Analysis of DTC-PC Options

October 15, 2022

Contributions:		
Michael Hoppe	Germany	BSI
Felix Bleckmann	Germany	BSI
R Rajeshkumar	Singapore	Auctorizium
Mark Stafford	USA	Infineon
Jens Urmann	Germany	Veridos
Kenichi Nakamura	Japan	Panasonic

Contents

Preamble

The current specifications for the DTC-PC are device agnostic. The specifications closely mirror the interactions as they currently occur between an eMRTD and the Inspection System and are defined for an NFC interface.

The roadmap is to extend the specifications to other protocols like BLE, which would then allow for a wider range of devices to be considered for use as a DTC-PC.

There are currently two work items in other ISO groups. Namely, ISO/IEC 18013-5, which defines a Mobile Driving Licence (mDL) application, and ISO/IEC 23220 series, which specifies building blocks for identity management via mobile devices.

The requirements for use of any technology for a border crossing scenario are pretty strict and a thorough analysis is required of the suitability of these specifications for the eMRTD space. Such an analysis is also helpful to the ICAO NTWG DTC Policy sub-group and the wider NTWG to decide on the roadmap for DTC-PC.

This document is an Information Paper that attempts to analyse the available options. A paper from Apple, detailing their concern about the current DTC-PC specifications having significant privacy and user experience limitations, was tabled in the Copenhagen meeting of WG3 and also at NTWG. This paper promoted the suitability of 18013-5 for consideration of the DTC-PC specifications. Similarly, a paper has been presented by Idemia, introducing the support of other physical transport protocols to the DTC-PC specifications (in particular BLE), using a profile based on ISO/IEC 18013-5, and has been published on October 4, 2022, and will be considered in both WG3 and the upcoming NTWG.

This paper is an attempt by a group of experts in assessing the suitability of both ISO/IEC 18013-5 and ISO/IEC 23220 to the eMRTD world. It is the personal opinion of the experts involved, and should not, in any way, be considered a WG3 position. The paper attempts to provide enough information for the DTC Policy sub-group and NTWG, to take an informed decision on the way forward based on the Apple document, the Idemia document and this paper.

The following sections detail our analysis.

Device Engagement via Wireless Connections

ISO/IEC 18013-5:2021 provides two mechanisms for device engagement, NFC or QR-code, which both exchange data to setup a secure connection between the mDL and the mDL reader.

In case of QR code based device engagement the inspection procedure is carried out in a similar way as for ICAO Doc 9303 compliant eMRTD. First, the QR code provides the necessary data for secure connection establishment (e.g. a CAN) and then the mDL is inspected via a wireless interface. Hereby, only a person / device can access the mDL who can visually retrieve the QR code from the mDL.

In case of NFC based device engagement the secure connection parameters are already initially exchanged via a wireless interface. This is in contradiction with the requirements from Doc 9303-11 section 4, which identifies the risk that an unencrypted wireless communication between a contactless IC and a reader can be eavesdropped within a distance of several metres and mandates the eMRTD issuer to implement measures that prevent skimming as well as eavesdropping. However, ISO/IEC 18013-5 explicitly allows unencrypted transmission of data for session establishment over NFC.

The mobile device hosting the mDL could limit the timeframe in which the NFC interface is active to narrow the window of opportunity for fraudulent readout. However, also during that timeframe the user cannot identify to which reader he is connected to from this point on, since the radiation direction of radio waves is generally not recognizable for the user. Thus, NFC based device engagement shall not be used for a DTC-PC.

The latter does not only apply to NFC based engagements, but to any wireless based connection engagement in general.

Key Agreement Protocol

Key agreement for session encryption is based on an anonymous ephemeral Diffie-Hellman key exchange, whereby both the mDL and the reader generate an ephemeral EC key pair. The ephemeral public key of the mDLreader is transmitted to the mDL reader during device engagement. Due to 2.1 the mDL cannot unambiguously identify the destinationoriginactual mDL reader it is exchanging of its a received public keys with in case of NFC based device engagement.

The key-agreement protocol requires to transfer the full public key during engagement over an interface that cannot be eavesdropped. Using a short password (e.g. a CAN) instead of the public key is not consideredpossible. Thus, entering this information manually in the inspection system as demanded by 9303 is effectively ruled out. In consequence, the inspection procedure could no longer be performed, if the automatic device engagement procedures fails (e.g. if the QR-code is damaged or not readable due to broken or dirty display). In case of a Type 2 DTC the underlying eMRTD could be used as a fallback option, which is however not possible for Type 3 DTCs. Support of short password could be achieved by implementing   the PACE protocol.

Session Encryption

Session encryption currently terminates at a not further defined endpoint in the mobile device. Contrary to physical eMRTDs this is not necessarily the secure storage area which holds sensitive keys (CA or AA) and the personal identification data. Thus, any communication between that endpoint and the secure is only protected by measures implemented by the handset vendor / mobile OS vendor. In consequence, the DTC-PC issuer has to consider all of these measures if he wants to assess the confidentiality protection of the identification data.

The authenticity of the identification data is not affected since the data is signed by the issuing authority and storage of mdoc authentication keys in the secure storage protects the mDL from being cloned (assuming the storage is sufficiently secure).

