RDW

mDoc for Domestic Vehicle Registration

Sample data structure and PKI for ISO/IEC18013-5 test event

Author	RDW
Version	0.4
Date	29-09-2021
Status	Draft
Classification	Public

RDW

Document information

Title document	mDoc for Domestic Vehicle Registration, Sample data structure and PKI for ISO/IEC18013-5 test event
Name file	20210929 mDoc for Domestic Vehicle Registration, sample data structure v0 4.docx
Keywords	ISO/IEC 18013-5:2021
Classification	Public
Status	Draft
Distribution	RDW, UL, mDL test event participants

Version history

Version	Date	Status	Authors
0.1	06-09-2021	Draft	RDW
0.2	07-09-2021	Draft	RDW
0.3	17-09-2021	Draft	RDW
0.4	29-09-2021	Draft	RDW

Change history

Version	Date	Change
0.2	07-09-2021	External review • Adding reference to Certificate profiles • Editorial • Remove not used references in definition field of table 1 • Set country to 2 characters • Updated used character sets for fields in paragraph 2.2
0.3	17-09-2021	Added appendix A.2 and A.3 with example material (informative)
0.4	29-09-2021	Corrected value in Issuer Alternative Name in the certificates; updated MSO accordingly, added private keys for IACA & DS certificate

Approval

Version	Date approval	Signed by

Contents

1 Introduction

The RDW issues documents within the Netherlands. Typical products are the Dutch Driver License, the Dutch Vehicle Registration Card and other documents.

The RDW anticipates providing documents to the holder conforming to the [ISO/IEC18013-5] standard.

1.1 Scope

Document type mEKB
This document describes an ISO/IEC18013-5 compliant mdoc for a domnestic vehicle registration certificate. It is to be read in conjunction with ISO/IEC18013-5, whereby this document replaces the mDL specifics in clause 7 with a document type and namespace for a “mobile example kenteken bewijs” (proof of vehicle registration), mEKB release 1. This is addressed in section 2.

Keys and certificates mEKB
In this document, the keys and certificates used are described. This is addressed in section 3.

1.2 Purpose

The document is intended to be used for ISO/IEC18013-5 test events, for the purpose of experimenting with device retrieval using an alternative mdoc to mDL, as well as experimenting with transactions in which multiple documents are requested.

This document can be used as a reference for issuers, verifiers, mdoc app providers and mdoc reader app providers.

1.3 Terms and definitions

Acronym	Term	Definition

1.4 References

Ref.	Title	Author	Status	Version	Date
[EC2003/127]	Commission Directive 2003/127/EC On the registration documents for vehicles	EU	Final		23-12-2003
[ISO/IEC18013-5]	ISO/IEC 18013-5:2021 Personal Identification – ISO – Compliant Driving Licence. Part 5 Mobile Driving Licence (mDL) application	ISO/IEC	2021	2021	09-2021
[ISO7367]	ISO/IEC 7367 Personal identification — Mobility related documents — Mobile vehicle registration (mVR)	RDW first draft contribution for ISO/IEC JTC1 SC 17 WG 10	WD		06-04-2021
RFC 3339	Date and Time on the Internet: Timestamps	ietf,org			July 2002
RFC 7049	Concise Binary Object Representation (CBOR)	ietf,org			October 2013
RFC 8610	Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures	ietf,org			June 2019
RFC 8943	Concise Binary Object Representation (CBOR) Tags for Date	ietf,org			November 2020

2 mEKB Data model

This section specifies the data model of an mEKB. for mEKB documents. This paragraph replaces section 7 in [ISO 18013-5] for mEKB.

As basis a selection of the elements of the RDW's first contribution for mVR to ISO [ISO7367] is chosen.

2.1 mEKB document type and namespace

The following document type and namespace shall be used:

`DocType` and `NameSpace` are used to encapsulate the document type and the space in which the data elements are defined.

The document type for an mEKB document shall be "nl.rdw.mekb.1". The number "1" in the document type might be increased in future versions of the mEKB.

The namespace for mEKB data defined in paragraph 2.2 shall be "nl.rdw.mekb.1". The number "1" in the namespace might be increased in future versions of the mEKB.

2.2 mEKB data

The mEKB data elements shall be as defined in Table 1 belong to namespace "nl.rdw.mekb.1", see paragraph 2.1. The structure is a copy from the proposed mVR data model for ISO [ISO7367]

- The "Identifier" column is used for `DataElementIdentifier` in the device retrieval mdoc request or server retrieval mdoc request.
- The "Presence" column indicates whether the presence of the element on an mEKB is mandatory (M), or optional (O).
- The "Encoding format" column indicates how the data elements shall be encoded. "tstr", "uint", "bstr", "bool" and "tdate" are CDDL representation types as defined in RFC 8610. This document specifies "full-date" as `full-date = #6.1004(tstr)`, where tag 1004 is specified in RFC 8943.
- In accordance with RFC 7049 Section 2.4.1, a tdate data item shall contain a date-time string as specified in RFC 3339. In accordance with RFC 8943, a `full-date` data item shall contain a full-date string as specified in RFC 3339.
- If data elements are encoded with JSON for the server retrieval methods, the data elements shall be encoded as specified in RFC 7049, Section 4.1.

- The following requirements shall apply to the representation of dates in mEKB data elements, unless otherwise indicated:
    - Fraction of seconds shall not be used.
    - No local offset from UTC shall be used, as indicated by setting the `time-offset` defined in RFC 3339 to "Z".

