NT2lJZ3E3OXcvZWZ1dlNpNUFYOEora0RvTFNFDQog
ICAgZjNkNXdPZ2tKWUFxVXFjUnhYVEVFdEtJekRNNmh6YUJRRmlBV3ZUbjlJbFZXZ250UWFtU1h2SCt0
eGFURjlpRQ0KICAgIGxIeFVmNUlOWUZWY2lDcHp0U3J5ZGVIdi9PQ05SZjcvTFZyaWNNU2xvOFJoK08z
eVA5VisydU5mM1g4c1FKTnQNCiAgICB1ZnJRTmFxcTE4d2lYbGlUTHVmU24wMi9nK21raElVaU5LZlRP
SnB2Q2pLZUNuQ0ZjeFFVMi9YVDNLaDNHOGdEDQogICAgSndzTzZFVlJqTVVKdDRBWUt6ZS9oRVVDd0Y1
NUlGMm0zakhJb0N1OGpWZmoyNENlRVg1ZG5mdlNyK1NWdk41UQ0KICAgIEIwdVowNU00cm15Wlh5cUJt
MHpLM2ZSK2lFMC9acEludXdMQzdYK1c4MnpYbG5Na3BsSTNRK0p4ZDdqZlExNVMNCiAgICBZTkUySzZy
dlJJVDAxdzBQOVpxeURGN2tuR0twUmxwN09xeGQzN2JEL1ZVYldwUTdnSUFmc0pOSDVLQkxvd0hKDQog
ICAgRkZqVyINCiAgXQ0KfQ.eyJsZWdhbEhlYWRlciI6IlJldHJpZXZhbCBhbmQgdXNlIG9mIHRoaXMgQ
kxPQiBpbmRpY2F0ZXMgYWNjZXB0YW5jZSBvZiB0aGUgYXBwcm9wcmlhdGUgYWdyZWVtZW50IGxvY2F0Z
WQgYXQgaHR0cHM6Ly9maWRvYWxsaWFuY2Uub3JnL21ldGFkYXRhL21ldGFkYXRhLWxlZ2FsLXRlcm1zL
yIsIm5vIjoxNSwibmV4dFVwZGF0ZSI6IjIwMjAtMDMtMzAiLCJlbnRyaWVzIjpbeyJhYWlkIjoiMTIzN
CM1Njc4IiwibWV0YWRhdGFTdGF0ZW1lbnQiOnsibGVnYWxIZWFkZXIiOiJodHRwczovL2ZpZG9hbGxpY
W5jZS5vcmcvbWV0YWRhdGEvbWV0YWRhdGEtc3RhdGVtZW50LWxlZ2FsLWhlYWRlci8iLCJkZXNjcmlwd
GlvbiI6IkZJRE8gQWxsaWFuY2UgU2FtcGxlIFVBRiBBdXRoZW50aWNhdG9yIiwiYWFpZCI6IjEyMzQjN
TY3OCIsImFsdGVybmF0aXZlRGVzY3JpcHRpb25zIjp7InJ1LVJVIjoi0J_RgNC40LzQtdGAIFVBRiDQs
NGD0YLQtdC90YLQuNGE0LjQutCw0YLQvtGA0LAg0L7RgiBGSURPIEFsbGlhbmNlIiwiZnItRlIiOiJFe
GVtcGxlIFVBRiBhdXRoZW50aWNhdG9yIGRlIEZJRE8gQWxsaWFuY2UifSwiYXV0aGVudGljYXRvclZlc
nNpb24iOjIsInByb3RvY29sRmFtaWx5IjoidWFmIiwic2NoZW1hIjozLCJ1cHYiOlt7Im1ham9yIjoxL
CJtaW5vciI6MH0seyJtYWpvciI6MSwibWlub3IiOjF9XSwiYXV0aGVudGljYXRpb25BbGdvcml0aG1zI
jpbInNlY3AyNTZyMV9lY2RzYV9zaGEyNTZfcmF3Il0sInB1YmxpY0tleUFsZ0FuZEVuY29kaW5ncyI6W
yJlY2NfeDk2Ml9yYXciXSwiYXR0ZXN0YXRpb25UeXBlcyI6WyJiYXNpY19mdWxsIl0sInVzZXJWZXJpZ
mljYXRpb25EZXRhaWxzIjpbW3sidXNlclZlcmlmaWNhdGlvbk1ldGhvZCI6ImZpbmdlcnByaW50X2lud
GVybmFsIiwiYmFEZXNjIjp7InNlbGZBdHRlc3RlZEZBUiI6MC4wMDAwMiwibWF4UmV0cmllcyI6NSwiY
mxvY2tTbG93ZG93biI6MzAsIm1heFRlbXBsYXRlcyI6NX19sImtleVByb3RlY3Rpb24iOlsiaGFyZ
HdhcmUiLCJ0ZWUiXSwiaXNLZXlSZXN0cmljdGVkIjp0cnVlLCJtYXRjaGVyUHJvdGVjdGlvbiI6WyJ0Z
WUiXSwiY3J5cHRvU3RyZW5ndGgiOjEyOCwiYXR0YWNobWVudEhpbnQiOlsiaW50ZXJuYWwiXSwidGNEa
XNwbGF5IjpbImFueSIsInRlZSJdLCJ0Y0Rpc3BsYXlDb250ZW50VHlwZSI6ImltYWdlL3BuZyIsInRjR
GlzcGxheVBOR0NoYXJhY3RlcmlzdGljcyI6W3sid2lkdGgiOjMyMCwiaGVpZ2h0Ijo0ODAsImJpdERlc
HRoIjoxNiwiY29sb3JUeXBlIjoyLCJjb21wcmVzc2lvbiI6MCwiZmlsdGVyIjowLCJpbnRlcmxhY2UiO
jB9XSwiYXR0ZXN0YXRpb25Sb290Q2VydGlmaWNhdGVzIjpbIk1JSUNQVENDQWVPZ0F3SUJBZ0lKQU91Z
Xh2VTNPeTJ3TUFvR0NDcUdTTTQ5QkFNQ01Ic3hJREFlQmdOVkJBU1GMU5oYlhCc1pTQkJkSFJsYzNSa
GRHbHZiaUJTYjI5ME1SWXdGQVlEVlFRS0RBMUdTVVJQSUVGc2JHbGhibU5sTVJFd0R3WURWUVFMREFoV
lFVWWdWRmRITERFU01CQUdBMVVFQnd3SlVHRnNieUJCYkhSdk1Rc3dDUVlEVlFRSURBSkRRVEVMTUFrR
0ExVUVCaE1DVlZNd0hoY05NVFF3TmpFNE1UTXpNek15V2hjTk5ERXhNVEF6TVRNek16TXlXakI3TVNBd
0hnWURWUVFEREJkVFlXMXdiR1VnUVhSMFpYTjBZWFJwYjI0Z1VtOXZkREVXTUJRR0ExVUVDZ3dOUmtsR
VR5QkJiR3hwWVc1alpURVJNQThHQTFVRUN3d0lWVUZHSUZSWFJ5d3hFakFRQmdOVkJBY01DVkJoYkc4Z
1FXeDBiekVMTUFrR0ExVUVDQXdDUTBFeEN6QUpCZ05WQkFZVEFsVlRNRmt3RXdZSEtvWkl6ajBDQVFZS
UtvWkl6ajBEQVFjRFFnQUVIOGh2MkQwSFhhNTkvQm1wUTdSWmVoTC9GTUd6RmQxUUJnOXZBVXBPWjNha
m51UTk0UFI3YU16SDMzblVTQnI4ZkhZRHJxT0JiNThweEdxSEpSeVgvNk5RTUU0d0hRWURWUjBPQkJZR
UZQb0hBM0NMaHhGYkMwSXQ3ekU0dzhoazVFSi9NQjhHQTFVZEl3UVlNQmFBRlBvSEEzQ0xoeEZiQzBJd
Dd6RTR3OGhrNUVKL01Bd0dBMVVkRXdRRk1BTUJBZjh3Q2dZSUtvWkl6ajBFQXdJRFNBQXdSUUloQUowN
```

