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.

Five Solutions for Remote Identity Proofing

Presentation at IIW 23

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 three 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

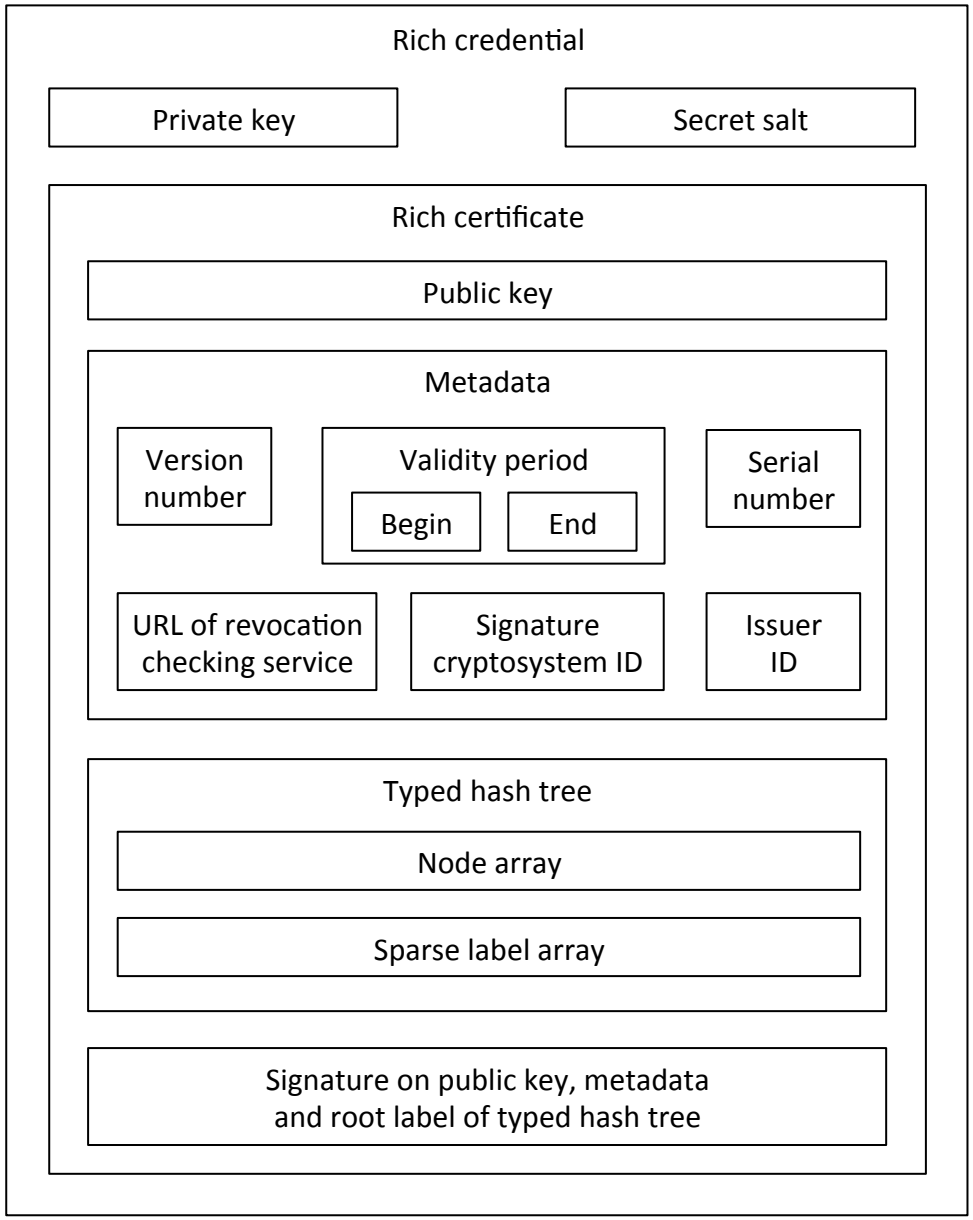
3F Verification w/o Prior Relationship Using a Rich Credential

1. Possession of private key
2. Knowledge of password
   - Not registered with verifier
   - Salted hash built into credential by issuer, then forgotten
   - Salted hash submitted to verifier
3. One or more biometric features
   - Biometric verification data built into the credential by the issuer
   - Remote biometric presentation to verifier, rather than to a device owned by the subject that may be compromised
   - Spoofing detection by the verifier