Identifier	Meaning	Definition	Presence	Encoding format
registration_info	Vehicle Registration Information	This data element contains the common vehicle registration information, including UN/EU elements, A and H.	M	See Clause 2.2.1
issue_date	Issue Date	Date when document was issued.	M	tdate or full-date
registration_holder	Vehicle Registration Holder Information	This data element identifies the holder of the registration certificate, including UN element C/EU table C.1 and EU element C.4.	M	See Clause 2.2.2
basic_vehicle_info	Basic Vehicle Information	This data element contains the basic vehicle information, including UN element D/EU table.	M	See Clause 2.2.3
vin	Vehicle Identification Number	Vehicle Identification Number defined by the vehicle manufacture, including UN/EU element E. It is also known as the serial number of the chassis or as the maker's production or serial number. The data element shall contain a valid VIN, as defined in ISO 3779.	M	tstr
Key Presence: M mandatory O optional				

Table 1: mEKB data elements

2.2.1 Registration Info

```
RegistrationInfo = {
  "issuingCountry" : tstr          ; country code in accordance with ISO 3166-1 alpha-2
  "competentAuthority" : tstr      ; name of the competent authority, the value shall only
                                   ; use Latin1[a] characters
  "registrationNumber" : tstr      ; UN/EU element A, the value shall use Latin1[a] characters
                                   ; and may only contain Arabic numerals, capital Latin
                                   ; letters and a dash ("-") as delimiter
  "validFrom" : tdate              ; Custom EKB element, valid from
  "validUntil" : tdate             ; Custom EKB element, valid until
}
```

[a] Latin1 is defined in ISO/IEC 8859-1 as Latin alphabet No. 1.

2.2.2 Registration Holder

```
RegistrationHolder = {
  "holderInfo" : PersonalData      ; UN element C and EU table C.1
  "ownershipStatus" : uint         ; EU element C.4
}


PersonalData = {
  "name" : tstr                    ; UN element C and EU element C.x.1, the value shall
                                   ; only use Latin1[a] characters
  "address" : Address              ; UN element C and EU element C.x.3
}

Address = {
  "streetName" : tstr              ; Street name, the value shall only use Latin1[a]
                                   ; characters
  "houseNumber" : uint             ; House number
  ? "houseNumberSuffix" : tstr     ; House number suffix , the value shall only use Latin1[a]
                                   ; characters
  "postalCode" : tstr              ; Postal code, the value shall only use Latin1[a]
                                   ; characters
  "placeOfResidence" : tstr        ; Residence, the value shall only use Latin1[a] characters

}
```

[a] Latin1 is defined in ISO/IEC 8859-1 as Latin alphabet No. 1.

2.2.3 Basic Vehicle Info

```
BasicVehicleInfo = {
  "vehicle" : Vehicle               ; UN element D and EU table D
}

Vehicle = {
  "make" : tstr                     ; UN element D and EU element D.1
                                    ; the value shall only use Latin1[a] characters

}
```

[a] Latin1 is defined in ISO/IEC 8859-1 as Latin alphabet No. 1.

3 Keys and certificates for mEKB

For the mEKB the following keys and certificates are used:

- IACA root key pair with a public key certificate according to the certificate profile in [ISO/IEC18013-5] annex B.1.2
- Document signer key pair with a public key certificate according to the certificate profile in [ISO/IEC18013-5] annex B.1.4
- mDoc authentication key pair according to [ISO/IEC18013-5] paragraph 9.1.3, of which the public key is included in the MSO.

A.1 Data structure examples (informative)

A.1.1 Introduction

This annex contains examples of data structures used in the document. Since CBOR results in binary structures, a diagnostic notation will be used together with the binary encoding, whenever CBOR examples are made in this annex.

A.1.2 Registration Info

An example of “registration_info” structure is given:

```
{"issuingCountry": "UT", "competentAuthority": "RDW", "registrationNumber": "E-
01-23", "validFrom": 0("2021-04-19T22:00:00Z"), "validUntil": 0("2023-04-
20T22:00:00Z")}
```

Example byte string:

```
A5 6E 69 73 73 75 69 6E 67 43 6F 75 6E 74 72 79 62 55 54 72 63 6F 6D 70 65 74 65 6E 74 41 75
74 68 6F 72 69 74 79 63 52 44 57 72 72 65 67 69 73 74 72 61 74 69 6F 6E 4E 75 6D 62 65 72 67
45 2D 30 31 2D 32 33 69 76 61 6C 69 64 46 72 6F 6D C0 74 32 30 32 31 2D 30 34 2D 31 39 54 32
32 3A 30 30 3A 30 30 5A 6A 76 61 6C 69 64 55 6E 74 69 6C C0 74 32 30 32 33 2D 30 34 2D 32 30
54 32 32 3A 30 30 3A 30 30 5A
```

This example is represented as the following byte string when encoded with CBOR:

```
A5                                      # map(5)
   6E                                   # text(14)
      69737375696E67436F756E747279      # "issuingCountry"
   62                                   # text(2)
      5554                              # "UT"
   72                                   # text(18)
      636F6D706574656E74417574686F72697479 # "competentAuthority"
   63                                   # text(3)
      524457                            # "RDW"
   72                                   # text(18)
      726567697374726174696F6E4E756D626572 # "registrationNumber"
   67                                   # text(7)
      452D30312D3233                    # "E-01-23"
   69                                   # text(9)
      76616C696446726F6D                # "validFrom"
   C0                                   # tag(0)
      74                                # text(20)
         323032312D30342D31395432323A30303A30305A # "2021-04-19T22:00:00Z"
   6A                                   # text(10)
      76616C6964556E74696C              # "validUntil"
   C0                                   # tag(0)
      74                                # text(20)
         323032332D30342D32305432323A30303A30305A # "2023-04-20T22:00:00Z"
```

A.1.3 Issue Date

An example of “issue_date” structure is given:

```
1004("2021-04-18")
```

Example byte string:

```
D9 03 EC 6A 32 30 32 31 2D 30 34 2D 31 38
```

This example is represented as the following byte string when encoded with CBOR:

```
D9 03EC                    # tag(1004)
   6A                      # text(10)
      323032312D30342D3138 # "2021-04-18"
```

