Privacy & Identity protection in mobile Driving License ecosystems

Version: 1.0 draft 3

Document Date: 2021-05-24

Editors: John Wunderlich, Loffie Jordaan, Christopher William, Richard Wilshire, Tom Jones

Contributors: See the [Discussion Group Participant Roster](https://kantarainitiative.org/confluence/display/mdl/Participant+Roster)

Produced by: PImDL DG

Status:

This document is a Group-Editors' Draft Kantara Initiative Candidate Report produced by the *Privacy & Identity in mobile Driving License Discussion Group (*PImDL DG). See the Kantara Initiative Operating Procedures for more information.

Abstract:

This report elaborates on the non-normative privacy and identity protections in ISO/IEC 18013-5 to enable implementors of software or hardware in mobile driving license ecosystems to take a proactive and user centric approach to privacy and identity.

IPR Option:

‑‑Error! **AutoText entry not defined.**

Suggested Citation:

*Privacy & Identity protection in mobile Driving License ecosystems 1.0 Draft 3.* Kantara Initiative PImDL DG. 2021-05-19. Kantara Initiative Report.

NOTICE

Copyright: The content of this document is copyright of Kantara Initiative, Inc.  
© 2021 Kantara Initiative, Inc.

Contents

1 Executive Summary 5

1.1 Scope of the Report 5

2 Introduction 7

2.1 Purpose of the Discussion Group 7

2.2 Risk Considerations 8

2.3 Other Considerations 9

3 The mDL International Standard 10

3.1 Overview 11

3.2 ISO/IEC 18013-5 Mechanics 11

3.3 Key management 12

3.4 AAMVA mDL Guidelines 13

3.5 3.5 Secure Technology Alliance 13

4 PImDL Overview 14

4.1 Privacy Considerations for the extended ecosystem 16

4.2 Identity Considerations for the extended architecture 24

5 Data Flows 30

5.1 Data Flow 1 (DF-1) 30

5.2 Data Flow 2 (DF-2) 32

5.3 Data Flow 3 (DF-3) 34

5.4 Data Flow A (DF-A) 36

5.5 Data Flow B (DF-B) 39

5.6 Data Flow C (DF-C) 41

5.7 Interoperability Risk 42

6 Summary 43

7 Appendices 44

7.1 Additional Considerations 44

7.2 Identifier Protection Summary 45

7.3 Bibliography 46

7.4 Terminology 46

Tables

[Table 1Scope Considerations 6](#_Toc72311623)

[Table 2 Identity Attributes in Context 28](#_Toc72311624)

[Table 3 Additional Security Considerations 44](#_Toc72311625)

Figures

[Figure 1 Interfaces from ISO/IEC 18013-5 10](#_Toc72311626)

[Figure 2 PImDL Data Flows 14](#_Toc72311627)

[Figure 3 List of Data Flows in Scope 15](#_Toc72311628)

[Figure 4 Data Flow 1 29](#_Toc72311629)

[Figure 5 Data Flow 2 31](#_Toc72311630)

[Figure 6 Data Flow 3 33](#_Toc72311631)

[Figure 7 Data Flow A.1 35](#_Toc72311632)

[Figure 8 Data Flow A.2 36](#_Toc72311633)

[Figure 9 Data Flow B.1 38](#_Toc72311634)

[Figure 10 Data Flow B.2 38](#_Toc72311635)

[Figure 11 Data Flow C 40](#_Toc72311636)

# Executive Summary

This report is the result of the work of the “Privacy & Identity Protection in mobile Driving License ecosystems”[[1]](#footnote-1) (PImDL) Discussion Group at the Kantara Initiative[[2]](#footnote-2). It provides the reader with an overview of mobile Driving License systems and guidance on protecting individual privacy and digital identifiers of individuals who carry or use mobile Driving Licenses.

## Scope of the Report

The intended audience of this report includes product managers, engineers, compliance teams, architects, developers, assessors, and others with responsibilities for implementing, supporting, or interfacing with mobile credentials that comply with ISO/IEC 18013-5 Personal identification — ISO-compliant driving license — Part 5: Mobile driving license (mDL) application (ISO/IEC 18013-5)[[3]](#footnote-3).

ISO/IEC 18013-5 provides clear and detailed guidance for implementing a mobile driving license or identity document. This report is not, nor should it be taken, as guidance in contradiction of that standard. In other words, ISO/IEC 18013-5 is the baseline upon which this report builds.

Although in some cases inadvisable, mobile Driving Licenses providers may allow access to mDL data using methods not defined in ISO/IEC 18013-5 (“undefined data access”). Examples are an ISO/IEC 18013-5 compliant application that allows access via a separate API, a completely non-compliant data exchange protocol, or a “flash pass.” The privacy and security considerations will equally apply to such methods and serve as guidance towards ISO/IEC 18013-5 compliant implementations. While this report does not explicitly cover undefined data access, where appropriate, it does expand on the privacy and security implications that may arise from such access[[4]](#footnote-4).

ISO/IEC designed 18013-5 to bring digitally secure driving licenses to mobile devices. Implementers of ISO/IEC 18013-5 will not be limited to public identity issuing authorities, such as motor vehicle administrators. Other entities, public and private, may choose to utilize this standard for issuing mobile identities for specific ecosystem use cases (e.g., national agencies, colleges and universities, private commercial organizations such as retail and healthcare, etc.) Even though such identities (i.e., compliant with the ISO/IEC 18013-5 standard and issued by non-driver’s license issuers) may not be able to interoperate within an mDL ecosystem, the security and privacy considerations of these identities are within the scope of this report.

### In Scope

1. Use of the mDL on a mobile device at the point of interaction;
2. Use of the mDL as a read-only data source for other systems, such as:
   1. As an input to Federated Identity Systems; or
   2. As an attribute source for a [W3C Verified Credential](https://www.w3.org/TR/vc-data-model/) (VC); or
   3. As part of a [W3C Decentralized Identifier](https://www.w3.org/TR/did-core/) (DID) method; or
   4. As an attribute source for Self-Sovereign Identity (SSI).
3. Privacy and security implications of making mDL data available via methods not supported in ISO/IEC 18013-5[[5]](#footnote-5)

### Out of Scope

If an item is not specifically “In Scope” then it is assumed to be out of scope. The following table captures in and out of scope considerations:

|  |  |  |
| --- | --- | --- |
|  | DL-ID Issuers | Other ID Issuers |
| ISO/IEC 18013-5 Compliant | In Scope   * Defined data access | In Scope   * Defined data access |
| ISO/IEC 18013-5 Non-compliant | In Scope   * Privacy and Identity considerations only * Undefined data access | Out of Scope   * Undefined data access |

Table 1 Scope Considerations

# Introduction

This section provides an outline of an ecosystem as described by ISO/IEC 18013-5. It explains how providers of hardware/software can meet or extend the privacy and identity considerations set out in ISO/IEC 18013-5, both for mDLs and non-mDL credentials issued in compliance with[[6]](#footnote-6) ISO/IEC 18013-5. The rest of the document discusses how implementers and entities on the ‘reading’ side and the ‘provisioning’ side of their ecosystem can meet stakeholder privacy expectations and protect identity attributes. The ‘reading’ side of the ecosystem includes entities with use cases that require them to read some or all of an ISO/IEC 18013-5 compliant credential. The ‘provisioning’ side consists of the providers of hardware or software that support the issuing of an ISO/IEC 18013-5 compliant credential and will support the process by which a credential holder shares information with a relying party.

