MACHINE READABLE TRAVEL DOCUMENTS TECHNICAL REPORT

Digital Travel Credentials (DTC)

Physical Component and Protocols

Version – 1.1 | October 2022

ISO/IEC JTC1 SC17 WG3/TF5

FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

Release Control

Release	Date	Description
0.01	Oct 2020	Initial Draft setting parameters for PC specifications
0.02	Nov 2020	Initial editors review and framework
0.03	Nov 2020	TF2 review
0.04	May 2021	Re-write to new structure
0.05	July 2021	Include contributions on NFC BLE handover, provisioning and re-using the mDL interface
0.06	Aug 2021	Outcome from NTWG policy group meeting. Moved BLE, provisioning and re-using mDL interface into a separate document for discussion
0.07	Mar 2022	Outcome from WG3/NTWG meetings Oct2021
0.08	May 2022	Outcome from WG3/NTWG meetings April 2022
1.0	September 2022	Outcome from WG3 TF meeting July 2022
1.1	Oct 2022	Outcome from WG3 Plenary meeting October 2022

R Rajeshkumar	Singapore	Auctorizium
Mark Stafford	USA	Infineon

Table of contents

1. Scope

This document specifies the Physical Component (PC) of the Digital Travel Credentials (DTC) and the associated interface to Inspection Systems.

These specifications are developed in accordance with decisions made by the Digital Travel Credential (DTC) Policy Sub-Group of the International Civil Aviation Organization (ICAO) New Technology Working Group (NTWG). Current agreed DTC policy outlines equivalent authenticity and integrity to the eMRTD, backwards compatibility and minimal disruption to existing border inspection systems as key tenets for specification development. Therefore, the intent of this version of the specification – which is the outcome of the phase 1 of this work - is to replicate the interactions as they currently occur between an eMRTD and the Inspection System. Design requirements for specific form factors were not considered for this first version of this specification. Therefore this first version does not specifically address implementation, usability and privacy issues for any form factor. As policy and technical options are explored further, future versions of this specification are anticipated to add additional DTC-PC physical transport protocols, and may introduce changes that breach backwards compatibility with this current version

1.1 Terminology

1.1.1 Technical report terminology

The key words "MUST", “MUST NOT”, "SHALL", “SHALL NOT”, "REQUIRED", "SHOULD", “SHOULD NOT”, "RECOMMENDED", "MAY", and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119]. The key word "CONDITIONAL" in this document is to be interpreted as described in [Doc 9303] part 1.

In case OPTIONAL features are implemented, they MUST be implemented as described in this Technical Report.

1.1.2 Terms and Definitions

Term	Definition
DTC	**Digital Travel Credential – Travel Credentials issued in a Digital Format**
DTC-VC	**DTC Virtual Component is a digital representation of the holder’s identity**
DTC-PC	**DTC Physical Component which has a cryptographic link to the DTC-VC**
eMRTD bound DTC	**A DTC no additional DTC-PC other than an underlying eMRTD**
eMRTD-PC bound DTC	**A DTC with an additional DTC-PC apart from the underlying eMRTD**
PC bound DTC	**A DTC where only a DTC-PC exists and there is no underlying eMRTD**
DTC Signer	**An entity that digitally signs the DTC-VC**

2. Overview of the DTC-PC

2.1 DTC Approach

The DTC consists of a DTC–VC (Virtual Component) and a DTC-PC (Physical Component). DTC-VC is a file that is stored on any medium and does not have any inherent access protection on its contents. In the case where an associated DTC-PC is issued, there will be a cryptographic link between the DTC-VC and the DTC-PC. The DTC-VC is stored on the DTC-PC, and will have access control as defined in this Technical Report.

There are two possibilities for the contents of the DTC-VC:

The contents of the DTC-VC may be identical to the LDS and SOD of an existing eMRTD;

The DTC-VC may be issued without any relation to an existing eMRTD, but with a relationship to a DTC-PC.

