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<AEGIRSDO
TTIR<<<<<

TinyImage (represented as hex)

0000000C6A5020200D0A870A00000014667479706A703220000000006A7032200000002D6A703268000000166968647200000000C7000000960001070700000000000000
F636F6C72010000000000110000038B6A703263FF4FFF5100290000000000960000000C7000000000000000000000096000000C700000000000000000000001070101FF5
200C0000001000504040001FF5C0013404048485048485048485048485048485048450FF64002500014372656174646564206279204F70656E4A5045472076657273696F6
E20322E352E30FF90000A00000000030A0001FF93DF4A000F471D59B54D9958F694C30EEC6A1859B678B60B7913951D7EB9F727F027FC65C7CA627D2663E528
0F8F941501EEBF27A56C624E9D0BAB18314CE965373F78C01C89B8FA2D4439BFE7E35A9D6F78896193B241BB017D6A80CC176803A95BB7C48C7908681DA67
1320892B7F389CF95C4F99DC7C6A41AA003588C3FCA13E05A5E96149C951B13C262E033734EF93CA3FD5708C5C631AA1546BEC657F8D89B3D183F9B0FF4B
33E0C045B0B4E9C4C7C94E6DCB519BFCC08EB9B89FEBB630E7334C61E04AB9A156AC71BF4BAEEF5F675A3977E9821C79E79F0768AC5554E60A7C2CF6AD4
74E7F79F7FB92FA54F34167193A7FB4B9D62AF3B8B6098FD6F2B6641AC639E18253D71E97359D139B23671EB53D747CF92F93E3B747C37E08DD338D6F78875
6560ED35F61348C0140ABC9717D6B18D4C4C2C4B9D54B0972ADD50EED8C563DB6970224F4873ABD557FD96D53FBDF35B79CF16493897BCF3C73405FD289
B8E11558AE839611DF1C8A28824538D26712A9DD4B768150C78F6C71575325980B8BE7CF970B936C69A15D460E3DB2C7CEAD2F762FC3D1831051F100A9B98
BCECCACAF36248A9C2EB0B7D3DEFB34B60C4D4AAAB3BE12A648481EC59F4D910F3AF57A48974AB9A0CDBFC7A19304389097204875E30F29243063CEF8ED
83FB3644E2A279F441537DA361C151CBDE39AB9042372E9F4DBC6184694A435B9792CD66B2E5F64D8982BF2EF2B6CCB32336089EF75C98F0BEF5F8B63F508
8E16BF846C4EEFD0C460342E681A6D67FE28F59B57248872E95F402605049C29CCA537021C09A4AE2D65CF87A227C0FC70C043AAFF405F63B6D6E1C5DE6C
14217EEC91896019C7F3BF7C804FAEEF7E0AAF8D903486B4BDEF1302C25B43307C10937EFE54684D0853AB0F0EA8618A43B522465647D56992A5883AEAEE4
6E375231B020D8EA4FB59693295A31B5D68D7BED39A286C1A6EDA45E4E2957A0DBD69ED6CA10574E3F29C7D1BC61F8A54B4DD29B90097545A14C952F047F
540940725DFD581F1D4CFA3C6E3D7F5253C1E96A5D116B5BCFD9E68166FAD41D80A4EC0F480FFD9AA1DC39E5552C38DC390555220C396535020C386474952
5344C39354544952

Full Name

ÞURÍÐUR ÖSP ÆGIRSDÓTTIR

Signature (in hex)

F93E4ECA282609BB4FE2EDE046AC48A853034AC085FC52795A28636B3F7EF7CD9587240ABEE95EC39CC3E54A919A
F2BB56095BB9CAC9C0826096DE2DD94A448B

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<AE
GIRSDOTTIR<<<<<

After replacing ‚<' with space – and encoding with C40
8C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B158E9A133C133C1
33C1343D1ABC542D95CB41E15038090CAC5D37FC23C133C

Hex representation of the payload structure before tag applicaton

ISSUING_COUNTRY(C40 encoded) + SIGNATURE_ALGORITHM + CERTIFICATE_REFERENCE + SIGNATURE_DATE + MRZ(C40 encoded) + TinyImage + FULL_NAME(utf8 encoded) + SIGNATURE

8E9A0397A3E9CC0F009AC1478C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B158E9A133C133C133C1343D1ABC542D95CB41E15038090CAC5D37FC23C133C0000000C6A(…)C39E5552C38DC390555220C396535020C3864749525344C39354544952F93E4ECA282609BB4FE2EDE046AC48A853034AC085FC52795A28636B3F7EF7CD9587240ABEE95EC39CC3E54A919AF2BB56095BB9CAC9C0826096DE2DD94A448B

DER-TLV application:

8E9A0397A3E9CC0F009AC147**61820439073C**8C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B158E9A133C133C133C1343D1ABC542D95CB41E15038090CAC5D37FC23C133C**AB8203D8**0000000C6A...**AA1D**C39E5552C38DC390555220C396535020C386474 9525344C39354544952**7F40**F93E4ECA282609BB4FE2EDE046AC48A853034AC085FC52795A28636B3F7EF7CD9587240ABEE95EC39CC3E54A919AF2BB56095BB9CAC9C0826096DE2DD94A448B

General tags used by IS

0x61 Message zone
0x07 MRZ zone
0x7F Signature Zone
0xAA Full name
0XAB Tiny Image

Application process

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

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

Full name
AA(tag)+1d(Length)+C39E5552C38DC390555220C396535020C3864749525344C39354544952

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

Message zone (Last DER-TLV step)

61(Tag)+820439(Length)+073C8C3…AA16C39… AB8203D8000…7F40F93…

Final Encodement

Payload before encodement

8E9A0397A3E9CC0F009AC14761820439073C8C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B158E9A133C133C13
3C1343D1ABC542D95CB41E15038090CAC5D37FC23C133CAB8203D80000000C6A5020200D0A870A00000014667479706A70322000000000
6A7032220000000026A70326800000016696864720000000C70000009600010707000000000F636F6C7201000000000110000038B6A703263F
F4FFF51002900000000000096000000C700000000000000000000000096000000C700000000000000000000001070101FF52000C0000000100050404000
1FF5C0013404048485048485048484850484850FF64002500014372656174657220627920A5045472076657273696F6E20322E
352E30FF90000A00000000030A0001FF93DF4A000F471D59B54D9958F694C30EEC6A1859B678B60B7913951D7EB9F727F027FC65C7CA627
D2663E5280F8F941501EEBF27A56C624E9D0BAB18314CE965373F78C01C89B8FA2D4439BFE7E35A9D6F78896193B241BB017D6A80CC17
6803A95BB7C48C7908681DA671320892B7F389CF95C4F99DC7C6A41AA003588C3FCA13E05A5E96149C951B13C262E033734EF93CA3FD5
708C5C631AA1546BEC657F8D89B3D183F9B0FF4B33E0C045B0B4E9C4C7C94E6DCB519BFCC08EB9B89FEBB630E7334C61E04AB9A156A
C71BF4BAEEF5F675A3977E9821C79E79F0768AC5554E60A7C2CF6AD474E7F79F7FB92FA54F34167193A7FB4B9D62AF3B8B6098FD6F2B6
641AC639E18253D71E97359D139B23671EB53D747CF92F93E3B747C37E08DD338D6F788756560ED35F61348C0140ABC9717D6B18D4C4C
2C4B9D54B0972ADD50EED8C563DB6970224F4873ABD557FD96D53FBDF35B79CF16493897BCF3C73405FD289B8E11558AE839611DF1C8
A28824538D26712A9DD4B768150C78F6C71575325980B8BE7CF970B936C69A15D460E3DB2C7CEAD2F762FC3D1831051F100A9B98BCEC
CACAF36248A9C2EB0B7D3DEFB34B60C4D4AAAB3BE12A648481EC59F4D910F3AF57A48974AB9A0CDBFC7A19304389097204875E30F292
43063CEF8ED83FB3644E2A279F441537DA361C151CBDE39AB9042372E9F4DBC6184694A435B9792CD66B2E5F64D8982BF2EF2B6CCB323
36089EF75C98F0BEF5F8B63F5088E16BF846C4EEFD0C460342E681A6D67FE28F59B57248872E95F402605049C29CCA537021C09A4AE2D6
5CF87A227C0FC70C043AAFF405F63B6D6E1C5DE6C14217EEC91896019C7F3BF7C804FAEEF7E0AAF8D903486B4BDEF1302C25B43307C1
0937EFE54684D0853AB0F0EA8618A43B522465647D56992A5883AEAEE46E375231B020D8EA4FB59693295A31B5D68D7BED39A286C1A6E
DA45E4E2957A0DBD69ED6CA10574E3F29C7D1BC61F8A54B4DD29B90097545A14C952F047F540940725DFD581F1D4CFA3C6E3D7F5253C
1E96A5D116B5BCFD9E68166FAD41D80A4EC0F480FFD9AA1DC39E5552C38DC390555220C396535020C3864749525344C393545449527F40
F93E4ECA282609BB4FE2EDE046AC48A853034AC085FC52795A28636B3F7EF7CD9587240ABEE95EC39CC3E54A919AF2BB56095BB9CAC9
C0826096DE2DD94A448B

ZLIB compression applied and then base32 encoded:

PCOOXG6FHR67DSZT7QGLGDV2E43LCWFS3P2NRH76T7G2PQDP7RGD2TPKSBEKQL4PWCGZXHXE37IHBV3UNHI34WOCGZQOQ7DR6VI
2PGZRLPSEJGI3E2ODU6VZ7YIFA5DVCPZQ2BQGA2PKYAAFAVPK45ROEBNSJLNEWIQKXQCIAHEGNAGSXJADUA2IRNSWNJAUAHU6GQB
4RWAZDHI5USDICPZZH6TYQEOMCRSGAYHOAYVE57XP747ZAQITFQ3A3KQBAZIPTDHMRSGP7AYYPBAEYBSWCYLANRX7GEGMEDQOD
YPADSHIP4FIGKQDUNZVC2TCJFVIUQSSUWBH6QLKTZLYBK53IJMWUULRMZ7J5AURT2UZ5QP7BEGCAPZQGBZQDTMZPTPYXAO7LU3HF
K7PZSEG6UYO6O64TEUI3RLLDDN3KJ4KU3G5Z3X6UH6U76SB4P4VKSVZN7CUQO7X7CRI4O5732SLOOJPZZTSV6LDB5DZTFVG4X3RICTH
HRZPLUL4X7OPD5D43TNP5BGJZPGJOE3WG3KWYMM7CDHGSXI5XD7UKRZGJSBOFM2OFGFU7VZ6P6NJI57M4PL6NSE5IAXGRAPPWU6
CB6ROFJUJZSMSULL4FDUYC4NR35HZXRL7YM4Y4HRTLQS6VNXPLD4I6G5TNUS6YZ7TP7MWZR6DCLG62N6HU5TMVMZ3LMS7PH7BPA6
3X4675ZSL4YUTMNZCZK3HRFTB3F76WLV53V3PUWF2PV6NKA6D5L7SINM5PUKQX6COLB6OM5OSS6P6PV7P2TX5UX7CMYUFSOL775U6
TO2N5OR3MHDN67HNGTDTLSPTERKG2C27CZDV5NG4MRLPQOXYXL57SSJ75WWEW2WMD72F5NVY6262GNBV4GW6SN3BR4BSEXD3U
2FV7W6Y5PR2HYZ5G5SMG5FNXMA663Q4JW7J2WNA4TXVDPH2NL4N62KX5X3X5DVOHQX6M2JRPXH6PYZGVR7TKZXXBGDHNPNQJSKP
26DCKGDUU4FPLKQ5NXBL3MZUI6JKXYOROLJVRJWNRMNP4ZT4CTVTMOZUJLZEHS7K2U7T5LJPPJB7WYJINLHSAJOLGZ7MPFZ6VVHHE
SHZLB26OPL5VPW75SOXBZGKVLK5MD5VKJNBVX2EP24ST4DZPX4JFTUS2WZXQ3X7VGJDI4HO4QWGE2MPGP4DJSMZZXTH3XYN7PGSS
7S25LZV2RGNN6M4TCGK5R6TY2ZHRNZNDSZPW6HUTOCNLFRLVM2S45NLMXT4ZKGRTWU73ZV6PHBWGJHOQ7C7PKZJ7635PR37EV4O
H2Y72LJZP3XS6HCJGDI4XEGKJX72P4LVO24EUR6RZN4AONKWSY4ZUZ4WTIZ4S4BOLGTZW6V6PWI7VAJ7AUDZYV75O6EE7XTW5XQ5C6
ZZEKFHK3ZGOYTEQHX7XS72NQL73X5TVLXVXUJUZWVV5R6S7TDUFDNNTICGMBZN3P4QBRPY5YGV7R6CWEV3TS3SVOMFXFP43HFU
WTB6VVJ3W7D2LSWSJS6H2S36I5TBUTK5FQOZW4L537SVSGRZKJ43OXE7HSNFVRN3G7ZW3TSC22JMPH7G2RFB7E7PBLMXEV3TE7B7J
EBISGJUCH64X45EYYKXXV73L4PDSXZYXDZ5X37FLVKGN3NNFC3CLP37ZHMXEGLL7VXRA2L57AJPBX7W7LUSHU6C6NHIODX6CCNBIEFI
PJYFA4UBY3TT64GAU5RZHQ4SJRBTVDPODJ4534UQ2NOO3X7I7XR6OBN6HMJCTDM6WQHLT6QMUKEN4RWPXOXPM6T3NK3Q5V5RS53
YZ3Q2OXQTM565UHOGDG67HVGJANGQTU7O5HPPI4XJAYAIS7XWRI======

Front applied(idb1) and padding ,=' removed:

Code snippet and additional info on github:

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

Download png to test and see end result barcode.

- Gísli Ragnar Axelsson