This report identifies privacy and identity-related requirements or expectations for the use of any ISO/IEC 18013-5 compliant credential to enable a robust and privacy-protective system for all stakeholders. By supporting the requirements and expectations in this report, Relying Parties can provide substantive and potentially verifiable assurances about how they protect individuals’ privacy and identity. There will be a difference between specific, technical conformance and interoperability with ISO/IEC 18013-5 and meeting jurisdictional requirements or stakeholder expectations. This report therefore identifies a baseline set of requirements and expectations for the protection of privacy and identity for mobile digital identifier stakeholders. The ISO/IEC 18013-5 standard provides a specific and secure architecture that stakeholders should start with. That being said, it is the case that some mDL issuing authorities are already issuing credentials using architectures that are not compliant with ISO/IEC 18013-5. This report provides privacy and identity guidance that can be applied in those circumstances. This serves two purposes; to foster good privacy and identity practices regardless of the architecture, and to identify possible pathways to bring mDL architectures into compliance with ISO/IEC 18013-5.

*Any implementers of a system that may collect, use, or disclose personal information; or process identity attributes, should consider using the information in this report as input to the functional or non-functional requirements for their implementation.*

## Purpose of the Discussion Group

The [Charter](https://kantarainitiative.org/confluence/display/mdl/Charter) of the discussion groups states,

Emerging standards around mobile Drivers Licenses, particularly ISO/IEC 18013-5 “Personal identification — ISO-compliant driving license”, raise questions of Identity Proofing and Individual Privacy. In particular, the issuing authorities for mobile Driving Licenses (mDLs) have a legitimate requirement for detailed and deeply personal information about individuals, while many relying parties will only have legitimate bases for selected subsets of the identity-related data available in an ISO/IEC 18013-5 compliant credential. Similarly, holders of such credentials will appreciate the convenience of having a standard verified credential that can be used in many contexts but will need assurances that their privacy will be protected and that their identity will be secure.

This Discussion Group engaged stakeholders to produce a report intended to enrich and inform the broader community that will create, deploy, administer, and use ISO/IEC 18013-5 compliant credentials. This report draws on prior Kantara reports and standards, the work of the Secure Technology Alliance and others to create a report that may[[7]](#footnote-7) be used as the basis for the creation of a Kantara Work Group to create and maintain a conformance standard for Privacy and Identity protective implementations of ISO/IEC 18013-5 compliant credentials.[[8]](#footnote-8)

## Risk Considerations

There is a risk that personally identifiable information (PII), once shared, can be used beyond the purpose for which it was shared. Therefore, transactions that consume identity attributes from an mDL need to incorporate considerations to reduce the risks to privacy and identity in any given operational context associated with the transaction.

This report identifies the general nature of risks that should be considered in the use of mDLs and offers a notional indication of the scale of risk. This report encompasses re-identification risk, identity theft risk, the risks of unauthorized or inappropriate use of personal information, and related risks. These risk considerations include:

1. The operational context in which the transaction is taking place. For example, is the transaction using a kiosk in a formalized setting, environment, or installation (such as airport security); or is it in a casual environment where the user is obliged to hold many more assumptions about the other parties involved in the transaction? Example of these more casual contexts could be street vendors, clubs, concerts, or other social contexts.
2. The specific types of identity attributes being required for the transaction:
   1. [Direct](#_s1i18e9e48yc) or [Unique](#_2h322lk7o2sq) Identifiers (e.g., name and dob, system identifier); or
   2. [Indirect](#_w5vp8m8fj9z) Identifiers (e.g., dob and address); or
   3. [Quasi-Identifiers](#_1mj9d78wsuq) (e.g., a true false indicator, e.g. eligibility based on age or any other characteristic, such as entitlement to operate specific classes of vehicles).
3. The use of data for purposes other than those specified when the data was collected.

Additionally, the report does not predicate control selection for the mitigation of these risks. Control suites abound, as do frameworks for managing information security risks, based on international and national standards and other publications and paradigms.

A final consideration is the extent to which any device, application, or service interacting with an mDL (whether automated or with human interaction involved) can be relied upon to protect the integrity and privacy of information stored in the mobile device[[9]](#footnote-9). This will require technical infrastructure to support this, both for the consuming devices, applications, and services; and for user devices, and may be performed internally to the user device or require access to supporting infrastructure (e.g., a register of assured devices, applications, and services). In addition to technical infrastructure, implementation will require governance and related processes to protect personal information. Future work may address these needs and provide assurance criteria and describe an appropriate certification scheme.

## Other Considerations

In the context of this report, considerations other than specific privacy or identity risks, were raised by the discussion group. These might be ‘orthogonal’ to the scope of the report but still germane to individuals concerned with building or enhancing an ecosystem that is more respectful of individual autonomy.

# The mDL International Standard

The mobile Driving License (mDL) International Standard referred to throughout this report is ISO/IEC 18013-5 Personal identification — ISO-compliant driving licence — Part 5: Mobile driving license (mDL) application (ISO/IEC 18013-5).[[10]](#footnote-10) This section of the report provides a summary of the standard with some ancillary information.

The figure below shows the mDL Interfaces:

1. Interface 1 is the interface between the Issuing Authority infrastructure and the mDL (Not in scope of ISO/IEC 18013-5).
2. Interface 2 is the interface between the mDL and the mDL Reader, as specified in ISO/IEC 18013-5.
3. Interface 3 is the interface between the Issuing Authority infrastructure and the mDL Reader, as specified in ISO/IEC 18013-5.

Diagram

Description automatically generated

Figure 1 Interfaces from ISO/IEC 18013-5

## Overview

From the introduction to ISO/IEC 18013-5:

*ISO/IEC 18013 (all parts) establishes guidelines for the design format and data content of an ISO-compliant driving license (IDL) with regard to human-readable features (ISO/IEC 18013-1), ISO machine-readable technologies (ISO/IEC 18013-2), access control, authentication and integrity validation (ISO/IEC 18013-3), and associated test methods (ISO/IEC 18013-4). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states in applying their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.*

*This document describes the interface and related requirements to facilitate ISO-compliant driving license (IDL) functionality on a mobile device. The requirements are specifically intended to enable verifiers not affiliated with or associated with the Issuing Authority to gain access to and authenticate the information. In addition, the requirements allow the holder of the driving license to decide what information to release to a verifier. Other characteristics include the ability to update information frequently and to authenticate information at a high level of confidence.*

*A mobile document conforming to this document primarily conveys the driving privileges associated with a person. It does so by providing means to associate the person presenting the mobile document with the mobile document itself. However, the transaction and security mechanisms in this document have been designed to support other types of mobile documents, specifically including identification documents. Consequently, the mechanisms in this document can be used for any type of mobile identification document, regardless of the additional attributes the mobile document may convey. The details of the data elements to be used by other mobile documents are left to the respective Issuing Authority and are not in the scope of this document.*

## ISO/IEC 18013-5 Mechanics

An mDL transaction commences with a user-initiated engagement step. Sufficient information is exchanged during this step to define the following data retrieval methods. Device engagement can occur using NFC or a QR code.

Two data retrieval methods are supported: device retrieval (sometimes referred to as the offline method), and server retrieval (sometimes referred to as the online method, and not to be confused with unattended use of an mDL over the Internet). Device retrieval can make use of BLE, NFC or Wi-Fi Aware. Server retrieval can make use of WebAPI or OIDC (both via the Internet).