Based on the above, the following three types of DTC are defined:

eMRTD bound –no additional DTC-PC other than an underlying eMRTD;

eMRTD-PC bound – there exists an additional DTC-PC apart from the underlying eMRTD;

PC bound – there is no underlying eMRTD, only a separate DTC-PC.

The DTC-VC that is common to all three types of DTCs has been specified in [DTC-VC]. This technical report specifies the Physical Component (PC), which is relevant for the implementation of the eMTRD-PC bound and PC bound DTC types, and not the eMRTD bound DTC.

2.2 Interaction between DTC-PC and Inspection System (IS)

If the Inspection System is to support a DTC, then it should be able to differentiate between an eMRTD and a DTC-PC, when presented with either. For eMRTDs, the first file that is read by the IS is the EF.CardAccess. The DTC-PC will also present an equivalent EF.CardAccess. The EF.CardAccess presented by the DTC-PC will contain an additional field called DTCCapabilitiesInfo, which is defined in the [DTC-VC] specification. If the EF.CardAccess does not contain DTCCapabilitiesInfo, then the presented token is an eMRTD. If it contains DTCCapabilitiesInfo, then it is a DTC-PC.

The DTC-PC MUST support the PACE secure communication protocols as defined in Doc 9303-11.

The cryptographic link between the DTC-VC and the DTC-PC will reuse anti cloning mechanisms already established in current eMRTDs. One of Chip Authentication, PACE-CAM, or Active Authentication MUST be present as defined in Doc 9303-11 and this document.

2.3 Interface between DTC-PC and Inspection Systems

Inspection systems need to be able to process both eMRTDs and DTC-PC. Therefore the minimum DTC-PC interface MUST be ISO/IEC 14443 with other communication interfaces as OPTIONAL.

2.3.1 Device engagement

The initial device engagement between the DTC-PC and the IS should mirror the current device engagement between an eMRTD chip and IS.

For eMRTDs, the IS reads the EF.CardAccess using the NFC interface. This provides it the parameters for setting up the PACE based secure messaging session. The actual keys to setup the PACE session are derived using an optical engagement (through an OCR of the MRZ). So, the DTC-PC MUST also provide an NFC engagement and an optical CAN engagement at the minimum. The optical engagement may be in the form of a 2D barcode that contains the information needed to set up the PACE session or a printed CAN as is the case for eMRTDs.

If the Inspection system is capable of reading the 2D barcode, this 2D barcode MAY also contain the EF.CardAccess, which will then obviate the need to do an NFC engagement to read EF.CardSecurity. This mechanism may be more appropriate when the interface between the DTC-PC and the IS uses the (yet to be defined) BLE interface, in which case NFC read is not necessary. The definition of the 2D barcode in this TR allows for this possibility in the future. The 2D barcode may also be used to provide any parameters that might be required for interfaces that are defined in the future.

2.3.2 Initialization Phase Interface

The initial interface between the DTC-PC and the IS uses either an interface specified in ISO/IEC 14443 or a 2D barcode.

Support for the ISO/IEC 14443 interface is REQUIRED for the DTC-PC, and Inspection Systems supporting DTC-PCs. Support for the 2D barcode is OPTIONAL for the DTC-PC and the IS.

Requirements for the ISO/IEC 14443 interface are defined in section 4.

Requirements for the 2D barcode interface are specified in section 3.

2.3.3 Data Transfer Interface

Subsequently, the data transfer interface is ISO/IEC 14443 (NFC).

2.4 Scope of DTC-PC specifications

In this iteration of the DTC-PC TR, the ISO/IEC 14443 interface is defined. Other interfaces will be defined in subsequent versions of the document.

The scope of the current specification is as follows:

- Default initialization phase interface;
- Initialization phase handoff, and;
- Interaction with Inspection Systems with the ISO/IEC 14443 communication interface, and; ISO/IEC 7816 data file structures defined as the contactless DTC-PC.

