The work reported here was sponsored by a SBIR Phase I grant from the US Department of Homeland Security. It does not necessarily reflect the position or policy of the US Government.

Multifactor Identity Verification without Prior Relationship

Five Techniques for Remote Identity Proofing

Francisco Corella
fcorella@pomcor.com
Karen Lewison
kplewison@pomcor.com

In-Person vs. Remote Identity Proofing

- Typically in-person identity proofing relies on
  - Primary evidence: picture ID
    - Driver's license, passport
  - Secondary evidence from other identity sources:
    - Ownership of utility, financial, mobile, or social network accounts
    - Address verification
- No problem with remote presentation of secondary evidence
- **Goal: replace picture ID with primary evidence that can be presented remotely**
- **We can do that with higher identity assurance than provided by a picture ID**

Multifactor Identity Verification without Prior Relationship

- Identity proofing is harder than authentication
  - No prior relationship between subject and verifier
- Authentication gold standard: provide 3 verification factors
  - Something you have: device containing private key
  - Something you know: password
  - Something you are: one or more biometric features
- But in identity proofing, without prior relationship:
  - The subject cannot have previously registered a password, nor enrolled a biometric sample with the verifier

Rich Credential

- **Achieves the gold standard** without prior relationship by certifying biometric and password verification data under a signature by the issuer
- **Allows multiple biometric modalities**
  - Both revocable and non-revocable
- And it provides **selective disclosure of attributes** and **selective presentation of verification factors**
  - … using a **typed hash tree** that provides **omission-tolerant integrity protection**

Remote biometrics

- A rich credential supports:
  - **Remote biometric presentation to a verifier**
    - Rather than to a device owned by the subject that may be compromised
  - **With spoofing detection by the verifier**

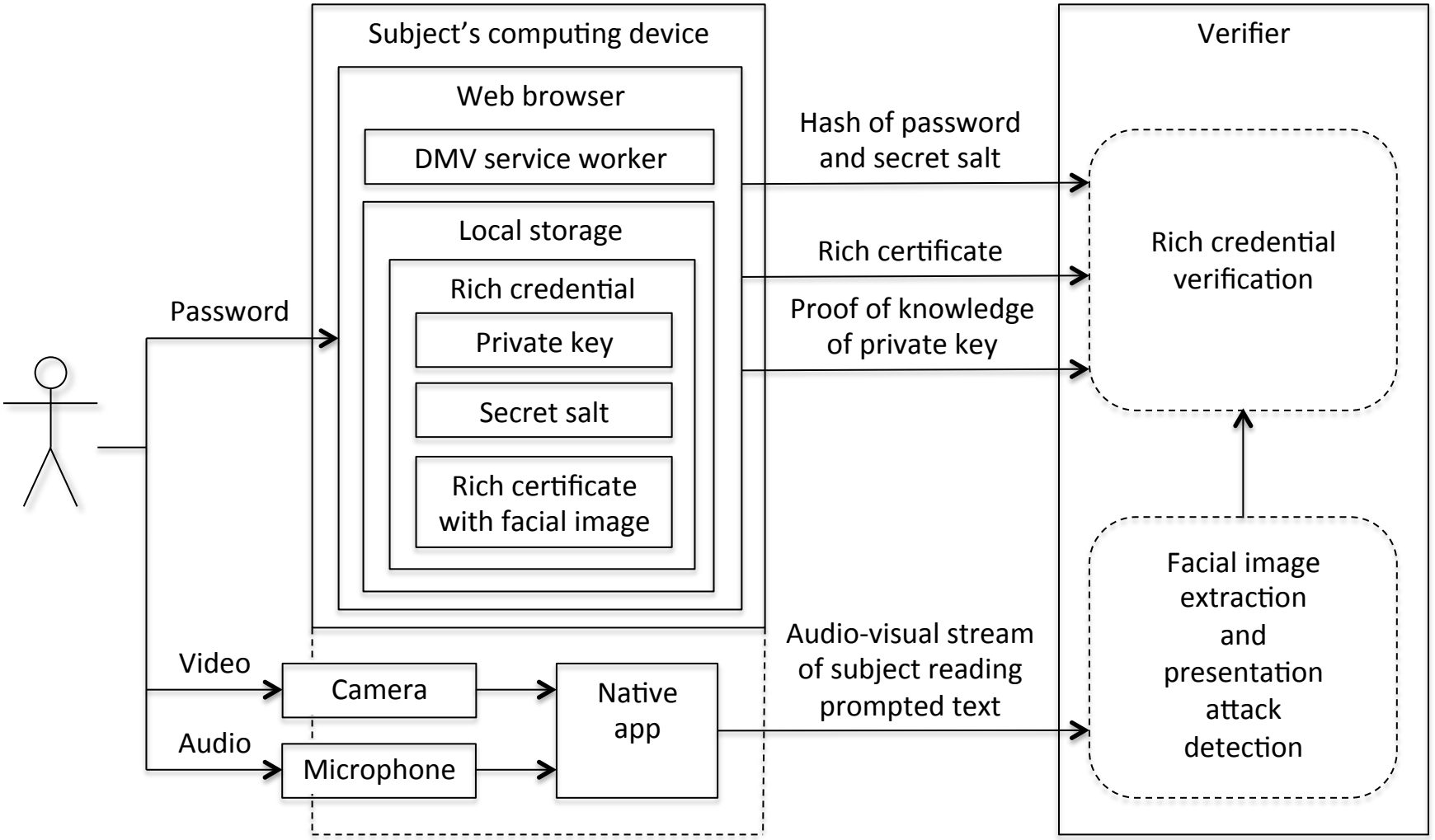
Remote spoofing detection with a rich credential

