

Data demonstration of IDB1-IS

Barcode Identifier

3.1.1 Barcode Identifier

The barcode Identifier MUST be in 4 characters by concatenating 'IDB' and version character of the barcode structure. The version of the barcode structure of this document is '1'. Therefore, the Barcode Identifier is 'IDB1'.

IDB1

Barcode Flag

3.1.2 Barcode Flag

The Barcode Flag is a 1 byte value that is used for storing bit value (true or false) of the Barcode Payload. The Barcode Flag is computed by getting the Barcode Bit Value and adding a constant value of 0x41 to it. The Barcode Bit Value is a 4 bit value, 2 bits are used in this document and 2 bits are reserved for future use. The least significant bit is used for "IsSigned".

- "1" means message is signed

- "0" means message is not signed

The second least signification bit is used for "IsCompressed". (Refer to section 3.1.4 below)

- "1" means barcode is compressed

- "0" means barcode is not compressed

D - Signed, Compressed

Header

Issuing Country

3.2.1 Country Identifier

A three-letter code identifying the issuing State or organization. The three-letter code is according to Doc 9303-3

ISL

Signature Algorithm

3.2.2 The signature algorithm used to produce the signature. Signatures MUST be created using ECDSA. Elliptic Curve Signature Algorithm (ECDSA) with a key length of at least 256 bit in combination with SHA-256 is a MUST.

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

Certificate Reference (represented in hex)

3.2.3 The Certificate reference value will be the last 5 bytes of the SHA1 Hash of the DER encoded Signer Certificate.

C7FC28A147

Signature Creation Date

3.2.4 The date when the signature was created

2024-01-03 (First of march)

Message Zone

3.3 Following the header is the message zone. The message zone **MUST** use the Barcode Information Group Template which allows the possibility to store different message types simultaneously. The Barcode Information Group Template **MUST** be encoded use DER-TLV.

MRZ

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

/

IDISLID11112481281075<6089<<<<<7510289M2702098ISL<<<<<<<<<<<6TH
URIDUR<OSP<AEVARSDOTTIR<<<<<<

Full Name

ÞURÍÐUR ÖSP ÆVARSDÓTTIR

TinyImage (represented as hex) (Originally in base-64)

00000000c6a5020200d0a870a00000014667479706a703220000000006a70322000000002d6a70326800000016696864
72000000780000005a0001070701000000000f636f6c7201000000000011000000006a703263ff4fff510029000000
00005a0000007800000000000000000000005a00000078000000000000000001070101ff52000c00010001000304
040000ff5c0017425f355f4c5f4c5f644803480348454fd24fd24f61ff90000a0000000003030001ff93cfadfc13ff
7f456e82b11c826ff20bbcd058cf767e531230f5b9c08d5de214d83cc940457d9b295798ed76ab0b3a11c95b79d8c
edc96df5802cf4b4c87415290cca36fb6fe3b68d27c85cc2b7bfcad49bd41657e7eb5d540552192d032465df5185f9
65c52579f324069b46915c00fb4daaf73abfe96a8f7b4976e26cca61944bcac7d1478fa29507c4d4c35f49b7c6e3a4
6ef546ea547548fce7bbb0331e52fa1d9bd01fbdef28f12bec180a48ab9b885d57c60ae3e0e9f91a7f2906fe05e1fc
7f007ae1bf3fdf4e7dc4021445f05b28cc975d41d07cd836f83d8980100ef6b6083e0c77fd1e470d7f7546f727ad8b
c14ddb2c35ff529b94c2c8967d3d926bb27ee3d2f0f9521abb957c46711531786c169f4cfd372a3c9270c66c82ebf1
a08e1d88f2e33fd0dc0bc6f157f3ddd4603efcc7b1653fa0c6b16bc02492053671ada3f824be7441ca104c0423525b
863fa4c7c5758f8ac50f82c8b24cf7422473258338bb132e200aa812bc2711f1ad032de7e1cb03e7fb108ae9c06793
755ddb3fbalb82c9668e16c66f851d1960ec420fea926bf42bb504d177d30e679bf821989891916901c3a77b24cfac
142fc127da18857afac0cc35cb1dcf92673d47483be66f967b3f22e76c994cdb978230bb56bdd1e472bd9638388e03
f553859f1358b5528bbf40c7516c57a5c5205c5fbc3655ea8a8e309d61d3060d3b9f9c9ab9d95b422542b3176e7b4d
4b990481b4f74d44766abc3eb4973dc7b4f7f3c5a777a2d65db871b3251b10b0c1de28b3caaa832a05a75cdec812df
4007ef601fa44cd48f106209d414d57893041aab9edee0d7562ab934a30226538589ac51441a24d12dddc3e0bd87c1
a700f11a8799eb7707331ba83390889f516a795c33debb7bd23dc41012f21c5ccaaba794badf4d538721c071fc1d4d
57e233e1fd39b0c3c5462b929a4fec81e68f7225f0db6012b273baa5981ad420a29d117f076d77cdaca3742104714d
aa592fc3041e7eff2e5a5d715c36906ce1030d6ee05b630d47f4c260a90c2dc923dc5a736f4bab6dbbaa3680547573
ffd9