Topics that may be considered in a subsequent iteration of this document include:

- DTC-PC bootstrapping - specify the process by which the DTC-PC either generates a key pair and presents the public key securely to the Issuing Authority for inclusion in the DTC-VC or a key pair is generated at the Issuing Authority and securely loaded onto the DTC-PC;
- Other optional communications with inspection systems i.e. BLE, UWB;
- Life cycle of the DTC-PC;
- Security assurances of the DTC-PC;
- Applications outside of the primary use case of border crossing inspection and existing infrastructures.

3. Secure Messaging parameters

In order to establish the secure messaging channel between inspection system and DTC-PC, the inspection system needs to retrieve the CAN from the DTC-PC. For this purpose the DTC-PC MUST provide the CAN.

- Either as specified in ICAO Doc 9303-4, or Doc 9303-5;
    - using the OCR-B font specified in Doc 9303-3 clause 4.4;
    - readable in visible light and near infrared (i.e. the B900 band defined in [ISO 1831];
    - security feature (if any) SHALL NOT interfere with accurate reading of the OCR characters at the B900 range, or;
- As a barcode as specified in the [IDB-TR]. In this case the CAN MUST also be presented in human readable form, or;
- Both.

NOTE 1: The OCR-B presentation is one possible human readable format
NOTE 2: The 2D barcode MUST use the format specified in the [IDB-TR] for the DTC.

4. ISO/IEC 14443 Interface

Any implementation of a DTC-PC MUST support the ISO/IEC 14443 interface at a minimum.

The DTC-PC structure provides space to store required and optional data elements. The information stored in the DTC-PC becomes static at the time of issuance, and MUST NOT be modified in any possible way after issuance. While the DTC-PC includes optional data fields that could be used to expand the use of the DTC-PC, the requirement of write-protecting DTC-PC data at the time of issuance is REQUIRED. If data fields are to be added to the DTC, a new DTC MUST be issued.

4.1 Minimum Requirements for Interoperability

The following MUST be the minimum requirements for interoperability of contactless DTC-PC:

- [ISO/IEC 14443-1], [ISO/IEC 14443-2], [ISO/IEC 14443-3], [ISO/IEC 14443-4] including all associated amendments and corrigenda;
- [ISO/IEC 10373-6] test specification compliant including all associated amendments and corrigendum;
- Type A or Type B signal interface;
- Support for an ISO/IEC 7816-4 file structure for variable length files as specified in this Technical Report;
- [ISO/IEC 18745-2] test command sequences for eMRTD for ISO/IEC 14443-4 protocol;
- Support the cryptographic protocols as specified in clause 5.1.1;
- EF.CardSecurity is present without application selection;
- EF.CardAcess is present without application selection.

NOTE 1: The presence of the Master File MF is OPTIONAL.

5. Contactless DTC-PC Device

Figure 1 illustrates the required, optional, and conditional file structure for the Contactless DTC-PC device using an ISO/IEC 14443 communication interface.