- Verifier receives an **audio-visual stream** of the subject reading prompted text selected at random with high entropy
- **Uses face recognition** to match a face in the stream to a facial image in the rich credential
- **Uses speech recognition** to verify that the subject is reading the prompted text
- **Verifies audio-visual synchrony** by tracking lip movement and matching distinguishable visemes to phonemes
- **Optionally uses speaker recognition** against a voiceprint in the rich credential
  - Possible because a rich credential supports multiple biometric modalities

Overview of the Five Solutions

	Solution 1	Solution 2	Solution 3	Solution 4	Solution 5
Identity Source	DMV	Bank	Credit card issuer	Medicare or medical insurance provider	State Department
Credential	Rich credential with facial image	Rich certificate asserted on a blockchain	Contactless EMV chip card	Medical ID smart card with signed facial image	Passport with signed facial image in RFID chip

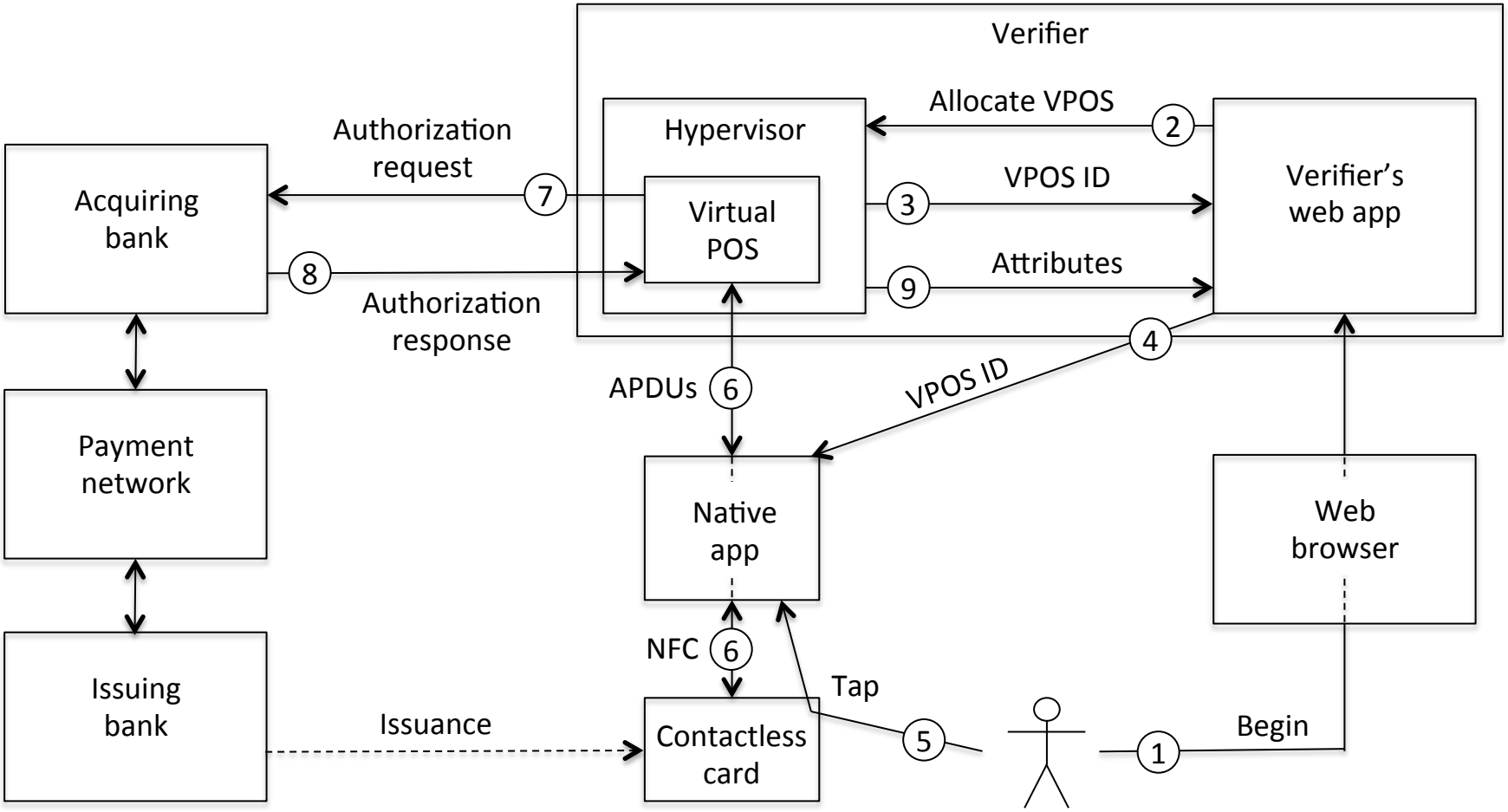
Solution 1: Rich Credential Issued by a DMV



Solution 2: Unsigned Rich Certificate Asserted by a Bank on a Blockchain

- Bank asserts certificate by placing hash of certificate in a storage location that it controls within the blockchain
- Bank revokes certificate by placing hash in another storage location
  - **Big improvement over CRLs and OCSP**
- Three-factor verification as in Solution 1
- Biometrics:
  - Speaker recognition, leveraging voiceprint used for customer authentication
  - Optional: face recognition as in Solution 1, to defeat voice morphing