Data retrieval generally commences with a request from the mDL reader to the mDL (Interface 2 in Figure 1). This request lists all the individual data elements the mDL reader would like to receive. For each data element, the mDL reader has to indicate whether it intends to retain the information once received. This approach supports the creation of apps that allow an mDL Holder full visibility of and control over what data elements are being requested, being released, and under what conditions.

ISO/IEC 18013-5 defines the set of data elements supported in an mDL implementation. Driving license issuing authorities (DL-ID Issuers) have the option to define additional local data elements. In addition, as noted in the extract from the ISO/IEC 18013-5 Introduction above, non-driving license issuing authorities (i.e., other DL-ID Issuers) can adapt the standard for other types of identity credentials.

For the device retrieval method, data freshness is controlled via the validity period of the Mobile Security Object (MSO).

## Key management

The authenticity of mDL data is confirmed using passive authentication. This requires the mDL verifier to possess the public key of the Issuing Authority signing key. It is a critical responsibility of the verifying party to apply a trusted process in obtaining the public keys it possesses for each trusted Issuing Authority. ISO/IEC 18013-5 defines and suggests the use of an mDL master list as a mechanism for the distribution of trusted public keys. Other methods may exist as well, such as obtaining public keys directly from trusted issuing authorities. Also, see ETSI TS 119 612 which defines a flexible and extensible structure for a human/machine parsable Trust Status List which could serve as an mDL Master List.

An initiative driven by AAMVA is currently (spring 2021) underway to identify viable and practical public-key collection and dissemination solutions for its members. It is envisioned that a public key administrator will act as a focal point for this purpose. In addition, the public key administrator will accept public keys only if the Issuing Authority complies with a minimum set of requirements determined by AAMVA and its members[[11]](#footnote-11). Other public-key administrators will exist for international issuers and non-AAMVA members and those public key administrators may adhere to different requirements for acceptance. Although there is an initiative to align such requirements between different mDL public key administrators, it is the responsibility of the verifier to understand the requirements set by a public key administrator to establish trust in the included issuing authorities.

## AAMVA mDL Guidelines

As a service to its members, AAMVA has published guidelines for IAs on mDL administration. The intent of the guidelines is to serve as a comprehensive set of requirements states can follow when setting up and operating an mDL solution. While the current version of the guidelines primarily addresses the interface between an mDL and an mDL reader, the next version is envisioned to also cover areas such as provisioning, app functionality, and local PKI operation. Within each area, requirements for functionality, privacy, security, and technology will be addressed as needed.

## 3.5 Secure Technology Alliance

The [Secure Technology Alliance](https://www.securetechalliance.org/) (STA), composed of members from the digital security industry, provides a neutral forum that brings together leading providers and adopters of end-to-end security solutions designed to protect individuals’ privacy and digital assets in a variety of vertical markets. As part of achieving this mission, the STA’s Identity Council has developed a set of educational materials directed broadly at all members of the mDL ecosystem[[12]](#footnote-12). These materials include a substantial white paper[[13]](#footnote-13) giving a technical overview of the mDL as described in ISO/IEC 18013-5, considerations for securing such ecosystems, and a number of use cases highlighting areas where the mDL provides a new value for Holders and Relying Parties. The STA also produced a series of educational webinars covering the content of their white paper. Additionally, the STA has produced the mDL Connection website ([www.mdlconnection.com](http://www.mdlconnection.com)) which contains links to the discussed white paper and webinars, as well as additional FAQs, implementers map, and other resources to inform and continually update the community on the development of mDLs in the United States.

# PImDL Overview

The diagram below shows the potential connections between actors; those identified in ISO/IEC 18013-5 on the left, and their equivalent in a more general view of the actors in an identity system on the right. This report is based on protecting mDL data issued by Issuing Authorities. While we acknowledge that there may be theoretical connections between all these entities, this report focuses on those interfaces that have the potential to have real-world use cases involving Issuing Authority issued mDLs. The numbered data flows: DF-1, DF-2, and DF-3 are the interfaces defined in ISO/IECISO/IEC 18013-5. The lettered data flows: DF-A, DF-B, and DF-C involve implementations involving Individuals and Relying Parties that exchange mDL data in an undefined manner.

It should be noted that “in real life”, the “mDL Holder” and the “Individual” actor will be the same natural person in any given operational context.

Diagram

Description automatically generated

Figure 2 PImDL Data Flows

Legend:

|  |  |
| --- | --- |
| DF-1: Issuing Authority – mDL Holder data flows | DF-A: mDL Holder – Individual data flows |
| DF-2: mDL Holder – mDL Verifier data flows | DF-B: mDL Verifier – Relying Party data flows |
| DF-3: Issuing Authority – mDL Verifier data flows | DF-C: Individual – Relying Party data flows |

Figure 3 List of Data Flows in Scope

Before we discuss the privacy and identity protection considerations of each of these six dataflows, we set out the general privacy and identity protection considerations for the extended ecosystem (i.e., all six dataflows).

For the purposes of this report an “Implementor” is a person or organization that is accountable or responsible for implementing one or more of the of endpoints identified in [Data Flows](#_o28b936n2gye) below. This may be software, hardware, infrastructure, or some combination of these elements as shown below:

| Data Flow | Implementors | Notes |
| --- | --- | --- |
| DF-1 | Issuing Authority | Self-explanatory in ISO/IEC 18013-5 |
| DF-1  DF-2  DF-A | mDL Developer | The mDL Developer is the entity that creates the mDL software being used by the mDL Holder on their chosen device. |
| DF-2  DF-3  DF-C | mDL Reader Developer | The mDL Reader Developer is the entity that creates and/or is responsible for the device that reads the mDL. This may be a dedicated hardware reader or software on a device that has the capability of reading the mDL when presented. |
| DF-A  DF-C | Mobile Device Developer | The Mobile Device Developer is the entity that creates the software (“wallet”) being used by an Individual who is also an mDL Holder on their chosen device. |
| DF-B  DF-C | RP Reader Developer | The RP Reader Developer is the entity that creates and/or is responsible for the device that reads the mDL. This may be a dedicated hardware reader or software on a device that has the capability of reading the mDL when presented. |

## Privacy Considerations for the extended ecosystem

Implementers may consider each of the following principles to determine how their implementation can demonstrate conformance with the privacy considerations in each of the following principles. Where implementers are not able to conform with the principle, they may choose to document the gap and the reasons for the gap (operationally unfeasible, regulatory requirement, etc.). Such gaps may be included in the product or system documentation and be made available to the mDL Holder, preferably proactively.[[14]](#footnote-14)

### Consent and Choice

The mDL Holder should consent to the processing of their personal information. Use cases where there is a non-consent-based authority for collecting information about the individual are out of the scope of this report. However, we note that the absence of consent does NOT imply a lack of authority NOR a reduction in the obligation of implementers to respect privacy and protect identity in their operational context. In the case of ISO/IEC 18013-5, the consent may be implicit because the mDL Holder has initiated the data flow by presenting their mDL in the context of an in-person transaction. The consent that can be implied will be specific to the context of the presentation. If the presentation is required for age verification, for example, consent to the sharing of age may be implied but not consent to the sharing of a birth date if the Issuing Authority included the necessary age statement in the credential.

Risk Considerations

Implementors should address the following considerations in developing their mDL applications:

The implementer should document the content and type of consent to be obtained. Consent may be implied or expressed, and the implementer should document the allowable uses of data for which consent will be obtained. If the implementer retains information from the mDL Holder, this creates a relationship with the mDL Holder, with ongoing obligations to respect the mDL Holder’s privacy preferences. The implementer may use a consent management system to accomplish this.

