**Data demonstration of IDB1-IS**

**Inputs**

**Barcode Identifier**

IDB1

**Barcode Flag**

D – Signed, Compressed

**Header**

**Issuing Country**

ISL

**Signature Algorithm (represented in decimal)**

3 - (0x03) - ECDSA With SHA-512 Hasing Algorithm

**Certificate Reference (represented in hex)**

97A3E9CC0F

**Signature Date**

2023-14-10

**Message Zone**

**MRZ**

IDISLID11112481281075<6089<<<<7510289M2702098ISL<<<<<<<<<<<6THURIDUR<OSP<AEGIRSDOTTIR<<<<<

**Full Name**

ÞURÍÐUR ÖSP ÆGIRSDÓTTIR

**Signature (in hex)**

F93E4ECA282609BB4FE2EDE046AC48A853034AC085FC52795A28636B3F7EF7CD9587240ABEE95EC39CC3E54A919AF2BB56095BB9CAC9C0826096DE2DD94A448B

**Initial encodements**

**Header**

**Issuing Country**

**Before**

ISL

**After Encoding with C40**

8E9A

**Date**

**Before**

2023-14-10

**After Encoding with specialized Date encoding**

009AC147

**MRZ**

**Before**IDISLID11112481281075<6089<<<<7510289M2702098ISL<<<<<<<<<<<6THURIDUR<OSP<AEGIRSDOTTIR<<<<<

**After replacing ‚<‘ with space – and encoding with C40**B5DBD2C1B8218DA3A93CB832755C133C133C133C133C133C133C133C135146575262285CD9C54C6D32FC55574BAA2628133C133C133C133C133DFE31

**Hex representation of the payload structure before tag applicaton**

**ISSUING\_COUNTRY(C40 encoded) + SIGNATURE\_ALGORITHM + CERTIFICATE\_REFERENCE + SIGNATURE\_DATE + MRZ(C40 encoded) + FULL\_NAME(utf8 encoded) + TinyImage + SIGNATURE**

8E9A0397A3E9CC0F009AC1478C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B158E9A133C133C133C1343D1ABC542D95CB41E15038090CAC5D37FC23C133CC39E5552C38DC390555220C396535020C3864749525344C393545449520000000C6A(…)F93E4ECA282609BB4FE2EDE046AC48A853034AC085FC52795A28636B3F7EF7CD9587240ABEE95EC39CC3E54A919AF2BB56095BB9CAC9C0826096DE2DD94A448B

**DER-TLV application:**

8E9A0397A3E9CC0F009AC147**61820439073C**8C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B158E9A133C133C133C1343D1ABC542D95CB41E15038090CAC5D37FC23C133C**AA16**C39E5552C38DC390555220C396535020C3864749525344C39354544952**AB8203D8**0000000C6A(…)**7F40**F93E4ECA282609BB4FE2EDE046AC48A853034AC085FC52795A28636B3F7EF7CD9587240ABEE95EC39CC3E54A919AF2BB56095BB9CAC9C0826096DE2DD94A448B

**General tags used by IS**

**0x61** Message zone  
**0x07** MRZ zone  
**0x7F** Signature Zone  
**0xAA** Full name  
**0XAB** Tiny Image ( not fully included in this example because of size )

**Application process**

**Mrz  
07(tag)+3C(Length)+**8C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B158E9A133C133C133C1343D1ABC542D95CB41E15038090CAC5D37FC23C133C

**Full name  
AA(tag)+16(Length)+**C39E5552C38DC390555220C396535020C3864749525344C39354544952

**TinyImage:   
AB(tag)+8203d8(length)** **0000000C6A**

**Signature  
7F(Tag)+40(Length)+**F93E4ECA282609BB4FE2EDE046AC48A853034AC085FC52795A28636B3F7EF7CD9587240ABEE95EC39CC3E54A919AF2BB56095BB9CAC9C0826096DE2DD94A448B

**Message zone (Last DER-TLV step)**

**61(Tag)+820439(Length)+073C**8C3…AA16C39… AB8203D8000…7F40F93…

**Final Encodement**

**Payload before encodement**



**ZLIB compression applied and then base32 encoded:**



**Front applied(idb1) and padding ‚=‘ removed:**

<https://github.com/GisliRAxels/SkraPub/blob/main/Barcode_img.png>

Download png to test and see end result for yourself.

* Gísli Ragnar Axelsson