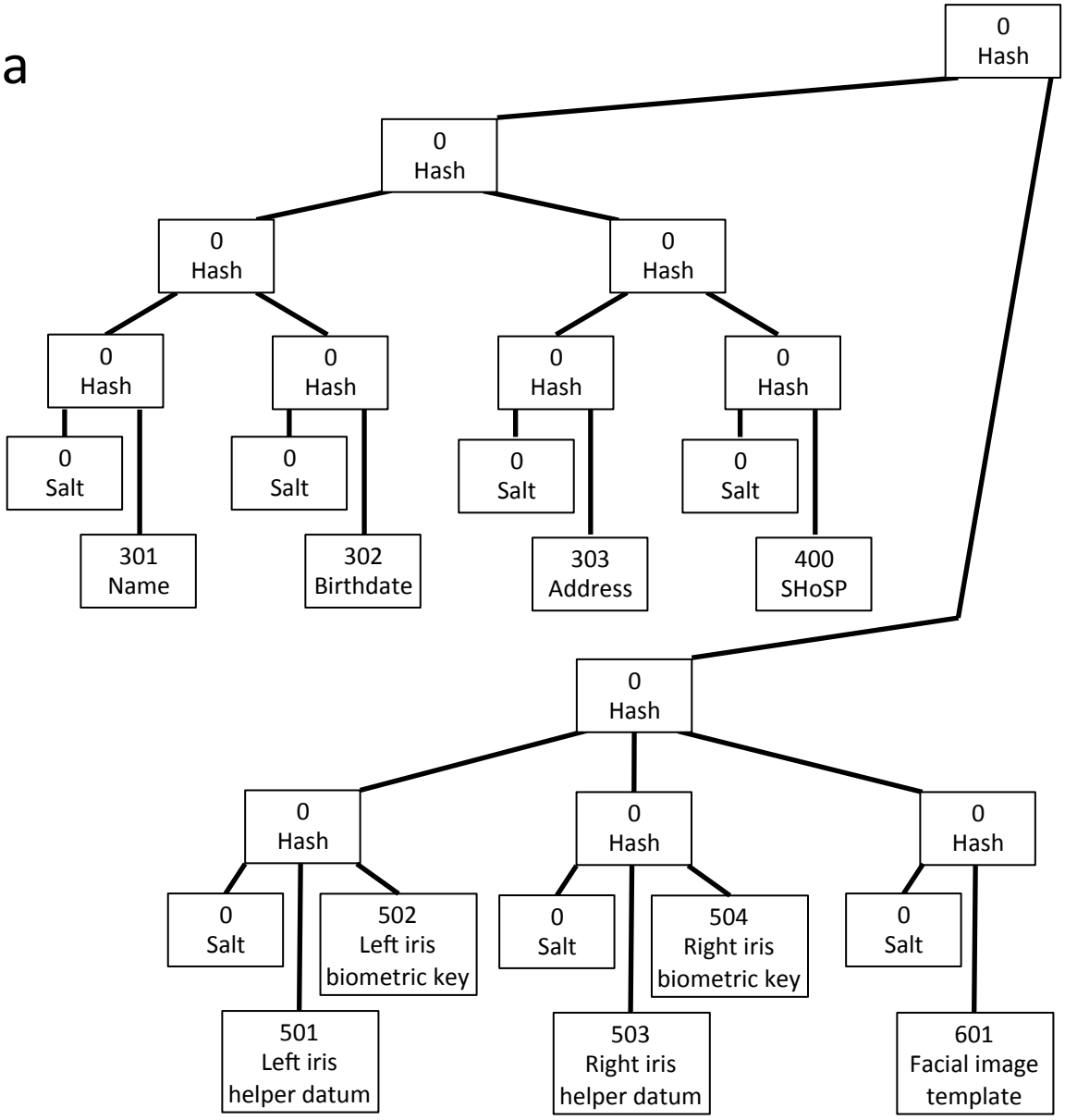
Privacy Features of a Rich Credential

- Selective disclosure of attributes
  - As provided by an anonymous credential, but without unlinkability
- Selective presentation of verification factors
  - May omit submission of (salted hash of) password
  - May omit biometric verification
  - May choose which biometric modalities to use, if multiple ones are built into the credential