```
lFTWHQ5aWhJYkVLWUtJanNQa3JpVmRMSWd0ZnNiRFN1N0VySmZ6cjRBaUJxb1lDWmYwK3pJNTVhUWVBS
GpJekE5WG02M3JydUF4Qlo5cHM5ejJYTmxRPT0iXSwiaWNvbiI6ImRhdGE6aW1hZ2UvcG5nO2Jhc2U2N
CxpVkJPUncwS0dnb0FBQUFOU1VoRVVnQUFBRThBQUFBdkNBWUFBQUNpd0pmY0FBQUFBWE5TUjBJQXJzN
GM2UUFBQUFSblFVMUJBQUN4and2OFlRVUFBQUFKY0VoWmN3QUFEc01BQUE3REFjZHZxR1FBQUFhaFNVU
kJWR2hEN1pyNWJ4UmxHTWY5S3pUQjhBTS9ZRWhFMlc3cFFaY1dLS0JjbFNwSEFUbEVMQVJFN2tORUNDQ
TNGa1dLMENLS1NDRklzS0JjZ1ZDRFdHTkVTZEFZaWR3Z2dnSkJpUmlNaEZjLzR3eTg4ODR6dTlOZGxuR
1RmWkpQMm4zbk8rKzg4OTMzZnZlQkJ4K1BxQ3pKa1RVdkJiTG1wVURXdkJUSW1wY0NTWnZYTENkWDlSM
DVTazE5YmI1YXRmNTk5ZkcrL2VyQTU0MXE0N2FQMUxMVmE5U0l5Vk5VaThJaThkNWtHVHNpMzBORnY3Y
Wk5bjdRWlBNd2JkeXMyZXJVMlhNcVVkeTgrWmNhTm1HaW1FOHlYTjNSVWQzYTE4bkYwZlVsb3ZaKzBDV
HpXcGQyVmorZU9tMWJFeXk2RHg0aTVwVU1HV3ZlbzUwNnEyMjdkdHVXQkl1ZmZyNm9XcFYwRlBOTGhvd
zE3NTFObTIxTHZQSDNyVnRXamZ6NjZMZnFsOHRYN0ZSbDlZRlNYc21Tc2ViOWNlT0diWWs3TU5VY0dQZ
zhac2JNZTlyZlFVYWFWL0pNWDlzcWR6RENTdnAwa1pIbVRaZzl4N2JMSGNNblRoYjE2ZUorbVZmUXE4e
WFVWlFORzY0aVhaKzAva3E2dU9aRk8wUXRhdGRXS2ZYblJROTlCajkxUjVPSUZuazU0ak4wbWtVaXFsT
zNYRFcrTWwrOThtS0I2dFc3cldwWmNQYyswemc0dExyWWxVYzg2RTZlR0RqSU11YlZwY3VzZWFyZmdJW
UdSazZicmhaVnIvSmNIem9vTDc1NTBqZWRMRXhvcFdjQXBpMlpVcWh1N0pMdnJWc1FVODF6a3pPUGVlb
U1SWXZWdVFzWDdQYmlEUVk1SnZab25mdEsrMVZZOEg5dXR4NTMwaDBvYitqbVJZcWo2b3VhWXZFZW5XL
1dsWWpwOGN3Yk1tNjgydFB3cVcxUjR0ai8yU0gxM0lSSllsNG1vWnZYcGlTcURyN2RYdFFIeGEvUEszL
ytCV3NLMWRUZ0h1NlY4dFFKM2J3Rmt3cEZyVU9RNTBzMXIzbGV2bTh6WmNxMTcrQkJhdzdLOGxFSzVxe
mtZZWFyazlBOHA3UDNHekRLK25kM0RRb3crNlVDOFNWTjgyaXV2MzhpbTdOdGFYdFYxQ1ZxNlJndzRwa
3NtYmRpM2J1MkRlN1lmYUJCeGNxZnZxUHJVakZRTlRRMjJsZmRVVlZUNjhyVEpLRjVEblNtVWpnZHFnN
G1TUzlwbXNmREpSM0c2VG9IMGlXOWFWN0xXTEhZWEtsbFREdDBMVEF0a1lJYWFtcDFRalZ2Kyt1eUdVe
FZkSjBETlZYU20rYjFxUnhwbDg0ZGRmWDFMcDFPL2Q2OXRzb2QwdnM1aEdyZTl4dThvK2ZwTFIxY0doT
lRENlo1N0M5S01XWGVmSmRPWjk0YmI5b3FkMVJPblM3cUlUVHpIaW1NcWl2Yk8zZzBEZFZ5azNXUUJoQ
np0SzM1WUtOZE9uYzhPM2FjUzZmRFpGZ0thWExzRUpwNXJkcmxpQnFwODljSmNzL203VHZzMHJrakdmT
jRiMGtQb1puM1VKdUlPcm5aMjJ5UDFmbXZVeCtPNWdTcWViVjFtK3pTdVlOVmhxN1RXYkRpTFZ2bGpwb
Exsb3A2Q0xYUCsycXR2R0xJTC8xdmltSVNkTUJnelNvRlp5dTZUcWQranp4Z3NQYVY5QkNxZWUvTmpZa
zZ2NmxLOWN3aVVjL1NUdGYxSERwTTNiNTkyeTdoM1RoeDVveks2OUhMcFlXdUF3YXFTNWN2MjZxN2NlY
jhlZlZZYVJlUDNpRlU4emoxa25Td1pYSE1tbkNqWTBPZ2FsbzdVUWZTQ00zcVFRcjJIL1hGUDdzc1h4N
DVZbDkxQnllQ2VwNG1vWm9IKzFmRzN4RDR0VDd4OGt3eWo4bndiOWV2MjZWMEI2ZCs3SDR6S3Z1ZEFIN
TM3RmpxeXpPSGRKbkhFdXptWHEvV2p4T2J2Tk1idjduaHl3c1gyYVZzV3RDOCs0OGFMZWFwRTdwNXdLW
mkwQTJBUVJWNW52UjRFK3VKYytiNjFrQXBxSW54QmdtZC80VjVRUC9tdDE4SERDN3NSSGZ0bWV1NWxta
FYwcm4vQUxYMjMyYnFkNEJGbkR4N1ZpMWNXUzJ1ZmYwSWJCNDdxZXh4bVVqOVF1dFlqdXBkM3RZRDZhY
ldCQk1yaCthcE5iT0tyTkYxK3VnQ2E0cmlYR2Z3TVBQdFZpYXZoVTNZTU9BQW51VWIvUjA3TDB5T1NlT
2FkRTg4QXBzWEZHZmYzMHluaGxKZ001MUNVNnZOOUV6Z25wdkhCRlV5aVZyYWVQaXdKNTNERjVaVFpub
21FTmc4NWtOVWQyb0ppMldwcjRPbW1rZk40eDR6SGZpVkZjOER2OE56dWhOcU9pZGlsR3ZBNkRHdWVad
083OEFBUW42Y2lFazYrcnc1VmN2anZxTkRZUE9vSVV3YUtTaHJ4QXVYTGxrSDRhWXVHZk1ZRGMxMFdGN
VRhMzFoUEpPZmNVaHJVL0psSU5pNmM2ZWxSWWRCcG82KytZZmp4NjFsR05mUm00TUQ1ckoxajNGb0dIb
mpEU0JOYXJZVWdNTHlNc3pLcGI3dFhwb0hmUHM4aDNXcDFMek5mTms1NFh4QzF3REdVbVl6WFllZmg2e
i9jS3RWbTRFQnhhOVZRR0R6WXIzTHJVTVJqSEVLa2s3emFGS1lRQTJoR1FVMXorODVORldwWERya3ozd
ngxMEdxeFE2QnplTmJvQms1bjhrNG5lYlJoK2sxaFdmeFRGMEQxRXlXVXM1bnYrZGdRcUtheHp1Q2RFM
GlzSGwwMk5ROGFoMG1YcjEyTGEzbTBmOXdpazkrd0xOVE1ZLzg2TVBvOHlpMzFPZnhtVDZQV29xRzkrR
Fp1a1luYTU2bVNadDVXV1N5NXFWQTFyd1V5SnFYQWxuemtpYWkvZ0hTRDdSa1R5aWhvZ0FBQUFCSlJVN
UVya0pnZ2c9PSJ9LCJzdGF0dXNSZXBvcnRzIjpbeyJzdGF0dXMiOiJGSURPX0NFUlRJRklFRCIsImVmZ
mVjdGl2ZURhdGUiOiIyMDE0LTAxLTA0In1dLCJ0aW1lT2ZMYXN0U3RhdHVzQ2hhbmdlIjoiMjAxNC0wM
S0wNCJ9LHsiYWFndWlkIjoiMDEzMmQxMTAtYmY0ZS00MjA4LWE0MDMtYWI0ZjVmMTJlZmU1IiwibWV0Y
WRhdGFTdGF0ZW1lbnQiOnsibGVnYWxIZWFkZXIiOiJodHRwczovL2ZpZG9hbGxpYW5jZS5vcmcvbWV0Y
WRhdGEvbWV0YWRhdGEtc3RhdGVtZW50LWxlZ2FsLWhlYWRlci8iLCJkZXNjcmlwdGlvbiI6IkZJRE8gQ
WxsaWFuY2UgU2FtcGxlIEZJRE8yIEF1dGhlbnRpY2F0b3IiLCJhYWd1aWQiOiIwMTMyZDExMC1iZjRlL
TQyMDgtYTQwMy1hYjRmNWYxMmVmZTUiLCJhbHRlcm5hdGl2ZURlc2NyaXB0aW9ucyI6eyJydS1SVSI6I
tCf0YDQuNC80LXRgCBGSURPMiDQsNGD0YLQtdC90YLQuNGE0LjQutCw0YLQvtGA0LAg0L7RgiBGSURPI
EFsbGlhbmNlIiwiZnItRlIiOiJFeGVtcGxlIEZJRE8yIGF1dGhlbnRpY2F0b3IgZGUgRklETyBBbGxpY
W5jZSIsInpoLUNOIjoi5L6G6IeqRklETyBBbGxpYW5jZeeahOekuuS-i0ZJRE8y6Lqr5Lu96amX6K2J5
ZmoIn0sInByb3RvY29sRmFtaWx5IjoiZmlkbzIiLCJzY2hlbWEiOjMsImF1dGhlbnRpY2F0b3JWZXJza
W9uIjo1LCJ1cHYiOlt7Im1ham9yIjoxLCJtaW5vciI6MH1dLCJhdXRoZW50aWNhdGlvbkFsZ29yaXRob
XMiOlsic2VjcDI1NnIxX2VjZHNhX3NoYTI1Nl9yYXciLCJyc2Fzc2FfcGtjc3YxNV9zaGEyNTZfcmF3I
l0sInB1YmxpY0tleUFsZ0FuZEVuY29kaW5ncyI6WyJjb3NlIl0sImF0dGVzdGF0aW9uVHlwZXMiOlsiY
mFzaWNfZnVsbCJdLCJ1c2VyVmVyaWZpY2F0aW9uRGV0YWlscyI6W1t7InVzZXJWZXJpZmljYXRpb25NZ
XRob2QiOiJub25lIn1dLFt7InVzZXJWZXJpZmljYXRpb25NZXRob2QiOiJwcmVzZW5jZV9pbnRlcm5hb
CJ9XSxbeyJ1c2VyVmVyaWZpY2F0aW9uTWV0aG9kIjoicGFzc2NvZGVfZXh0ZXJuYWwiLCJjYURlc2MiO
nsiYmFzZSI6MTAsIm1pbkxlbmd0aCI6NH19XSxbeyJ1c2VyVmVyaWZpY2F0aW9uTWV0aG9kIjoicGFzc
2NvZGVfZXh0ZXJuYWwiLCJjYURlc2MiOnsiYmFzZSI6MTAsIm1pbkxlbmd0aCI6NH19LHsidXNlclZlc
mlmaWNhdGlvbk1ldGhvZCI6InByZXNlbmNlX2ludGVybmFsIn1dXSxbeyJ1c2VyVmVyaWZpY2F0aW9uTWV0aG9kIjoicGFzc
XJkd2FyZSIsInNlY3VyZV9lbGVtZW50Il0sIm1hdGNoZXJQcm90ZWN0aW9uIjpbIm9uX2NoaXAiXSwiY
```

3J5cHRvU3RyZW5ndGgiOjEyOCwiYXR0YWNobWVudEhpbnQiOlsiZXh0ZXJuYWwiLCJ3aXJlZCIsIndpc
mVsZXNzIiwibmZjIl0sInRjRGlzcGxheSI6W10sImF0dGVzdGF0aW9uUm9vdENlcnRpZmljYXRlcyI6W
yJNSUlDUFRDQ0FlT2dBd0lCQWdJSkFPdWV4dlUzT3kyd01Bb0dDQ3FHU000OUJBTUNNSHN4SURBZUJnT
lZCQU1NRjFOaGJYQnNaU0JCZEhSbGMzUmhkR2x2YmlCU2IyOTBNUll3RkFZRFZRUUtEQTFHU1VSUElFR
nNiR2xoYm1ObE1SRXdEd1lEVlFRTERBaFZRVVlnVkZkSExERVNNQkFHQTFVRUJ3d0pVR0ZzYnlCQmJIU
nZNUXN3Q1FZRFZRUUlEQUpEUVRFTE1Ba0dBMVVFQmhNQ1ZWTXdIaGNOTVRRd05qRTRNVE16TXpNeVdoY
05OREV4TVRBek1UTXpNek15V2pCN01TQXdIZ1lEVlFRRERCZFRZVzF3YkdVZ1FYUjBaWE4wWVhScGIyN
GdVbTl2ZERFV01CUUdBMVVFQ2d3TlJrbEVUeUJCYkd4cFlXNWpaVEVSTUE4R0ExVUVDd3dJVlVGR0lGU
lhSeXd4RWpBUUJnTlZCQWNNQ1ZCaGJHOGdRV3gwYnpFTE1Ba0dBMVVFQ0F3Q1EwRXhDekFKQmdOVkJBW
VRBbFZUTUZrd0V3WUhLb1pJemowQ0FRWUlLb1pJemowREFRY0RRZ0FFSDhodjJEMEhYYTU5L0JtcFE3U
lplaEwvRk1HekZkMVFCZzl2QVVwT1ozYWpudVE5NFBSN2FNekgzM25VU0JyOGZIWURycU9CYjU4cHHhHc
UhKUnlYLzZOUU1FNHdIUVlEVlIwT0JCWUVGUG9IQTNDTGh4RmJDMEl0N3pFNHc4aGs1RUovTUI4R0ExV
WRJd1FZTUJhQUZQb0hBM0NMaHhGYkMwSXQ3ekU0dzhoazVFSi9NQXdHQTFVZEV3UUZNQU1CQWY4d0NnW
UlLb1pJemowRUF3SURTQUF3UlFJaEFKMDZRU1h0OWloSWJFS1lLSWpzUGtyaVZkTElndGZzYkRTdTdFc
kpmenI0QWlCcW9ZQ1pmMCt6STU1YVFlQUhqSXpBOVhtNjNycnVBeEJaOXBzOXoyWE5sUT09Il0sImljb
24iOiJkYXRhOmltYWdlL3BuZztiYXNlNjQsaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUU4QUFBQXZDQ
VlBQUFDaXdKZmNBQUFBQVhOU1IwSUFyczRjNlFBQUFBUm5RVTFCQUFDeGp3djhZUVVBQUFBSmNFaFpjd
0FBRHNNQUFBN0RBY2R2cUdRQUFBYWhTVVJCVkdoRDdacjVieFJsR01mOUt6VEI4QU0vWUVoRTJXN3BRW
mNXS0tCY2xTcEhBVGxFTEFSRTdrTkVDQ0EzRmtXSzBDS0tTQ0ZJc0tCY2dWQ0RXR05FU2RBWWlkd2dnZ
0pCaVJpTWhGYy80d3k4ODg0enU5TmRsbkdUZlpKUDJuM25PKys4ODkzM2Z2ZUJCeCtQcUN6SmtUVXZCY
kxtcFVEV3ZCVEltcGNDU1p2WExDZFg5UjA1U2sxOWJiNWF0ZjU5OWZHKy9lckE1NDFxNDdhUDFMTFZhO
VNJeVZOVWk4SWk4ZDVrR1RzaTMwTkZ2N2FpOW43UVpQTXdiZHlzMmVyVTJYTXFVZHk4K1pjYU5tR2ltR
Th5WE4zUlVkM2ExOG5GMGZVbG92WiswQ1R6V3BkMlZqK2VPbTFiRXl5NkR4NGk1cFVNR1d2ZW81MDZxM
jI3ZHR1V0JJdWZmcjZvV3BWMEZQTkxob3cxNzUxTm0yMUx2UEgzclZ0V2pmejY2TGZxbDh0WDdGUmw5W
UZTWHNtU3NlYjljZU9HYllrN01OVWNHUGc4WnNiTWU5cmZRVWFhVi9KTVg5c3FkekRDU3ZwMGtaSG1UW
mc5eDdiTEhjTW5UaGIxNmVKK21WZlFxOHlhVVpRTkc2NGlYWiswL2txNnVPWkZPMFF0YXRkV0tmWG5SU
Tk5Qmo5MVI1T0lGbms1NGpOMG1rVWlxbE8zWERXK01sKzk4bUtCNnRXN3JXcFpjUGMrMHpnNHRMcllsV
WM4NkU2ZUdEaklNdWJWcGN1c2VhcmZnSVlHUms2YnJoWlZyL0pjSHpvb0w3NTUwamVkTEV4b3BXY0Fwa
TJaVXFodTdKTHZyVnNRVTgxemt6T1BlZW1NUll2VnVRc1g3UGJpRFFZNUp2Wm9uZnRLKzFWWThIOXV0e
DUzMGgwb2Iram1SWXFqNm91YVl2RWVuVy9XbFlqcDhjd2JNbTY4MnRQd3FXMVI0dGovMlNIMTNJUkpZb
DRtb1p2WHBpU3FEcjdkWHRRSHhhL1BLMy8rQldzSzFkVGdIdTZWOHRRSjNid0Zrd3BGclVPUTUwczFyM
2xldm04elpjcTE3K0JCYXc3SzhsRUs1cXprWWVhcms5QThwN1AzR3pESytuZDNEUW93KzZVQzhTVk44M
ml1djM4aW03TnRhWHRWMUNWcTZSZ3c0cGtzbWJkaTNidTJEZTdZZmFCQnhjcWZ2cVByVWpGUU5UUTIyb
GZkVVZWVDY4clRKS0Y1RG5TbVVqZ2RxZzRtU1M5cG1zZkRKUjNHNlRvSDBpVzlhVjdMV0xIWVhLbGxUR
HQwTFRBdGtZSWFhbXAxUWpWdisrdXlHVXhWZEowRE5WWFNtK2IxcVJ4cGw4NGRkZlgxTHAxTy9kNjl0c
29kMHZzNWhHcmU5eHU4bytmcExSMWNHaE5URDZaNTdDOUtNV1hlZkpkT1o5NGJiOW9xZDFST25TN3FJV
FR6SGltTXFpdmJPM2cwRGRWeWszV1FCaEJ6dEszNVlLTmRPbmM4TzNhY1M2ZkRaRmdLYVhMc0VKcDVyZ
HJsaUJxcDg5Y0pjcy9tN1R2czBya2pHZk40YjBrUG9abjNVSnVJT3JuWjIyeVAxZm12VXgrTzVnU3FlY
lYxbSt6U3VZTlZocTdUV2JEaUxWdmxqcGxMbG9wNkNMWFArMnF0dkdMSUwvMXZpbUlTZE1CZ3pTb0Zae
XU2VHFkK2p6eGdzUGFWOUJDcWVlL05qWWs2djZsSzljd2lVYy9TVHRmMUhEcE0zYjU5Mnk3aDNUaHg1b
3pLNjlITHBZV3VBd2FxUzVjdjI2cTdjZWI4ZWZWWWFSZVAzaUZVOHpqMWtuU3daWEhNbW5DalkwT2dhb
G83VVFmU0NNM3FRUXIySC9YRlA3c3NYeDQ1WWw5MUJ5ZUNlcDRtb1pvSCsxZkczeEQ0dFQ3eDhrd3lqO
G53YjlldjI2VjBCNmQrN0g0ekt2dWRBSDUzN0ZqcXl6T0hkSm5IRXV6bVhxL1dqeE9idk5NYnY3bmh5d
3NYMmFWc1d0QzgrNDhhTGVhcEU3cDV3S1ppMEEyQVFSVjVudlI0RSt1SmMrYjYxa0FwcUlueEJnbWQvN
FY1UVAvbXQxOEhEQzdzUkhmdG1ldTVsbWhWMHJuL0FMWDIzMmJxZDRCRm5EeDdWaTFjV1MydWZmMEliQ
jQ3cWV4eG1VajlRdXRZanVwZDN0WUQ2YWJXQkJNcmgrYXBOYk9Lck5GMSt1Z0NhNHJpWEdmd01QUHRWa
WF2aFUzWU1PQUFudVViL1IwN0wweU9TZU9hZEU4OEFwc1hGR2ZmMzB5bmhsSmdNNTFDVTZ2TjlFemduc
HZIQkZVeWlWcmFlUGl3SjUzREY1WlRabm9tRU5nODVrTlVkMm9KaTJXcHI0T21ta2ZONHg0ekhmaVZGY
zhEdjhOenVoTnFPaWRpbEd2QTZER3VlWndPNzhBQVFuNmNpRWs2K3J3NVZjdmp2cU5EWVBPb0lVd2FLU
2hyeEF1WExxa0g0YVl1R2ZNWURjMTBXRjVUYTMxaFBKT2ZjVWhyVS9KbElOaTZjNmVsUllkQnBvNisrW
WZqeDYxbEdOZlJtNE1ENXJKMWozRm9HSG5qRFNCTmFyWVVnTUx5TXN6S3BiN3RYcG9IZlBzOGgzV3AxT
HpOZk5rNTRYeEMxd0RHVW1ZelhZZWZoNnovY0t0Vm00RUJ4YTlWUUdEellyM0xyVU1SakhFS2trN3phR
ktZUUEyaEdRVTF6Kzg1TkZXcFhEcmt6M3Z4MTBHcXhRNkJ6ZU5ib0JrNW44azRuZWJSaCtrMWhXZnhUR
jBEMUV5V1VzNW52K2RnUXFLYXh6dUNkRTBpc0hsMDJOUThhaDBtWHIxMkxhM20wZjl3aWs5K3dMTlRNW
S84Nk1Qbzh5aTMxT2Z4bVQ2UFdvcUc5K0RadWtZbmE1Nm1TWnQ1V1dTeTVxVkExcndVeUpxWEFsbnpra
WFpL2dIU0Q3UmtUeWlob2dBQUFBQkpSVTVFcmtKZ2dnPT0iLCJzdXBwb3J0ZWRFeHRlbnNpb25zIjpbe
yJpZCI6ImhtYWMtc2VjcmV0IiwiZmFpbF9pZl91bmtub3duIjpmYWxzZX0seyJpZCI6ImNyZWRQcm90Z
WN0IiwiZmFpbF9pZl91bmtub3duIjpmYWxzZX1dLCJhdXRoZW50aWNhdG9yR2V0SW5mbyI6eyJ2ZXJza
W9ucyI6WyJVMkZfVjIiLCJGSURPXzJfMCJdLCJleHRlbnNpb25zIjpbImNyZWRQcm90ZWN0IiwiaG1hY
y1zZWNyZXQiXSwiYWFndWlkIjoiMDEzMmQxMTBiZjRlNDIwOGE0MDNhYjRmNWYxMmVmZTUiLCJvcHRpb
25zIjp7InBsYXQiOiJmYWxzZSIsInJrIjoidHJ1ZSIsImNsaWVudFBpbiI6InRydWUiLCJ1cCI6InRyd
WUiLCJ1diI6InRydWUiLCJ1dlRva2VuIjoiZmFsc2UiLCJjb25maWciOiJmYWxzZSJ9LCJtYXhNc2dTa
XplIjoxMjAwLCJwaW5VdkE1dGhQcm90b2NvbHMiOlsxXSwibWE4Q3JlZGVudGlhbENydW50SW5MaXN0I