Signature (in hex)

005d4e47ce55dbac04a01290fef991e557bac36c198a4c2615e68efbf5e882
92c59c87dc9eedcf56a7081d8715720e9566ef85f0b6a6e9dde74939b9863e
8bad53ab002f1952571e7a60f0bc677b55348daf3b5d9d88e31d57efc392e1
a098623e78a6ff5abb37210b3771e7bcad2be53ddfc17e79718eb44b9dd042
f5ff7d5118aeb95b

Initial encodements

Header

Issuing Country

Before

ISL

After C40 encoding, represented in hex

8E9A

Date

Before

2023-03-01

After Encoding with specialized Date encoding

002df5b8

Encoding date; 2024-03-01 13:37:00

converted: 03012024

Encoded date in hex format: 002df5b8

length of date byte: 4

Message Zone

MRZ

Before

IDISLID11112481281075<6089<<<<7510289M2702098ISL<<<<<<<<<<6TH
URIDUR<OSP<AEGIRSDOTTIR<<<<<

After replacing ,<' with space – and encoding with C40

8c3fcbff6b0e200f33e627661ac214554d0c133c462e19fd555745671b158e
9a133c133c133c1343d1abc542d95cb41e1503dd10cac5d37fc23c133c

Full name

Þuríður Ösp Ævarsdóttir

hexed

c39e7572c3adc3b0757220c396737020c3867661727364c3b374746972

Hex representation of the payload structure before tag applicaton

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

```
8E9A03C7FC28A147002DF5B88C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B158E9A133C13
3C133C1343D1ABC542D95CB41E1503DD10CAC5D37FC23C133CC39E7572C3ADC3B0757220C396737020C38676617273
64C3B37474697200000000C6A5020200D0A870A00000014667479706A703220000000006A70322000000002D6A703268
0000001669686472000000780000005A0001070701000000000F636F6C72010000000000110000000006A703263FF4F
FF5100290000000005A00000078000000000000000000000005A000000780000000000000000001070101FF52000C
00010001000304040000FF5C0017425F355F4C5F4C5F644803480348454FD24FD24F61FF90000A00000000003030001
FF93CFADFC13FF7F456E82B11C826FF20BBCDD058CF767E531230F5B9C08D5DE214D83CC940457D9B295798ED76AB0