A.1.4 Registration Holder

An example of “registration_holder” structure is given:

```
{"holderInfo": {"name": "Sample Name", "address": {"streetName": "teststraat",
"houseNumber": 86, "postalCode": "1234 AA", "placeOfResidence": "Samplecity"}},
"ownershipStatus": 2}
```

Example byte string:

```
A2 6A 68 6F 6C 64 65 72 49 6E 66 6F A2 64 6E 61 6D 65 6B 53 61 6D 70 6C 65 20 4E 61 6D 65 67
61 64 64 72 65 73 73 A4 6A 73 74 72 65 65 74 4E 61 6D 65 6A 74 65 73 74 73 74 72 61 61 74 6B
68 6F 75 73 65 4E 75 6D 62 65 72 18 56 6A 70 6F 73 74 61 6C 43 6F 64 65 67 31 32 33 34 20 41
41 70 70 6C 61 63 65 4F 66 52 65 73 69 64 65 6E 63 65 6A 53 61 6D 70 6C 65 63 69 74 79 6F 6F
77 6E 65 72 73 68 69 70 53 74 61 74 75 73 02
```

This example is represented as the following byte string when encoded with CBOR:

```
2                                  # map(2)
   6A                               # text(10)
      686F6C646572496E666F          # "holderInfo"
   A2                               # map(2)
      64                            # text(4)
         6E616D65                   # "name"
      6B                            # text(11)
         53616D706C65204E616D65     # "Sample Name"
      67                            # text(7)
         61646472657373             # "address"
      A4                            # map(4)
         6A                         # text(10)
            7374726565744E616D65    # "streetName"
         6A                         # text(10)
            74657374737472616174    # "teststraat"
         6B                         # text(11)
            686F7573654E756D626572  # "houseNumber"
         18 56                      # unsigned(86)
```

```
      6A                              # text(10)
         706F7374616C436F6465         # "postalCode"
      67                              # text(7)
         31323334204141               # "1234 AA"
      70                              # text(16)
         706C6163654F665265736964656E6365 # "placeOfResidence"
      6A                              # text(10)
         53616D706C6563697479         # "Samplecity"
   6F                                 # text(15)
      6F776E6572736869705374617473    # "ownershipStatus"
   02                                 # unsigned(2)
```

A.1.5 Basic Vehicle Info:

An example of “basic_vehicle_info” structure is given:

```
{"vehicle": {"make": "Dummymobile"}}
```

Example byte string:

```
A1 67 76 65 68 69 63 6C 65 A1 64 6D 61 6B 65 6B 44 75 6D 6D 79 6D 6F 62 69 6C 65
```

This example is represented as the following byte string when encoded with CBOR:

```
A1                              # map(1)
   67                           # text(7)
      76656869636C65            # "vehicle"
   A1                           # map(1)
      64                        # text(4)
         6D616B65               # "make"
      6B                        # text(11)
         44756D6D796D6F62696C65 # "Dummymobile"
```

A.1.6 Vin

An example of “vin” structure is given:

```
"1M8GDM9AXKP042788"
```

Example byte string:

```
71 31 4D 38 47 44 4D 39 41 58 4B 50 30 34 32 37 38 38
```

This example is represented as the following byte string when encoded with CBOR:

```
71                                  # text(17)
   314D3847444D3941584B50303432373838 # "1M8GDM9AXKP042788"
```

A.2 Data examples with random and signature (informative)

A.2.1 Introduction

Device engagement is as specified in ISO/IEC18013-5:2021. Examples for data retrieval of an “org.iso.18013.5.1.mDL” namespace can be found in Annex D.4 of ISO/IEC 18013-5:2021.

In this section examples of signed data of the “nl.rdw.mekb.1” namespace is given.

A.2.2 Registration Info

elementName:

```
"registration_info"
```

digestID:

```
00
```

random:

```
56 94 EB 8D EC 72 3A 59 C7 97 08 5C E2 4A 27 AA
```

digest:

```
52 9A 60 F7 00 3E 5E 53 8E 9F 99 D7 7F CA 5C CB 3A B0 83 B0 7E 2B EA 7A 31 1A 07 B1 E0 90 A9
1E
```

elementValue:

```
A5 6E 69 73 73 75 69 6E 67 43 6F 75 6E 74 72 79 62 55 54 72 63 6F 6D 70 65 74 65 6E 74 41 75
74 68 6F 72 69 74 79 63 52 44 57 72 72 65 67 69 73 74 72 61 74 69 6F 6E 4E 75 6D 62 65 72 67
45 2D 30 31 2D 32 33 69 76 61 6C 69 64 46 72 6F 6D C0 74 32 30 32 31 2D 30 34 2D 31 39 54 32
32 3A 30 30 3A 30 30 5A 6A 76 61 6C 69 64 55 6E 74 69 6C C0 74 32 30 32 33 2D 30 34 2D 32 30
54 32 32 3A 30 30 3A 30 30 5A
```

IssuerSignedItemBytes:

```
D8 18 58 DA A4 68 64 69 67 65 73 74 49 44 00 66 72 61 6E 64 6F 6D 50 56 94 EB 8D EC 72 3A 59
C7 97 08 5C E2 4A 27 AA 71 65 6C 65 6D 65 6E 74 49 64 65 6E 74 69 66 69 65 72 71 72 65 67 69
73 74 72 61 74 69 6F 6E 5F 69 6E 66 6F 6C 65 6C 65 6D 65 6E 74 56 61 6C 75 65 A5 6E 69 73 73
75 69 6E 67 43 6F 75 6E 74 72 79 62 55 54 72 63 6F 6D 70 65 74 65 6E 74 41 75 74 68 6F 72 69
74 79 63 52 44 57 72 72 65 67 69 73 74 72 61 74 69 6F 6E 4E 75 6D 62 65 72 67 45 2D 30 31 2D
32 33 69 76 61 6C 69 64 46 72 6F 6D C0 74 32 30 32 31 2D 30 34 2D 31 39 54 32 32 3A 30 30 3A
30 30 5A 6A 76 61 6C 69 64 55 6E 74 69 6C C0 74 32 30 32 33 2D 30 34 2D 32 30 54 32 32 3A 30
30 3A 30 30 5A
```

