What's new in ISO mDL?

Update to W3C CCG 2023-12-12 by AndrewHughes3000@gmail.com

Items for today

- A note about the International Organization for Standardization (ISO) and ISO-IEC JTC 1
- A brief history of ISO/IEC mDL standards family
- ISO/IEC 18013-7 for mDL presentation "over the internet"
- What's coming next?

International Organization for Standardization

ISO: Global standards for trusted goods and services

- Standards define what great looks like, setting consistent benchmarks for businesses and consumers alike — ensuring reliability, building trust, and simplifying choices.
- Making lives easier, safer and better.

ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 169 national standards bodies.

ISO is over 75 Years old

ISO has developed over 25,086 International Standards in 825 Technical committees and subcommittees

For in-depth information: https://www.iso.org/structure.html

Source: iso.org

ISO-IEC Joint Technical Committee 1

ISO-IEC Joint Technical Committee (JTC 1) is a consensus based, voluntary international standards group focussing on information technology (IT)

JTC 1 is committed to developing, maintaining, promoting and facilitating information technology (IT) standards required by global markets meeting business and user requirements.

ISO/IEC JTC 1 members are National Bodies, which include representatives from producers, governmental and public agencies, academia, businesses and other users. The diversity ensures a broad-based, open and balanced representation in the standards development process, which also considers societal aspects of the standards.

For in-depth information: https://jtc1info.org/sd-2-history/

JTC 1 was formed in 1987 and has published over 3000 ISO standards

Source: jtc1info.org

The family of mDL projects within ISO-IEC JTC 1/SubCommittee 17

ISO/IEC 23220 project family for generic mobile eID

ISO/IEC 23220-n are framework specifications for the mdoc format and protocols.
They can be (and have been) profiled to specific scenarios such as ISO/IEC 18013-5 & ISO/IEC 18013-7 for mDL.

- ISO/IEC 23220-1   Part 1: Generic system architectures of mobile eID systems [Published 2023]
- ISO/IEC 23220-2[†]   Part 2: Data objects and encoding rules for generic eID systems
- ISO/IEC 23220-3[†]   Part 3: Protocols and services for issuing phase
- ISO/IEC 23220-4[†]   Part 4: Protocols and services for operational phase
- ISO/IEC 23220-5[†]   Part 5: Trust models and confidence level assessment
- ISO/IEC 23220-6   Part 6: Mechanism for use of certification on trustworthiness of secure area

[†] *These projects started in 2019, hit their ISO Publication Process limit dates and were formally restarted in 2023.*
Deadline for publication is no later than mid-2025.

ISO/IEC 18013-5 timeline

- Preparatory work started 2015
- Project approved 2018
- ISO/IEC 18013-5 published as an International Standard September 2021
- Mandatory periodic review in 2026

Stage	Version	Description	Go to draft	Target date	Limit date	Started	Status
10.00	1	Proposal for new project registered				2015-05-06	Closed
10.20	1	New project ballot initiated				2015-05-06	Closed
10.60	1	Close of voting				2015-08-08	Closed
00.60	1	Close of review				2015-08-11	Closed
10.00	2	Proposal for new project registered				2017-10-02	Closed
10.20	2	New project ballot initiated		2017-10-03		2017-10-03	Closed
10.60	2	Close of voting		2017-12-26		2017-12-28	Closed
10.99	2	New project approved				2018-03-27	Closed
20.00	1	New project registered in TC/SC work programme				2018-03-27	Closed
30.00	1	Committee draft (CD) registered				2018-04-26	Closed
30.20	1	CD study/ballot initiated				2018-04-27	Closed
30.60	1	Close of voting/comment period				2018-06-23	Closed
30.92	1	CD referred back to Working Group				2019-03-27	Closed
30.00	2	Committee draft (CD) registered				2019-03-27	Closed
30.20	2	CD study/ballot initiated				2019-03-28	Closed
30.60	2	Close of voting/comment period				2019-05-24	Closed
30.99	2	CD approved for registration as DIS				2019-11-26	Closed
40.00	1	DIS registered		2020-01-30	2021-03-27	2019-12-03	Closed
40.20	1	DIS ballot initiated		2020-02-04		2020-02-04	Closed
40.60	1	Close of voting		2020-04-28		2020-04-29	Closed
40.99	1	Full report circulated: DIS approved for registration as FDIS				2021-02-16	Closed
50.00	1	Final text received or FDIS registered for formal approval		2021-02-27		2021-02-23	Closed
50.20	1	Proof sent to Secretariat or FDIS ballot initiated: 2 months		2021-06-22		2021-06-22	Closed
50.60	1	Close of voting -- Proof returned by Secretariat		2021-08-17		2021-08-18	Closed
60.00	1	International Standard under publication				2021-08-18	Closed
60.60	**1**	**International Standard published**		**2021-09-29**	**2022-03-27**	**2021-09-29**	**Current**
90.20	1	International Standard under periodical review		2026-07-14			Awaiting
90.60	1	Close of review		2026-12-01			Awaiting
90.92	1	International Standard to be revised					Awaiting
90.93	1	International Standard confirmed					Awaiting
90.99	1	Withdrawal of International Standard proposed by TC or SC					Awaiting
95.99	1	Withdrawal of International Standard					Awaiting

Other relevant 18013-n projects

ISO/IEC 18013-6   Part 6: mDL test methods

ISO/IEC TS 7367   ISO-compliant vehicle mobile registration certificate

Interoperability test events

In parallel (but separate) to ISO, the members have been holding one or two interoperability test events per year for 18013-5 and 18013-7 functions.