B3A11C95B79D8CEDC96DF5802CF4B4C87415290CCA36FB6FE3B68D27C85CC2B7BFCAD49BD41657E7EB5D540552192D
032465DF5185F965C52579F324069B46915C00FB4DAAF73ABFE96A8F7B4976E26CCA61944BCAC7D1478FA29507C4D4
C35F49B7C6E3A46EF546EA547548FCE7BBB0331E52FA1D9BD01FBDEF28F12BEC180A48AB9B885D57C60AE3E0E9F91A
7F2906FE05E1FC7F007AE1BF3FDF4E7DC4021445F05B28CC975D41D07CD836F83D8980100EF6B6083E0C77FD1E470D
7F7546F727AD8BC14DDB2C35FF529B94C2C8967D3D926BB27EE3D2F0F9521ABB957C46711531786C169F4CFD372A3C
9270C66C82EBF1A08E1D88F2E33FD0DC0BC6F157F3DDD4603EFCC7B1653FA0C6B16BC02492053671ADA3F824BE7441
CA104C0423525B863FA4C7C5758F8AC50F82C8B24CF7422473258338BB132E200AA812BC2711F1AD032DE7E1CB03E7
FB108AE9C06793575DDB3FBA1B82C9668E16C66F851D1960EC420FEA926BF42BB504D177D30E679BF8219898919169
01C3A77B24CFAC142FC127DA18857AFAC0CC35CB1DCF92673D47483BE66F967B3F22E76C994CDB978230BB56BDD1E4
72BD9638388E03F553859F1358B5528BBF40C7516C57A5C5205C5FBC3655EA8A8E309D61D3060D3B9F9C9AB9D95B42
2542B3176E7B4D4B990481B4F74D44766ABC3EB4973DC7B4F7F3C5A777A2D65DB871B3251B10B0C1DE28B3CAAA832A
05A75CDEC812DF4007EF601FA44CD48F106209D414D57893041AAB9EDEE0D7562AB934A30226538589AC51441A24D1
2DDDC3E0BD87C1A700F11A8799EB7707331BA83390889F516A795C33DEBB7BD23DC41012F21C5CCAABA794BADF4D53
8721C071FC1D4D57E233E1FD39B0C3C5462B929A4FEC81E68F7225F0DB6012B273BAA5981AD420A29D117F076D77CD
ACA3742104714DAA592FC3041E7EFF2E5A5D715C36906CE1030D6EE05B630D47F4C260A90C2DC923DC5A736F4BAB6D
BBAA3680547573FFD9005D4E47CE55DBAC04A01290FEF991E557BAC36C198A4C2615E68EFBF5E88292C59C87DC9EED
CF56A7081D8715720E9566EF85F0B6A6E9DDE74939B9863E8BAD53AB002F1952571E7A60F0BC677B55348DAF3B5D9D
88E31D57EFC392E1A098623E78A6FF5ABB37210B3771E7BCAD2BE53DDFC17E79718EB44B9DD042F5FF7D5118AEB95B
```