IssuerSignedItemBytes decoded:

```
24(<< {"digestID": 0, "random": h'5694EB8DEC723A59C797085CE24A27AA', "elementIdentifier":
"registration_info", "elementValue": {"issuingCountry": "UT", "competentAuthority": "RDW",
"registrationNumber": "E-01-23", "validFrom": 0("2021-04-19T22:00:00Z"), "validUntil":
0("2023-04-20T22:00:00Z")}}>>)
```

A.2.3 Issue Date

elementName:

```
"issue_date"
```

digestID:

```
01
```

random:

```
06 35 AA F9 FD 96 BF 43 39 D5 82 58 A8 C2 77 0A
```

digest:

```
D6 88 4F 63 4E 34 C9 2E 2C BC 0C D0 DF 83 DC 0C DC 2E FA 77 72 80 EA 14 5C 37 BB 22 17 9C 86
26
```

elementValue:

```
D9 03 EC 6A 32 30 32 31 2D 30 34 2D 31 38
```

IssuerSignedItemBytes:

```
D8 18 58 5B A4 68 64 69 67 65 73 74 49 44 01 66 72 61 6E 64 6F 6D 50 06 35 AA F9 FD 96 BF 43
39 D5 82 58 A8 C2 77 0A 71 65 6C 65 6D 65 6E 74 49 64 65 6E 74 69 66 69 65 72 6A 69 73 73 75
65 5F 64 61 74 65 6C 65 6C 65 6D 65 6E 74 56 61 6C 75 65 D9 03 EC 6A 32 30 32 31 2D 30 34 2D
31 38
```

IssuerSignedItemBytes decoded:

```
24(<<{"digestID": 1, "random": h'0635AAF9FD96BF4339D58258A8C2770A', "elementIdentifier":
"issue_date", "elementValue": 1004("2021-04-18")}>>)
```

A.2.4 Registration Holder

elementName:

```
"registration_holder"
```

digestID:

```
02
```

random:

```
76 50 E2 B6 3F 40 7B 5C BE D9 1D 94 6A 88 D1 37
```

digest:

```
4D 55 44 BB D2 13 91 55 8F 1F 9A 36 CB 3B 3D 76 08 ED 87 E0 EB D3 35 13 8D AD DB BB D3 88 E1
61
```

elementValue:

```
A2 6A 68 6F 6C 64 65 72 49 6E 66 6F A2 64 6E 61 6D 65 6B 53 61 6D 70 6C 65 20 4E 61 6D 65 67
61 64 64 72 65 73 73 A4 6A 73 74 72 65 65 74 4E 61 6D 65 6A 74 65 73 74 73 74 72 61 61 74 6B
68 6F 75 73 65 4E 75 6D 62 65 72 18 56 6A 70 6F 73 74 61 6C 43 6F 64 65 67 31 32 33 34 20 41
41 70 70 6C 61 63 65 4F 66 52 65 73 69 64 65 6E 63 65 6A 53 61 6D 70 6C 65 63 69 74 79 6F 6F
77 6E 65 72 73 68 69 70 53 74 61 74 75 73 02
```

IssuerSignedItemBytes:

```
D8 18 58 E1 A4 68 64 69 67 65 73 74 49 44 02 66 72 61 6E 64 6F 6D 50 76 50 E2 B6 3F 40 7B 5C
BE D9 1D 94 6A 88 D1 37 71 65 6C 65 6D 65 6E 74 49 64 65 6E 74 69 66 69 65 72 73 72 65 67 69
73 74 72 61 74 69 6F 6E 5F 68 6F 6C 64 65 72 6C 65 6C 65 6D 65 6E 74 56 61 6C 75 65 A2 6A 68
6F 6C 64 65 72 49 6E 66 6F A2 64 6E 61 6D 65 6B 53 61 6D 70 6C 65 20 4E 61 6D 65 67 61 64 64
72 65 73 73 A4 6A 73 74 72 65 65 74 4E 61 6D 65 6A 74 65 73 74 73 74 72 61 61 74 6B 68 6F 75
73 65 4E 75 6D 62 65 72 18 56 6A 70 6F 73 74 61 6C 43 6F 64 65 67 31 32 33 34 20 41 41 70 70
6C 61 63 65 4F 66 52 65 73 69 64 65 6E 63 65 6A 53 61 6D 70 6C 65 63 69 74 79 6F 6F 77 6E 65
72 73 68 69 70 53 74 61 74 75 73 02
```

IssuerSignedItemBytes decoded:

```
24(<<{"digestID": 2, "random": h'7650E2B63F407B5CBED91D946A88D137', "elementIdentifier":
"registration_holder", "elementValue": {"holderInfo": {"name": "Sample Name", "address":
{"streetName": "teststraat", "houseNumber": 86, "postalCode": "1234 AA", "placeOfResidence":
"Samplecity"}}, "ownershipStatus": 2}}>>)
```

A.2.5 Basic Vehicle Info

elementName:

```
"basic_vehicle_info"
```

digestID:

```
03
```

random:

```
8C F3 6F C2 43 CC 21 0F 98 76 C1 43 3C 81 8C 61
```

digest:

```
AB AB 85 3F 0A 22 52 47 42 1C E1 65 B9 78 38 A5 02 C6 81 A9 13 42 EF AF FF 8F 25 51 1D 53 37
61
```

elementValue:

```
A1 67 76 65 68 69 63 6C 65 A1 64 6D 61 6B 65 6B 44 75 6D 6D 79 6D 6F 62 69 6C 65
```