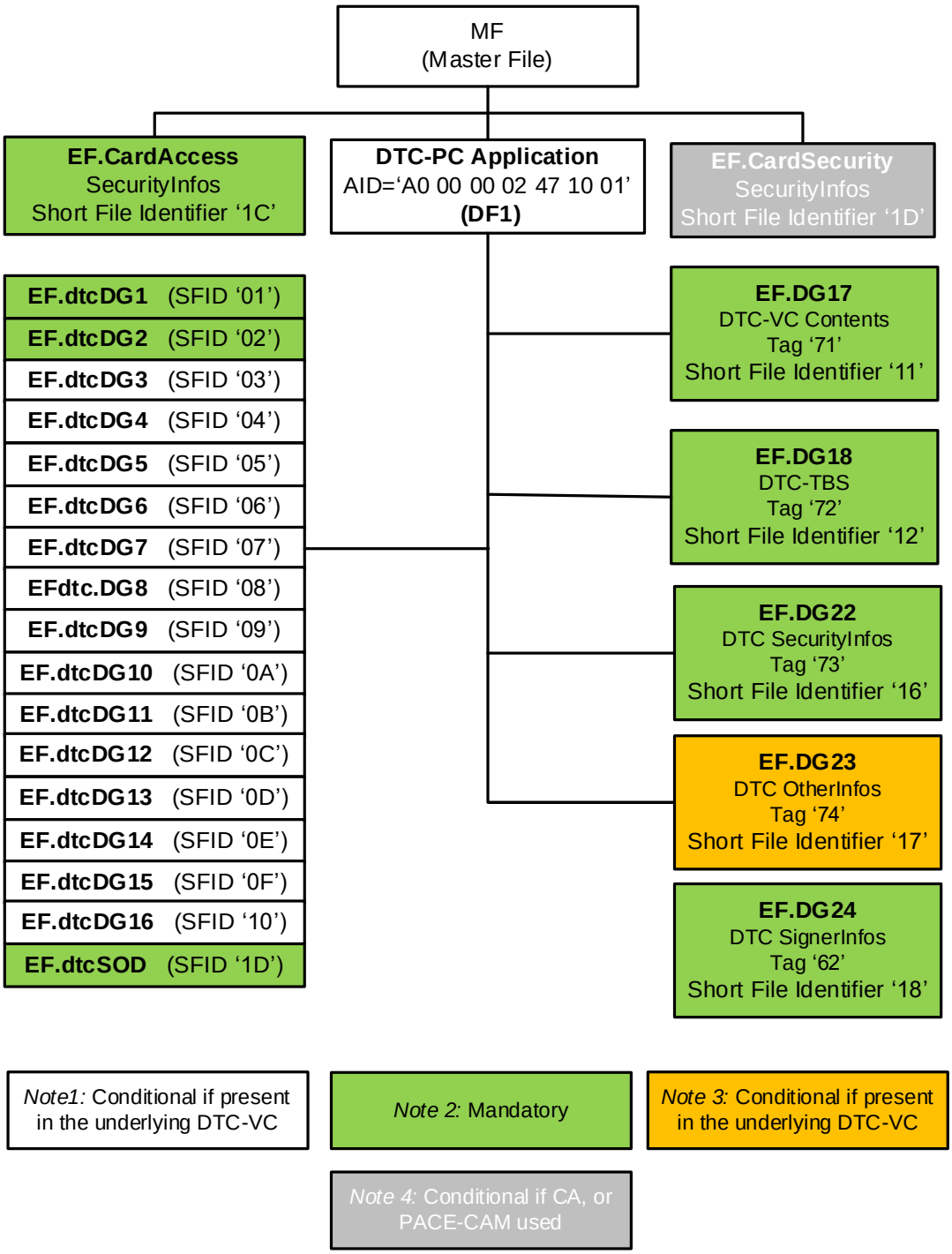
MF
(Master File)
EF.CardAccess
SecurityInfos
Short File Identifier '1C'
DTC-PC Application
AID='A0 00 00 02 47 10 01'
(DF1)
EF.CardSecurity
SecurityInfos
Short File Identifier '1D'
EF.dtcDG1 (SFID '01')
EF.dtcDG2 (SFID '02')
EF.dtcDG3 (SFID '03')
EF.dtcDG4 (SFID '04')
EF.dtcDG5 (SFID '05')
EF.dtcDG6 (SFID '06')
EF.dtcDG7 (SFID '07')
EFdtc.DG8 (SFID '08')
EF.dtcDG9 (SFID '09')
EF.dtcDG10 (SFID '0A')
EF.dtcDG11 (SFID '0B')
EF.dtcDG12 (SFID '0C')
EF.dtcDG13 (SFID '0D')
EF.dtcDG14 (SFID '0E')
EF.dtcDG15 (SFID '0F')
EF.dtcDG16 (SFID '10')
EF.dtcSOD (SFID '1D')
EF.DG17
DTC-VC Contents
Tag '71'
Short File Identifier '11'
EF.DG18
DTC-TBS
Tag '72'
Short File Identifier '12'
EF.DG22
DTC SecurityInfos
Tag '73'
Short File Identifier '16'
EF.DG23
DTC OtherInfos
Tag '74'
Short File Identifier '17'
EF.DG24
DTC SignerInfos
Tag '62'
Short File Identifier '18'
Note1: Conditional if present in the underlying DTC-VC
Note 2: Mandatory
Note 3: Conditional if present in the underlying DTC-VC
Note 4: Conditional if CA, or PACE-CAM used

