2015 region III information exchange
Oak Brook, IL | November 3-5

# mDL…driven by functional needs

## November 4, 2015

Geoff Slagle – Director, Identity Management
AAMVA

# Overview

- Card Countermeasure “Tool box”
- mDL Standardization
- Moving forward globally…

# Current Countermeasures for Cards

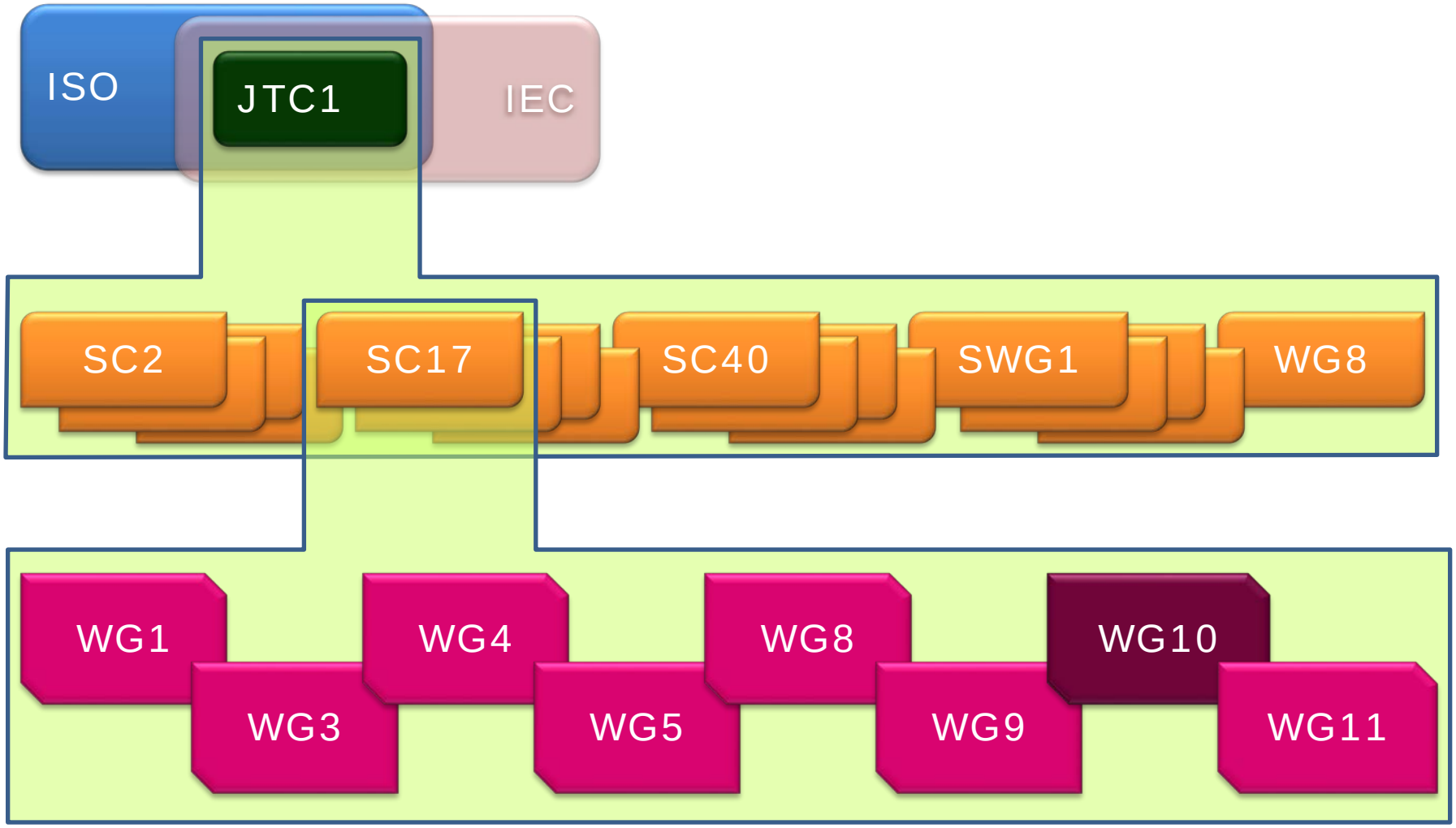
- Warning Systems ⓘ Balance of who has access
  - Something done, Something coming
- Training ⓘ General Access
  - Genuine, Fraudulent, People, Behavior
- Authentication ⓘ Direct collaboration vs. Reverse engineered
  - Document authentication
- Source Verification ⓘ Document not addressed
  - Data verification
- Standards ⓘ Voluntary
  - Secure, Uniform, Interoperable
- Legislation ⓘ Slap on the wrist (non-obvious prosecution routes)
  - Penalties