```
joxNiwibWF4Q3JlZGVudGlhbElkTGVuZ3RoIjoxMjgsInRyYW5zcG9ydHMiOlsidXNiIiwibmZjIl0sI
mFsZ29yaXRobXMiOlt7InR5cGUiOiJwdWJsaWMta2V5IiwiYWxnIjotN30seyJ0eXBlIjoicHVibGljL
WtleSIsImFsZyI6LTI1N31dLCJtYXhBdXRoZW50aWNhdG9yQ29uZmlnTGVuZ3RoIjoxMDI0LCJkZWZhd
Wx0Q3JlZFByb3RlY3QiOjIsImZpcm13YXJlVmVyc2lvbiI6NX19LCJzdGF0dXNSZXBvcnRzIjpbeyJzd
GF0dXMiOiJGSURPX0NFUlRJRklFRCIsImVmZmVjdGl2ZURhdGUiOiIyMDE5LTAxLTA0In0seyJzdGF0d
XMiOiJGSURPX0NFUlRJRklFRF9MMSIsImVmZmVjdGl2ZURhdGUiOiIyMDIwLTExLTE5IiwiY2VydGlma
WNhdGlvbkRlc2NyaXB0b3IiOiJGSURPIEFsbGlhbmNlIFNhbXBsZSBGSURPMiBBdXRoZW50aWNhdG9yI
iwiY2VydGlmaWNhdGVOdW1iZXIiOiJGSURPMjEwMDAyMDE1MTIyMTAwMSIsImNlcnRpZmljYXRpb25Qb
2xpY3lWZXJzaW9uIjoiMS4wLjEiLCJjZXJ0aWZpY2F0aW9uUmVxdWlyZW1lbnRzVmVyc2lvbiI6IjEuM
C4xIn1dLCJ0aW1lT2ZMYXN0U3RhdHVzQ2hhbmdlIjoiMjAxOS0wMS0wNCJ9XX0
```


and finally we have to append another period (".") followed by the base64url-encoded signature.

ISSUE 1 Update this example

EXAMPLE: JWT