DER-TLV application

General tags used by IS

0x61 Message zone

0x07 MRZ zone

0xAA Full name

0xAB Tiny Image

0x7F Signature Zone

8E9A03C7FC28A147002DF5B86182040F073C8C3FCBFF6B0E200F33E627661AC214554D0C133C462E19FD555745671B
158E9A133C133C133C1343D1ABC542D95CB41E1503DD10CAC5D37FC23C133CAA1DC39E7572C3ADC3B0757220C39673
7020C3867661727364C3B374746972AB8203AE0000000C6A502020D0A870A00000014667479706A70322000000000
6A7032200000002D6A7032680000001669686472000000780000005A0001070701000000000F636F6C720100000000
0011000000006A703263FF4FFF51002900000000005A00000078000000000000000000000005A000000780000000000
000000001070101FF52000C00010001000304040000FF5C0017425F355F4C5F4C5F644803480348454FD24FD24F61
FF90000A0000000003030001FF93CFADFC13FF7F456E82B11C826FF20BBCDD058CF767E531230F5B9C08D5DE214D83
CC940457D9B295798ED76AB0B3A11C95B79D8CEDC96DF5802CF4B4C87415290CCA36FB6FE3B68D27C85CC2B7BFCAD4
9BD41657E7EB5D540552192D032465DF5185F965C52579F324069B46915C00FB4DAAF73ABFE96A8F7B4976E26CCA61
944BCAC7D1478FA29507C4D4C35F49B7C6E3A46EF546EA547548FCE7BBB0331E52FA1D9BD01FBDEF28F12BEC180A48
AB9B885D57C60AE3E0E9F91A7F2906FE05E1FC7F007AE1BF3FDF4E7DC4021445F05B28CC975D41D07CD836F83D8980
100EF6B6083E0C77FD1E470D7F7546F727AD8BC14DDB2C35FF529B94C2C8967D3D926BB27EE3D2F0F9521ABB957C46
711531786C169F4CFD372A3C9270C66C82EBF1A08E1D88F2E33FD0DC0BC6F157F3DDD4603EFCC7B1653FA0C6B16BC0
2492053671ADA3F824BE7441CA104C0423525B863FA4C7C5758F8AC50F82C8B24CF7422473258338BB132E200AA812
BC2711F1AD032DE7E1CB03E7FB108AE9C06793575DDB3FBA1B82C9668E16C66F851D1960EC420FEA926BF42BB504D1
77D30E679BF821989891916901C3A77B24CFAC142FC127DA18857AFAC0CC35CB1DCF92673D47483BE66F967B3F22E7
6C994CDB978230BB56BDD1E472BD9638388E03F553859F1358B5528BBF40C7516C57A5C5205C5FBC3655EA8A8E309D
61D3060D3B9F9C9AB9D95B422542B3176E7B4D4B990481B4F74D44766ABC3EB4973DC7B4F7F3C5A777A2D65DB871B3
251B10B0C1DE28B3CAA832A05A75CDEC812DF4007EF601FA44CD48F106209D414D57893041AAB9EDEE0D7562AB934
A30226538589AC51441A24D12DDDC3E0BD87C1A700F11A8799EB7707331BA83390889F516A795C33DEBB7BD23DC410
12F21C5CCAABA794BADF4D538721C071FC1D4D57E233E1FD39B0C3C5462B929A4FEC81E68F7225F0DB6012B273BAA5
981AD420A29D117F076D77CDACA3742104714DAA592FC3041E7EFF2E5A5D715C36906CE1030D6EE05B630D47F4C260
A90C2DC923DC5A736F4BAB6DBBAA3680547573FFD97F8184005D4E47CE55DBAC04A01290FEF991E557BAC36C198A4C
2615E68EFBF5E88292C59C87DC9EEDCF56A7081D8715720E9566EF85F0B6A6E9DDE74939B9863E8BAD53AB002F1952
571E7A60F0BC677B55348DAF3B5D9D88E31D57EFC392E1A098623E78A6FF5ABB37210B3771E7BCAD2BE53DDFC17E79
718EB44B9DD042F5FF7D5118AEB95B

Application process

(tag) + (Length) + Content

Mrz

07+3C+8C...

Full name

AA+1D+C3...

TinyImage:

AB+8203AE+0000000C6A...

Signature

7F+8184+005...

Message zone (Last DER-TLV step)

61+82040F+073C8C...