IssuerSignedItemBytes:

```
D8 18 58 70 A4 68 64 69 67 65 73 74 49 44 03 66 72 61 6E 64 6F 6D 50 8C F3 6F C2 43 CC 21 0F
98 76 C1 43 3C 81 8C 61 71 65 6C 65 6D 65 6E 74 49 64 65 6E 74 69 66 69 65 72 72 62 61 73 69
63 5F 76 65 68 69 63 6C 65 5F 69 6E 66 6F 6C 65 6C 65 6D 65 6E 74 56 61 6C 75 65 A1 67 76 65
68 69 63 6C 65 A1 64 6D 61 6B 65 6B 44 75 6D 6D 79 6D 6F 62 69 6C 65
```

IssuerSignedItemBytes decoded:

```
24(<<{"digestID": 3, "random": h'8CF36FC243CC210F9876C1433C818C61', "elementIdentifier":
"basic_vehicle_info", "elementValue": {"vehicle": {"make": "Dummymobile"}}}>>)
```

A.2.6 Vin

elementName:

```
"vin"
```

digestID:

```
04
```

random:

```
D7 A1 C7 67 C3 E8 48 5F E8 BB 46 67 14 1D D8 36
```

digest:

```
F9 F5 C6 2E 43 4A 97 BE E7 5A D9 58 FF 8C BB E2 7F 9B 75 F6 D1 D4 34 60 3C A4 2B AA D7 5E 93
23
```

elementValue:

```
71 31 4D 38 47 44 4D 39 41 58 4B 50 30 34 32 37 38 38
```

IssuerSignedItemBytes:

```
D8 18 58 58 A4 68 64 69 67 65 73 74 49 44 04 66 72 61 6E 64 6F 6D 50 D7 A1 C7 67 C3 E8 48 5F
E8 BB 46 67 14 1D D8 36 71 65 6C 65 6D 65 6E 74 49 64 65 6E 74 69 66 69 65 72 63 76 69 6E 6C
65 6C 65 6D 65 6E 74 56 61 6C 75 65 71 31 4D 38 47 44 4D 39 41 58 4B 50 30 34 32 37 38 38
```

IssuerSignedItemBytes decoded:

```
24(<<{"digestID": 4, "random": h'D7A1C767C3E8485FE8BB4667141DD836', "elementIdentifier":
"vin", "elementValue": "1M8GDM9AXKP042788"}>>)
```

A.3 Used example key material (informative)

A.3.1 Used IACA certificate

A.3.1.1 Text

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:02:03:04:05:06:07:08:00:00:00:00:00:00:00:00
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = UT, CN = UL TEST IACA Vehicle Registration
        Validity
            Not Before: Sep  7 00:00:00 2021 GMT
            Not After : Sep  7 00:00:00 2030 GMT
        Subject: C = UT, CN = UL TEST IACA Vehicle Registration
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:1d:0b:a7:6a:3f:10:97:75:9a:6b:7c:41:41:18:
                    ca:e6:0b:76:dc:c6:f4:7c:c7:f2:52:93:9b:10:b2:
                    40:99:37:f9:c3:4c:59:51:d8:0f:cc:d4:df:2c:20:
                    98:b5:d0:6f:f2:b3:cc:23:dd:c8:56:58:19:5d:ba:
                    e1:e6:9a:29:da:70:5a:3f:8b:65:30:81:35:b9:47:
                    ac:0a:07:a9:a4:16:01:50:e3:a9:a8:4a:50:42:65:
                    b3:9f:ec:cc:e4:38:bc
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                5D:96:AC:21:C9:16:89:F6:ED:36:A1:37:C7:BB:E3:8D:8B:3D:DD:AA
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Issuer Alternative Name:
                URI:https://www.ul.com
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
    Signature Algorithm: ecdsa-with-SHA384
         30:64:02:30:5e:b0:36:f8:00:e3:d6:f7:47:42:d1:f8:b6:42:
         5d:b9:6e:77:29:62:2a:7f:41:b1:38:d9:29:16:42:a5:eb:c8:
         c9:c0:34:0a:1f:42:69:7b:33:61:52:2a:c3:c4:1f:98:02:30:
         3a:5f:ca:38:6c:91:76:f6:14:51:e2:ca:7d:64:84:50:ee:86:
         b7:99:a9:be:e8:08:f5:cc:64:3f:9e:db:cf:43:27:37:fb:d2:
         94:91:31:7f:97:ab:9d:b2:a5:33:ec:14
```

A.3.1.2 PEM

```
-----BEGIN CERTIFICATE-----
MIICEDCCAZegAwIBAgIQAQIDBAUGBwgAAAAAAAAAADAKBggqhkjOPQQDAzA5MQsw
CQYDVQQGEwJVVDEqMCgGA1UEAwwhVUwgVEVTVCBJQUNBIFZlaGljbGUgUmVnaXN0
cmF0aW9uMB4XDTIxMDkwNzAwMDAwMFoXDTMwMDkwNzAwMDAwMFowOTELMAkGA1UE
BhMCVVQxKjAoBgNVBAMMIVVMIFRFU1QgSUFDQSBWZWhpY2xlIFJlZ2lzdHJhdGlv
bjB2MBAGByqGSM49AgEGBSuBBAAiA2IABB0Lp2o/EJd1mmt8QUEYyuYLdtzG9HzH
8lKTmxCyQJk3+cNMWVHYD8zU3ywgmLXQb/KzzCPdyFZYGV264eaaKdpwWj+LZTCB
NblHrAoHqaQWAVDjqahKUEJls5/szOQ4vKNkMGIwHQYDVR0OBBYEFF2WrCHJFon2
7TahN8e7442LPd2qMA4GA1UdDwEB/wQEAwIBBjAdBgNVHRIEFjAUhhJodHRwczov
L3d3dy51bC5jb20wEgYDVR0TAQH/BAgwBgEBAQIBADAKBggqhkjOPQQDAwNnADBk
AjBesDb4AOPW90dC0fi2Ql25bncpYip/QbE42SkWQqXryMnANAofQml7M2FSKsPE
H5gCMDpfyjhskXb2FFHiyn1khFDuhreZqb7oCPXMZD+e289DJzf70pSRMX+Xq52y
pTPsFA==
-----END CERTIFICATE-----
```

A.3.1.3 Private key

The private key, PEM / PKCS#8 / X9.62 encoded.