```
eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6WyJNSUlDWlRDQ0FndWdBd0lCQWdJQkFUQUtC
Z2dxaGtqT1BRUURBakNCb3pFbk1DVUdBMVVFQXd3ZVJWaEJUVkJNUlNCTlJGTXpJRlJGVTFRZ1NVNVVS
VkpOUlVSSlFWUkZNU0l3SUFZSktvWklodmNOQVFrQkZoTmxlR0Z0Y0d4bFFHVjRZVzF3YkdVdVkyOXRN
UlF3RWdZRFZRUUtEQXRGZUdGdGNHeGxJRTlTUnpFUU1BNEdBMVVFQ3d3SFJYaGhiWEJzWlRFTE1Ba0dB
MVVFQmhNQ1ZWTXhDekFKQmdOVkJBZ01BazFaTVJJd0VBWURWUVFIREFsWFlXdGxabWxsYkdRd0hoY05N
akV3TkRFNU1URXpOVEEzV2hjTk16RXdOREUzTVRFek5UQTNXakNCcFRFcE1DY0dBMVVFQXd3Z1JWaEJU
VkJNUlNCTlJGTXpJRk5KUjA1SlRrY2dRMFZTVkVsR1NVTkJWRVV4SWpBZ0Jna3Foa2lHOXcwQkNRRVdF
MlY0WVcxd2JHVkFaWGhoYlhCc1pTNWpiMjB4RkRBU0JnTlZCQW9NQzBWNFlXMXdiR1VnVDFKSE1SQXdE
Z1lEVlFRTERBZEZlR0Z0Y0d4bE1Rc3dDUVlEVlFRR0V3SlZVekVMTUFrR0ExVUVDQXdDVFZreEVqQVFC
Z05WQkFjTUNWZGhhMlZtYVdWc1pEQlpNQk1HQnlxR1NNNDlBZ0VHQ0NxR1NNNDlBd0VIQTBJQUJOUUpz
NndUcWl4YytTK1ZEQWFqRmxQTmF0MTBLRVdKRTVqY1dPdm02cXBPOVNEQUFNWnZiNEhIcnZzK1A1WVJw
SHJTbFVQZHZLK3VFUWJkV2czMVA5dWpMREFxTUFrR0ExVWRFd1FDTUFBd0hRWURWUjBPQkJZRUZMcXNh
cGNYVjRab1ZIQW5ScFBad1FlN1l5MjBNQW9HQ0NxR1NNNDlCQU1DQTBnQU1FVUNJUUM2N3phOEVJdXlS
aUtnTkRYSVAxczFhTHIzanpIOVdWWGZIeDRiSit6Q3NnSWdHL3RWQnV0T0pVVSt2dm9ISW8vb3RBVUFj
SDViTkhQM3VJemlEUytQVFVjPSIsIk1JSUVIekNDQWdlZ0F3SUJBZ0lCQWpBTkJna3Foa2lHOXcwQkFR
c0ZBRENCbXpFZk1CMEdBMVVFQXd3V1JWaEJUVkJNUlNCTlJGTXpJRlJGVTFRZ1VrOVBWREVpTUNBR0NT
cUdTSWIzRFFFSkFSWVRaWGhoYlhCc1pVQmxlR0Z0Y0d4bExtTnZiVEVVTUJJR0ExVUVDZ3dMUlhoaGJY
QnNaU0JQVWtjeEVEQU9CZ05WQkFzTUIwVjRZVzF3YkdVeEN6QUpCZ05WQkFZVEFsVlRNUXN3Q1FZRFZR
UUlEQUpOV1RFU01CQUdBMVVFQnd3SlYyRnJaV1pwWld4a01CNFhEVEl4TURReE9URXhNelV3TjFvWERU
UTRNRGt3TkRFeE16VXdOMW93Z2FNeEp6QWxCZ05WQkFNTUhrVllRVTFRVEVVZ1RVUlRNeUJVUlZOVUlF
bE9WRVZTVFVWRVNVRlVSVEVpTUNBR0NTcUdTSWIzRFFFSkFSWVRaWGhoYlhCc1pVQmxlR0Z0Y0d4bExt
TnZiVEVVTUJJR0ExVUVDZ3dMUlhoaGJYQnNaU0JQVWtjeEVEQU9CZ05WQkFzTUIwVjRZVzF3YkdVeEN6
QUpCZ05WQkFZVEFsVlRNUXN3Q1FZRFZRUUlEQUpOV1RFU01CQUdBMVVFQnd3SlYyRnJaV1pwWld4a01G
a3dFd1lIS29aSXpqMENBUVlJS29aSXpqMERBUWNEUWdBRU5HdW1CYlluRlFuVGpQMVJTZmM3MGhzaGdi
aUkxWnRwd1E1bjZ4UkxBL1dxMFBTQ2ZMbDVxUStyN2RsY0sxZDNyM3ZMYSt2bTZHNnZLSEdDUEVlVXpx
TXZNQzB3REFZRFZSMFRCQVV3QXdFQi96QWRCZ05WSFE0RUZnUVVOazZGNFJKbkdHVkZlKzAvY2Jad2Zy
WmQ3WlV3RFFZSktvWklodmNOQVFFTEJRQURnZ0lCQUNucDFmbTBGS2xXbVV0VHBsTHVZZzdtcHM0eFAv
Q091OGRuYjM4dTFuTURWdU9UNCtDWmFpTTlBR3ozMTNHRDIyaGpMR3JtUHVZbjg2d0dPS0kzSE9yRXBz
R2RNbWZ5N3RUbUtYL2VNL2VTM0ZFRFhabkU4MlBuNW9GSXlCVC9mOHNHdVh5T3NGWnFXQnZWZEJJSURs
ZENwRDRteE1RWlpPWnRUcmx2M1d2QlFNQy9kc2ljT3hlM1FLWHZXSGk2UWIvUmh1YWlwM3JQbXdNZis0
SnBuSk8rSk1QcUFhVTFjQUg4SFZzZnJMQU1vS3MxNDhqMitjdmJwYVdtc1Q1cklvSC9lelZyUGFHL01P
aUlncTc5dy9lZnV2U2k1QVg4SitrRG9MU0VmM2Q1d09na0pZQXFVcWNSeFhURUV0S0l6RE02aHphQlFG
aUFXdlRuOUlsVldnbnRRYW1TWHZIK3R4YVRGOWlFbEh4VWY1SU5ZRlZjaUNwenRTcnlkZUh2L09DTlJm
Ny9MVnJpY01TbG84UmgrTzN5UDlWKzJ1TmYzWDhzUUpOdHVmclFOYXFxMTh3aVhsaVRMdWZTbjAyL2cr
bWtoSVVpTktmVE9KcHZDaktlQ25DRmN4UVUyL1hUM0toM0c4Z0RKd3NPNkVWUmpNVUp0NEFZS3plL2hF
VUN3RjU1SUYybTNqSElvQ3U4alZmajI0Q2VFWDVkbmZ2U3IrU1Z2TjVRQjB1WjA1TTRybXlaWHlxQm0w
ekszZlIraUUwL1pwSW51d0xDN1grVzgyelhsbk1rcGxJM1ErSnhkN2pmUTE1U1lORTJLNnJ2UklUMDF3
MFA5WnF5REY3a25HS3BSbHA3T3F4ZDM3YkQvVlViV3BRN2dJQWZzSk5INUtCTG93SEpGRmpXIl19.eyJ
sZWdhbEhlYWRlciI6IlJldHJpZXZhbCBhbmQgdXNlIG9mIHRoaXMgQkxPQiBpbmRpY2F0ZXMgYWNjZXB
0YW5jZSBvZiB0aGUgYXBwcm9wcmlhdGUgYWdyZWVtZW50IGxvY2F0ZWQgYXQgaHR0cHM6Ly9maWRvYWx
saWFuY2Uub3JnL21ldGFkYXRhL21ldGFkYXRhLWxlZ2FsLXRlcm1zLyIsIm5vIjoxNSwibmV4dFVwZGF
0ZSI6IjIwMjAtMDMtMzAiLCJlbnRyaWVzIjpbeyJhYWlkIjoiMTIzNCM1Njc4IiwibWV0YWRhdGFTdGF
0ZW1lbnQiOnsibGVnYWxIZWFkZXIiOiJodHRwczovL2ZpZG9hbGxpYW5jZS5vcmcvbWV0YWRhdGEvbWV
0YWRhdGEtc3RhdGVtZW50LWxlZ2FsLWhlYWRlci8iLCJkZXNjcmlwdGlvbiI6IkZJRE8gQWxsaWFuY2U
gU2FtcGxlIFVBRiBBdXRoZW50aWNhdG9yIiwiYWFpZCI6IjEyMzQjNTY3OCIsImFsdGVybmF0aXZlRGV
```