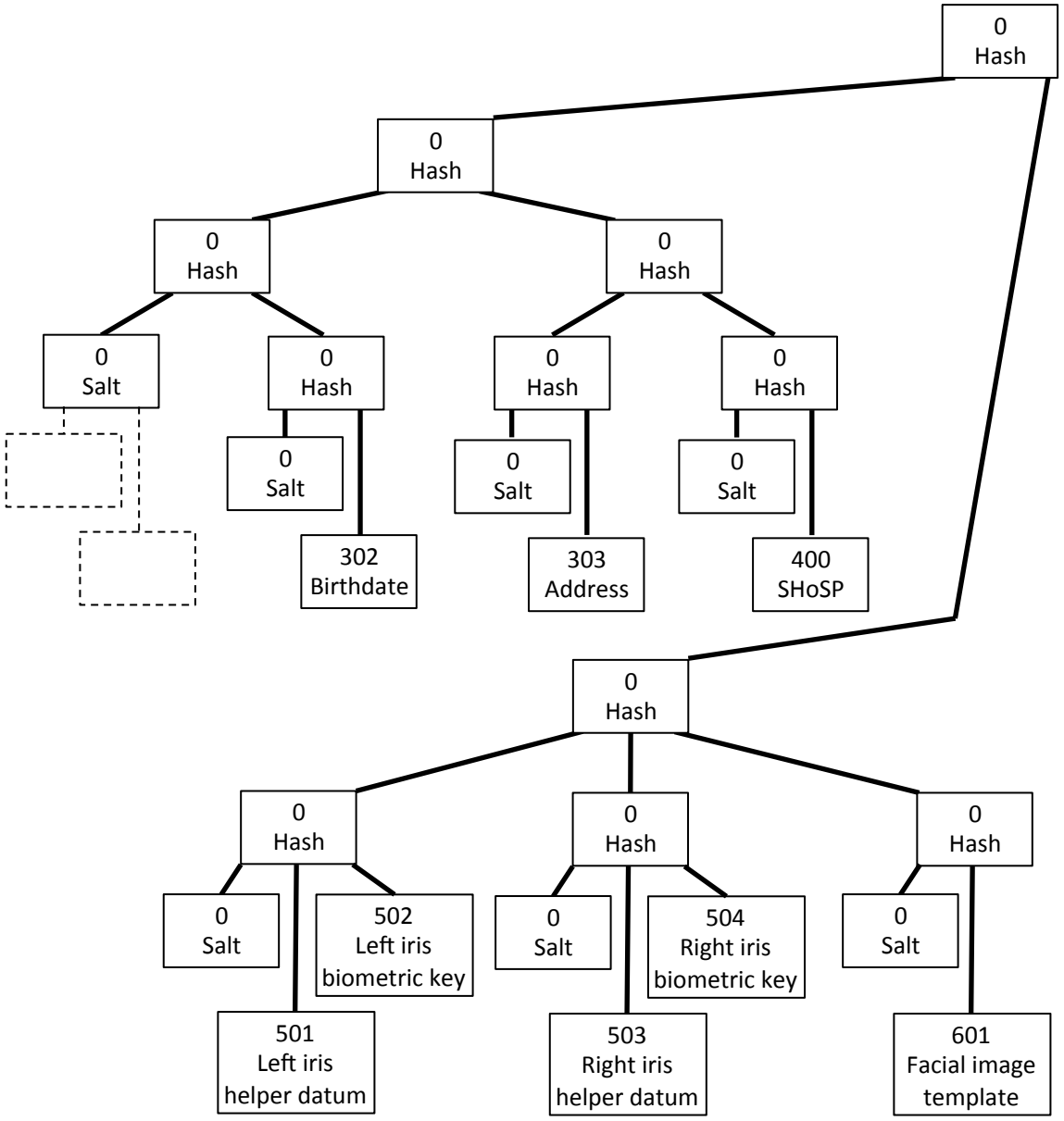
Components of a rich credential



Example of a typed hash tree

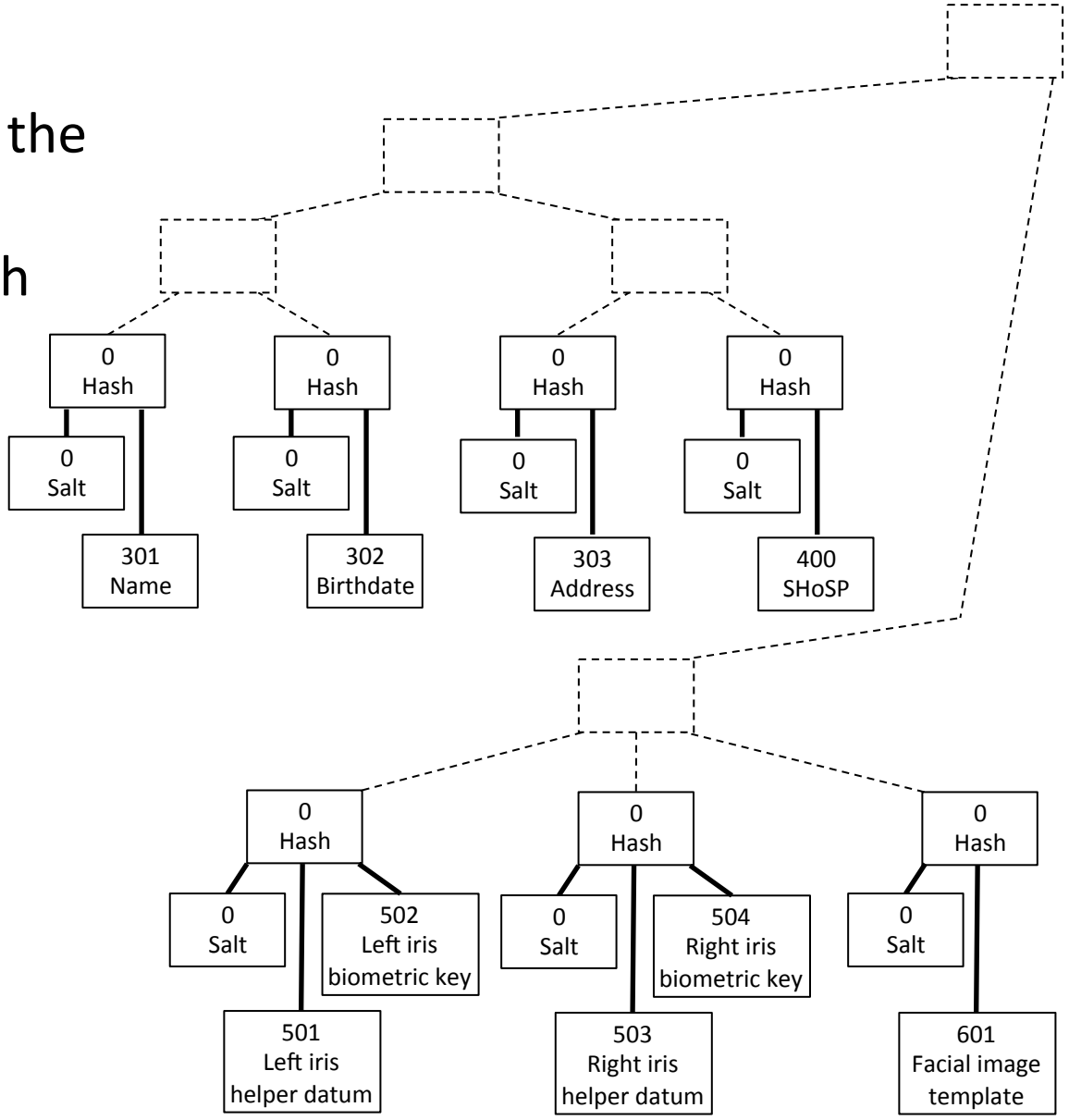