Final Encodement

Payload before encodement

8e9a03c7fc28a147002df5b86182040f073c8c3fcbff6b0e200f33e627661ac214554d0c133c462e19fd555745671b
158e9a133c133c133c1343d1abc542d95cb41e1503dd10cac5d37fc23c133caa1dc39e7572c3adc3b0757220c39673
7020c3867661727364c3b374746972ab8203ae0000000c6a5020200d0a870a00000014667479706a7032200000000
6a7032200000002d6a7032680000001669686472000000780000005a0001070701000000000f636f6c720100000000
0011000000006a703263ff4ffff5100290000000005a00000078000000000000000000000005a000000780000000000
0000000001070101ff52000c00010001000304040000ff5c0017425f355f4c5f4c5f644803480348454fd24fd24f61
ff90000a0000000003030001ff93cfadfc13ff7f456e82b11c826ff20bbcd058cf767e531230f5b9c08d5de214d83
cc940457d9b295798ed76ab0b3a11c95b79d8cedc96df5802cf4b4c87415290cca36fb6fe3b68d27c85cc2b7bfcad4
9bd41657e7eb5d540552192d032465df5185f965c52579f324069b46915c00fb4daaf73abfe96a8f7b4976e26cca61
944bcac7d1478fa29507c4d4c35f49b7c6e3a46ef546ea547548fce7bbb0331e52fa1d9bd01fbdef28f12bec180a48
ab9b885d57c60ae3e0e9f91a7f2906fe05e1fc7f007aeb1bf3fdf4e7dc4021445f05b28cc975d41d07cd836f83d8980
100ef6b6083e0c77fd1e470d7f7546f727ad8bc14ddb2c35ff529b94c2c8967d3d926bb27ee3d2f0f9521abb957c46
711531786c169f4cfd372a3c9270c66c82ebf1a08e1d88f2e33fd0dc0bc6f157f3ddd4603efcc7b1653fa0c6b16bc0
2492053671ada3f824be7441ca104c0423525b863fa4c7c5758f8ac50f82c8b24cf7422473258338bb132e200aa812
bc2711f1ad032de7e1cb03e7fb108ae9c06793575ddb3fba1b82c9668e16c66f851d1960ec420fea926bf42bb504d1
77d304e579bf821989891916901c3a77b24cfac142fcl127da18857afac0cc35cb1dcf92673d47483be66f7b7b3f2e7
6c994cdb978230bb56bdd1e472bd9638388e03f553859f1358b5528bbf40c7516c57a5c5205c5fbc3655ea8a8e309d
61d3060d3b9f9c9ab9d95b422542b3176e7b4d4b990481b4f74d44766abc3eb4973dc7b4f7f3c5a777a2d65db871b3
251b10b0c1de28b3caaa832a05a75cdec812df4007ef601fa44cd48f106209d414d57893041aab9edee0d7562ab934
a30226538589ac51441a24d12dddc3e0bd87c1a700f11a8799eb7707331ba83390889f516a795c33debb7b7b3f2e7
12f21c5ccaaba794badf4d538721c071fc1d4d57e233e1fd39b0c3c5462b929a4fec81e68f7225f0db6012b273baa5
981ad420a29d117f076d77cdaca3742104714daa592fc3041e7eff2e5a5d715c36906ce1030d6ee05b630d47f4c260
a90c2dc923dc5a736f4bab6dbbaa3680547573ff97f8184005d4e47ce55dbac04a01290fef991e557bac36c198a4c
2615e68efbf5e88292c59c87dc9eedcf56a7081d8715720e9566ef85f0b6a6e9dde74939b9863e8bad53ab002f1952
571e7a60f0bc677b55348daf3b5d9d88e31d57efc392e1a098623e78a6ff5abb37210b3771e7bcad2be53ddfc17e79
718eb44b9dd042f5ff7d5118aeb95b

ZLIB compression applied → base32 encodement → Depadding:

PDNOXG6FPT6I7RSCO4DN3LZ3CKNVR6GZNV5OYT77Z7TFHYBXP2TJ4JTVJASNJF2H3DDE2T7SN5ULQ252WRUN6LDBDMYHJP
VY7KUNHTMYFVZKFTDXAVHB3PK4P4ECROSK63YLZUVCYVNVQ63ZIFVJDQPFNXXBAOC4C3LFRFC4OK4HGSKJMZIWVZXGGXGEYD
B4DEAUUCR4DSWVZQDWJCNEZSKBKZAVDAUQBWAOKNMBOSDFAFULBTEOSQQSCXABYRIA2DHHM5SGSARP5ZH4TQRTDCSACGVST
6N7737ECBSMWBMKBKVCBSQ7GGOZDEM76BRQ6AYDCAZBGFMQWA6C7YMQO4FHPDJXQHRBJTYGAB2DK77EUQE7B7QEA6IQAG
MZTANRX7SPH277JD7S754NNPNGRUYU76E7XD252ZPO7KOPZVKT7I7HWDH2Z5ITP6OMSSLHBG4U3U3LPMXOPLKYPTIKM2TW
7H626D3GP3WVA6PS4WCMS2FGR4U7GH5Z2733LKW7RC43IPN7NHV3GL4IQW736HK3AINOIKILVTLJLP3QGW76UUVJLH6V3
BTLWMTMMH4G307KXPK75F6Z7VKZ5ZMPOLHCKTTRH32XYIX374RKT3GHVYOI456473WHDEV4V7XK6QWKHV7DZX5YHMK42A
X5TWIX4T335V7YVD6UNAWLMP26ZDWY6BRVZDY7XT6CSVNPZH3I75PBT55INKUH7PW6766VDZQRE4P5CCWXCZT2VTRYLGQ3
MY7WYOY3AT4L43PDWDRST7ZL47HFWX7K6ZOX23PXIHP5WOVG76BWM7Z2ZORRFVLPNUTWE25MPF567QGJEVW5WVDK3UGUGCR
MO3B6J7P7GLI3JGCUO4U2L37VYUBH3NY6TMP5QW55YR56QZ73465FIFXM74MNVH3IXDTN2Q7KAMUJKWWPB3LCT6VHWSU4J
4EXQMF1Q5CTOWNPXF7DINF75OUP6UYJZW7F6HOURJKZWLWPBWNVST4BNCNDCHLXYOGWTG3XTQ6T2TH77S3UHV6JAPVZHQ3D
N7NO5ETNHKN5MJDJXFW7FMVJR4OHRH7NJJPWF7NVUWBPSPZ6OS477VBHBR4NREJTTGGIPF2XVOOF6I5CP5IP3FSENPK26A3H
JRH4XHU7SRXOX3TB7UWH6WVXXJPHHEZH232ONY25QHNV67RJHI542IWCZ64YX4DLPTQWR3MBXVN533QHGYCO7HJGKCR6
B5M2Q27OX2BTTCMXTG4O2Z4P3H23HJXUKOVJHJXRPTVJ632Z5SGRXPT3XLKKLLLR3OZN2NXY23XZ7T5OV4PTI3LWASQWNV
LJIFGYOLZJ5R7HKKUZRN23STD52OBDOXOYD7T4QL7RHHJK7UAEXHCWI2WFM7LGSFNT5367QHVGGWJ2J4KTDKYGWZ22YCLW
SFILXK3Y67YYDP7PA6KDA7UXNGPPROM43ZMXTBHSQWG7TAKZSYZ4N53XKZO3EPBAEH3EUJHG2XV6MULX3X3A63CUHRJ7UR
6UGX6ZH46CX6LBWDI7O3IJ6N6J75H6FMX5EPLQ7NASQU3RN3S3HJBOVCWBUK4YB5PNXPTWJVRNFRIRIWKPVVLUL2Q7M2I2X6
5PC4KVGWDDGYQ6OIJTN7PIH2DEL33S7BYSK3ZORHSUXYJVLHHPXU5HP5ZKWODJBUXC7436WG23DBRP3XGPPQXP5Q5SIBUM
FP47COPYN3Z2TQR5TZNDE35KZ37X24LU3E4OZZU36M7P5X43BZI4WLW2ERL4KPJ55N363C3OZZO546PJMO635S5NOBVP3
IJODAKS6VUV6FQE66TVVFEO66XL3G4R3D3FYPPB5HXVODAI2JF3RNS75I3XTIVXHGXQX7PLGV73VHW73A3VSWCXW544ZP
HB672XY3FCYW4ZZUABAK2DZY

Prefix and flag applied (IDB1+D) and barcode generated.

Code snippet and additional info on github:

<https://github.com/GisliRaxels/SkraPub/blob/main>

Download png to test and see end result barcode.

- Gísli Ragnar Axelsson