```
2T35pCHRpb25zIjp7InJlZVJvIjo0J_KgNC40L2QtdGA1FVBRiBQsNGD0LQtdC90LQuNGE0LjQutC
w0YLQvtGA0LAg0L7RgiBGSURPIEFsbGlhbmNlIiwiZnItRlIiOiJFeGVtcGxlIFVBRiBhdXRoZW50aWN
hdG9yIGRlIEZJRE8gQWxsaWFuY2UifSwiYXV0aGVudGljYXRvclZlcnNpb24iOjIsInByb3RvY29sRmF
taWx5IjoidWFmIiwic2NoZW1hIjozLCJ1cHYiOlt7Im1ham9yIjoxLCJtaW5vciI6MH0seyJtYWpvciI
6MSwibWlub3IiOjF9XSwiYXV0aGVudGljYXRpb25BbGdvcml0aG1zIjpbInNlY3AyNTZyMV9lY2RzYV9
zaGEyNTZfcmF3Il0sInB1YmxpY0tleUFsZ0FuZEVuY29kaW5ncyI6WyJlY2NfeDk2Ml9yYXciXSwiYXR
0ZXN0YXRpb25UeXBlcyI6WyJiYXNpY19mdWxsIl0sInVzZXJWZXJpZmljYXRpb25EZXRhaWxzIjpbW3s
idXNlclZlcmlmaWNhdGlvbk1ldGhvZCI6ImZpbmdlcnByaW50X2ludGVybmFsIiwiYmFEZXNjIjp7InN
lbGZBdHRlc3RlZEZBUiI6MC4wMDAwMiwibWF4UmV0cmllcyI6NSwiYmxvY2tTbG93ZG93biI6MzAsIm1
heFRlbXBsYXRlcyI6NX19XV0sImtleVByb3RlY3Rpb24iOlsiaGFyZHdhcmUiLCJ0ZWUiXSwiaXNLZXl
SZXN0cmljdGVkIjp0cnVlLCJtYXRjaGVyUHJvdGVjdGlvbiI6WyJ0ZWUiXSwiY3J5cHRvU3RyZW5ndGg
iOjEyOCwiYXR0YWNobWVudEhpbnQiOlsiaW50ZXJuYWwiXSwidGNEaXNwbGF5IjpbImFueSIsInRlZSJ
dLCJ0Y0Rpc3BsYXlDb250ZW50VHlwZSI6ImltYWdlL3BuZyIsInRjRGlzcGxheUhlaWdodCI6MTAyNCw
zdGljcyI6W3sid2lkdGgiOjMyMCwiaGVpZ2h0Ijo0ODAsImJpdERlcHRoIjoxNiwiY29sb3JUeXBlIjo
yLCJjb21wcmVzc2lvbiI6MCwiZmlsdGVyIjowLCJpbnRlcmxhY2UiOjB9XSwiYXR0ZXN0YXRpb25Sb29
0Q2VydGlmaWNhdGVzIjpbIk1JSUNQVENDQWVPZ0F3SUJBZ0lKQU91ZXh2VTNPeTJ3TUFvR0NDcUdTTTQ
5QkFNQ01Ic3hJREFlQmdOVkJBTU1GMU5oYlhCc1pTQkJkSFJsYzNSaGRHbHZiaUJTYjI5ME1SWXdGQVl
EVlFRS0RBMUdTVVJQSUVGc2JHbGhibU5sTVJFd0R3WURWUVFMREFoVlFVWWdWRmRITERFU01CQUdBMVV
FQnd3SlVHRnNieUJCYkhSdk1Rc3dDUVlEVlFRSURBSkRRVEVMTUFrR0ExVUVCaE1DVlZNd0hoY05NVFF
3TmpFNE1UTXpNek15V2hjTk5ERXhNVEF6TVRNek16TXlXakI3TVNBd0hnWURWUVFEREJkVFlXMXdiR1V
nUVhSMFpYTjBZWFJwYjI0Z1VtOXZkREVXTUJRR0ExVUVDZ3dOUmtsRVR5QkJiR3hwWVc1alpURVJNQTh
HQTFVRUN3d0lWVUZHSUZSWFJ5d3hFakFRQmdOVkJBY01DVkJoYkc4Z1FXeDBiekVMTUFrR0ExVUVDQXd
DUTBFeEN6QUpCZ05WQkFZVEFsVlRNRmt3RXdZSEtvWkl6ajBDQVFZSUtvWkl6ajBEQVFjRFFnQUVIOGh
2MkQwSFhhNTkvQm1wUTdSWmVoTC9GTUd6RmQxUUJnOXZBVXBPWjNham51UTk0UFI3YU16SDMzblVTQnI
4ZkhZRHJxT0JiNThweEdxSEpSeVgvNk5RTUU0d0hRWURWUjBPQkJZRUZQb0hBM0NMaHhGYkMwSXQ3ekU
0dzhoazVFSi9NQjhHQTFVZEl3UVlNQmFBRlBvSEEzQ0xoeEZiQzBJdDd6RTR3OGhrNUVKL01Bd0dBMVV
kRXdRRk1BTUJBZjh3Q2dZSUtvWkl6ajBFQXdJRFNBQXdSUUloQUowNlFTWHQ5aWhJYkVLWUtJanNQa3J
pVmRMSWd0ZnNiRFN1N0VySmZ6cjRBaUJxb1lDWmYwK3pJNTVhUWVBSGpJekE5WG02M3JydUF4Qlo5cHM
5ejJYTmxRPT0iXSwiaWNvbiI6ImRhdGE6aW1hZ2UvcG5nO2Jhc2U2NCxpVkJPUncwS0dnb0FBQUFOU1V
oRVVnQUFBRThBQUFBdkNBWUFBQUNpd0pmY0FBQUFBWE5TUjBJQXJzNGM2UUFBQUFSblFVMUJBQUN4and
2OFlRVUFBQUFKY0VoWmN3QUFEc01BQUE3REFjZHZxR1FBQUFhaFNVUkJWR2hEN1pyNWJ4UmxHTWY5S3p
UQjhBTS9ZRWhFMlc3cFFaY1dLS0JjbFNwSEFUbEVMQVJFN2tORUNDQTNGa1dLMENLS1NDRklzS0JjZ1Z
DRFdHTkVTZEFZaWR3Z2dnSkJpUmlNaEZjLzR3eTg4ODR6dTlOZGxuR1RmWkpQMm4zbk8rKzg4OTMzZnZ
lQkJ4K1BxQ3pKa1RVdkJiTG1wVURXdkJUSW1wY0NTWnZYTENkWDlSMDVTazE5YmI1YXRmNTk5ZkcrL2V
yQTU0MXE0N2FQMUxMVmE5U0l5Vk5VaThJaThkNWtHVHNpMzBORnY3YWk5bjdRWlBNd2JkeXMyZXJVMlh
NcVVkeTgrWmNhTm1HaW1FOHlYTjNSVWQzYTE4bkYwZlVsb3ZaKzBDVHpXcGQyVmorZU9tMWJFeXk2RHg
0aTVwVU1HV3ZlbzUwNnEyMjdkdHVXQkl1ZmZyNm9XcFYwRlBOTGhvdzE3NTFObTIxTHZQSDNyVnRXamZ
6NjZMZnFsOHRYN0ZSbDlZRlNYc21Tc2ViOWNlT0diWWs3TU5VY0dQZzhac2JNZTlyZlFVYWFWL0pNWDl
zcWR6RENTdnAwa1pIbVRaZzl4N2JMSGNNblRoYjE2ZUorbVZmUXE4eWFVWlFORzY0aVhaKzAva3E2dU9
aRk8wUXRhdGRXS2ZYblJROTlCajkxUjVPSUZuazU0ak4wbWtVaXFsTzNYRFcrTWwrOThtS0I2dFc3cld
wWmNQYyswemc0dExyWWxVYzg2RTZlR0RqSU11YlZwY3VzZWFyZmdJWUdSazZicmhaVnIvSmNIem9vTDc
1NTBqZWRMRXhvcFdjQXBpMlpVcWh1N0pMdnJWc1FVODF6a3pPUGVlbU1SWXZWdVFzWDdQYmlEUVk1SnZ
ab25mdEsrMVZZOEg5dXR4NTMwaDBvYitqbVJZcWo2b3VhWXZFZW5XL1dsWWpwOGN3Yk1tNjgydFB3cVc
xUjR0ai8yU0gxM0lSSllsNG1vWnZYcGlTcURyN2RYdFFIeGEvUEszLytCV3NLMWRUZ0h1NlY4dFFKM2J
3Rmt3cEZyVU9RNTBzMXIzbGV2bTh6WmNxMTcrQkJhdzdLOGxFSzVxemtZZWFyazlBOHA3UDNHekRLK25
kM0RRb3crNlVDOFNWTjgyaXV2MzhpbTdOdGFYdFYxQ1ZxNlJndzRwa3NtYmRpM2J1MkRlN1lmYUJCeGN
xZnZxUHJVakZRTlRRMjJsZmRVVlZUNjhyVEpLRjVEblNtVWpnZHFnNG1TUzlwbXNmREpSM0c2VG9IMGl
XOWFWN0xXTEhZWEtsbFREdDBMVEF0a1lJYWFtcDFRalZ2Kyt1eUdVeFZkSjBETlZYU20rYjFxUnhwbDg
0ZGRmWDFMcDFPL2Q2OXRzb2QwdnM1aEdyZTl4dThvK2ZwTFIxY0doTlRENlo1N0M5S01XWGVmSmRPWjk
0YmI5b3FkMVJPblM3cUlUVHpIaW1NcWl2Yk8zZzBEZFZ5azNXUUJoQnp0SzM1WUtOZE9uYzhPM2FjUzZ
mRFpGZ0thWExzRUpwNXJkcmxpQnFwODljSmNzL203VHZzMHJrakdmTjRiMGtQb1puM1VKdUlPcm5aMjJ
5UDFmbXZVeCtPNWdTcWViVjFtK3pTdVlOVmhxN1RXYkRpTFZ2bGpwbExsb3A2Q0xYUCsycXR2R0xJTC8
xdmltSVNkTUJnelNvRlp5dTZUcWQranp4Z3NQYVY5QkNxZWUvTmpZazZ2NmxLOWN3aVVjL1NUdGYxSER
wTTNiNTkyeTdoM1RoeDVveks2OUhMcFlXdUF3YXFTNWN2MjZxN2NlYjhlZlZZYVJlUDNpRlU4emoxa25
Td1pYSE1tbkNqWTBPZ2FsbzdVUWZTQ00zcVFRcjJIL1hGUDdzc1h4NDVZbDkxQnllQ2VwNG1vWm9IKzF
mRzN4RDR0VDd4OGt3eWo4bndiOWV2MjZWMEI2ZCs3SDR6S3Z1ZEFINTM3RmpxeXpPSGRKbkhFdXptWHE
vV2p4T2J2Tk1idjduaHl3c1gyYVZzV3RDOCs0OGFMZWFwRTdwNXdLWmkwQTJBUVJWNW52UjRFK3VKYyt
iNjFrQXBxSW54QmdtZC80VjVRUC9tdDE4SERDN3NSSGZ0bWV1NWxtaFYwcm4vQUxYMjMyYnFkNEJGbkR
4N1ZpMWNXUzJ1ZmYwSWJCNDdxZXh4bVVqOVF1dFlqdXBkM3RZRDZhYldCQk1yaCthcE5iT0tyTkYxK3V
nQ2E0cmlYR2Z3TVBQdFZpYXZoVTNZTU9BQW51VWIvUjA3TDB5T1NlT2FkRTg4QXBzWEZHZmYzMHluaGx
KZ001MUNVNnZOOUV6Z25wdkhCRlV5aVZyYWVQaXdKNTNERjVaVFpub21FTmc4NWtOVWQyb0ppMldwcjR
PbW1rZk40eDR6SGZpVkZjOER2OE56dWhOcU9pZGlsR3ZBNkRHdWVad083OEFBUW42Y2lFazYrcnc1VmN
2anZxTkRZUE9vSVV3YUtTaHJ4QXVYTGxrSDRhWXVHZk1ZRGMxMFdGNVRhMzFoUEpPZmNVaHJVL0psSU5
```