```
-----BEGIN PRIVATE KEY-----
MIG2AgEAMBAGByqGSM49AgEGBSuBBAAiBIGeMIGbAgEBBDBM+OeqPizsGZlGjp1d
FAq4Ybw3ktJc8cQ1fJf1wfU4H7aXETO9VpEW2U7yNoMVsxihZANiAAQdC6dqPxCX
dZprfEFBGMrmC3bcxvR8x/JSk5sQskCZN/nDTFlR2A/M1N8sIJi10G/ys8wj3chW
WBlduuHmminacFo/i2UwgTW5R6wKB6mkFgFQ46moSlBCZbOf7MzkOLw=
-----END PRIVATE KEY-----
```

A.3.2 Used DS certificate

A.3.2.1 Text

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:02:03:04:05:06:07:08:00:00:00:00:00:00:00:01
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = UT, CN = UL TEST IACA Vehicle Registration
        Validity
            Not Before: Sep  7 00:00:01 2021 GMT
            Not After : Dec  7 00:00:01 2022 GMT
        Subject: C = UT, CN = UL TEST DS Vehicle Registration
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:20:cd:df:58:24:7d:b4:a2:83:e9:2d:91:96:7a:
                    eb:f5:8c:a1:83:2d:5f:2b:fd:1c:84:08:ac:fe:25:
                    f1:5f:b0:e4:b1:f2:1a:e2:e7:02:65:4a:0f:b3:f8:
                    4a:3e:f6:b4:0f:b4:47:6b:96:bb:b3:10:bb:8a:15:
                    4f:ef:e2:fa:f9
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:5D:96:AC:21:C9:16:89:F6:ED:36:A1:37:C7:BB:E3:8D:8B:3D:DD:AA

            X509v3 Subject Key Identifier:
                E2:46:6A:42:BB:A3:04:65:21:0B:56:63:A0:2B:21:05:64:8C:E5:0C
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Issuer Alternative Name:
```

```
            URI:https://www.ul.com/
        X509v3 Extended Key Usage: critical
            2.16.528.1.1010.2.2.1
Signature Algorithm: ecdsa-with-SHA384
     30:65:02:31:00:9d:9b:d1:d9:9e:90:be:91:db:42:65:fa:19:
     2f:66:7e:59:d5:3e:3a:71:3d:56:d2:53:d8:b5:31:b5:3d:48:
     64:6f:41:10:59:e1:43:6a:5b:17:36:d7:05:ae:4d:94:53:02:
     30:2d:4d:97:03:20:8e:80:48:b4:50:ef:e8:ff:f2:0d:6f:96:
     b1:9b:f3:13:2d:10:b1:10:44:7b:be:06:bb:4d:ac:0a:67:70:
     b0:8e:cf:15:74:5a:90:20:67:86:46:f2:f8
```

A.3.2.2 PEM

```
-----BEGIN CERTIFICATE-----
MIICGzCCAaGgAwIBAgIQAQIDBAUGBwgAAAAAAAAAATAKBggqhkjOPQQDAzA5MQsw
CQYDVQQGEwJVVDEqMCgGA1UEAwwhVUwgVEVTVCBJQUNBIFZlaGljbGUgUmVnaXN0
cmF0aW9uMB4XDTIxMDkwNzAwMDAwMVoXDTIyMTIwNzAwMDAwMVowNzELMAkGA1UE
BhMCVVQxKDAmBgNVBAMMH1VMIFRFU1QgRFMgVmVoaWNsZSBSZWdpc3RyYXRpb24w
WTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQgzd9YJH20ooPpLZGWeuv1jKGDLV8r
/RyECKz+JfFfsOSx8hri5wJlSg+z+Eo+9rQPtEdrlruzELuKFU/v4vr5o4GMMIGJ
MB8GA1UdIwQYMBaAFF2WrCHJFon27TahN8e7442LPd2qMB0GA1UdDgQWBBTiRmpC
u6MEZSELVmOgKyEFZIzlDDAOBgNVHQ8BAf8EBAMCB4AwHgYDVR0SBBcwFYYTaHR0
cHM6Ly93d3cudWwuY29tLzAXBgNVHSUBAf8EDTALBglghBABh3ICAgEwCgYIKoZI
zj0EAwMDaAAwZQIxAJ2b0dmekL6R20Jl+hkvZn5Z1T46cT1W0lPYtTG1PUhkb0EQ
WeFDalsXNtcFrk2UUwIwLU2XAyCOgEi0UO/o//INb5axm/MTLRCxEER7vga7TawK
Z3Cwjs8VdFqQIGeGRvL4
-----END CERTIFICATE-----
```

A.3.2.3 Private key

The private key, PEM / PKCS#8 / X9.62 encoded.

```
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBAQQgtunXJTbw/thEIgZh
BJT+p5SpTPfFoHcwnjbE8Sg3o7KhRANCAAQgzd9YJH20ooPpLZGWeuv1jKGDLV8r
/RyECKz+JfFfsOSx8hri5wJlSg+z+Eo+9rQPtEdrlruzELuKFU/v4vr5
-----END PRIVATE KEY-----
```

