Spring Workshop mDL Presentation

2016-03-09
Presentation overview

- CDS Committee & eID WG
- What is a mDL?
- Functional requirements
- Additional considerations
- Solution concepts
- What next?
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
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
Additional considerations

- Financial
  - Solution cost
  - Revenue streams
- Legal
- Operational
- Multiple mDLs for the same person
- Procurement
Solution concepts

- Barcode
- “Container on phone” model
- “Cloud” model

Sources:
- Vendor input & participation in the CDS/eID group
- International discussions within ISO
- Presentations at international conferences
Barcodes

- All DL information stored in a barcode
- Barcode includes portrait image
- Consumer matches mDL holder to portrait image from barcode
Barcodes

• Benefits:
  • Standard already exists
  • Authentication mechanisms already standardized
  • Relatively simple cross jurisdictional use
  • Works on any phone that can display a barcode
  • Offline use

• Challenges:
  • Data release: All or nothing
  • Data currency
  • Barcode capacity (and readability)
“Container on phone” model

• Data stored on device in a secure container
• Device interacts with reader using standardized commands
• Could use NFC, Bluetooth, etc.
• “Secure element” needed to protect data
• Data released only if:
  • mDL holder provides consent
  • Consumer is authorized
• Benefits:
  • Increased data capacity
  • Improved data protection

• Challenges:
  • Multiple device platforms to support
  • Not all devices use the same communication method
  • Speed
  • Cross-jurisdictional use
Data always retrieved from issuer

Data released only if:
  • mDL holder provides consent
  • Consumer is authorized

Process-driven:
  • Consumer sends a request for information to mDL holder’s device
  • mDL holder’s device obtains a one-time token from the issuer, adds approval for information release, and exchanges this with the consumer
  • Exchange between mDL holder and consumer can be via barcode, NFC, Bluetooth, etc.
  • Consumer submits approved token to issuer, and retrieves information
“Cloud” model

• Benefits:
  • No data on mDL holder’s device
  • Data is always current

• Challenges:
  • Off-line operation
  • Speed
  • Cross-jurisdictional use
Draft mDL standard
For More Information

Contact:

Loffie Jordaan
ljordaan@aamva.org

Geoff Slagle
gslagle@aamva.org