Subtree pruning

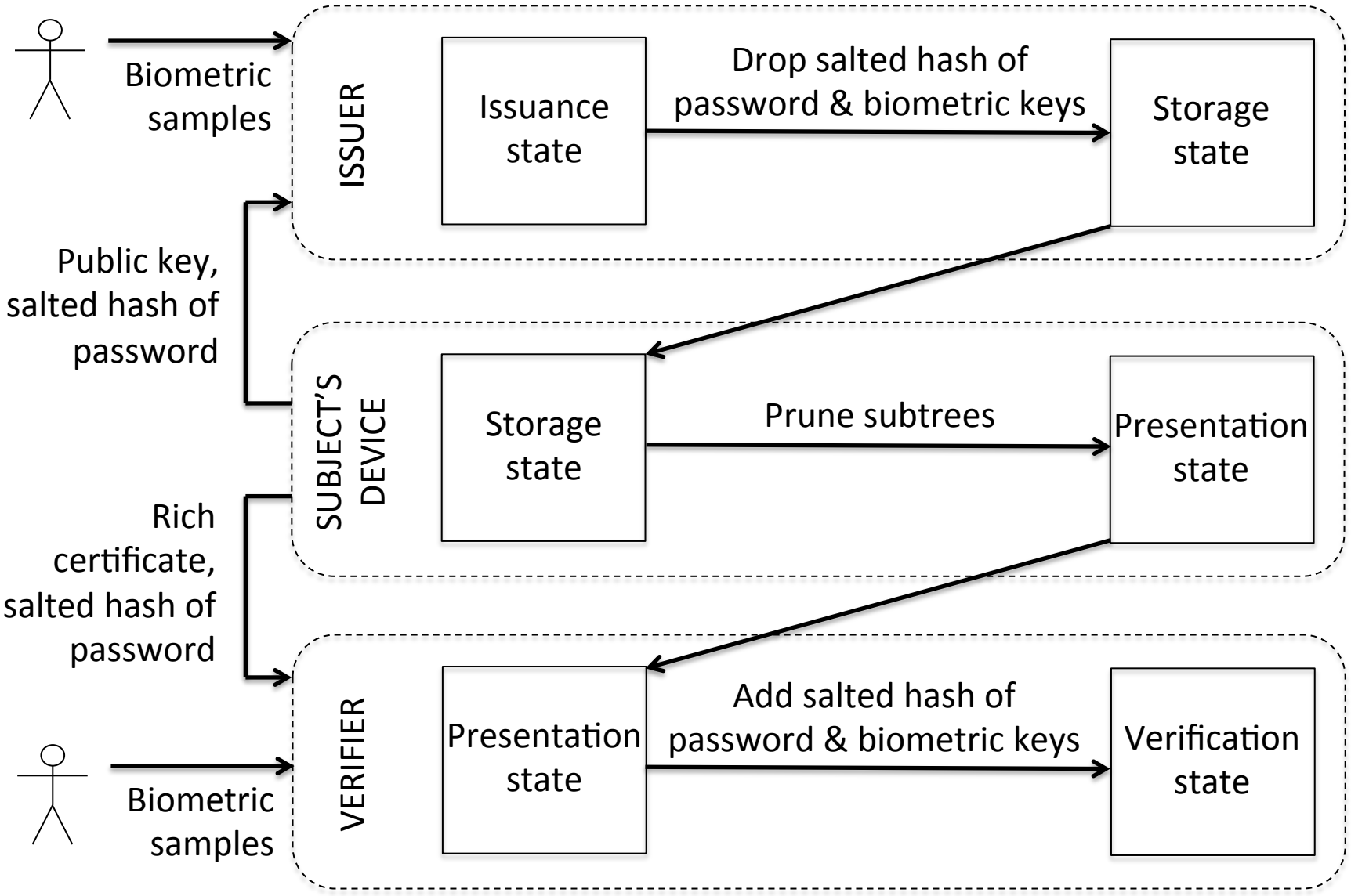


Root label is omission-tolerant cryptogaphic checksum

Peripheral subtrees of the typed hash tree of a rich credential