A.3.3 Static device key pair

A.3.3.1 Private key

The hexadecimal encoding of a PKCS#8 /ANSI X9.62 encoded private key :

```
30 81 93 02 01 00 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48 CE 3D 03 01 07 04 79 30 77
02 01 01 04 20 65 E6 C1 C4 1F DD 35 A3 A8 15 37 49 D4 EC 7D B2 10 CD 27 3A 3E 52 4A 52 35 E0
82 D1 D9 AC 52 64 A0 0A 06 08 2A 86 48 CE 3D 03 01 07 A1 44 03 42 00 04 1C 96 81 B5 B4 97 A3
CF E7 B5 DB 51 87 D5 75 9D 2A BB 14 6A 0B 35 2D 1B 89 45 99 38 8C E8 C9 5D 01 C8 16 1D 3F A4
61 7B 59 48 E1 A0 83 87 2D AC 93 3F 23 FA 6F 29 A9 C8 EE B2 8F 2E FA F5 16 85
```

A.3.3.2 Public key

The hexadecimal encoding of an X.509 SubjectPublicKeyInfo /ANSI X9.62 encoded public key:

```
30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48 CE 3D 03 01 07 03 42 00 04 1C 96 81 B5
B4 97 A3 CF E7 B5 DB 51 87 D5 75 9D 2A BB 14 6A 0B 35 2D 1B 89 45 99 38 8C E8 C9 5D 01 C8 16
1D 3F A4 61 7B 59 48 E1 A0 83 87 2D AC 93 3F 23 FA 6F 29 A9 C8 EE B2 8F 2E FA F5 16 85
```

The hexadecimal encoding of a the public key as a COSE key:

```
A4 01 02 20 01 21 58 20 1C 96 81 B5 B4 97 A3 CF E7 B5 DB 51 87 D5 75 9D 2A BB 14 6A 0B 35 2D
1B 89 45 99 38 8C E8 C9 5D 22 58 20 01 C8 16 1D 3F A4 61 7B 59 48 E1 A0 83 87 2D AC 93 3F 23
FA 6F 29 A9 C8 EE B2 8F 2E FA F5 16 85
```

A.4 Generated MSO & COSE_Sign1

A.4.1 MSO

The following MSO is being generated, hexadecimal encoded:

```
D8 18 59 01 D7 A6 67 76 65 72 73 69 6F 6E 63 31 2E 30 6F 64 69 67 65 73 74 41 6C 67 6F 72 69
74 68 6D 67 53 48 41 2D 32 35 36 6C 76 61 6C 75 65 44 69 67 65 73 74 73 A1 6D 6E 6C 2E 72 64
77 2E 6D 65 6B 62 2E 31 A5 00 58 20 52 9A 60 F7 00 3E 5E 53 8E 9F 99 D7 7F CA 5C CB 3A B0 83
B0 7E 2B EA 7A 31 1A 07 B1 E0 90 A9 1E 01 58 20 D6 88 4F 63 4E 34 C9 2E 2C BC 0C D0 DF 83 DC
0C DC 2E FA 77 72 80 EA 14 5C 37 BB 22 17 9C 86 26 02 58 20 4D 55 44 BB D2 13 91 55 8F 1F 9A
36 CB 3B 3D 76 08 ED 87 E0 EB D3 35 13 8D AD DB BB D3 88 E1 61 03 58 20 AB AB 85 3F 0A 22 52
47 42 1C E1 65 B9 78 38 A5 02 C6 81 A9 13 42 EF AF FF 8F 25 51 1D 53 37 61 04 58 20 F9 F5 C6
2E 43 4A 97 BE E7 5A D9 58 FF 8C BB E2 7F 9B 75 F6 D1 D4 34 60 3C A4 2B AA D7 5E 93 23 6D 64
65 76 69 63 65 4B 65 79 49 6E 66 6F A1 69 64 65 76 69 63 65 4B 65 79 A4 01 02 20 01 21 58 20
1C 96 81 B5 B4 97 A3 CF E7 B5 DB 51 87 D5 75 9D 2A BB 14 6A 0B 35 2D 1B 89 45 99 38 8C E8 C9
5D 22 58 20 01 C8 16 1D 3F A4 61 7B 59 48 E1 A0 83 87 2D AC 93 3F 23 FA 6F 29 A9 C8 EE B2 8F
2E FA F5 16 85 67 64 6F 63 54 79 70 65 6D 6E 6C 2E 72 64 77 2E 6D 65 6B 62 2E 31 6C 76 61 6C
69 64 69 74 79 49 6E 66 6F A3 66 73 69 67 6E 65 64 C0 74 32 30 32 31 2D 30 39 2D 30 39 54 30
30 3A 30 30 3A 30 30 5A 69 76 61 6C 69 64 46 72 6F 6D C0 74 32 30 32 31 2D 30 39 2D 30 39 54
30 30 3A 30 30 3A 30 30 5A 6A 76 61 6C 69 64 55 6E 74 69 6C C0 74 32 30 32 32 2D 30 39 2D 30
39 54 30 30 3A 30 30 3A 30 30 5A
```