Figure 1. DTC-PC File Structure Summary

5.1 Access to the Contactless DTC-PC

The inspection system MUST be provided with initial information to initiate encrypted communications prior to being able to read the contactless DTC-PC. The initial information has to be retrieved optically/visually from the DTC-PC from the REQUIRED CAN specified in Doc 9303 and the OPTIONAL 2D Barcode. It also MUST be possible for an inspector to enter this information manually in the inspection system used for a manual inspection in case machine-reading of the information is not possible.

The initialization, protocols, and secure messaging methods that MUST be employed can be found in Doc 9303 Part 11. At the end of the Initialization Phase, the communication is switched to the interface defined in the Data Transfer Interface, and a secure Communication Channel using PACE has been established.

5.1.1 Cryptographic Protocols

The eMRTD-PC bound. and PC bound DTC-PC SHOULD NOT support the following protocols and algorithms specified in Doc 9303-11:

- PACE algorithms that establish 3DES session keys;
- Chip Authentication algorithms that establish 3DES session keys;
- Active Authentication algorithms that makes use of SHA-1.

The DTC-PC MUST support the following cryptographic protocols that are specified in Doc 9303-11:

- At least one PACE Generic Mapping or Integrated Mapping algorithm that establishes AES session keys;
- At least one Active Authentication or Chip Authentication algorithm with the following constraints;
    - Active Authentication that does not make use of SHA-1;
    - Chip Authentication which establishes AES session keys.

The DTC-PC MAY support PACE with Chip Authentication mapping as specified in Doc 9303-11.

Inspection Systems that support DTC-PCs MUST support the following cryptographic algorithms specified in Doc 9303-11 for the inspection of DTC-PCs:

- All PACE Generic and Integrated mapping algorithms that establish AES session keys;
- All Chip Authentication algorithms that establish AES session keys;
- All Active Authentication algorithms with the exception of algorithms that use SHA-1.

Inspection systems that support DTC-PCs MAY support PACE with Chip Authentication Mapping as specified in Doc 9303-11 for the inspection of DTC-PCs.

Chip Authentication MUST be performed from within the MRTD application.

5.2 Command Set

The form factor of a DTC-PC is not explicitly defined in the specifications. It can be a contactless card, a mobile device or any form factor that implements the interface as defined in this technical report. The mention on an elementary file is to be consistent with the terminology of 7816-4. Essentially, the command set defines the method to read the contents and does not place any requirements on the storage of the content within the DTC-PC device.

All commands, formats, and their status bytes are defined in [ISO/IEC 7816-4]. The DTC-PC application MUST support the commands:

SELECT;

READ BINARY.

As specified in Doc 9303-10.

In addition the DTC-PC MUST support the commands according to Doc 9303-11 for the required cryptographic protocols.

5.2.1 SELECT

For elementary file selection the DTC-PC MUST support two structure selection methods that are file identifier and short EF identifier. Inspection Systems MUST support at least one of the two methods. The file identifier and Short EF Identifier is REQUIRED for the contactless DTC-PC.

For application selection the DTC-PC and the Inspection System MUST support the SELECT command variant specified in Doc 9303-10.

5.2.2 READ BINARY

The support of the READ BINARY command with an odd INS byte by a DTC-PC is CONDITIONAL. The DTC-PC MUST support this command variant if it supports data groups with 32 768 bytes or more.

5.3 Application Selection

The DTC-PC application MUST be selected by use of the Application Identification (AID) as a reserved DF name. The AID MUST consist of the Registered Application Identifier assigned by ISO according to [ISO/IEC 7816-5] and a Proprietary Application Identifier Extension (PIX) as specified within this document:

- The Registered Application Identifier is ’A000000247’;
- The issuer stored data application MUST use PIX = ’1001’;
- The full AID of the DTC-PC application is ‘A0 00 00 02 47 10 01’.