The implementer should allow a user to choose not to consent to any collection or use of their data. If a service consists of multiple elements, and if only partial consent is obtained, those elements of the service for which consent was obtained should continue to be provided and should not be impacted by the refusal;

Where the transaction is on-line there should be some means of proof of presence supplied by the mobile device. For example, using a mobile phone biometric proof of presence such as facial recognition;

Consent choices of the mDL Holder may be stored by the verifier as well as by mDL application on the holder’s mobile device for future transactions. Depending on the stage of the mDL transaction the storage location of the consent choices may vary and be inaccessible to either party. If modification or withdrawal of consent choices is outside the direct control of the mDL Holder, the verifier should allow consent for any future transactions to be withdrawn or modified at any time:

The verifier may consider the use of consent receipts for the purpose of informing the mDL Holder of what the mDL Verifier has recorded;

If consent is withdrawn, the verifier should inform the user of the types of uses of their data that have already been completed and cannot be deleted or withdrawn.

Other considerations

Where transactions are in-person, the possibility of a coerced presentation exists and implementers are encouraged to explore UX options for the mDL Holder to identify coerced presentations.

### Purpose legitimacy and specification

The mDL Holder should be fully aware of the purpose for which their personal data is being collected, processed, and potentially stored. Upon or prior to the presentation of their mDL to the verifier the mDL Holder should receive a notice that identifies the purpose of collection and the uses of the data after collection.

Risk Considerations

The implementer should ensure that the purposes for which they are collecting mDL data are legitimate (legal, required for the purpose of collection, and with risks to privacy proportionate to the proposed use of mDL data) before the implementation of their solution.

The implementer should provide a notice to mDL Holders that is appropriate to the operational context. mDL Holders should understand what information about them will be collected before they present their mDL or before data is transferred from the mDL. A notice may be a posted or printed notice, a text message or application pop-up, or spoken communication. The notice should be in advance of any collection of personal information about the individual.

The implementer should consider the holder’s understanding of the completed interaction. Where any user data is retained a notice or consent receipt should be provided to the holder in printed or electronic format.[[15]](#footnote-15)

The implementer should consider the use of notice and consent receipts[[16]](#footnote-16) in their workflow to document both the notice provided by the mDL Verifier, and the consent received that the mDL Verifier will use.

Other considerations

If the implementation flow allows a meaningful (as opposed to a ‘click through’) notice and consent transaction, consent will be expressed consent, although still with the caveats above. This kind of flow has limited support with ISO/IEC 18013-5. For example, verbal consent is not supported but may be used by the Implementor.

### Collection Limitation

The mDL Verifier should only collect the data necessary for its purpose and should only collect data consistent with these considerations. Necessary in this context refers to the necessity to complete the business purpose(s) specified in the notice provided to the user.

Risk Considerations

Implementers should document the business purpose for each field of the mDL to be collected. ([4.2 Identity Considerations for the extended architecture](#_nded8wb3wr9i))

Implementers should identify whether express or implied consent is required based on the sensitivity of the operational context. Express consent requires affirmative action from the individual (like an ‘opt-in’ option) where implied consent is implied from the context of the transaction. Express consent is usually regarded as more likely to be necessary for processing sensitive information. Implementers may consider using a Privacy Impact Assessment to make this determination.

Other considerations

The necessity for collection should be determined from the point of view of the user and what they would reasonably expect in the operational context.

### Data Minimization

Processing (collection, use, retention, accessing, sharing, disclosing, or other manipulation or viewing of data) of mDL data should be minimized to that specifically necessary for the purpose specified.

Risk Considerations

Issuing Authorities should provide data minimizing options, such as including “birth year” in addition to “date of birth”.

Implementers should only process data for the purposes identified in the notice provided to the mDL Holder.

Implementers may consider the processing of de-identified data for other purposes if a measurable and reliable de-identification technique[[17]](#footnote-17) is applied with appropriate controls to minimize the risk of re-identification.

### Use, Retention and Disclosure Limitation

The mDL Verifier should not use, retain, or disclose the personal data of the mDL Holder except for the purposes specified and consistent with these other principles. mDL data should only be retained for the period necessary to provide the service.

Risk Considerations

Implementers should only use data for the purposes identified in the notice provided to the mDL Holder.

Implementers should retain mDL data only so long as the data is being used for purposes identified in the notice provided to the mDL Holder.

Implementers should destroy all copies of mDL data when the retention period for the data has expired.

Implementers may maintain records of the destruction of mDL data. Where such records are required, Implementers should not retain identifying information.

Implementers should document and implement a retention schedule for mDL data.

Other considerations

Implementers should work with their procurement and legal teams to ensure that third party processors are bound by the implementation rules for use, retention, and disclosure.

### Accuracy and quality

High accuracy of data being processed and held is in the best interest of the mDL Holder and mDL Verifiers should take measures to ensure accuracy.

Risk Considerations

The implementer should implement procedures to maintain the accuracy, quality, and integrity of the mDL data.

Other considerations

Implementers should consider retention of data as an integral part of data quality, and ensure that data is current and, where operationally appropriate, a retention limit.

### Openness, transparency and access

What mDL data and how mDL data is being processed should be well-known to the mDL Holder, including obtaining consent, and posting and updating clear notices.

Risk Considerations

The implementer should create a public privacy commitment that describes how it processes mDL data and its consent practices.

The implementer should publish or make available its public privacy commitment on one or more of the following:

The implementer’s web site; or

The implementer’s phone number for privacy information; or

The implementer’s corporate mailing address;

An equivalent mechanism to make the commitment readily available.

The implementer should respond to any enquiries about its public privacy commitment within 30 days of receiving an enquiry

Other considerations

Where appropriate protocols and options exist, implementers should consider systems that give individuals ongoing control over their own personal information.

### Individual participation and access

The mDL Holder should be involved in or informed about the collection, consent, processing, and storage management of their personal data.

Risk Considerations

The implementer should, to the extent practicable in the operational context, require mDL Holder participation in the mDL data processing data flows.

Where participation in the mDL data flows is not practicable, the implementer should make records of mDL data processing, including processing by sub-processor, available upon request

The implementer should put in place procedures to verify the identity of the mDL Holder to ensure that only the mDL Holder may access their own data. If this is not practicable in the operational context then the notice and consent process should make clear to the mDL Holder that they will not have access to their own data.

Other considerations

Where participation and access is unfeasible, extra care should be taken to ensure openness and auditability

### Accountability

The mDL Verifier should be accountable for all aspects of the processing of mDL Holder data and provide audit logs and auditability to the mDL Holder.

Risk Considerations

The implementor should have a privacy policy and process to give effect to the considerations in this report

The implementer should appoint a senior executive to be accountable for ensuring the privacy of mDL Holders

The implementer should make the name and the contact details of the accountable privacy officer publicly available and readily accessible.

Other considerations

Where accountability is unfeasible, such as in Use Cases where the processing of mDL Holder data is ephemeral and no data is retained, extra care should be taken with respect to ensuring that Openness and Notice principles are observed.

### Information Security

Personal data of the mDL Holder should be protected by security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

Risk Considerations

The implementer should have an Information Security Management System (ISMS) with safeguards appropriate for the sensitivity of the information it protects.

The ISMS should include:

Administrative safeguards (i.e., contracts or training)

Physical safeguards (i.e., secure facilities)

Technical safeguards (i.e., access control, encryption, etc.)

