Mobile Driver’s License

2017 Region IV
May 24, 2017
Seattle, WA
Presenter:

Loffie Jordaan

Senior Project Manager, AAMVA
• Introduction & background
  • CDS Committee & eID WG
  • What is a mDL?
  • Functional requirements
  • Additional considerations
  • Solution concepts

• What is happening now:
  • Standardization
  • Hot topics
  • Initiatives (including AAMVA/RDW Proof of Concept)
Joint initiative between:

- Card Design Standard Committee
  - Interoperability (including DLs)
  - Representing jurisdictional views to other stakeholders (e.g. standards organizations)
- eID WG
  - Standards for electronic identity
  - mDL a first manifestation

AAMVA mDL White Paper
What is a mDL?

- A driver’s license stored on or accessed via a device such as a smart phone or tablet

- One-function wearables (e.g. to prove age) are being discussed
mDL Functional requirements

- Confirm the mDL holder’s identity
- Convey driving privileges
- Work off-line
- Be trusted
- Work across jurisdictions
- Support selective information release (by mDL holder)
- Support remote management (by jurisdiction)
- Easy to use
- Acceptable processing time
- Unattended verification
Use case examples

- TSA
  - 600 million + verification actions per year
- Road stop
  - 26 million + verification actions per year
- Age verification for alcohol purchases
  - 400 million + verification actions per year
- Car rental
- Identification to receive social services
- Hotel check-in
- Identification for financial services
Additional considerations

- Financial
  - Solution cost
    - Reader infrastructure
    - Office processes
    - Systems
    - Outreach/education/training
  - Revenue streams

- Legal
  - Existing legislation may be inadequate
  - Model legislation available
Additional considerations

- Operations
  - Remote revocation of privileges
  - Multiple mDLs for the same person
- What happens to released information?
- Procurement
  - Different needs
  - Shorter lifecycle
Solution concepts

Issuing Authority

mDL

Verifying Entity

Reader & infrastructure

Safe Drivers · Safe Vehicles · Secure Identities · Saving Lives
Areas of standardization

Issuing Authority

1

mDL

2

Verifying Entity

3

Reader & infrastructure

Safe Drivers · Safe Vehicles · Secure Identities · Saving Lives
Standards impacted by:

- Location of data
  - “Container on a phone”
  - “Get PII from the source”
- Attended vs. Unattended
- Data exchange protocol
- Trust model
“Container on phone”

- Data stored on device in a secure container
- Container security up to the Issuing Authority
- Reader verifies data authenticity using IA’s public certificate
- Also referred to as the “offline” model
• Data always retrieved from IA; always current
• No PII on mDL itself
• Secure tokens used to convey mDL holder’s consent to release information to requestor
• Real-time connection to IA required (i.e. no offline option) (hence also referred to as the “online” model)
• IA to maintain a 24/7 real-time interface
• Attended: Portrait image ties mDL holder to mDL
  • Standard approach with physical card
  • Comparison typically performed by a human

• Unattended: Something mDL holder has/knows ties mDL holder to mDL
  • Need first identified by Japan for vending machine use
  • Would allow online use of mDL to confirm identity
• Crucial for mDL holder to know who is reading mDL
  • Tap
  • Show barcode on device
• Subsequent exchange of information via:
  • Barcode
  • Bluetooth
  • NFC
• Somewhere in the process, mDL holder explicitly identifies information to be shared
Verifier needs something from the IA
- Needs to establish a relationship, directly or indirectly
- Needs to establish that the IA is “genuine”
- Needs a mechanism for data exchange

“Container on a phone” model
- Need IA’s public certificate
- Challenge: Confirming origin of public certificate
  - A trusts C because A trusts B and B trusts C
- Logistics of certificate exchange
  - TBD
  - ICAO: Central PKD
  - Blockchain?

“Get PII from source” model
- Need address from which to request data
- Need to prevent “honey pot” attacks
Current standardization focus

- Now:
  - Offline attended
  - Online attended
  - Basic functionality only

- Later:
  - Enhancements to attended cases
  - Offline unattended
  - Online unattended
Current topics

• Terminal registration
• Financial model
• Unattended use
• Scope
Revenue possibilities

• Terminal registration required:
  • Verifying entity can be charged
    • Reader license fee
    • Online: Each read action

• Terminal registration not required:
  • Charging verifying entity challenging
Privacy (online solution)

- Terminal registration required:
  - Issuing Authority can track where mDL was read
  - Technical solutions possible to make tracking more difficult
  - Protection by policy

- Terminal registration not required:
  - Issuing Authority does not know where mDL was read

- (For online solution, Issuing Authority always knows that a mDL was read)
Registration effort

- Terminal registration required:
  - Issuing Authority has to register, directly or indirectly, all verifiers (law enforcement, government, private sector, citizens, world-wide)

- Terminal registration not required:
  - No registration effort
Where can mDL be used?

• Terminal registration required:
  • Only at registered verifiers

• Terminal registration not required:
  • Anywhere
Terminal registration

Public certificate (trust model)

- Terminal registration required:
  - Can potentially be exchanged during registration process

- Terminal registration not required:
  - Verifying entity has to obtain Issuing Authority’s public certificate
Liability

• Terminal registration required:
  • Issuing Authority can potentially held liable if verifying entity misuses information

• Terminal registration not required:
  • No liability of data misuse on Issuing Authority
Revenue options

• User pays
  • Per app download
  • Per period of app use (e.g. per year)

• Verifying entity pays
  • Terminal registration
  • Pay per read (online solution only)
  • License reader
- On mDL standardization development path
- Not part of initial focus
Traditional DL good for:

• Proving identity
• Proving age
• Proving address
• Conveying driving privileges
mDL additionally good for:

• Data minimization, mDL holder control
• Improved data freshness
• Improved data accuracy
• Unattended use
• “Coolness”
Current initiatives

- Iowa pilot, RFP
- VA pilot
- Studies by other states
- DVLA (UK)
- Trafi (Finland)
- ICAO
- Vendor solutions
- AAMVA/RDW proof of concept
Based on AAMVA White Paper
Focus on mDL / reader interaction
Free participation
Goal: Enable an issuing authority to explore mDL/reader interaction operationally

Limitations:
- Does not cover reader / issuing authority interaction
- Supports 100s of mDL holders, not 1,000s
- No actual PII allowed (other than image)