```
pNmM2ZWx5WWRCcG82KytZZmp4NjFsR05mUm00TUQ1cKoxajNGb0d1bmpEU0JUYXJ2VWdNTHlNc3pLcGI
3dFhwb0hmUHM4aDNXcDFMek5mTms1NFh4QzF3REdVbVl6WFllZmg2ei9jS3RWbTRFQnhhOVZRR0R6WXI
zTHJVTVJqSEVLa2s3emFGS1lRQTJoR1FVMXorODVORldwWERya3ozdngxMEdxeFE2QnplTmJvQms1bjh
rNG5lYlJoK2sxaFdmeFRGMEQxRXlXVXM1bnYrZGdRcUtheHp1Q2RFMGlzSGwwMk5ROGFoMG1YcjEyTGE
zbTBmOXdpazkrd0xOVE1ZLzg2TVBvOHlpMzFPZnhtVDZQV29xRzkrRFp1a1luYTU2bVNadDVXV1N5NXF
WQTFyd1V5SnFYQWxuemtpYWkvZ0hTRDdSa1R5aWhvZ0FBQUFCSlJVNUVya0pnZ2c9PSJ9LCJzdGF0dXN
SZXBvcnRzIjpbeyJzdGF0dXMiOiJGSURPX0NFUlRJRklFRCIsImVmZmVjdGl2ZURhdGUiOiIyMDE0LTA
xLTA0In1dLCJ0aW1lT2ZMYXN0U3RhdHVzQ2hhbmdlIjoiMjAxNC0wMS0wNCJ9LHsiYWFndWlkIjoiMDE
zMmQxMTAtYmY0ZS00MjA4LWE0MDMtYWI0ZjVmMTJlZmU1IiwibWV0YWRhdGFTdGF0ZW1lbnQiOnsibGV
nYWxIZWFkZXIiOiJodHRwczovL2ZpZG9hbGxpYW5jZS5vcmcvbWV0YWRhdGEvbWV0YWRhdGEtc3RhdGV
tZW50LWxlZ2FsLWhlYWRlci8iLCJkZXNjcmlwdGlvbiI6IkZJRE8gQWxsaWFuY2UgU2FtcGxlIEZJRE8
yIEF1dGhlbnRpY2F0b3IiLCJhYWd1aWQiOiIwMTMyZDExMC1iZjRlLTQyMDgtYTQwMy1hYjRmNWYxMmV
mZTUiLCJhbHRlcm5hdGl2ZURlc2NyaXB0aW9ucyI6eyJydS1SVSI6ItCf0YDQuNC80LXRgCBGSURPMiD
QsNGD0YLQtdC90YLQuNGE0LjQutCw0YLQvtGA0LAg0L7RgiBGSURPIEFsbGlhbmNlIiwiZnItRlIiOiJ
FeGVtcGxlIEZJRE8yIGF1dGhlbnRpY2F0b3IgZGUgRklETyBBbGxpYW5jZSIsInpoLUNOIjoi5L6G6Ie
qRklETyBBbGxpYW5jZeeahOekuuS-i0ZJRE8y6Lqr5Lu96amX6K2J5ZmoIn0sInByb3RvY29sRmFtaWx
5IjoiZmlkbzIiLCJzY2hlbWEiOjMsImF1dGhlbnRpY2F0b3JWZXJzaW9uIjo1LCJ1cHYiOlt7Im1ham9
yIjoxLCJtaW5vciI6MH1dLCJhdXRoZW50aWNhdGlvbkFsZ29yaXRobXMiOlsic2VjcDI1NnIxX2VjZHN
hX3NoYTI1Nl9yYXciLCJyc2Fzc2FfcGtjc3YxNV9zaGEyNTZfcmF3Il0sInB1YmxpY1tleUFsZ0FuZEV
uY29kaW5ncyI6WyJjb3NlIl0sImF0dGVzdGF0aW9uVHlwZXMiOlsiYmFzaWNfZnVsbCJdLCJ1c2VyVmV
yaWZpY2F0aW9uRGV0YWlscyI6W1t7InVzZXJWZXJpZmljYXRpb25NZXRob2QiOiJub25lIn1dLFt7InV
zZXJWZXJpZmljYXRpb25NZXRob2QiOiJwcmVzZW5jZV9pbnRlcm5hbCJ9XSxbeyJ1c2VyVmVyaWZpY2F
0aW9uTWV0aG9kIjoicGFzc2NvZGVfZXh0ZXJuYWwiLCJjYURlc2MiOnsiYmFzZSI6MTAsIm1pbkxlbmd
0aCI6NH19XSxbeyJ1c2VyVmVyaWZpY2F0aW9uTWV0aG9kIjoicGFzc2NvZGVfZXh0ZXJuYWwiLCJjYUR
lc2MiOnsiYmFzZSI6MTAsIm1pbkxlbmd0aCI6NH19LHsidXNlclZlcmlmaWNhdGlvbk1ldGhvZCI6InB
yZXNlbmNlX2ludGVybmFsIn1dXSwia2V5UHJvdGVjdGlvbiI6WyJoYXJkd2FyZSIsInNlY3VyZV9lbGV
tZW50Il0sIm1hdGNoZXJQcm90ZWN0aW9uIjpbIm9uX2NoaXAiXSwiY3J5cHRvU3RyZW5ndGgiOjEyOCw
iYXR0YWNobWVudEhpbnQiOlsiZXh0ZXJuYWwiLCJ3aXJlZCIsIndpcmVsZXNzIiwibmZjIl0sInRjRGl
zcGxheSI6W10sImF0dGVzdGF0aW9uUm9vdENlcnRpZmljYXRlcyI6WyJNSUlDUFRDQ0FlT2dBd0lCQWd
JSkFPdWV4dlUzT3kyd01Bb0dDQ3FHU000OUJBTUNNSHN4SURBZUJnTlZCQU1NRjFOaGJYQnNaU0JCZEh
SbGMzUmhkR2x2YmlCU2IyOTBNUll3RkFZRFZRUUtEQTFHU1VSUElFRnNiR2xoYm1ObE1SRXdEd1lEVlF
RTERBaFZRVVlnVkZkSExERVNNQkFHQTFVRUJ3d0pVR0ZzYnlCQmJIUnZNUXN3Q1FZRFZRUUlEQUpEUVR
FTE1Ba0dBMVVFQmhNQ1ZWTXdIaGNOTVRRd05qRTRNVE16TXpNeVdoY05OREV4TVRBek1UTXpNek15V2p
CN01TQXdIZ1lEVlFRRERCZFRZVzF3YkdVZ1FYUjBaWE4wWVhScGIyNGdVbTl2ZERFV01CUUdBMVVFQ2d
3TlJrbEVUeUJCYkd4cFlXNWpaVEVSTUE4R0ExVUVDd3dJVlVGR0lGUlhSeXd4RWpBUUJnTlZCQWNNQ1Z
CaGJHOGdRV3gwYnpFTE1Ba0dBMVVFQ0F3Q1EwRXhDekFKQmdOVkJBWVRBbFZUTUZrd0V3WUhLb1pJemo
wQ0FRWUlLb1pJemowREFRY0RRZ0FFSDhodjJEMEhYYTU5L0JtcFE3UlplaEwvRk1HekZkMVFCZzl2QVV
wT1ozYWpudVE5NFBSN2FNekgzM25VU0JyOGZIWURycU9CYjU4cHhHcUhKUnlYLzZOUU1FNHdIUVlEVlI
wT0JCWUVGUG9IQTNDTGh4RmJDMEl0N3pFNHc4aGs1RUovTUI4R0ExVWRJd1FZTUJhQUZQb0hBM0NMaHh
GYkMwSXQ3ekU0dzhoazVFSi9NQXdHQTFVZEV3UUZNQU1CQWY4d0NnWUlLb1pJemowRUF3SURTQUF3UlF
JaEFKMDZRU1h0OWloSWJFS1lLSWpzUGtyaVZkTElndGZzYkRTdTdFckpmenI0QWlCcW9ZQ1pmMCt6STU
1YVFlQUhqSXpBOVhtNjNycnVBeEJaOXBzOXoyWE5sUT09Il0sImljb24iOiJkYXRhOmltYWdlL3BuZzt
iYXNlNjQsaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUU4QUFBQXZDQVlBQUFDaXdKZmNBQUFBQVhOU1I
wSUFyczRjNlFBQUFBUm5RVTFCQUFDeGp3djhZUVVBQUFBSmNFaFpjd0FBRHNNQUFBN0RBY2R2cUdRQUF
BYWhTVVJCVkdoRDdacjVieFJsR01mOUt6VEI4QU0vWUVoRTJXN3BRWmNXS0tCY2xTcEhBVGxFTEFSRTd
rTkVDQ0EzRmtXSzBDS0tTQ0ZJc0tCY2dWQ0RXR05FU2RBWWlkd2dnZ0pCaVJpTWhGYy80d3k4ODg0enU
5TmRsbkdUZlpKUDJuM25PKys4ODkzM2Z2ZUJCeCtQcUN6SmtUVXZCYkxtcFVEV3ZCVEltcGNDU1p2WEx
DZFg5UjA1U2sxOWJiNWF0ZjU5OWZHKy9lckE1NDFxNDdhUDFMTFZhOVNJeVZOVWk4Swk4ZDVrR1RzaTM
wTkZ2N2FpOW43UVpQTXdiZHlzMmVyVTJYTXFVZHk4K1pjYU5tR2ltRTh5WE4zUlVkM2ExOG5GMGZVbG9
2WiswQ1R6V3BkMlZqK2VPbTFiRXl5NkR4NGk1cFVNR1d2ZW81MDZxMjI3ZHR1V0JJdWZmcjZvV3BWMEZ
QTkxob3cxNzUxTm0yMUx2UEgzclZ0V2pmejY2TGZxbDh0WDdGUmw5WUZTWHNtU3NlYjljZU9HYllrN01
OVWNHUGc4WnNiTWU5cmZRVWFhVi9KTVg5c3FkekRDU3ZwMGtaSG1UWmc5eDdiTEhjTW5UaGIxNmVKK21
WZlFxOHlhVVpRTkc2NGlYWiswL2txNnVPWkZPMFF0YXRkV0tmWG5SUTk5Qmo5MVI1T0lGbms1NGpOMG1
rVWlxbE8zWERXK01sKzk4bUtCNnRXN3JXcFpjUGMrMHpnNHRMcllsVWM4NkU2ZUdEaklNdWJWcGN1c2V
hcmZnSVlHUms2YnJoWlZyL0pjSHpvb0w3NTUwamVkTEV4b3BXY0FwaTJaVXFodTdKTHZyVnNRVTgxemt
6T1BlZW1NUll2VnVRc1g3UGJpRFFZNUp2Wm9uZnRLKzFWWThIOXV0eDUzMGgwb2Iram1SWXFqNm91YVl
2RWVuVy9XbFlqcDhjd2JNbTY4MnRQd3FXMVI0dGovMlNIMTNJUkpZbDRtb1p2WHBpU3FEcjdkWHRRSHh
hL1BLMy8rQldzSzFkVGdIdTZWOHRRSjNid0Zrd3BGclVPUTUwczFyM2xldm04elpjcTE3K0JCYXc3Szh
sRUs1cXprWWVhcms5QThwN1AzR3pESytuZDNEUW93KzZVQzhTVk44Mml1djM4aW03TnRhWHRWMUNWcTZ
SZ3c0cGtzbWJkaTNidTJEZTdZZmFCQnhjcWZ2cVByVWpGUU5UUTIybGZkVVZWVDY4clRKS0Y1RG5TbVV
qZ2RxZzRtU1M5cG1zZkRKUjNHNlRvSDBpVzlhVjdMV0xIWVhLbGxURHQwTFRBdGtZSWFhbXAxUWpWdis
rdXlHVXhWZEowRE5WWFNtK2IxcVJ4cGw4NGRkZlgxTHAxTy9kNjl0c29kMHZzNWhHcmU5eHU4bytmcEx
SMWNHaE5URDZaNTdDOUtNV1hlZkpkT1o5NGJiOW9xZDFST25TN3FJVFR6SGltTXFpdmJPM2cwRGRWeWs
```

```
zV1FCaEJ6dEszNVlLTmRPbmM4TzNhY1M2ZkRaRmdLYVhMc0VKcDVyZHJsaUJxcDg5Y0pjcy9tN1R2czB
ya2pHZk40YjBrUG9abjNVSnVJT3JuWjIyeVAxZm12VXgrTzVnU3FlYlYxbSt6U3VZTlZocTdUV2JEaUx
WdmxqcGxMbG9wNkNMWFArMnF0dkdMSUwvMXZpbUlTZE1CZ3pTb0ZaeXU2VHFkK2p6eGdzUGFWOUJDcWV
lL05qWWs2djZsSzljd2lVYy9TVHRmMUhEcE0zYjU5Mnk3aDNUaHg1b3pLNjlITHBZV3VBd2FxUzVjdjI
2cTdjZWI4ZWZWWWFSZVAzaUZVOHpqMWtuU3daWEhNbW5DalkwT2dhbG83VVFmU0NNM3FRUXIySC9YRlA
3c3NYeDQ1WWw5MUJ5ZUNlcDRtb1pvSCsxZkczeEQ0dFQ3eDhrd3lqOG53YjlldjI2VjBCNmQrN0g0ekt
2dWRBSDUzN0ZqcXl6T0hkSm5IRXV6bVhxL1dqeE9idk5NYnY3bmh5d3NYMmFWc1d0QzgrNDhhTGVhcEU
3cDV3S1ppMEEyQVFSVjVudlI0RSt1SmMrYjYxa0FwcUlueEJnbWQvNFY1UVAvbXQxOEhEQzdzUkhmdG1
ldTVsbWhWMHJuL0FMWDIzMmJxZDRCRm5EeDdWaTFjV1MydWZmMEliQjQ3cWV4eG1VajlRdXRZanVwZDN
0WUQ2YWJXQkJNcmgrYXBOYk9Lck5GMSt1Z0NhNHJpWEdmd01QUHRWaWF2aFUzWU1PQUFudVViL1IwN0w
weU9TZU9hZEU4OEFwc1hGR2ZmMzB5bmhsSmdNNTFDVTZ2TjlFemducHZIQkZVeWlWcmFlUGl3SjUzREY
1WlRabm9tRU5nODVrTlVkMm9KaTJXcHI0T21ta2ZONHg0ekhmaVZGYzhEdjhOenVoTnFPaWRpbEd2QTZ
ER3VlWndPNzhBQVFuNmNpRWs2K3J3NVZjdmp2cU5EWVBPb0lVd2FLU2hyeEF1WExsa0g0YVl1R2ZNWUR
jMTBXRjVUYTMxaFBKT2ZjVWhyVS9KbElOaTZjNmVsUllkQnBvNisrWWZqeDYxbEdOZlJtNE1ENXJKMWo
zRm9HSG5qRFNCTmFyWVVnTUx5TXN6S3BiN3RYcG9IZlBzOGgzV3AxTHpOZk5rNTRYeEMxd0RHVW1Zelh
ZZWZoNnovY0t0Vm00RUJ4YTlWUUdEellyM0xyVU1SakhFS2trN3phRktZUUEyaEdRVTF6Kzg1TkZXcFh
Ecmt6M3Z4MTBHcXhRNkJ6ZU5ib0JrNW44azRuZWJSaCtrMWhXZnhURjBEMUV5V1VzNW52K2RnUXFLYXh
6dUNkRTBpc0hsMDJOUThhaDBtWHIxMkxhM20wZjl3aWs5K3dMTlRNWS84Nk1Qbzh5aTMxT2Z4bVQ2UFd
vcUc5K0RadWtZbmE1Nm1TWnQ1V1dTeTVxVkExcndVeUpxWEFsbnpraWFpL2dIU0Q3UmtUeWlob2dBQUF
BQkpSVTVFcmtKZ2dnPT0iLCJzdXBwb3J0ZWRFeHRlbnNpb25zIjpbeyJpZCI6ImhtYWMtc2VjcmV0Iiw
iZmFpbF9pZl91bmtub3duIjpmYWxzZX0seyJpZCI6ImNyZWRQcm90ZWN0IiwiZmFpbF9pZl91bmtub3d
uIjpmYWxzZX1dLCJhdXRoZW50aWNhdG9yR2V0SW5mbyI6eyJ2ZXJzaW9ucyI6WyJVMkZfVjIiLCJGSUR
PXzJfMCJdLCJleHRlbnNpb25zIjpbImNyZWRQcm90ZWN0IiwiaG1hYy1zZWNyZXQiXSwiYWFndWlkIjo
iMDEzMmQxMTBiZjRlNDIwOGE0MDNhYjRmNWYxMmVmZTUiLCJvcHRpb25zIjp7InBsYXQiOiJmYWxzZSI
sInJrIjoidHJ1ZSIsImNsaWVudFBpbiI6InRydWUiLCJ1cCI6InRydWUiLCJ1diI6InRydWUiLCJ1dlR
va2VuIjoiZmFsc2UiLCJjb25maWciOiJmYWxzZSJ9LCJtYXhNc2dTaXplIjoxMjAwLCJwaW5VdkF1dGh
Qcm90b2NvbHMiOlsxXSwibWF4Q3JlZGVudGlhbENvdW50SW5MaXN0IjoxNiwibWF4Q3JlZGVudGlhbEl
kTGVuZ3RoIjoxMjgsInRyYW5zcG9ydHMiOlsidXNiIiwibmZjIl0sImFsZ29yaXRobXMiOlt7InR5cGU
iOiJwdWJsaWMta2V5IiwiYWxnIjotN30seyJ0eXBlIjoicHVibGljLWtleSIsImFsZyI6LTI1N31dLCJ
tYXhBdXRoZW50aWNhdG9yQ29uZmlnTGVuZ3RoIjoxMDI0LCJkZWZhdWx0Q3JlZFByb3RlY3QiOjIsImZ
pcm13YXJlVmVyc2lvbiI6NX19LCJzdGF0dXNSZXBvcnRzIjpbeyJzdGF0dXMiOiJGSURPX0NFUlRJRkl
FRCIsImVmZmVjdGl2ZURhdGUiOiIyMDE5LTAxLTA0In0seyJzdGF0dXMiOiJGSURPX0NFUlRJRklFRF9
MMSIsImVmZmVjdGl2ZURhdGUiOiIyMDIwLTExLTE5IiwiY2VydGlmaWNhdGlvbkRlc2NyaXB0b3IiOiJ
GSURPIEFsbGlhbmNlIFNhbXBsZSBGSURPMiBBdXRoZW50aWNhdG9yIiwiY2VydGlmaWNhdGVOdW1iZXI
iOiJGSURPMjEwMDAyMDE1MTIyMTAwMSIsImNlcnRpZmljYXRpb25Qb2xpY3lWZXJzaW9uIjoiMS4wLjE
iLCJjZXJ0aWZpY2F0aW9uUmVxdWlyZW1lbnRzVmVyc2lvbiI6IjEuMC4xIn1dLCJ0aW1lT2ZMYXN0U3R
hdHVzQ2hhbmdlIjoiMjAxOS0wMS0wNCJ9XX0.-kc1wrorJA16bxLXXzeDkFEOCsbKAy2WDEzoCY-Aej_
N0bWIOAmhpHGxSa3CXgmwFwgAuy230Eq_BHTO_RshsA
```

The line breaks are for display purposes only.

The signature in the example above was computed with the following ECDSA key