The most recent before last week was August-September 2023 coordinated by SpruceID for 18013-7 remote presentation.

Report is here:
https://blog.spruceid.com/iso-iec-18013-7-interoperability-event-results/

ISO/IEC 18013-7
a.k.a. "mDL over the internet"

ISO/IEC 18013-7

ISO-compliant driving licence — Part 7: Mobile driving licence (mDL) add-on functions

Scope:
This document augments the capabilities of the mobile driving licence (mDL) standardized in ISO/IEC 18013-5 with the following additional functionality:
—Presentation of a mobile driving licence to a reader over the internet.

What is included in ISO/IEC 18013-7?

Interface 2:
—when the mDL Reader is a website rendered on a mobile device web browser

—and the mDL app is located **on the same device**.

Protocols:
—"mdoc device retrieval to a website" (a.k.a. The REST API) and
—"OpenID for Verifiable Presentations mDL profile" (OpenID4VP)
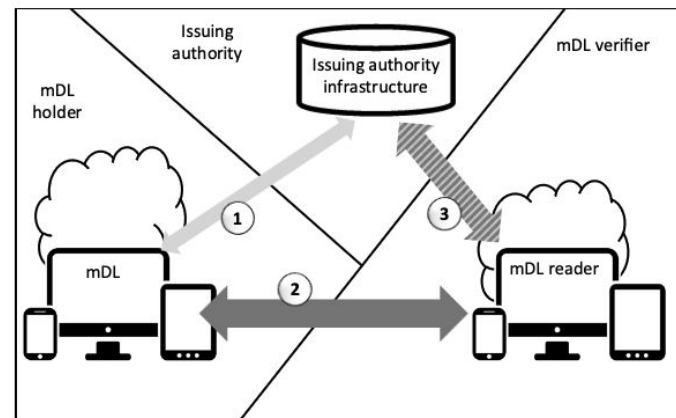

Figure 1 - mDL interfaces

…but, it's complicated…

A note about protocol initiation direction

In 18013-5 the mDL app (typically) offers engagement data to the mDL reader - to establish a secure channel.

In 18013-7 this is conceptually reversed - the mDL reader offers engagement data to the mDL app.

> However, 18013-7 also permits the possibility that the engagement data is supplied to the mDL app out-of-band, using a pre-existing channel, or in other ways.

What is included in ISO/IEC 18013-7?

ISO/IEC 18013-7 is additional functions for ISO/IEC 18013-5.

Things that carry over from part 5:

- Data structures and data elements models - i.e. part 7 is for mdoc/mDL data structures
- The "interfaces" conceptual model
- Many security mechanisms including encryption, session management, mdoc/reader roles

The *intention* of ISO/IEC 18013-7 is to transport mdoc/mDL "over the internet" *just like* Part 5 transports mdoc/mDL over BLE, NFC, WiFi Aware.

Mobile Devices Are... Different

A mobile device is not like a super-small laptop

Mobile device operating systems, software constraints, hardware constraints, and the strict level of app sandboxing are different from desktop systems. Assumptions made about the mobile device environment are often wrong.

Some functionality works differently, notably
—the ability of one app to have any information about any system resources or other installed apps, and
—'everything' operates in a sandbox which controls what is visible or available to an app.

Challenges for the ISO WG

In no particular order:

- We want guarantees that the mdoc app has domain origin info from where it received the engagement information, so that it can pass this to the mdoc reader, to detect malicious forwarding of engagement data
  - There are no guarantees available - some mobile browsers support this some of the time
- Typical methods used to invoke native apps on a mobile device are not fit for mdoc purposes
  - URL schemes/handlers: do not provide consistent outcomes on mobile devices, particularly when more than one "wallet app" is available
  - Universal/App Links: behaviour when target app not installed gives poor UX and may leak info
- If there are many wallets installed, do we really expect normal people to receive a digital credential request on their mobile device, know where the credential might be stored, then select/send the intended and correct credential?
  - Seems optimistic or foolish depending on your level of cynicism.

No easy solutions

The ISO WG is negotiating internally how to standardize in non-harmful ways that are implementable and have reasonable UX potential.

- Related work in W3C Web Incubator CG underway on identity-credential browser API
  - The concept is that a web page rendered in a mobile browser can call a mobile browser API to initiate credential/wallet selection, transfer of credential request information to the correct app, retrieval of the credential, and delivery (in some manner) of the credential to the requesting web site
  - Major browsers/mobile OS vendors are active participants
  - The work was proposed by ISO WG members (but is not controlled by the ISO committee in any way)
  - Standardization will not happen soon enough - not clear what will be done to make implementations emerge
  - Tons of complexity involved in the 'many wallets, many credentials' scenario

The near future

Timeframe for Part 7

ISO Committee is meeting (this week!) to discuss the latest round of proposals.

- Goal is to produce a draft that National Bodies can review and vote (with comments for improvements).
- If everything goes well with an interim solution, publication could happen in 2024.

NIST/DHS is getting ready for a project on mDL implementation - call opened in Fall 2023

After 18013-7 is published, the ISO Committee will evaluate our burndown list and decide what to work on next.

- Person-as-credential-subject binding/proving is very high on the priority list.

Andrew Hughes

FaceTec Inc.

VP of Global Standards
(as of November 2023!)

andrew@facetec.com
andrewhughes3000@gmail.com