Other considerations

Systems that process mDL data should consider following a structure security framework such as ISO 2700, COBIT, or the NIST Security Guideline

### Privacy compliance

The mDL Verifier should be accountable for all aspects of the processing of mDL data and should provide audit logs and auditability to the mDL Holder.

Risk Considerations

The implementer should maintain records of mDL data processing

Upon confirmation of the identity of the requestor, the implementer will provide them with copies or access to records of their mDL data processing.

Other considerations

Compliance efforts’ successes depends on ensuring that the implementer’s organization is aware of the current state of regulations and industry practices. This requires a proactive regulatory and standards monitoring program.

## Identity Considerations for the extended architecture

The security of the core mDL transaction under ISO/IEC 18013-5 relies on issuers being the only party allowed to generate and sign mDL attributes. While not included explicitly in the standard, DF-1 is the only interface which is allowed for the generation and modification of the mDL on the Holder’s devices.[[18]](#footnote-18) The dataset contained on the device is limited to the mandatory and optional attributes defined in ISO/IEC 18013-5 and any additional namespace attributes defined by and specific to the issuer. Within the compliant mDL ecosystem, an mDL will have only one valid Issuing Authority. While not required by the ISO/IEC 18013-5 standard, in most cases the mDL Issuer will maintain a database, within their control, which contains a duplication of the datasets for each issued mDL. The requirements for these identity databases will vary based on the local jurisdiction’s regulations and laws.

It is foreseeable that multiple issuers may wish to provide an individual with attribute data under ISO/IEC 18013-5. For example, a Game & Fish regulator of a state may wish to include an individual’s hunting or fishing license within the mDL dataset issued by the DMV. This can be accomplished by one issuer (the DMV in this example) taking the authority and liability to include other attribute namespaces within their mDL issuing infrastructure and issue the mDL credential with the added namespace attributes. Another potential mechanism is creating data attributes which themselves are third-party signed objects such as a Verifiable Credential (VC), JSON Web Signature (JWS) object, or other type of signed data payload to be included within the mDL dataset. If this architecture is used it should be made clear through additional attributes if the third-party signed data was validated at the time of provisioning. Relying parties are advised to consult the relevant namespace standard to confirm the extent to which the issuer assumes responsibility for third-party signed data objects. For completeness, relying parties are advised to include individual validation for third-party signed data objects within their own business processes and should not rely solely on the validation performed during issuance. In lieu of an architecture which includes third-party signed objects, the simplest solution may be a holder’s device containing multiple ISO/IEC 18013-5 compliant documents from different issuers.

In the context of the extended ecosystem, other parties (mDL Holder, mDL verifier, an individual, or relying party for the scope of this report) will only be able to read and verify mDL data. Because the mDL is a composite dataset of Direct Identifiers, Indirect Identifiers, Unique Identifiers, and Quasi-Identifiers, for a given transaction the specific data elements exchanged will determine the level of identity risk. It is the responsibility of the parties involved in the transaction to appropriately handle identity information according to local regulations and good privacy practices during and after the transaction for each type of identifier. Good practice is to ensure that all involved parties in an mDL transaction can adequately assess the transaction risk and then make an informed decision about identity protection requirements by adopting the following principles at a minimum:

1. Adopting the principles of data minimization for all transactions
2. Implementing use, retention, and disclosure limitations
3. Providing the mDL Holder with consent and choice over the release of their attribute data

Additional considerations are presented in the following sections for specific types of identifiers found in the mDL data. A summary table of these considerations are included in Sec. 7.2

### Direct Identifiers

Direct identifiers are attributes that alone enable the unique identification of a data principal within a specific operational context. [REF ISO 20889] For mDL data, like the facial portrait or biometric data, direct identifiers may be self-contextualizing and fully identify the data principal with their solitary release.

Risk Considerations

Direct Identifiers should be encrypted at rest

Direct Identifiers should only be transacted through encrypted channels

Direct Identifiers should not be collected and stored by relying parties without the informed consent of the data principal

If collected, Direct Identifiers should only be stored for the minimum length of time needed to complete business need and comply with applicable jurisdictional and contractual obligations (See [4.1.5 Use, Retention and Disclosure Limitation](#_qwu3w76ebo4p)) after which they should be securely destroyed

**Note**: In most cases for mDL Identification Data, the data principal’s direct identifiers will be core identity information like their name, facial image or other biometric data. The storage and collection of these direct identifiers is inherently high risk because they can identify an individual without context and in perpetuity. This data is difficult, if not impossible, to change after it has been compromised. For all relying parties, it is strongly encouraged that business processes are pursued that do not require the storage of Direct Identifiers[[19]](#footnote-19).

### Indirect Identifiers

Indirect identifiers are attributes that enable unique identification of a data principal within a specific operational context. This context can be provided by the combination with other attributes which may be in the dataset or external to it. [REF ISO 20889]

Risk Considerations

Indirect Identifiers should be encrypted at rest

Indirect Identifiers should only be transacted through encrypted channels

Indirect Identifiers should not be collected and stored by relying parties without the informed consent of the data principal

If collected and stored, Indirect Identifiers should undergo a process of de-identification to protect data principle while meeting business needs

If collected, Indirect Identifiers should only be stored for the minimum length of time needed to complete business need after which they should be securely destroyed

**Note**: In the case of mDLs all collected data can be considered indirect identifiers because the dataset is cryptographically linked through the MSO. Implementers should pursue business processes that do not require the collection and storage of indirect identifiers. If indirect identifiers are collected, business processes should be pursued that make use of de-identification techniques to protect individual identity within the dataset.

### Unique Identifiers

Unique identifiers are attributes in a dataset that alone single out a data principal in the dataset [REF ISO 20889].

Risk Considerations

Unique Identifiers should be encrypted at rest when aggregated with the contextual dataset

Unique Identifiers should only be transacted through encrypted channels

Unique Identifiers should only be collected and stored by relying parties with the informed consent of the data principal

If collected and stored, Indirect Identifiers should undergo a process of de-identification to protect data principle while meeting business needs

Unique Identifiers should not be stored beyond the length of time determined by the business need and should be destroyed securely after they are no longer needed

**Note**: In the case of mDL datasets, all data associated with the mDL are unique identifiers when held on the device as part of the holder’s mDL dataset. In addition to mDL attributes, this includes device keys and any transaction data which may persist on the device such as ephemeral keys, transaction history, or consent receipts when bound to the identifying dataset. Implementers should provide tools and protection measures for this data such as encryption and de-identification techniques.

### Quasi-Identifiers

Quasi-identifiers are attributes in a dataset that single out a data principal when considered in conjunction with other attributes in the dataset [REF ISO 20889]

Risk Considerations

Quasi-Identifiers should only be transacted through encrypted channels

Quasi-Identifiers should only be collected and stored by relying parties with the informed consent of the data principal

If collected and stored, Quasi-Identifiers should undergo a process of de-identification to protect data principle while meeting business needs

Quasi-Identifiers should not be stored beyond the length of time determined by the business need and should be destroyed securely after they are no longer needed

**Note**: The collection of quasi-identifiers is coupled with the additional risk from aggregation. Attributes which may not be identifying on their own can become identifiers when combined with other datasets. The source of this data may be additional attributes collected from the mDL dataset or attributes collected from other datasets like health records or loyalty programs. Data principals will bear the negative outcome from this.