```
EXAMPLE: ECDSA KEY USED FOR SIGNATURE COMPUTATION
-----BEGIN CERTIFICATE-----
MIICZTCCAgugAwIBAgIBATAKBggqhkjOPQQDAjCBozEnMCUGA1UEAwweRVhBTVBM
RSBNRFMzIFRFU1QgSU5URVJNRURJQVRFMSIwIAYJKoZIhvcNAQkBFhNleGFtcGxl
QGV4YW1wbGUuY29tMRQwEgYDVQQKDAtFeGFtcGxlIE9SRzEQMA4GA1UECwwHRXhh
bXBsZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1ZMRIwEAYDVQQHDAlXYWtlZmll
bGQwHhcNMjEwNDE5MTEzNTA3WhcNMzEwNDE3MTEzNTA3WjCBpTEpMCcGA1UEAwwg
RVhBTVBMRSBNRFMzIFNJR05JTkcgQ0VSVElGSUNBVEUxIjAgBgkqhkiG9w0BCQEW
E2V4YW1wbGVAZXhhbXBsZS5jb20xFDASBgNVBAoMC0V4YW1wbGUgT1JHMRAwDgYD
VQQLDAdFeGFtcGxlMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTVkxEjAQBgNVBAcM
CVdha2VmaWVsZDBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABNQJs6wTqixc+S+V
DAajFlPNat10KEWJE5jcWOvm6qpO9SDAAMZvb4HHrvs+P5YRpHrSlUPdvK+uEQbd
Wg31P9ujLDAqMAkGA1UdEwQCMAAwHQYDVR0OBBYEFLqsapcXV4ZoVHAnRpPZwQe7
Yy20MAoGCCqGSM49BAMCA0gAMEUCIQC67za8EIuyRiKgNDXIP1s1aLr3jzH9WVXf
Hx4bJ+zCsgIgG/tVButOJUU+vvoHIo/otAUAcH5bNHP3uIziDS+PTUc=
-----END CERTIFICATE-----

-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIFNpFhJvod3jKvbrLLzKTWKFxzaZ4l7kMchx3NyytQYUoAoGCCqGSM49
AwEHoUQDQgAE1AmzrBOqLFz5L5UMBqMWU81q3XQoRYkTmNxY6+bqqk71IMAAxm9v
gceu+z4/lhGketKVQ928r64RBt1aDfU/2w==
-----END EC PRIVATE KEY-----
```

The root certificate to validate certificate path in the X5C is:

```
EXAMPLE: CERTIFICATE PATH ROOT CERTIFICATE
-----BEGIN CERTIFICATE-----
MIIGGTCCBAGgAwIBAgIUdT9qLX0sVMRe8l0sLmHd3mZovQ0wDQYJKoZIhvcNAQEL
BQAwgZsxHzAdBgNVBAMMFkVYQU1QTEUgTURTMyBURVNUIFJPT1QxIjAgBgkqhkiG
9w0BCQEWE2V4YW1wbGVAZXhhbXBsZS5jb20xFDASBgNVBAoMC0V4YW1wbGUgT1JH
MRAwDgYDVQQLDAdFeGFtcGxlMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTVkxEjAQ
BgNVBAcMCVdha2VmaWVsZDAeFw0yMTA0MTkxMTM1MDdaFw00ODA5MDQxMTM1MDda
MIGbMR8wHQYDVQQDDBZFWEFNUExFIE1EUzMgVEVTVCBST09UMSIwIAYJKoZIhvcN
AQkBFhNleGFtcGxlQGV4YW1wbGUuY29tMRQwEgYDVQQKDAtFeGFtcGxlIE9SRzEQ
MA4GA1UECwwHRXhhbXBsZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1ZMRIwEAYD
VQQHDAlXYWtlZmllbGQwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDD
jF5wyEWuhwDHsZosGdGFTCcI677rW881vV+UfW38J+K2ioFFNeGVsxbcebK6AVOi
CDPFj0974IpeD9SFOhwAHoDu/LCfXdQWp8ZgQ91ULYWoW8o7NNSp01nbN9zmaO6/
xKNCa0bzjmXoGqglqnP1AtRcWYvXOSKZy1rcPeDv4Dhcpdp6W72fBw0eWIqOhsrI
tuY2/N8ItBPiG03EX72nACq4nZJ/nAIcUbER8STSFPPzvE97TvShsi1FD8aO6l1W
kR/QkreAGjMI++GbB2Qc1nN9Y/VEDbMDhQtxXQRdpFwubTjejkN9hKOtF3B71Yrw
Irng3V9RoPMFdapWMzSlI+WWHog0oTj1PqwJDDg7+z1I6vSDeVWAMKr9mq1w1OGN
zgBopIjd9lRWkRtt2kQSPX9XxqS4E1gDDr8MKbpM3JuubQtNCg9D7Ljvbz6vwvUr
bPHH+oREvucsp0PZ5PpizloepGIcLFxDQqCulGY2n7Ahl0JOFXJqOFCaK3TWHwBv
ZsaY5DgBuUvdUrwtgZNg2eg2omWXEepiVFQn3Fvj43Wh2npPMgIe5P0rwncXvROx
aczd4rtajKS1ucoB9b9iKqM2+M1y/FDIgVf1fWEHwK7YdzxMlgOeLdeV/kqRU5PE
UlLU9a2EwdOErrPbPKZmIfbs/L4B3k4zejMDH3Y+ZwIDAQABo1MwUTAdBgNVHQ4E
FgQU8sWwq1TrurK7xMTwO1dKfeJBbCMwHwYDVR0jBBgwFoAU8sWwq1TrurK7xMTw
O1dKfeJBbCMwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAFw6M
1PiIfCPIBQ5EBUPNmRvRFuDpolOmDofnf/+mv63LqwQZAdo/W8tzZ9kOFhq24SiL
w0H7fsdG/jeREXiIZMNoW/rA6Uac8sU+FYF7Q+qp6CQLlSQbDcpVMifTQjcBk2xh
+aLK9SrrXBqnTAhwS+offGtAW8DpoLuH4tAcQmIjlgMlN65jnELCuqNR/wpA+zch
8LZW8saQ2cwRCwdr8mAzZoLbsDSVCHxQF3/kQjPT7Nao1q2iWcY3OYcRmKrieHDP
67yeLUbVmetfZis2d6ZlkqHLB4ZW1xX4otsEFkuTJA3HWDRsNyhTwx1YoCLsYut5
Zp0myqPNBq28w6qGMyyoJN0Z4RzMEO3R6i/MQNfhK55/8O2HciM6xb5t/aBSuHPK
lBDrFWhpRnKYkaNtlUo35qV5IbKGKau3SdZdSRciaXUd/p81YmoF01UlhhMz/Rqr
1k2gyA0a9tF8+awCeanYt5izl8YO0FlrOU1SQ5UQw4szqqZqbrf4e8fRuU2TXNx4
zk+ImE7WRB44f6mSD746ZCBRogZ/SA5jUBu+OPe4/sEtERWRcQD+fXgce9ZEN0+p
eyJIKAsl5Rm2Bmgyg5IoyWwSG5W+WekGyEokpslou2Yc6EjUj5ndZWz5EiHAiQ74
hNfDoCZIxVVLU3Qbp8a0S1bmsoT2JOsspIbtZUg=
-----END CERTIFICATE-----
```

3.2. Metadata BLOB object processing rules§

The FIDO Server MUST follow these processing rules:

1. Download (see here for considerations) and cache the root signing trust anchor from the respective MDS root location "mds.fidoalliance.org". More information can be found at https://fidoalliance.org/metadata/

   > The FIDO server should pass the serial number of the latest cached Metadata Service BLOB to the service (`GET /?localCopySerial=77`). In that case, the MDS will return HTTP code 304 (Not Modified) if no newer MDS blob is available. Alternatively, the serial number of the local copy could be provided through the "If-None-Match" header field. The server will always return the serial number in the ETag header field. If both, the "localCopySerial" parameter and the "If-None-Match" header are provided, the server will only process the "localCopySerial" parameter.

2. To validate the digital certificates used in the digital signature, the certificate revocation information MUST be available in the form of CRLs at the respective MDS CRL location e.g. More information can be found at https://fidoalliance.org/metadata/
3. The FIDO Server MUST be able to download the latest metadata BLOB object from the well-known URL when appropriate, e.g. https://mds.fidoalliance.org/. The serial number of the latest local copy SHOULD be provided in order to avoid unnecessary data transfers.
4. If the `x5u` attribute is present in the JWT Header, then:
   1. The FIDO Server MUST verify that the URL specified by the`x5u` attribute has the same web-origin as the URL used to download the metadata BLOB from. The FIDO Server SHOULD ignore the file if the web-origin differs (in order to prevent loading objects from arbitrary sites).
   2. The FIDO Server MUST download the certificate (chain) from the URL specified by the`x5u` attribute [JWS]. The certificate chain MUST be verified to properly chain to the metadata BLOB signing trust anchor according to [RFC5280]. All certificates in the chain MUST be checked for revocation according to [RFC5280].
   3. The FIDO Server SHOULD ignore the file if the chain cannot be verified or if one of the chain certificates is revoked.

      > The requirements for verifying certificate revocation, are only applicable to the MDS BLOB payload certificates. It is up to the server vendors whether to enforce CRL check for the certificates in the individual metadata statements.

5. If the `x5u` attribute is missing, the chain should be retrieved from the`x5c` attribute. If that attribute is missing as well, Metadata BLOB signing trust anchor is considered the BLOB signing certificate chain.
6. Verify the signature of the Metadata BLOB object using the BLOB signing certificate chain (as determined by the steps above). The FIDO Server SHOULD ignore the file if the signature is invalid. It SHOULD also ignore the file if its number (`no`) is less or equal to the number of the last Metadata BLOB object cached locally.
7. Write the verified object to a local cache as required. Remember the "iat" ("issued at") time as needed.
8. Iterate through the individual entries (of type `MetadataBLOBPayloadEntry`). For each entry:
   1. Ignore the entry if the AAID, AAGUID or attestationCertificateKeyIdentifiers is not relevant to the relying party (e.g. not acceptable by any policy)

      > Note: To remain compatible with future versions the FIDO Server SHOULD ignore unrecognized fields when processing any element of an entry. The addition, subtraction or change in interpretation of any fields in an entry of this specification which substantively changes the processing logic of a consumer will only occur alongside an update to the major version number of the specification.

   2. Check whether the status report of the authenticator model has changed compared to the cached entry by looking at the fields `timeOfLastStatusChange` and `statusReport`.

      Update the status of the cached entry. It is up to the relying party to specify behavior for authenticators

with status reports that indicate a lack of certification, or known security issues. However, the status `REVOKED` indicates significant security issues related to such authenticators.

> Authenticators with an unacceptable status should be marked accordingly.This information is required for building registration and authentication policies included in the registration request and the authentication request [UAFProtocol].

3. Update the cached metadata statement.

> It is possible that an MDS entry representing an authenticator disappears in a future update of the BLOB. This should not affect the processing of any other MDS entries.

4. Considerations§

This section is not normative.

This section describes the key considerations for designing this metadata service.

Need for Authenticator Metadata

When defining policies for acceptable authenticators, it is often better to describe the required authenticator characteristics in a generic way than to list individual authenticator AAIDs. The metadata statements provide such information. Authenticator metadata also provides the trust anchor required to verify attestation objects.

The metadata service provides a standardized method to access such metadata statements.

Integrity and Authenticity

Metadata statements include information relevant for the security. Some business verticals might even have the need to document authenticator policies and trust anchors used for verifying attestation objects for auditing purposes.

It is important to have a strong method to verify and proof integrity and authenticity and the freshness of metadata statements. We are using a single digital signature to protect the integrity and authenticity of the Metadata BLOB object and all metadata statements.

Organizational Impact

The FIDO Alliance has control over the FIDO certification process and authentication vendors provide the metadata as part of that process. With this metadata service, the list of known authenticators and their metadata statements need to be updated, signed and published regularly. A single signature needs to be generated in order to protect the integrity and authenticity of the metadata BLOB object and all embedded metadata statements.

Performance Impact

Metadata BLOB objects and metadata statements can be cached by the FIDO Server.

The update policy can be specified by the relying party.

The metadata BLOB object includes a date for the next scheduled update. As a result there is*no additional impact* to the FIDO Server during FIDO Authentication or FIDO Registration operations.

High Security Environments

Some high security environments might only trust internal policy authorities. FIDO Servers in such environments could be restricted to use metadata BLOB objects from a proprietary trusted source only. The metadata service is the baseline for most relying parties.

Extended Authenticator Information

Some relying parties might want additional information about authenticators before accepting them. The policy configuration is under control of the relying party, so it is possible to only accept authenticators for which additional data is available and meets the requirements.

Implementer Guidance

For typical applications, we recommend checking for updated Metadata Statements once a day. This ensures up-to-date information about available security keys and passkey providers and their respective characteristics and certification status.

In order to minimize bandwidths needs and system load, we also recommend providing the serial number of the most recent local copy that is available, see section Metadata BLOB object processing rules for more details. This avoids downloading the data again if there is no change.

Note that the nextUpdate field will be removed in the future.

Index§

Terms defined by this specification§

- aaguid
- aaid
- attestationCertificateKeyIdentifiers
- "ATTESTATION_KEY_COMPROMISE"
- AuthenticatorStatus
- authenticatorVersion
- batchCertificate
- BiometricStatusReport
- biometricStatusReports
- certificate
- certificateNumber
  - dict-member for BiometricStatusReport
  - dict-member for StatusReport
- certificationDescriptor
  - dict-member for BiometricStatusReport
  - dict-member for StatusReport
- certificationPolicyVersion
  - dict-member for BiometricStatusReport
  - dict-member for StatusReport
- certificationProfiles
- certificationRequirementsVersion
  - dict-member for BiometricStatusReport
  - dict-member for StatusReport
- certLevel
- date
- effectiveDate
  - dict-member for BiometricStatusReport
  - dict-member for StatusReport

entries

"FIDO_CERTIFIED"

"FIDO_CERTIFIED_L1"

"FIDO_CERTIFIED_L1plus"

"FIDO_CERTIFIED_L2"

"FIDO_CERTIFIED_L2plus"

"FIDO_CERTIFIED_L3"

"FIDO_CERTIFIED_L3plus"

"FIPS140_CERTIFIED_L1"

"FIPS140_CERTIFIED_L2"

"FIPS140_CERTIFIED_L3"

"FIPS140_CERTIFIED_L4"

fipsPhysicalSecurityLevel

fipsRevision

legalHeader

MetadataBLOBPayload

MetadataBLOBPayloadEntry

metadataStatement

modality

nextUpdate

no

"NOT_FIDO_CERTIFIED"

"RETIRED"

"REVOKED"

RogueListEntry

rogueListHash

rogueListURL

"SELF_ASSERTION_SUBMITTED"

sk

status

StatusReport

statusReports

sunsetDate

timeOfLastStatusChange

"UPDATE_AVAILABLE"

url

"USER_KEY_PHYSICAL_COMPROMISE"

"USER_KEY_REMOTE_COMPROMISE"

"USER_VERIFICATION_BYPASS"

Terms defined by reference§

[ECMASCRIPT] defines the following terms:

- Number

[WebIDL] defines the following terms:

- DOMString
- unsigned long
- unsigned short

References§

Normative References§

[ECMASCRIPT]
ECMAScript Language Specification. URL: https://tc39.es/ecma262/multipage/

[FIDOAuthenticatorSecurityRequirements]
Rolf Lindemann; Dr. Joshua E. Hill; Douglas Biggs. *FIDO Authenticator Security Requirements*. November 2020. Final Draft. URL: https://fidoalliance.org/specs/fido-security-requirements/fido-authenticator-security-requirements-v1.4-fd-20201102.html

[FIDOBiometricsRequirements]
Stephanie Schuckers; et al. *FIDO Biometrics Requirements*. October 2020. URL: https://fidoalliance.org/specs/biometric/requirements/Biometrics-Requirements-v2.0-fd-20201006.html

[FIDOMetadataStatement]
B. Jack; R. Lindemann; Y. Ackermann. *FIDO Metadata Statements*. 21 May 2025. Proposed Standard. URL: https://fidoalliance.org/specs/mds/fido-metadata-statement-v3.1-ps-20250521.html

[JWS]
M. Jones; J. Bradley; N. Sakimura. *JSON Web Signature (JWS)*. May 2015. RFC. URL: https://tools.ietf.org/html/rfc7515

[JWT]
M. Jones; J. Bradley; N. Sakimura. *JSON Web Token (JWT)*. May 2015. RFC. URL: https://tools.ietf.org/html/rfc7519

[RFC4648]
S. Josefsson. *The Base16, Base32, and Base64 Data Encodings (RFC 4648)*. October 2006. URL: http://www.ietf.org/rfc/rfc4648.txt

[RFC5280]
D. Cooper; et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. May 2008. URL: https://tools.ietf.org/html/rfc5280

[RFC7519]
M. Jones; J. Bradley; N. Sakimura. *JSON Web Token (JWT)*. May 2015. Proposed Standard. URL: https://www.rfc-editor.org/rfc/rfc7519

[WebIDL]
Edgar Chen; Timothy Gu. *Web IDL Standard*. Living Standard. URL: https://webidl.spec.whatwg.org/

[WebIDL-ED]
Cameron McCormack. *Web IDL*. 13 November 2014. Editor's Draft. URL: http://heycam.github.io/webidl/

Informative References§

[FIDOEcdaaAlgorithm]
R. Lindemann; et al. *FIDO ECDAA Algorithm*. 23 May 2022. Proposed Standard. URL: https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-ecdaa-algorithm-v2.0-id-20180227.html

[FIDOGlossary]
R. Lindemann; et al. *FIDO Technical Glossary*. 23 May 2022. Proposed Standard. URL: https://fidoalliance.org/specs/common-specs/fido-glossary-v2.1-ps-20220523.html

[FIDOKeyAttestation]

FIDO 2.0: Key attestation format. URL: https://fidoalliance.org/specs/fido-v2.0-ps-20150904/fido-key-attestation-v2.0-ps-20150904.html

[ITU-X690-2008]
X.690: Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), (T-REC-X.690-200811). November 2008. URL: https://www.itu.int/rec/T-REC-X.690-200811-S

[RFC2119]
S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels* March 1997. Best Current Practice. URL: https://tools.ietf.org/html/rfc2119

[UAFProtocol]
R. Lindemann; et al. *FIDO UAF Protocol Specification v1.2*. Proposed Standard. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-protocol-v1.2-ps-20201020.html

IDL Index§

```
dictionary MetadataBLOBPayloadEntry {
    AAID                        aaid;
    AAGUID                      aaguid;
    DOMString[]                 attestationCertificateKeyIdentifiers;
    required MetadataStatement  metadataStatement;
    BiometricStatusReport[]     biometricStatusReports;
    required StatusReport[]     statusReports;
    required DOMString          timeOfLastStatusChange;
    DOMString                   rogueListURL;
    DOMString                   rogueListHash;
};

dictionary BiometricStatusReport {
    required unsigned short certLevel;
    required DOMString      modality;
    DOMString               effectiveDate;
    DOMString               certificationDescriptor;
    DOMString               certificateNumber;
    DOMString               certificationPolicyVersion;
    DOMString               certificationRequirementsVersion;
};

dictionary StatusReport {
    required AuthenticatorStatus status;
    DOMString                    effectiveDate;
    unsigned long                authenticatorVersion;
    DOMString                    batchCertificate;
    DOMString                    certificate;
    DOMString                    url;
    DOMString                    certificationDescriptor;
    DOMString                    certificateNumber;
    DOMString                    certificationPolicyVersion;
    DOMString[]                  certificationProfiles;
    DOMString                    certificationRequirementsVersion;
    DOMString                    sunsetDate;
    unsigned long                fipsRevision;
    unsigned long                fipsPhysicalSecurityLevel;
};

enum AuthenticatorStatus {
    "NOT_FIDO_CERTIFIED",
    "FIDO_CERTIFIED",
    "USER_VERIFICATION_BYPASS",
    "ATTESTATION_KEY_COMPROMISE",
```

```
    "USER_KEY_REMOTE_COMPROMISE",
    "USER_KEY_PHYSICAL_COMPROMISE",
    "UPDATE_AVAILABLE",
    "RETIRED",
    "REVOKED",
    "SELF_ASSERTION_SUBMITTED",
    "FIDO_CERTIFIED_L1",
    "FIDO_CERTIFIED_L1plus",
    "FIDO_CERTIFIED_L2",
    "FIDO_CERTIFIED_L2plus",
    "FIDO_CERTIFIED_L3",
    "FIDO_CERTIFIED_L3plus",
    "FIPS140_CERTIFIED_L1",
    "FIPS140_CERTIFIED_L2",
    "FIPS140_CERTIFIED_L3",
    "FIPS140_CERTIFIED_L4"
};

dictionary RogueListEntry {
    required DOMString sk;
    required DOMString date;
};

dictionary MetadataBLOBPayload {
    DOMString                          legalHeader;
    required Number                    no;
    required DOMString                 nextUpdate;
    required MetadataBLOBPayloadEntry[] entries;
};
```

Issues Index§

ISSUE 1 Update this example ↵