The DTC-PC MUST reject the selection of an application if the extension for this application is absent.

5.4 EF.CardAccess (REQUIRED)

EF.CardAccess is REQUIRED for the PACE access control as defined in Doc 9303-11, with the addition of the REQUIRED DTC-PC DTCCapabilitesInfo. A full description of SecurityInfos for PACE can be found in Doc 9303-11.

Table 1. EF.CardAccess

File Name	EF.CardAccess
File ID	’011C’
Short EF ID	’1C’
Read Access	ALWAYS
Write Access	NEVER
Size	Variable
Content	DER encoded SecurityInfos as per eMRTD in Doc 9303-11 DER encoded DTCCapabilitiesInfo. See [DTC-VC].

5.5 EF.CardSecurity (CONDITIONAL)

EF.CardSecurity contained in the Master File is REQUIRED if one of the following corresponding authentication protocols is used:

- The DTC-PC uses PACE with Chip Authentication Mapping as defined in Doc 9303-11, or,
- The DTC-PC Chip Authentication protocol performed in the eMRTD application as defined in Doc 9303-11.

A full description of SecurityInfos for PACE with Chip Authentication Mapping can be found in Doc 9303-11.

Table 2. EF.CardSecurity Storage on the DTC-PC

File Name	EF.CardSecurity
File ID	‘011D’
Short EF ID	‘1D’
Read Access	PACE
Write Access	NEVER
Size	Variable

EF.CardSecurity at minimum should contain;

- If the optional Chip Authentication is used, then it is REQUIRED to include ChipAuthenticationInfo as specified in Doc 9303-11;
- PACEDomainParameterInfo MUST be present. See 9303-11;
- PACEInfo MUST be present. See Doc 9303-11.

For the complete contents of EF.CardSecurity, see Doc 9303-10.

5.6 dtcDataGroups 1-16

dtcDataGroups 1 through 16 when present in the DTCContentInfo of the DTC-VC MUST be as follows;

Table 3. dtc Data Group Summary

DTC-PC Data Group	eMRTD EF Name	DTC-PC Short EF Identifier	DTC-PC EF Identifier	DTC-PC Tag
EF.dtcDG1	EF.DG1	‘01’	‘01 01’	‘61’
EF.dtcDG2	EF.DG2	‘02’	‘01 02’	‘75’
EF.dtcDG3	EF.DG3	‘03’	‘01 03’	‘63’
EF.dtcDG4	EF.DG4	‘04’	‘01 04’	‘76’
EF.dtcDG5	EF.DG5	‘05’	‘01 05’	‘65’
EF.dtcDG6	EF.DG6	‘06’	‘01 06’	‘66’
EF.dtcDG7	EF.DG7	‘07’	‘01 07’	‘67’
EF.dtcDG8	EF.DG8	‘08’	‘01 08’	‘68’
EF.dtcDG9	EF.DG9	‘09’	‘01 09’	‘69’
EF.dtcDG10	EF.DG10	‘0A’	‘01 0A’	‘6A’
EF.dtcDG11	EF.DG11	‘0B’	‘01 0B’	‘6B’
EF.dtcDG12	EF.DG12	‘0C’	‘01 0C’	‘6C’
EF.dtcDG13	EF.DG13	‘0D’	‘01 0D’	‘6D’
EF.dtcDG14	EF.DG14	‘0E’	‘01 0E’	‘6E’
EF.dtcDG15	EF.DG15	‘0F’	‘01 0F’	‘6F’
EF.dtcDG16	EF.DG16	‘10’	‘01 10’	‘70’

5.7 dtcSOD

The dtcSOD when present in the DTCContentinfo MUST be as follows;

Table 4. dtcSOD

DTC-PC Data Group	eMRTD EF Name	Short EF Identifier	EF Identifier	Tag
EF.dtcSOD	EF.SOD	‘1D’	‘01 1D’	‘77’

5.8 DATA GROUP 17 — DTC-VC (REQUIRED)

Data Group 17 contains the DTCContentInfo of the DTC-VC and encoded as defined in [DTC-VC].