### Identity Attributes in Context

The attributes below are a subset of the ISO/IEC 18013-5 data elements that have been identified for the purposes of this report as identity attributes. To understand the identity risk posed for a transaction, each attribute should be considered on its own without context and within the operational context of the two most common datasets that will be encountered. The first being the dataset that is an individual’s mDL data as held by their mobile device and the second dataset is any collection of mDL data attributes from multiple mDL Holders collected by a relying party or held by the Issuing Authority. Once the risk to identity is understood in its operational context business processes can be chosen to minimize harm posed to involved parties by each risk.

| Attribute | Necessity | Operational Context | | |
| --- | --- | --- | --- | --- |
| Solitary Release | Within holder’s mDL Dataset | Within dataset of multiple mDL Holders or other non-mDL datasets |
| Family Name | Required | Indirect Identifier | Direct Identifier | Direct Identifier |
| Given Name | Required | Indirect Identifier | Direct Identifier | Direct Identifier |
| Birth Date | Required | Indirect Identifier | Unique Identifier | Quasi-Identifier |
| Document Number | Required | Indirect Identifier | Unique Identifier | Unique Identifier |
| Administrative number | Optional | Indirect Identifier | Unique Identifier | Unique Identifier |
| Sex | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Height | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Weight | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Eye Color | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Hair Color | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Birthplace | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Resident Address | Optional | Direct Identifier | Direct Identifier | Direct Identifier |
| Portrait | Required | Direct Identifier | Direct Identifier | Direct Identifier |
| Age in Years | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Birth Year | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| age\_over\_NN | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Nationality | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Resident City | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Resident State | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Resident Post Code | Optional | Not Identifying | Unique Identifier | Quasi-Identifier |
| Biometric template | Optional | Direct Identifier | Direct Identifier | Direct Identifier |
| Name in National Characters | Optional | Direct Identifier | Direct Identifier | Direct Identifier |
| Signature Mark | Optional | Direct Identifier | Direct Identifier | Direct Identifier |

Table 2 Identity Attributes in Context

# Data Flows

## Data Flow 1 (DF-1)

### Overview

Data Flow 1 is the primary flow by which an Issuing Authority issues an mDL to an mDL Holder. This will tend to be proscribed by the Issuing Authority, and each of the interfaces, a & b, below contain several data flows and technical requirements defined outside of ISO/IEC 18013-5.

Graphical user interface, application

Description automatically generated

Figure 4 Data Flow 1

### Specific Privacy Requirements for DF-1

In addition to the general privacy requirements for the extended architecture, implementation should consider the following:

Issuing Authorities may consider following the general privacy requirements for the Issuing Authority Infrastructure for the collection, use, and disclosure of driver personal data outside the confines of the18013 standard for mDL data.

### Specific Identity Considerations for DF-1

In addition to the general identity considerations for the extended architecture, implementation should consider the following:

Out-of-Band confirmation of Holder mobile device control should be used as part of authentication during the provisioning process.

**Note 1**: Holders should take additional consideration in understanding the terms and conditions issuers may place on their mobile devices and management of the mDL. Generally, issuers should prefer a passive management model, relying on mDL validity periods which are as short as possible. If an active management model is pursued holders should be made aware of additional permissions or device management functionally an issuer may request. Additional device access creates the potential for serious privacy implications for the holder through both unreasonable access by an issuer and the potential for unintended consequences due to programmatic bugs which may be exploited.

**Note 2**:DF-1 represents the only channel available for provisioning and management of the mDL on the Holder’s mobile device. (See Section 4.2). Specifically, for the case of provisioning, issuers should weigh the risk of remote interactions with the Holder where privacy and identity risk is greater than an in-person issuance action. These risks are higher because issuance and provisioning necessitates the creation and collection of all identifying elements in the mDL, including the collection of biometrics to create the basis for identity binding in ISO/IEC 18013-5.

## Data Flow 2 (DF-2)

### Overview

DF-2 is the data flow that occurs on the interface between the mDL (presumptively a mobile phone application acting as software wallet containing the mDL) and the mDL Reader. The data flow includes:

1. Engagement through a positive mDL Holder action such as a gesture, NFC tap, or similar positive step.
2. Data Exchange

**Note**: Privacy considerations are more likely to be administrative, such as policies or contracts, while identity considerations are more likely to be technical, such as input validation or encryption.

Graphical user interface, diagram, application

Description automatically generated

Figure 5 Data Flow 2

### Specific Privacy Requirements for DF-2

In addition to the general privacy requirements for the extended architecture, implementation should consider the following:

The implementer should consider physical controls to ensure that the information received by the mDL Verifier is not displayed to others.

The implementer should perform a test of holder presence in the transaction flow as a means to ensure positive holder control of the data released. In ISO/IEC 18013-5 this is achieved through the physical engagement process using an NFC tap or QR code scan.

### Specific Identity Considerations for DF-2

In addition to the general identity considerations for the extended architecture, implementation should consider the following:

The implementer should make clear the intended use and storage policy for the data requested. If the intention cannot be made clear in a single transaction, multiple data transactions should be used to allow the holder fully informed consent. (E.g., an age-verification sale combined with the sign-up for a loyalty program. While this data could all be transmitted in one transaction, the consent to collect and store may not be clear enough to the user and the age verification transaction should be separate from the loyalty sign-up process to ensure the holder has full control over the data release.)

## Data Flow 3 (DF-3)

### Overview

5.3.2 DF-3 is the date flow by which a Verifier requests an mDL Holder’s data directly from the Issuing authority. As defined in ISO/IEC 18013-5, the Verifier must obtain the Holder’s server retrieval token to perform the DF-3 data request. This is accomplished through the use of DF-2 and all Privacy and Identity considerations from DF-2 should apply.

Graphical user interface, diagram

Description automatically generated

Figure 6 Data Flow 3

### Specific Privacy Requirements for DF-3

In addition to the general privacy requirements for the extended architecture, implementation should consider the following:

To protect against surveillance, mDL Verifiers should minimize the information about the mDL Holder from an mDL transaction transferred to the Issuing Authority and the information requested from the Issuing Authority.

In addition to surveillance of the holder’s behavior, DF-3 creates the potential for an Issuer to surveil mDL Verifiers. This risk should be weighed when evaluating the use of DF-3 over DF-2 for mDL verification.

Due to the higher privacy risks, DF-2 should be favored over DF-3 unless required by business need or compliance with applicable jurisdictional and contractual obligations

### Specific Identity Considerations for DF-3

In addition to the general identity considerations for the extended architecture, implementation should consider the following:

The implementers should make the Holder aware that their data is being retrieved online from the Issuer and the Verifier provides no guarantees against the surveillance of the transaction.

## Data Flow A (DF-A)

### 5.4.1 Overview

This data flow has two instances, based on the fact that the mDL Holder actor and the Individual Actor are, in real life, the same natural person holding a single mobile device. It is conceptually the case that mDL data can be held in an app that also holds other or the same information as part of another ecosystem such as a multifunction wallet. It is also the case that the person may have a need to have their ‘wallet’ app read data from their mDL app. These are variants A.1 and A.2 below. DF-A.1 is an “in app” variant where mDL identity attributes are made available as read only fields. DF-A.2 is an on-device variant where another app reads identity attributes from an mDL app. We assume that the mDL is a read-only store for these purposes. Only the mDL issuer should alter the attributes in an mDL.