State transitions of a rich certificate



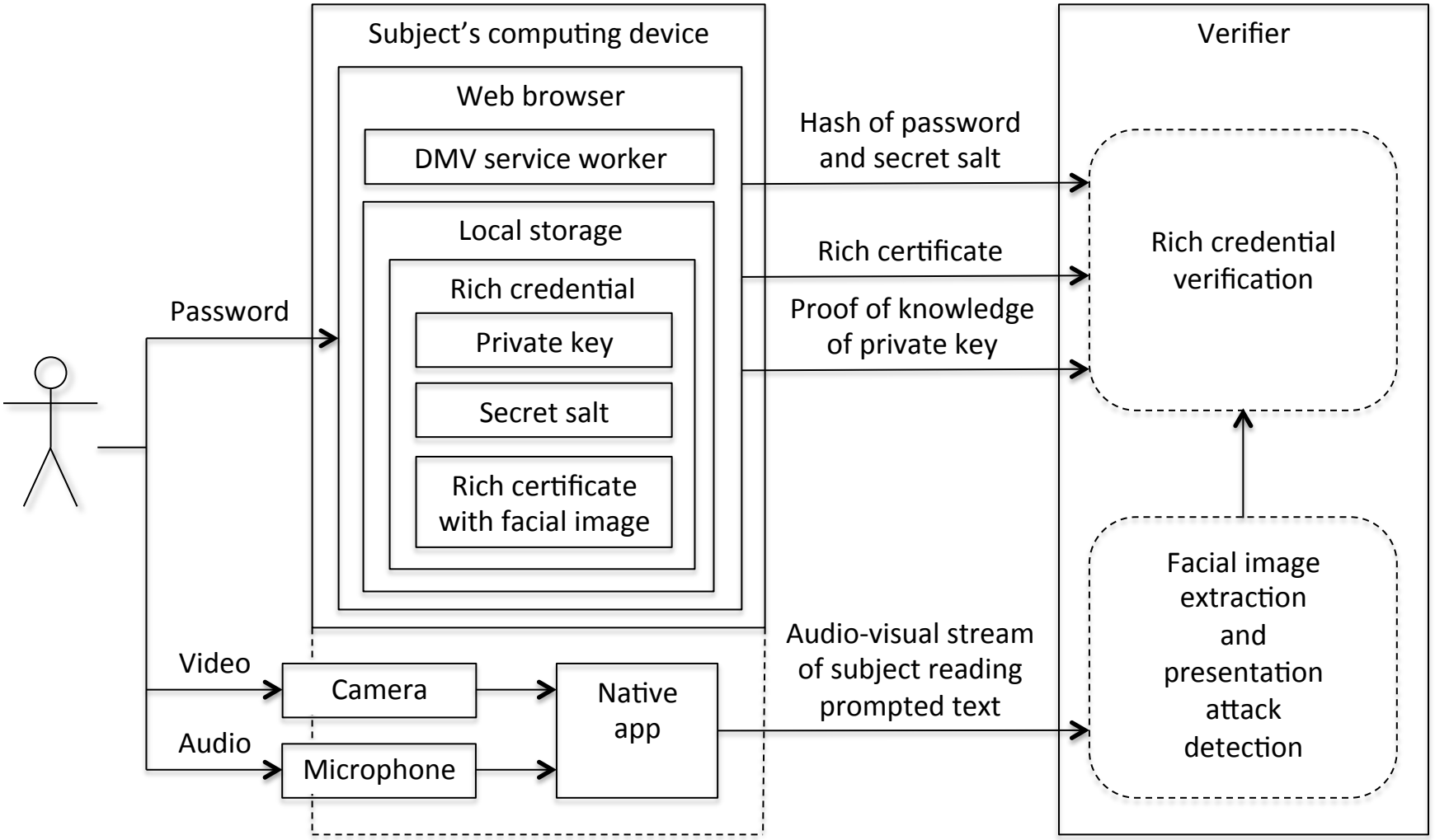
Remote spoofing detection with a rich credential