Solution 3: Remote Proof of Possession of a Contactless EMV Chip Card

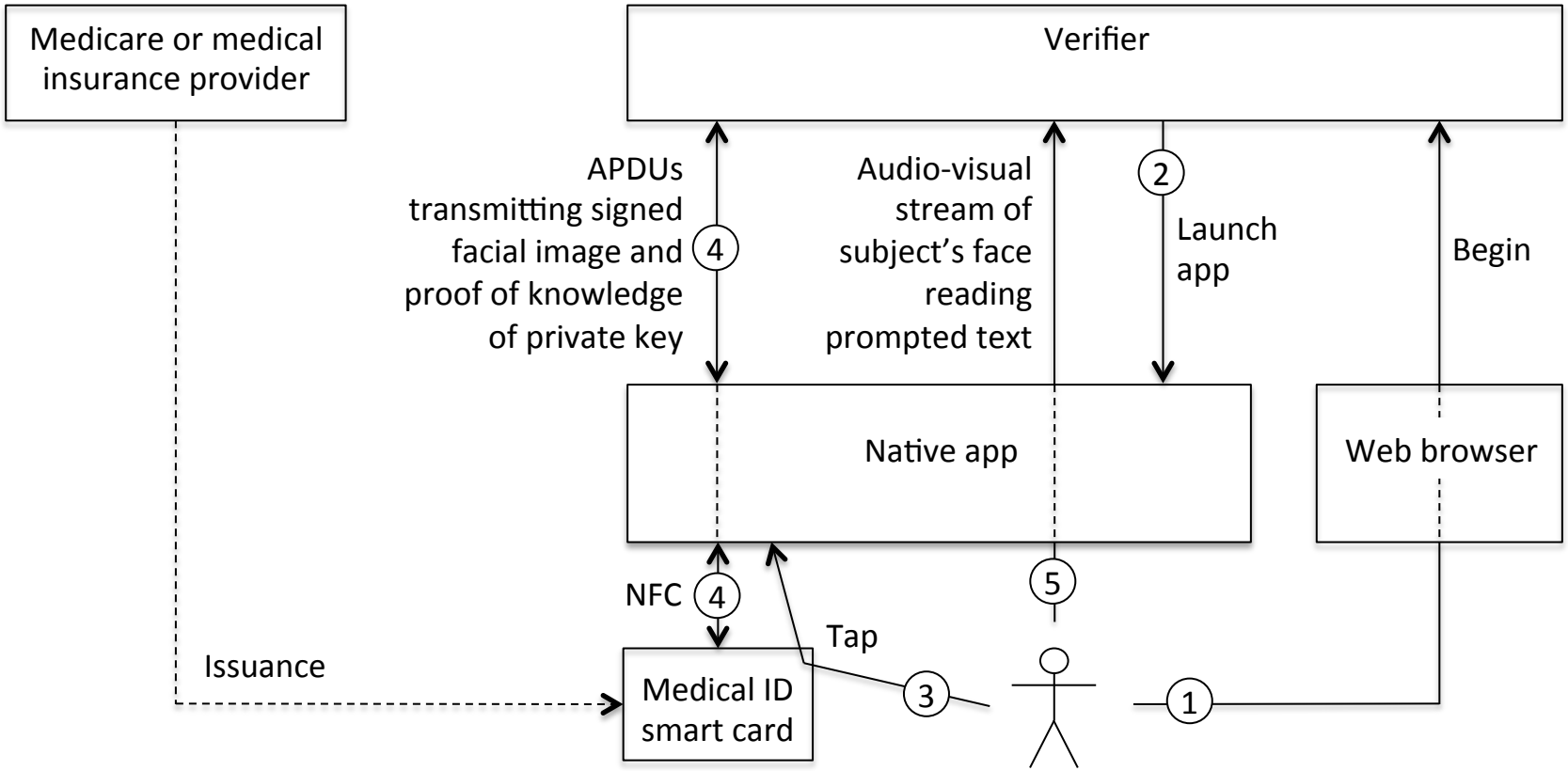


pomcor
pomcor.com

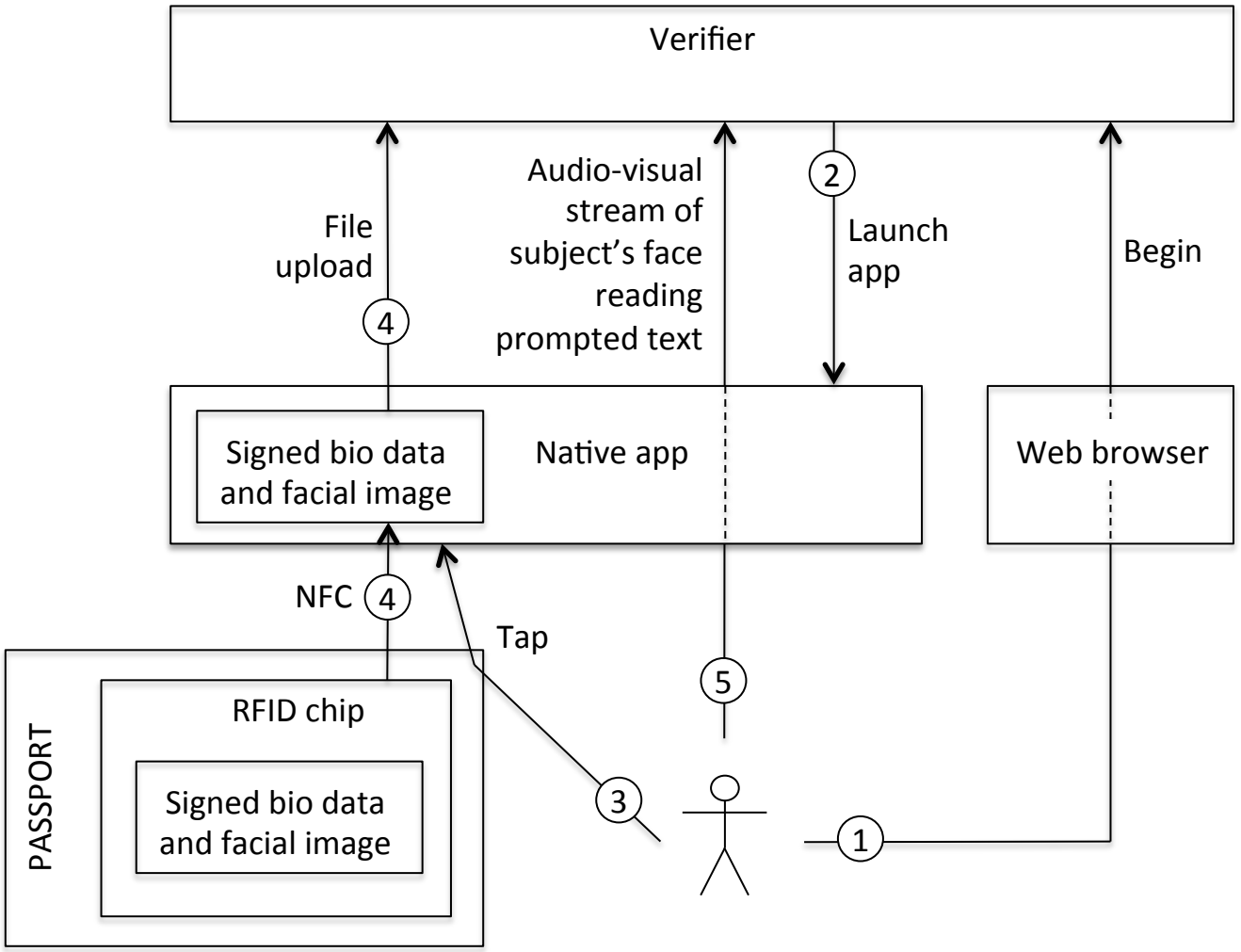
Solution 3 Enhancements

- As described above, Solution 3 provides only one verification factor:
  - Possession of contactless EMV card
- An "indirect" factor can be added
  - By asking the subject to demonstrate ownership of the account by reporting the amounts of the transactions
- The issuing bank could add a face recognition factor by placing a signed facial image in the card

Solution 4: Medical ID Smart Card with Signed Facial Image



Solution 5: Passport with Signed Facial Image in RFID chip



Solution 5 Enhancements

- As described above, Solution 5 provides only one verification factor:
  - Face recognition
- A strong proof of possession could be added by storing a key pair in the RFID
  - As specified by ICAO Doc 9303 Part 11, but not implemented in US passports
- A weaker proof of possession can be added by asking subject to show passport data page in audio-visual stream
  - Next generation passports will add more physical security features (but no private key?!)

Recap of Verification Factors Provided by the Five Solutions

	Solution 1	Solution 2	Solution 3	Solution 4	Solution 5
Identity source	DMV	Bank	Credit card issuer	Medicare or medical insurance provider	State Department
Credential	Rich credential with facial image	Rich certificate asserted on a blockchain	Contactless EMV chip card	Medical ID smart card with signed facial image	Passport with signed facial image in RFID chip
Verification factors	3 strong	3 strong	1 strong + 1 indirect	2 strong	1 strong + 1 weak

Thank you for your attention!

For more information:
Web site: pomcor.com
Blog: pomcor.com/blog/
Paper: https://pomcor.com/techreports/RichCredentials.pdf

Francisco Corella
fcorella@pomcor.com
Karen Lewison
kplewison@pomcor.com

Any questions?