DF-A.1

Diagram

Description automatically generated

Figure 7 Data Flow A.1

DF-A.2

Graphical user interface, diagram

Description automatically generated

Figure 8 Data Flow A.2

### Specific Privacy Requirements for DF-A

In addition to the general privacy requirements for the extended architecture, implementation should consider the following:

The flow of mDL information to the Wallet should be a read-only flow.

mDL information used to populate fields in a wallet should be under the control of the Individual, such that they can delete the non-mDL fields or their contents from the Wallet

### Specific Identity Considerations for DF-A

In addition to the general identity considerations for the extended architecture, implementation should consider the following:

Because DF-A is occurring on the device, consent of data release may exist beyond a single transaction. Implementers should take appropriate action to inform the Holder of any ongoing consent, including periodic re-authorization.

On-device management and access of mDL data is not in scope of the ISO/IEC 18013-5 standard and all data access over DF-A is undefined data access. If mDL applications make this channel available to mDL Holders and/or mDL implementers the on-device interfaces may be proprietary APIs and may not be standardized between different application vendors which creates additional risk in the ecosystem. Without standardized privacy and identity controls mDL Holders, mDL issuers, and mDL verifiers will carry this additional risk and may not be aware when the level or risk has changed relative to the standardized data flows.

**Note 1**: Holders will carry significant risk when data is transacted over the DF-A interface because they may not be made aware of the operations of DF-A when the mDL application is operating under a non-standard API. One of the most significant risks associated with undefined data access is the potential loss of consent over data release. Holders should be made aware if mDL data is being accessed without their consent. Additionally, data access and identity disclosure risk may change without notifying the mDL Holder because this type of notification is not required during undefined data access. Changes in risk which are not indicated to parties in the transaction creates the potential for increased harm. Holders should exercise increased caution when completing mDL transactions using undefined data access.

**Note 2**: Implementers should pursue business processes which prioritize the use of data flows defined in the ISO/IEC 18013-5 standard. If business processes necessitate the use of DF-A considerations should be taken to meet the privacy and identity considerations discussed herein to protect the mDL Holder’s identity attributes. Also, processes should be pursued to communicate changes of risk level to all parties involved in an identity transaction. Special consideration should be taken to ensure that mDL Holders are given the ability to consent and control the release of their data over DF-A. Holders should be made aware of these risks and the controls available to mitigate these risks.

## Data Flow B (DF-B)

### Overview

This data flow also has two instances for similar use cases as in DF-A. Also note that the ‘mDL Verifier’ and the ‘Relying Party’ in these data flows will be the same entity reading the mDL attributes presented by an mDL Holder.

DF-B.1

A picture containing diagram

Description automatically generated

Figure 9 Data Flow B.1

DF-B.2

Diagram

Description automatically generated with medium confidence

Figure 10 Data Flow B.2

### Specific Privacy Requirements for DF-B

In addition to the general privacy requirements for the extended architecture, implementation should consider the following:

Data from the mDL Reader may only flow to the RP Read Software/Hardware if the Relying Party has provided adequate notice to the mDL Holder about how their mDL data will be consumed by the RP Reader.

### Specific Identity Considerations for DF-B

In addition to the general identity considerations for the extended architecture, implementation should consider the following:

Implementers should consider the impact of combining mDL data with other non-mDL datasets and evaluate the changes of operational context which may occur for the collected identifiers.

## Data Flow C (DF-C)

### Overview

DF-C represents the transport of mDL data off the Holder’s device through any channel not defined in ISO/IEC 18013-5. This data flow presents a very high risk to the mDL Holder because it is not standardized and will be subject to proprietary processes that may not have clear privacy and identity protection by design.

DF-C

Diagram

Description automatically generated

Figure 11 Data Flow C

### Specific Privacy Requirements for DF-C

In addition to the general privacy requirements for the extended architecture, implementation should consider the following:

If using Verified Credentials, consider using the Issuing Authority Infrastructure

Simple graphical captures of physical cards (flash passes) bypass the physical security of the card without substituting any digital equivalent to ensure validity and integrity of the credential.

See the considerations for DF-2

### Specific Identity Considerations for DF-C

In addition to the general identity considerations for the extended architecture, implementation should consider the following:

Due to the largely proprietary nature of the DF-C data flow mDL Holder’s may not be aware of changes in operational context. Implementers should take extra considerations to ensure Holders are informed and provide adequate consent for data released.

## Interoperability Risk

Interoperability of an mDL with an mDL Verifier’s hardware becomes a significant privacy consideration when it interrupts the normal course of business. In most cases when the mDL transaction fails due to interoperability issues the verifier and/or holder, not wanting to abandon the transaction, may attempt to find a work around by leveraging DF-C in an unintended way. When either party pursues a transaction solution outside of scope of the ISO/IEC 18013-5 standard there may be no remaining technical controls in place to protect the Holder’s privacy or identity data. An example of such a work around may be reverting to using the application displayed on the Holder’s device as a flash pass to fulfill the requirements of visual data transmission which is the current method with physical ID cards.

While this work around may interoperate with existing point of sale systems which are designed for the verifier to read data off a physical card, the data minimization and selective data release mechanism built into the ISO/IEC 18013-5 standard may no longer be available to the holder if the mDL vendor has designed their application in that manner. Further, the verifier loses the ability to cryptographically verify the identity information provided and will be limited to making a risk decision based on the visual appearance of a mobile application. In most cases cloning the visual aspects of a mobile application is significantly easier than the security features of a physical ID and puts the verifier at risk of accepting a counterfeit mDL.

Verifiers and Issuing authorities should work together with mobile handset manufacturers and mDL application developers to ensure broad interoperability within the mDL ecosystem. For added protection, mDL developers may build applications which by design cannot be used in a manner other than intended. One such method is to create applications which do not display sufficient information on the mDL Holder’s mobile device to use the application as a flash pass.

# Summary

This report provides identity and privacy considerations for product managers, engineers, compliance teams, architects, developers, assessors, and others with responsibilities for implementing, supporting, or interfacing with mobile credentials. The intent of these considerations to ensure that an mDL Holder can be assured that their privacy and their identity attributes will be protected through the entire life cycle of that information. These considerations include ensuring that the analog protections provided by anti-counterfeiting controls in physical driving licenses do not get bypassed by digital processes that reduce identity protections, such as ‘flash passes’. It is the case that the more control that is vested in the mDL Holder with respect to their own information, the more likely it is that the mDL solution will be able to build trust. The guidance provided here in the Report lays the groundwork for subsequent conformance by developing assessment criteria for each emerging requirement, provided there is ecosystem demand and support to do so, and in a workgroup chartered to do so.