- 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

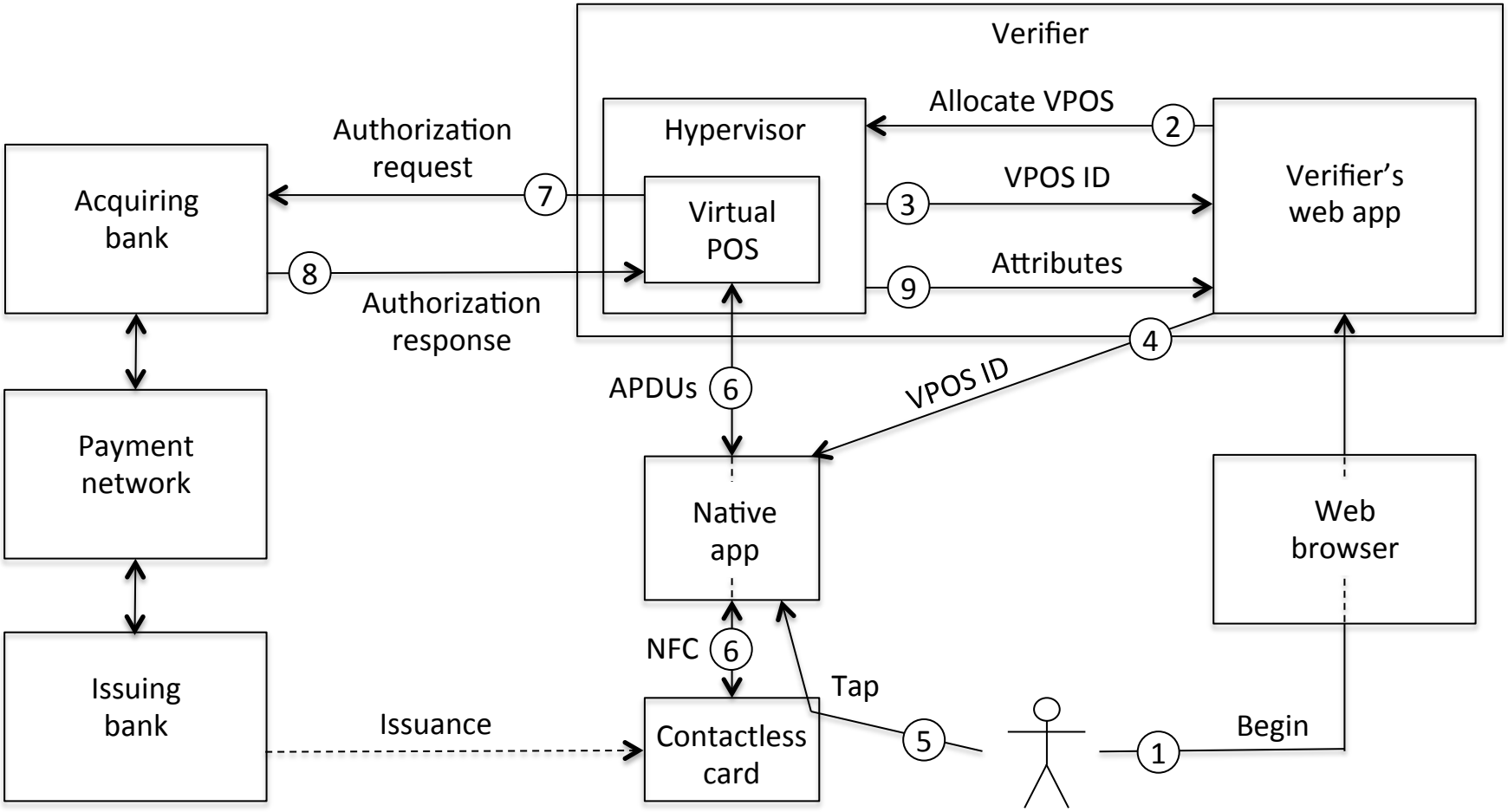
Solution 1: Rich Credential Issued by a DMV