Table 5. EF.DG17 Storage on the DTC-PC

File Name	EF.DG17
File ID	‘0111’
Short EF ID	‘11’
Read Access	PACE
Write Access	NEVER
Size	Variable

Table 6. Data Group 17 Tags

Tag	L	Value
71	Var	See [DTC-VC].

5.9 DATA GROUP 18 — dtcTBS (REQUIRED)

Data Group 18 contains the contents of DTCTBS.

Table 7. EF.DG18 Storage on the IC

File Name	EF.DG18
File ID	‘0112’
Short EF ID	‘12’
Read Access	PACE
Write Access	NEVER
Size	Variable

Table 8. Data Group 18 Tags

Tag	L	Value
72	Var	See [DTC-VC].

5.10 DATA GROUP 22 — DTCSecurityInfo (REQUIRED)

Data Group 22 contains the contents of DTCSecurityInfo.

Table 9. EF.DG22 Storage on the DTC-PC

File Name	EF.DG22
File ID	‘0116’
Short EF ID	‘16’
Read Access	PACE
Write Access	NEVER
Size	Variable

Table 10. Data Group 22 Tags

Tag	L	Value
73	Var	See [DTC-VC].

5.11 DATA GROUP 23 — DTCOtherInfos (CONDITIONAL)

This Data Group contains the dtcOtherInfos contained in the associated DTC-VC and is REQUIRED when the OPTIONAL dtcOtherInfos is present in the DTC-VC or DTC-PC DG17.

Table 11. EF.DG23 Storage on the DTC-PC

File Name	EF.DG23
File ID	‘0117’
Short EF ID	‘17’
Read Access	PACE
Write Access	NEVER
Size	Variable

Table 12. Data Group 23 Tags

Tag	L	Value
74	Var	See [DTC-VC].

5.12 DATA GROUP 24 — DTCSignerInfo (REQUIRED)

This Data Group contains the dtcSignerInfo contained in the associated DTC-VC.

Table 13. EF.DG24 Storage on the DTC-PC

File Name	EF.DG24
File ID	‘0118’
Short EF ID	‘18’
Read Access	PACE
Write Access	NEVER
Size	Variable

Table 14. Data Group 24 Tags

Tag	L	Value
62	Var	See [DTC-VC].

