Critiquing the Three Party Model

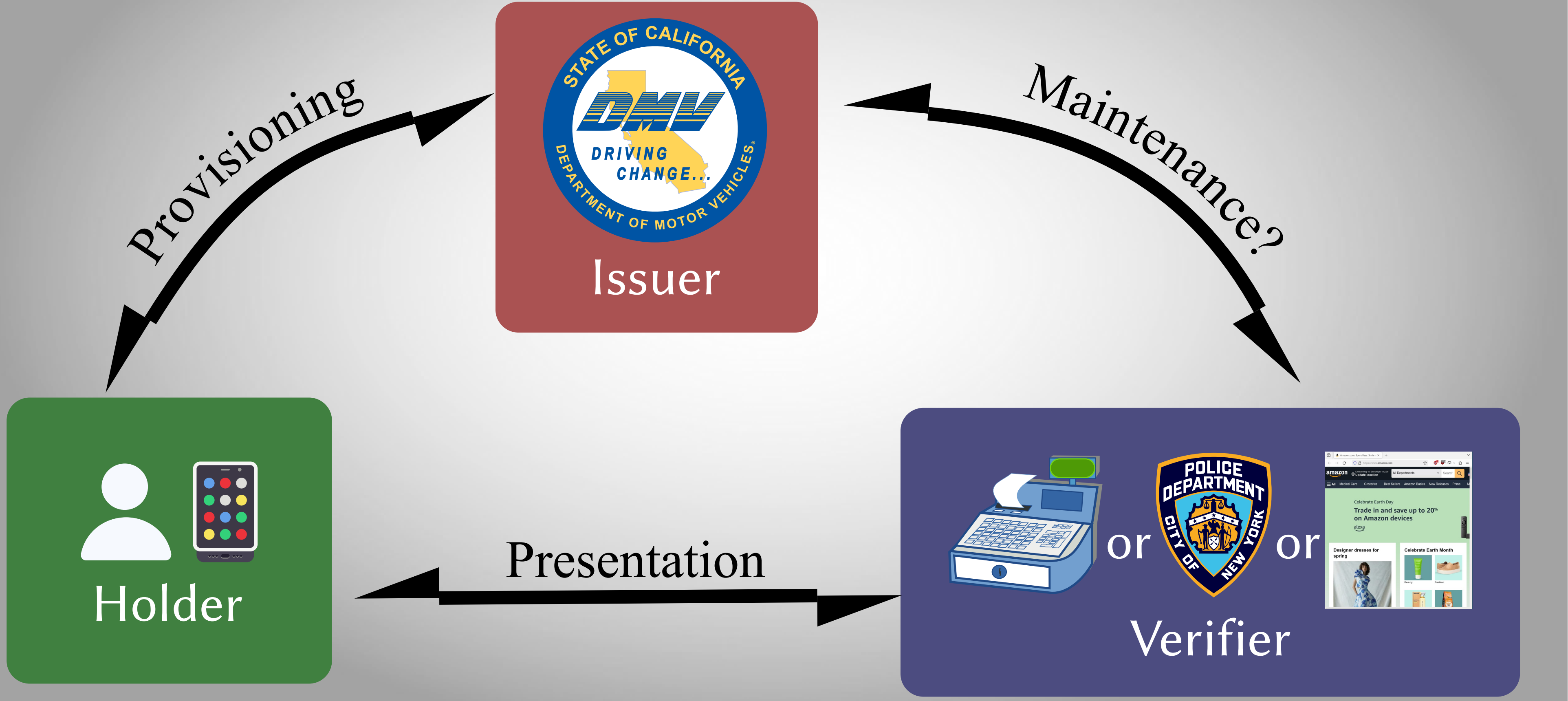
Protocol Analysis of Digital Credential Systems

Daniel Kahn Gillmor <dkg@aclu.org>

ReCAP Workshop 2024

Digital Credentials

Three-party model



Issuer

Holder

Verifier

Provisioning

Maintenance?

Presentation

Formal Actors

- Holder
  - Person who the credential is supposed to reflect
- Issuer
  - Agency the credential comes from (DMV, Employer, Gov’t)
- Verifier
  - Entity confirming something about the person

Other participants

- Contractor (works for Issuer or Verifier)
- OS Vendor (provides Holder with device/APIs)
- Wallet Supplier (provides Holder with software)
- Verification Vendor (provides hardware/software for use by verifier)
- Network Operator (sees traffic between actors)

Actions

- Provisioning
  - How does the Holder get a credential from the Issuer on their device?
- Presentation
  - How does the Holder prove their identity (or an attribute) to a Verifier?
- Maintenance/Configuration
  - How does a Verifier know which Issuers to rely on? How do they get updates or confirmation?

Sensitive Negative Outcomes

- Forgery (impersonation)
- Forgery (invalid attributes)
- Leakage of sensitive information about the Holder
- Metadata harvesting (who did what when?)
- Credential Misuse (e.g. after revocation or expiration)

Who is the **Adversary**?

- Provisioning typically defends the Issuer from a malicious **Holder**, requiring a Holder to demonstrate things about themselves and their devices
- Presentation typically defends a Verifier from a dishonest, malicious, expired, or revoked **Holder**
- Maintenance and Configuration are rarely specified, or are treated as “out-of-band”

Who is the **Adversary**? (continued)

- **Holder Device** Attestation
  - In Presentation or Provisioning, does the **Holder's device** prove that it is running known code on known hardware? (it is *not in the Holder's control*)
- Biometrics (or other "device binding")
  - Can the Verifier be certain that the human operating the **Holder's device** is the correct human?

Optional Mitigations

- “Offline” Presentation
  - Presentation only requires synchronous communication between Holder and Verifier (but Verifier could retain data and transmit later)
- Selective Attribute Disclosure (Presentation)
  - (e.g., “21+”) Defends details about the Holder from a nosy Verifier (but Verifier might still link one use with another at a later time; depends on size of anonymity set)
- Unlinkable Presentations
  - Defends persistent tracking of a Holder from colluding Verifiers (only works with selective disclosure, with large anonymity sets, and depends on no other corroborative linkage)

Rare Defenses of the Holder

- Verifier Identity
  - How does the Holder know who the Verifier is?
- Right to Request
  - How does the Holder know that the Verifier can legitimately request what they are requesting?
- Verifier Device Attestation
  - Does the Holder know that the Verifier’s device is doing what it claims to do?
- Key/Certificate Transparency
  - Lets the Holder (or their agent) detect when Issuer produces fake credentials

Examples

- ISO 18013-5
- W3C's Verifiable Credentials
- OAuth
- ...