# 

# Appendices

## Additional Considerations

### Security Considerations:

During the discussions leading to this report, a number of particular threat scenarios were identified:

| Threat | Notes |
| --- | --- |
| Issuer private keys are compromised |  |
| Spoofing  that is where the attacker can authenticate using another’s mDL data.  It can also be that the verifier spoofs a known site the user trusts.  Somehow the trust registries need to be made known to the verifier and perhaps to the user. | mDL authentication is performed using a public key. In the Day 1 solution, after authentication, the RP has to tie the authenticated data to the person presenting the data using the authenticated portrait image. The attack here would be a person trying to match the mDL portrait image of someone else. This is a problem with physical cards already, and is expected to become more challenging in the case of a mDL given the higher quality and larger portrait image involved.  The current version of 18013-5 does not address unattended use (i.e., use over the Internet). |
| Unauthorized Information Disclosure (loss of privacy) | 18013-5 supports selective disclosure of information (and informing the mDL holder of the RP's intent to retain the information or not) to address exactly this concern. Having said that, a big concern is that once data is released, the mDL holder has no control any more. |
| Linking | A form of disclosure where one set of attributes are aggregated to the point where the real-world user is identified. |
| Repudiation | This is where a user is able to deny having provided the information. 18013-5 intentionally did not design the mDL for non-repudiation use. |
| Denial of Service | This is where a user is unable to access the resource desired. Note that this includes both intentional and unintentional outages and could be a reliability issue. |
| Tampering | This is where an attacker is able to change the data in-flight. This can be just a form of Denial of Service, or this can result in spoofing one of the attributes, like age.  The mDL in 18013-5 was designed to specifically guard against MITM attacks, and otherwise changing data would require breaking the private document signer key. |

Table 3 Additional Security Considerations

## Identifier Protection Summary

The following table is a summary of identity protection considerations for the types of identifiers contained in the mDL dataset.

|  | Direct Identifier | Indirect Identifier | Unique Identifier | Quasi-Identifier |
| --- | --- | --- | --- | --- |
| Encrypted at Rest | Yes | Yes | Yes | Yes, if stored in identifying context |
| Encrypted in transit | Yes | Yes | Yes | Yes |
| Collected and stored without consent | No | No | No | No |
| Stored for minimum length of time needed | Yes | Yes | Yes | Yes |
| Undergo a process of de-identification if stored | Yes, but storage should be minimized if possible | Yes | Yes | Yes |

## Bibliography

The Mobile Driver’s License (mDL) and Ecosystem, The Secure Technology Alliance, Version 1, March 2020, https://www.securetechalliance.org/wp-content/uploads/Mobile-Drivers-License-WP-FINAL-Update-March-2020-4.pdf

## Terminology

This section defines terms and abbreviations as they are used in this report.

| Term | Definition(s) |
| --- | --- |
| API | Application Programming Interface |
| APDU | Application Protocol Data Unit |
| BER | Basic Encoding Rules |
| BLE | Bluetooth Low Energy |
| BT SIG | Bluetooth Special Interest Group |
| CA | Certificate Authority |
| CBOR | Concise Binary Object Representation |
| CDDL | Concise data definition language |
| COSE | CBOR Object Signing and Encryption |
| CSPRNG | Cryptographically Secure |
| CRL | Certificate Revocation List |
| DER | Distinguished Encoding Rules |
| DO | Data Object |
| DS | Document Signer |
| ECDH | Elliptic Curve Diffie-Hellman |
| Flash Pass | Visual presentation of an image of a mobile ID without cryptographic verification |
| GATT | Generic Attribute Profile |
| GUID | Globally Unique Identifiers |
| HKDF | HMAC-based Extract-and-Expand Key Derivation Function |
| IA | Issuing Authority |
| IACA | Issuing Authority Certificate Authority |
| IAPC | Issuing Authority Point of Contact |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EdDSA | Edwards-curve Digital Signature Algorithm |
| IDL | ISO-compliant driving licence |
| IKM | Input Keying Material |
| JWT | JSON Web Token |
| JWS | JSON Web Signature |
| JWA | JSON Web Algorithms |
| KDF | Key Derivation Function |
| MAC | Message Authentication Code |
| MITM | Man-in-the-middle attack |
| ML | Master List |
| MSO | Mobile Security Object |
| MTU | Maximum Transmission Unit |
| NDEF | NFC Data Exchange Format |
| NFC | Near Field Communication |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OIDC | OpenID Connect |
| PIX | Proprietary Application Identifier Extension |
| PKI | Public Key Infrastructure |
| RID | Registered Application Provider Identifier |
| TLS | Transport Layer Security |
| TLV | Tag Length Value |
| UHF | Ultra-High Frequency |
| Undefined data access | Access of mDL data by a method not included in ISO/IEC 18013-5 |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UTC | Coordinated Universal Time |
| UUID | Universally unique identifier |

*Table 5.*

1. <https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=136675376> [↑](#footnote-ref-1)
2. <https://kantarainitiative.org> [↑](#footnote-ref-2)
3. ISO/IEC 18013-5 Personal Identification — ISO-compliant driving license — Part 5: Mobile driving license (mDL) application. At the time of writing this draft, the standard is at the DIS (Draft International Standard) and should be finalized in 2021. [↑](#footnote-ref-3)
4. Mobile device manufacturers may enable various ID credential API’s or capabilities, for example. [↑](#footnote-ref-4)
5. We note that at the time of writing, the mDL standard does NOT include the use of on-line transactions. Because extending the mDL ecosystem to include on-line transaction and unattended mDL Holder authentication is planned, the report may include commentary or suggestions related to on-line presentation of mDL both with and without unattended authentication, these elements of the report will be preliminary or suggestive. Online mDL functionality is now expected to be released in ISO/IEC 18013-7. [↑](#footnote-ref-5)
6. For purposes of this Report, a credential that uses a data model different from what is described in clause 7 of ISO/IEC 18013-5 but otherwise follows ISO/IEC 18013-5 is considered compliant with ISO/IEC 18013-5. [↑](#footnote-ref-6)
7. The charter says ‘will’, but the DG notes that we can’t predict this for sure. [↑](#footnote-ref-7)
8. Discussion Group Charter: <https://kantarainitiative.org/confluence/display/mdl/Charter> [↑](#footnote-ref-8)
9. Future developments of mDL’s, while out of scope of this report, are likely to include a need for validating devices, applications, and services and for that validation to be verified dynamically at the time of transaction. [↑](#footnote-ref-9)
10. The table of contents and some of the introductory material is viewable on the ISO Online Browsing Platform at <https://www.iso.org/obp/ui/#iso:std:iso-iec:18013:-5:dis:ed-1:v1:en> [↑](#footnote-ref-10)
11. The intent is to leverage existing standards and/or best practices as far as possible. [↑](#footnote-ref-11)
12. See the Mobile Driver’s License Initiative on the STA website: <https://www.securetechalliance.org/mobile-drivers-license-initiative/> [↑](#footnote-ref-12)
13. <https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/> [↑](#footnote-ref-13)
14. See Annex E of ISOISO/IECISO/IEC 18013-5 or ISO/IEC 29100 for a list of the privacy principles enumerated here. [↑](#footnote-ref-14)
15. Examples are available in the Kantara Consent Receipt Specification 1.1 [https://kantarainitiative.org/download/7902/](https://www.google.com/url?q=https://kantarainitiative.org/download/7902/&sa=D&source=editors&ust=1618701314264000&usg=AOvVaw2LMvH3EH1d0TN-bJrEETgh) or the JLINC protocol [https://protocol.jlinc.org/](https://www.google.com/url?q=https://protocol.jlinc.org/&sa=D&source=editors&ust=1618701314264000&usg=AOvVaw05inMvTRmGbMPsRfWqyBY3" \o "https://www.google.com/url?q=https://protocol.jlinc.org/&sa=D&source=editors&ust=1618701314264000&usg=AOvVaw05inMvTRmGbMPsRfWqyBY3) which includes a log of permissions and an Information Sharing Agreement in JSON-LD [↑](#footnote-ref-15)
16. See the Kantara Consent Receipt 1.1 data structure, ISO 27560 (in process), UMA, JLINC as potential examples [↑](#footnote-ref-16)
17. ISO/IEC 20889 [↑](#footnote-ref-17)
18. DF-1 will be explicitly covered under the forthcoming standard ISO/IEC 23220 [↑](#footnote-ref-18)
19. The Kantara Initiative Report on Blinding Identity Taxonomy may be useful for some use cases. [↑](#footnote-ref-19)