6. Appendix 1 (INFORMATIVE)

6.1 DTC-PC Device Engagement Flow

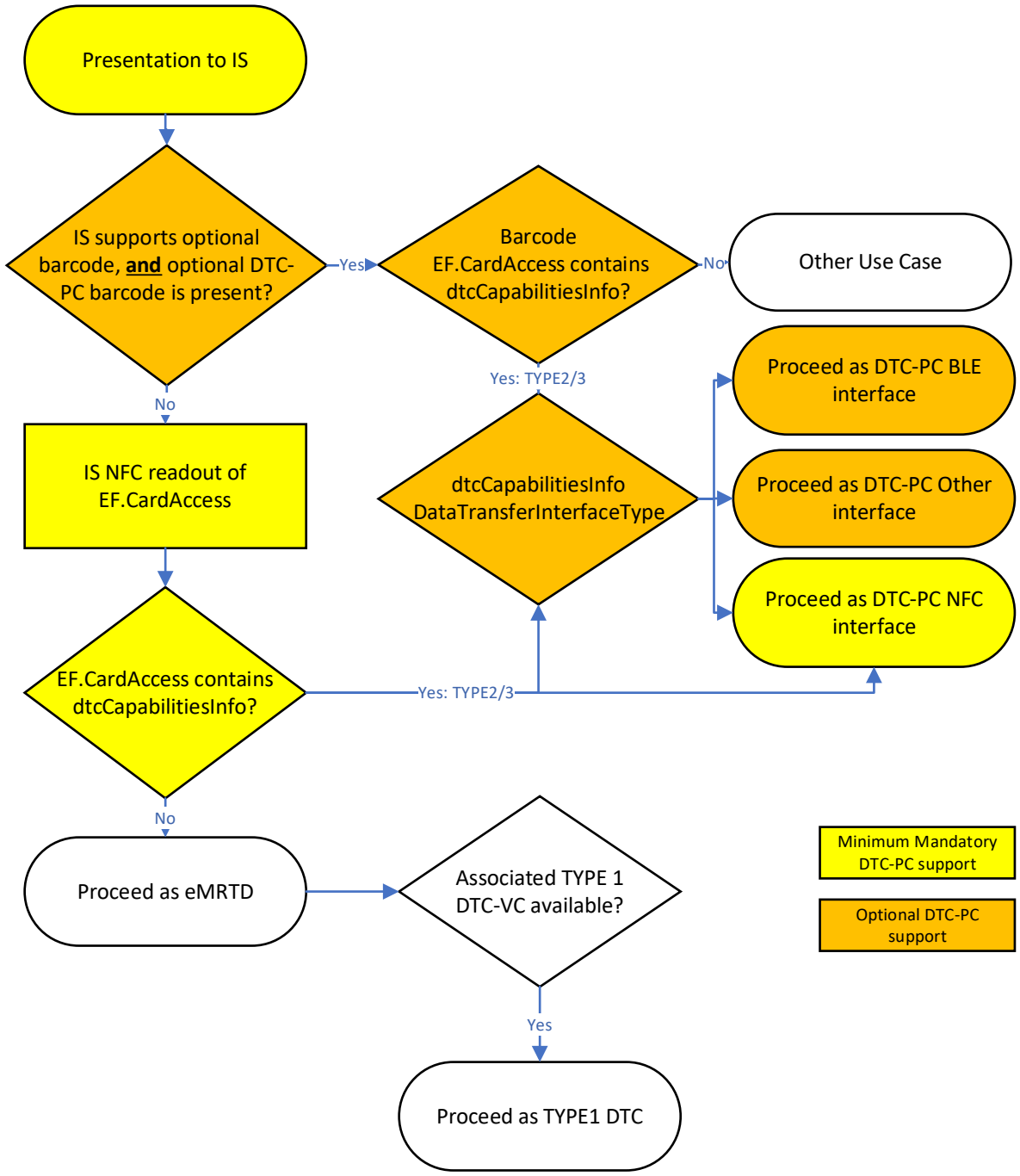

Figure 2. DTC-PC Engagement

7. Reference documentation

The following documentation served as reference for this Technical Report:

[RFC 2119] RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[Doc 9303]	ICAO Doc 9303, 8th Edition, “Machine Readable Travel Documents”
[RFC 5280]	RFC 5280, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, , “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008
[ISO/IEC 23220]	ISO/IEC 23220 Cards and security devices for personal identification — Building blocks for identity management via mobile devices (working draft)
[DTC-VC]	ICAO Technical Report "Digital Travel Credentials (DTC) Virtual Component Data Structure and PKI Mechanisms", Version – 1.2, October 2020
[ISO/IEC 14443-1]	ISO/IEC 14443-1:2018, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics*
[ISO/IEC 14443-2]	ISO/IEC 14443-2:2020, *Identification car*ds *— Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface*
[ISO/IEC 14443-3]	ISO/IEC 14443-3:2016, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 3: Initialization and Anticollision*
[ISO/IEC 14443-4]	ISO/IEC 14443-4:2018, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*
[ISO/IEC 10373-6]	ISO/IEC 10373-6:2016, *Identification cards — Test methods — Part 6: Proximity cards*
[ISO/IEC 7816-4]	ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*
[ISO/IEC 7816-5]	ISO/IEC 7816-5:2004, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*
[IDB-TR]	ICAO Datastructure for Barcode V1.1
[ISO/IEC 18745-2]	ISO/IEC 18745-2:2021 *Test methods for machine readable travel documents (MRTD) and associated readers — Part 2:Test methods for the contactless interface*