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

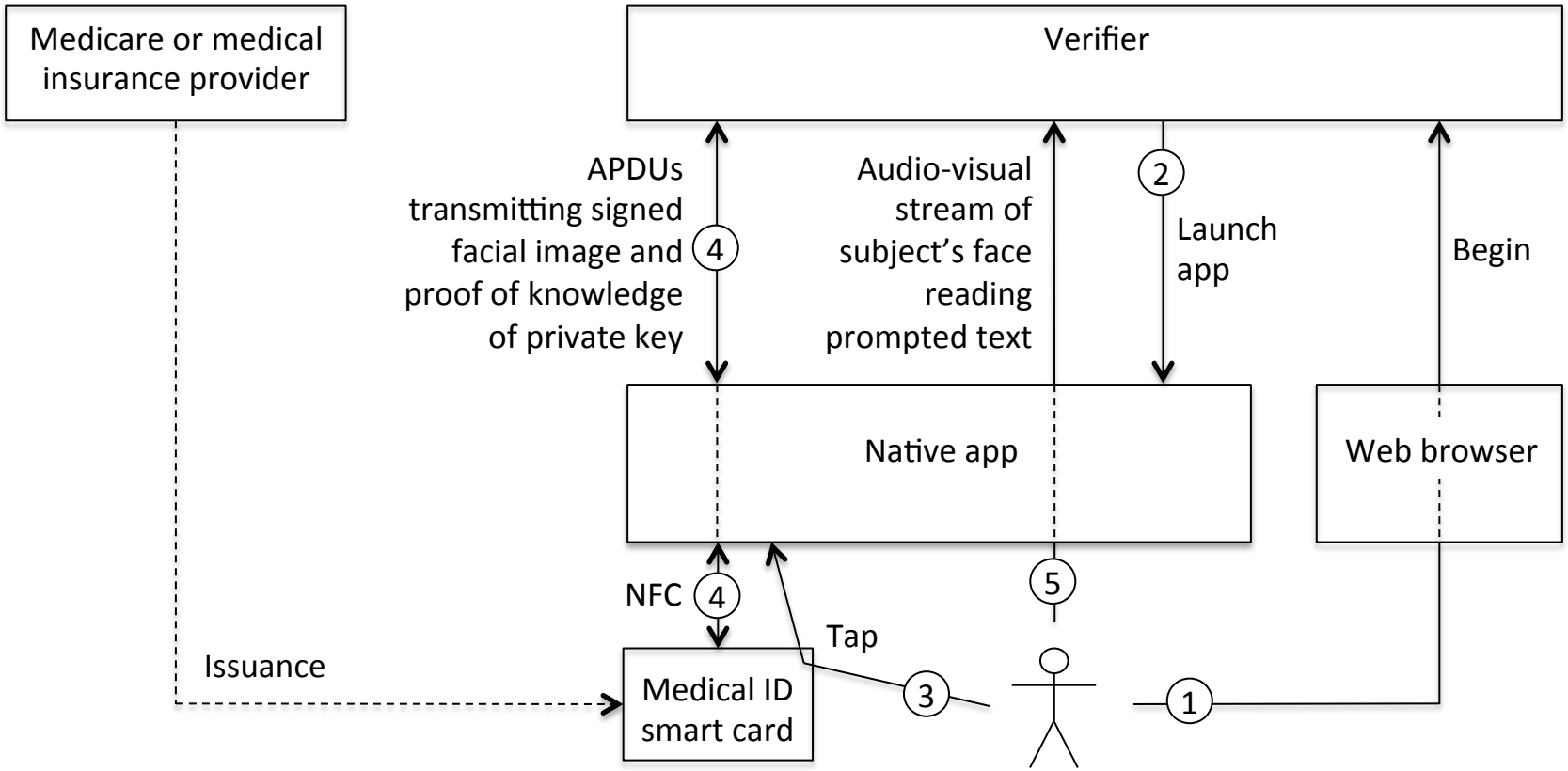


pomcor
pomcor.com

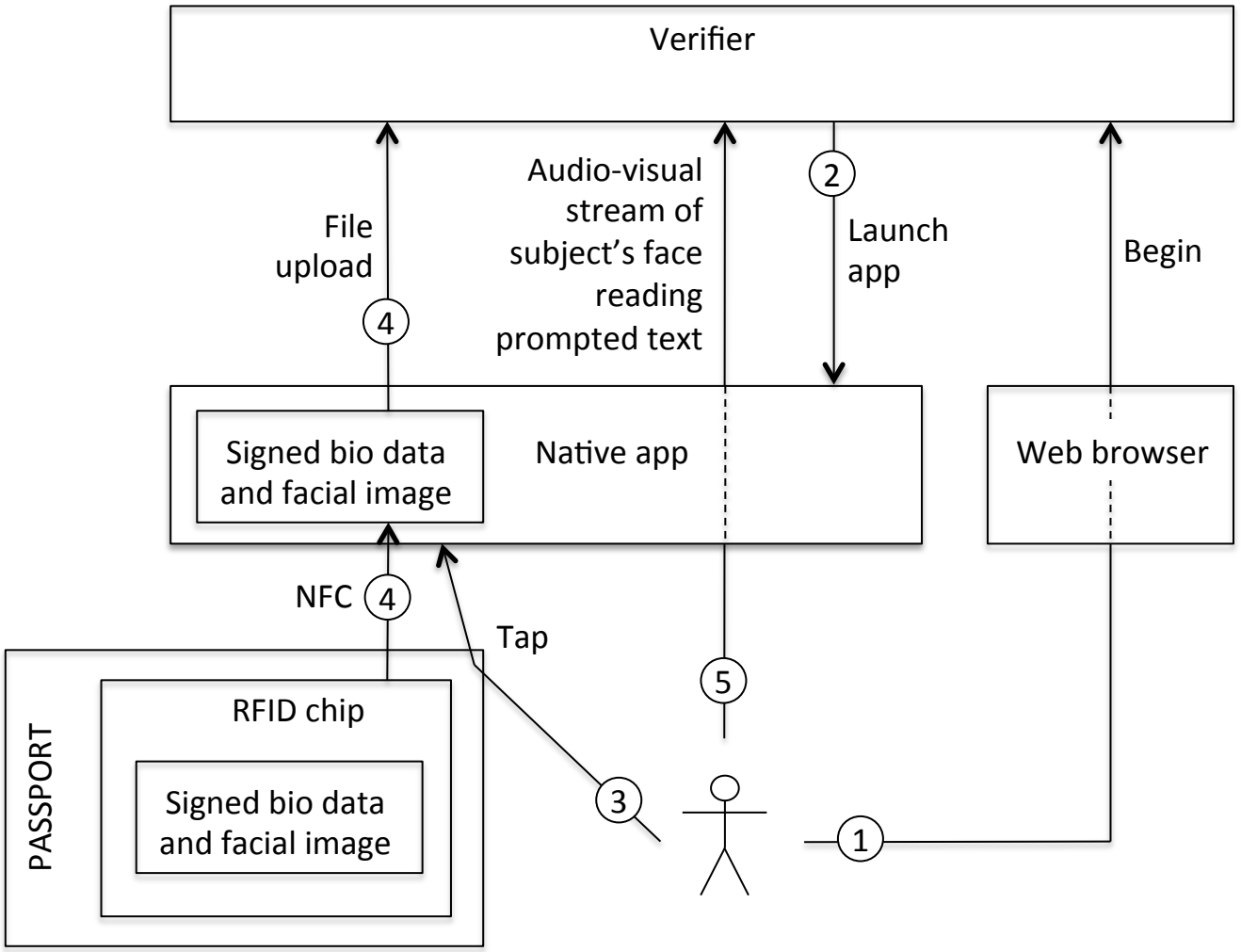
Solution 3 Enhancements

- 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:
pomcor.com
pomcor.com/blog/
https://pomcor.com/techreports/RichCredentials.pdf
https://pomcor.com/techreports/BlockchainPKI.pdf

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

Any questions?