A potential security certification gets much more challenging, when different components of the mobile device must be addressed. While the latter is not in scope of the DTC-PC TR [1], this should be considered to allow the development of products that eventually meet the demands of the governments.

The session encryption itself is based on commonly accepted cryptographic standards (ECKA-DH + HKDF + AES-GCM). Currently, ISO 18013-5 only allows one cipher suite, which is, but is not compatible with the algorithms and formats in current inspection systems   as defined by Doc 9303. This can be overcome by including further cipher suites into the standard.

Proof of Possession in case of connected devices

Since the secure connection does not terminate in the secure storage, an inspection system cannot verify whether the private key used to authenticate the mDL is hosted within or controlled by the mobile device the IS is connected to. An attacker in control of the mobile device’s OS could potentially relay the communication to another device hosting a secure storage area with valid authentication keys.

The latter is even valid if the secure connection ends in the secure storage. If an IS inspects a device with an online connection the IS has no assurance whether the communication actually terminates at that device or is relayed via the online connection to any place in the world.

In consequence, the proof of possession that is assumed for a physical offline eMRTD cannot be assumed equally for a DTC-PC hosted on a device with online connection.

Note: This issue is not unique to mDL. It also applies to the current draft version of the DTC-PC TR as well – if implemented on a device with online connection.

Authentication of the DTC-PC / Assurance level

So far, no attestation mechanisms is defined for the secure storage that allows an IS to determine the security properties of the DTC-PC. Thus, inspection systems cannot distinguish the security mechanism/assurance provided by an mDL based DTC-PC. Anything from software solutions to TEE to certified smartcards would be recognized as a valid DTC-PC by the IS.

Thus, any government that wants to distinguish DTC-PCs by assurance or security levels would need to maintain lists of all types of issued DTC-PCs for every issuing country.

The DTC-VC data structure reserves the securityAssuranceLevelIndicator field for this purpose, which is however based on a self-assessment by the issuing authority. The encoding is intended to be published in the upcoming ISO/IEC 23220-5 specification. However, as of date, we are not aware of such an encoding having been specified in ISO/IEC 23220-5.

Provisioning/Bootstrapping

Before an mDL can be used for identification two processes must be performed. First, the mDL application must be provisioned to the device hosting the mDL. This includes the initialization of a secure area within the secure storage on the device that allows storing und using the key material (and possibly also personal identification data) required by the mDL, as well as the installation of all required components required for communication between the secure area and the external interfaces of the domain.

Hereby, the process must check whether the device is actually eligible to host an mDL and satisfies the security requirements of the issuer (i.e. whether the secure area protects the key material against unauthorized access, tampering or cloning).

Furthermore, the some kind of attestation mechanism must be provided that allows the issuer to check whether the mDL application is genuine.

In a second process, the issuer personalizes the empty mDL application with the identification data of the mDL holder, establishing the binding between the mDL and the holder.

In contrast to eMRTDS, the device hosting the mDL including the secure storage and potentially also the mDL application are not under control of the issuer. Thus, the issuer needs to rely on the device or mDL manufacturer.

Provisioning and personalization/issuance is not addressed by ISO/IEC 18013-5, since it is out-of-scope. Instead, ISO/IEC 23220-3 aims at addressing these processes. The standard introduces a three layer trust model, which address the security of the secure domain, the mDL application and the issued mDL respectively and defines attestation data formats for them. These are however only container and do not cover neither well-defined assurance or confidence levels nor an assessment methodology and depth to validate claimed assurance.

ISO/IEC 23220-5 is intended to define confidence levels and ISO/IEC 23220-6 envisages to specify mechanisms for certification of the secure area. Both standards are still work in progress and still require extensive further development before they can be considered suitable.

Security Features / Requirements

Security requirements regarding storage of credential information are out of scope of ISO/IEC 18013-5 and also ISO/IEC 23220-4 does not impose hardware constraints by itself.

Provisioning/ Personalisation is within the scope of ISO/IEC 23220-3. We may be able to re-use the specifications when they are ready.

Intellectual Property

As for now, it cannot be concluded on whether there exist patent holders or not. The ICAO position on intellectual property as this position deviates from the ISO/IEC position.

According to ISO/IEC, there is not necessarily a problem with patents as long as the patent holder grants licenses on a non-discriminatory basis on reasonable terms and conditions, see https://www.iso.org/iso-standards-and-patents.html

As far as we know ICAO's position is to avoid any patents, if no free of charge licences on a non-discriminatory basis are granted. However, we are not sure if this is a common understanding (*SC17/WG3 has always considered this principle when creating specifications in the past*) or if there is any documentation to this effect. We intend to ask NTWG to clarify this issue.

Cryptographic Agility

The ISO/IEC 18013-5 cipher suite 1 supports Elliptic Curve based cryptography including ECDH, but neither RSA nor DH.

For the sake of cryptographic agility most of the ICAO Doc 9303 eMRTD security protocols support ECDSA / ECDH as well as RSA and DH. The exception are security protocols for use cases with size constraints which support only Elliptic Curve based cryptography.