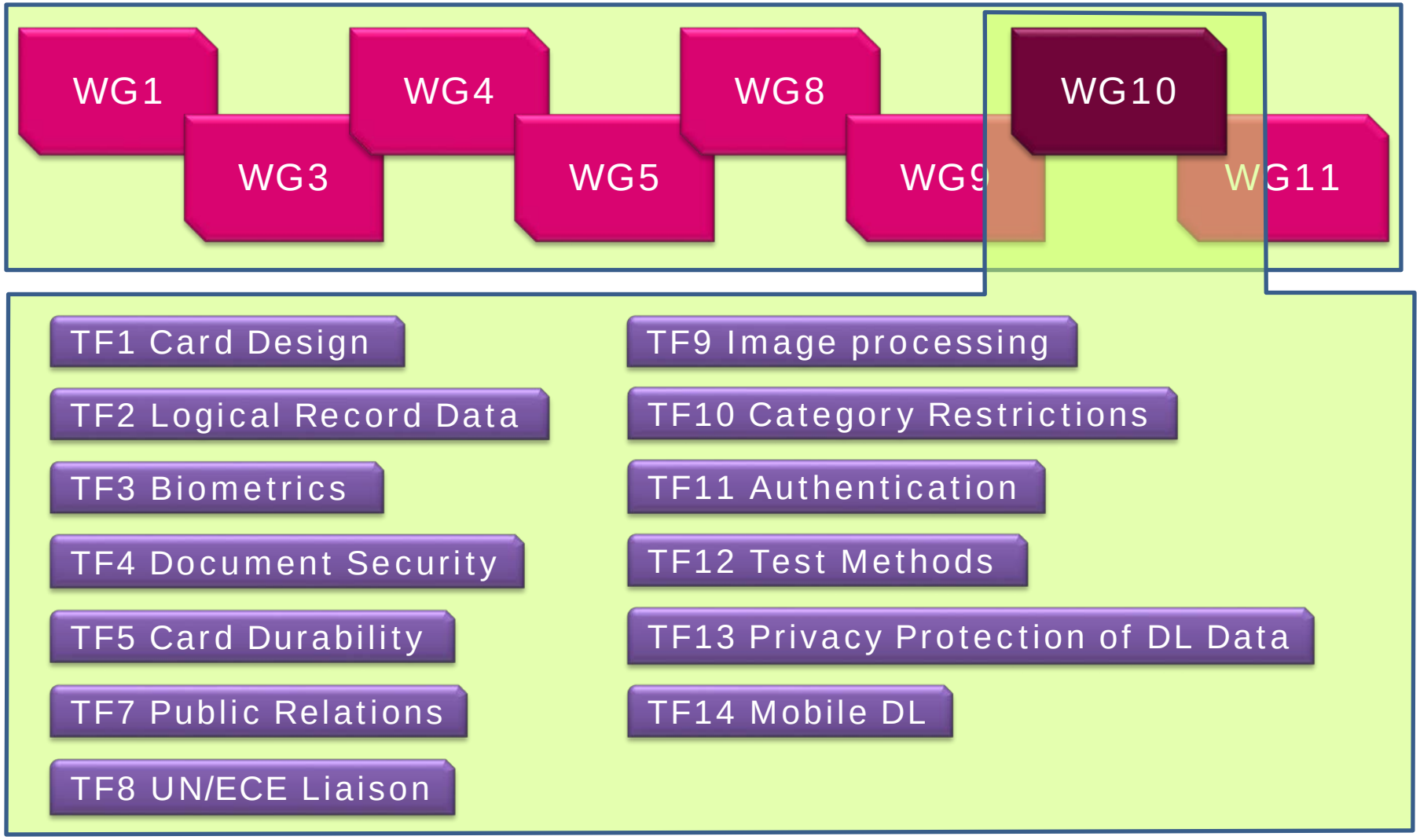
# Reality Check

- "Give-a-darn-ameter"
- Subjectivity with overdependence on human inspection (flash pass is alive and well…unfortunately)
- Future of identity will involve a migration away from "physical" proof and will be a electronic exercise (e.g. smart phone instead of card) – significant driver eID/NSTIC

# Current/Ongoing efforts

- Joint AAMVA Committee (CDS/eID)
  - Complementary scopes
  - Functional requirements
  - Actual standardization
  - November 17 – 19 meeting – “Industry day”
- Global efforts around mDL standardization
  - Payments industry lessons learned
  - ID value to mDL = ***game changer***





Functionally a mDL must…

- Convey driving privileges
- Tie the holder to the license
  - Typically using portrait image
  - Biometrics are possible
- Be trusted; “Consumer” must have confidence that…
  - License was issued as claimed
  - No unauthorized changes since issuance

Entities that have a need to read and authenticate a mDL include:

- Issuing authorities
- Law enforcement
- Commercial establishments (e.g. banks, bars, car rental)
- Citizens (e.g. to exchange information after a crash)

**Reading and authentication solution should work for all of these entities**

# Binding

- Biometrics, PIN, other mechanisms can be used to link mDL to holder
- Alternatives may augment, but may require additional training and equipment

# Form factor

- Physical solution should allow simultaneous view of:
  - DL holder, and
  - Portrait image extracted from mDL
  - Biographical information as seen on physical card

# Online/Offline

- For most use cases, offline use is the exception
- For some DL consumers, offline use may be the norm

- Processing time important
  - For many applications, should be comparable to using physical card
- Minimize additional reading equipment (e.g. to be carried by Law Enforcement)
- Limit physical contact between mDL carrier and reading equipment
  - Liability issues
  - Reading distance influences operational procedures

# Financial Considerations

- Reader infrastructure, everywhere a mDL is consumed
- Changes in office processes
- System infrastructure
- Outreach/education/training
- Impact on existing revenue streams

# Legal/policy considerations

- Recognition (Jurisdictional statute change, CDL pinned to standards)
- Process when mDL cannot be read successfully
- Unavailability of reading equipment
- Existing legislation
- Number of mDLs
- Remote revocation of driving privileges
- Control by mDL holder of information released

DL administrators (Globally) are looking to Industry to devise solutions that:

- Reliable mechanism to issue, revoke/suspend, terminate and transfer mDL
- Enable a wide variety DL consumers to read and to establish trust in a mDL
- Require minimal additional reading equipment
- Support offline use
- Support interoperability (i.e. cross-jurisdictional and cross-vendor use)

# Questions?

Geoff Slagle
Director, Identity Management
AAMVA
4401 Wilson Blvd., Suite 700
Arlington, VA 22203
Phone: 703.342.7459
Email: **gslagle@aamva.org**