A.4.2 COSE_Sign1

The following COSE_Sign1 is being generated, hexadecimal encoded:

```
84 43 A1 01 26 A1 18 21 59 02 1F 30 82 02 1B 30 82 01 A1 A0 03 02 01 02 02 10 01 02 03 04 05
06 07 08 00 00 00 00 00 00 00 01 30 0A 06 08 2A 86 48 CE 3D 04 03 03 30 39 31 0B 30 09 06 03
55 04 06 13 02 55 54 31 2A 30 28 06 03 55 04 03 0C 21 55 4C 20 54 45 53 54 20 49 41 43 41 20
56 65 68 69 63 6C 65 20 52 65 67 69 73 74 72 61 74 69 6F 6E 30 1E 17 0D 32 31 30 39 30 37 30
30 30 30 30 31 5A 17 0D 32 32 31 32 30 37 30 30 30 30 30 31 5A 30 37 31 0B 30 09 06 03 55 04
06 13 02 55 54 31 28 30 26 06 03 55 04 03 0C 1F 55 4C 20 54 45 53 54 20 44 53 20 56 65 68 69
63 6C 65 20 52 65 67 69 73 74 72 61 74 69 6F 6E 30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08
2A 86 48 CE 3D 03 01 07 03 42 00 04 20 CD DF 58 24 7D B4 A2 83 E9 2D 91 96 7A EB F5 8C A1 83
2D 5F 2B FD 1C 84 08 AC FE 25 F1 5F B0 E4 B1 F2 1A E2 E7 02 65 4A 0F B3 F8 4A 3E F6 B4 0F B4
47 6B 96 BB B3 10 BB 8A 15 4F EF E2 FA F9 A3 81 8C 30 81 89 30 1F 06 03 55 1D 23 04 18 30 16
80 14 5D 96 AC 21 C9 16 89 F6 ED 36 A1 37 C7 BB E3 8D 8B 3D DD AA 30 1D 06 03 55 1D 0E 04 16
04 14 E2 46 6A 42 BB A3 04 65 21 0B 56 63 A0 2B 21 05 64 8C E5 0C 30 0E 06 03 55 1D 0F 01 01
FF 04 04 03 02 07 80 30 1E 06 03 55 1D 12 04 17 30 15 86 13 68 74 74 70 73 3A 2F 2F 77 77 77
2E 75 6C 2E 63 6F 6D 2F 30 17 06 03 55 1D 25 01 01 FF 04 0D 30 0B 06 09 60 84 10 01 87 72 02
02 01 30 0A 06 08 2A 86 48 CE 3D 04 03 03 03 68 00 30 65 02 31 00 9D 9B D1 D9 9E 90 BE 91 DB
42 65 FA 19 2F 66 7E 59 D5 3E 3A 71 3D 56 D2 53 D8 B5 31 B5 3D 48 64 6F 41 10 59 E1 43 6A 5B
17 36 D7 05 AE 4D 94 53 02 30 2D 4D 97 03 20 8E 80 48 B4 50 EF E8 FF F2 0D 6F 96 B1 9B F3 13
2D 10 B1 10 44 7B BE 06 BB 4D AC 0A 67 70 B0 8E CF 15 74 5A 90 20 67 86 46 F2 F8 59 01 DC D8
18 59 01 D7 A6 67 76 65 72 73 69 6F 6E 63 31 2E 30 6F 64 69 67 65 73 74 41 6C 67 6F 72 69 74
68 6D 67 53 48 41 2D 32 35 36 6C 76 61 6C 75 65 44 69 67 65 73 74 73 A1 6D 6E 6C 2E 72 64 77
2E 6D 65 6B 62 2E 31 A5 00 58 20 52 9A 60 F7 00 3E 5E 53 8E 9F 99 D7 7F CA 5C CB 3A B0 83 B0
7E 2B EA 7A 31 1A 07 B1 E0 90 A9 1E 01 58 20 D6 88 4F 63 4E 34 C9 2E 2C BC 0C D0 DF 83 DC 0C
DC 2E FA 77 72 80 EA 14 5C 37 BB 22 17 9C 86 26 02 58 20 4D 55 44 BB D2 13 91 55 8F 1F 9A 36
CB 3B 3D 76 08 ED 87 E0 EB D3 35 13 8D AD DB BB D3 88 E1 61 03 58 20 AB AB 85 3F 0A 22 52 47
42 1C E1 65 B9 78 38 A5 02 C6 81 A9 13 42 EF AF FF 8F 25 51 1D 53 37 61 04 58 20 F9 F5 C6 2E
43 4A 97 BE E7 5A D9 58 FF 8C BB E2 7F 9B 75 F6 D1 D4 34 60 3C A4 2B AA D7 5E 93 23 6D 64 65
76 69 63 65 4B 65 79 49 6E 66 6F A1 69 64 65 76 69 63 65 4B 65 79 A4 01 02 20 01 21 58 20 1C
96 81 B5 B4 97 A3 CF E7 B5 DB 51 87 D5 75 9D 2A BB 14 6A 0B 35 2D 1B 89 45 99 38 8C E8 C9 5D
22 58 20 01 C8 16 1D 3F A4 61 7B 59 48 E1 A0 83 87 2D AC 93 3F 23 FA 6F 29 A9 C8 EE B2 8F 2E
FA F5 16 85 67 64 6F 63 54 79 70 65 6D 6E 6C 2E 72 64 77 2E 6D 65 6B 62 2E 31 6C 76 61 6C 69
64 69 74 79 49 6E 66 6F A3 66 73 69 67 6E 65 64 C0 74 32 30 32 31 2D 30 39 2D 30 39 54 30 30
3A 30 30 3A 30 30 5A 69 76 61 6C 69 64 46 72 6F 6D C0 74 32 30 32 31 2D 30 39 2D 30 39 54 30
30 3A 30 30 3A 30 30 5A 6A 76 61 6C 69 64 55 6E 74 69 6C C0 74 32 30 32 32 2D 30 39 2D 30 39
54 30 30 3A 30 30 3A 30 30 5A 58 40 C5 39 C6 7A 9D 00 51 CD EF A1 90 49 68 45 30 82 63 A3 D5
53 3F 79 F7 A2 1F 15 89 AB 9C E2 EF 4E 4C 29 1A B8 D0 98 B0 3F 15 F8 3A 89 F3 4C 89 96 60 36
EF DE 7B CF 67 B9 03 32 BD 48 98 6C DD 37
```