NASS Remote Notarization Task Force

Knowledge-Based Verification

David Temoshok

Applied Cybersecurity

IT Laboratory

National Institute of Standards and Technology (NIST)




Today's Discussion

- NIST and Identity Management
- Authentication and Identity Proofing
- How does Knowledge-Based Verification (Authentication) work
- Concerns about KBV
- What does NIST SP 800-63-3 say about KBV
- What does NIST SP 800-63-3 say about remote ID proofing
- NSTIC Pilots with States
- Questions and Comments

NIST and Identity Management

- Implement the National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf
- Build public-private sector partnerships for trusted IDs
  - https://www.idesg.org/
- Establish pilot programs to demonstrate trusted IDs
  - 20+ pilots in 25+ states
  - https://www.nist.gov/itl/tig/pilot-projects
- Provide identity management guidance, direction and standards
  - Special Publication 800-63-3, Digital Identity Guidelines
  - https://pages.nist.gov/800-63-3/

What is the difference between Identity Proofing and Authentication

- Identity Proofing
  - The process by which a service provider collects and verifies information about a person for the purpose of allowing access to protected resources/applications or issuing credentials to that person.
  - 3 key steps:
    1. **Identity resolution** (confirmation that an identity has been resolved to a unique individual within a particular context),
    2. **Identity validation** (confirmation of the accuracy of the identity as established by an authoritative source)
    3. **Identity verification** (confirmation that the identity is claimed by the rightful individual).

- Authentication
  - Process of determining the validity of one or more credentials used to claim a digital identity.

  - Authenticator: Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity.

How does KBV (KBA) work

- Static and dynamic KBV
- Collect and link data
- Resolve identity
  - Use identity attributes (name, address, DOB, SSN, other) to resolve identity to a unique individual.
  - NASPO report “Establishment of Core Attribute Sets” :
    - https://naspo.info/sdo-projects/ansi-sdo-projects/naspo-idpv-project/
  - LexisNexis studyreported 5 identity attribute sets: (name, location, DOB, place of birth, SSN) produced 95+% resolution for U.S. population.
  - Michigan DHHS pilot – 95+% resolution using name, DOB, address
    - https://www.rti.org/sites/default/files/resources/mdhhs_nstic_pilot_rti_evaluation_vf.pdf
- Generate dynamic KB questions
- Score responses
  - Scoring can be adjusted : All, 4 of 5, 3 of 4 correct to determine positive response
  - Michigan pilot
    - 3 out of 4 correct responses for successful completion produced 60% positive responses
    - 40% did not complete
    - Of the 60% that did complete KBV, 58% were successfully completed

How does KBV (KBA) work

- Static and dynamic KBV
- Collect and link data
- Resolve identity
  - Use identity attributes (name, address, DOB, SSN, other) to resolve identity to a unique individual.
  - NASPO report “Establishment of Core Attribute Sets” :
    - https://naspo.info/sdo-projects/ansi-sdo-projects/naspo-idpv-project/
  - LexisNexis studyreported 5 identity attribute sets: (name, location, DOB, place of birth, SSN) produced 95+% resolution for U.S. population.
  - Michigan DHHS pilot – 95+% resolution using name, DOB, address
    - https://www.rti.org/sites/default/files/resources/mdhhs_nstic_pilot_rti_evaluation_vf.pdf
- Generate dynamic KB questions
- Score responses
  - Scoring can be adjusted : All, 4 of 5, 3 of 4 correct to determine positive response
  - Michigan pilot
    - 3 out of 4 correct responses represented successful KBV completion
    - 40% did not complete, for remaining 60%, 58% were completed successfully.

Concerns about KBV (KBA)

- Non-completion rate – 40% in Michigan pilot
- Sensitivity to questions about individual's past (privacy).
- People forget or make mistakes – leads to high failure rates (42% in Michigan pilot)
- Increasing Fraud attacks on multiple KBV systems

Attacks on IRS "Get Transcript" and "E-File PIN" apps resulted in apps being shut down due to widespread fraudulent access to taxpayers filings and information (200,000 - 700,000 accounts).

"We're confident that these are not amateurs. These are extremely sophisticated criminals with access to a tremendous amount of data." IRS Commissioner John Koskinen blaming the breach on organized crime. Associated Press

"In this sophisticated effort, third parties succeeded in clearing a multi-step authentication process that required prior personal knowledge about the taxpayer, including Social Security information, date of birth, tax filing status and street address before accessing IRS systems. The multi-layer process also requires an additional step, where applicants must correctly answer several personal identity verification questions that typically are only known by the taxpayer."

What does NIST SP 800-63-3 say about KBV?

KBV may be used to resolve to a unique, claimed identity without restrictions.

KBV may be used to verify identity provided that the KB service:

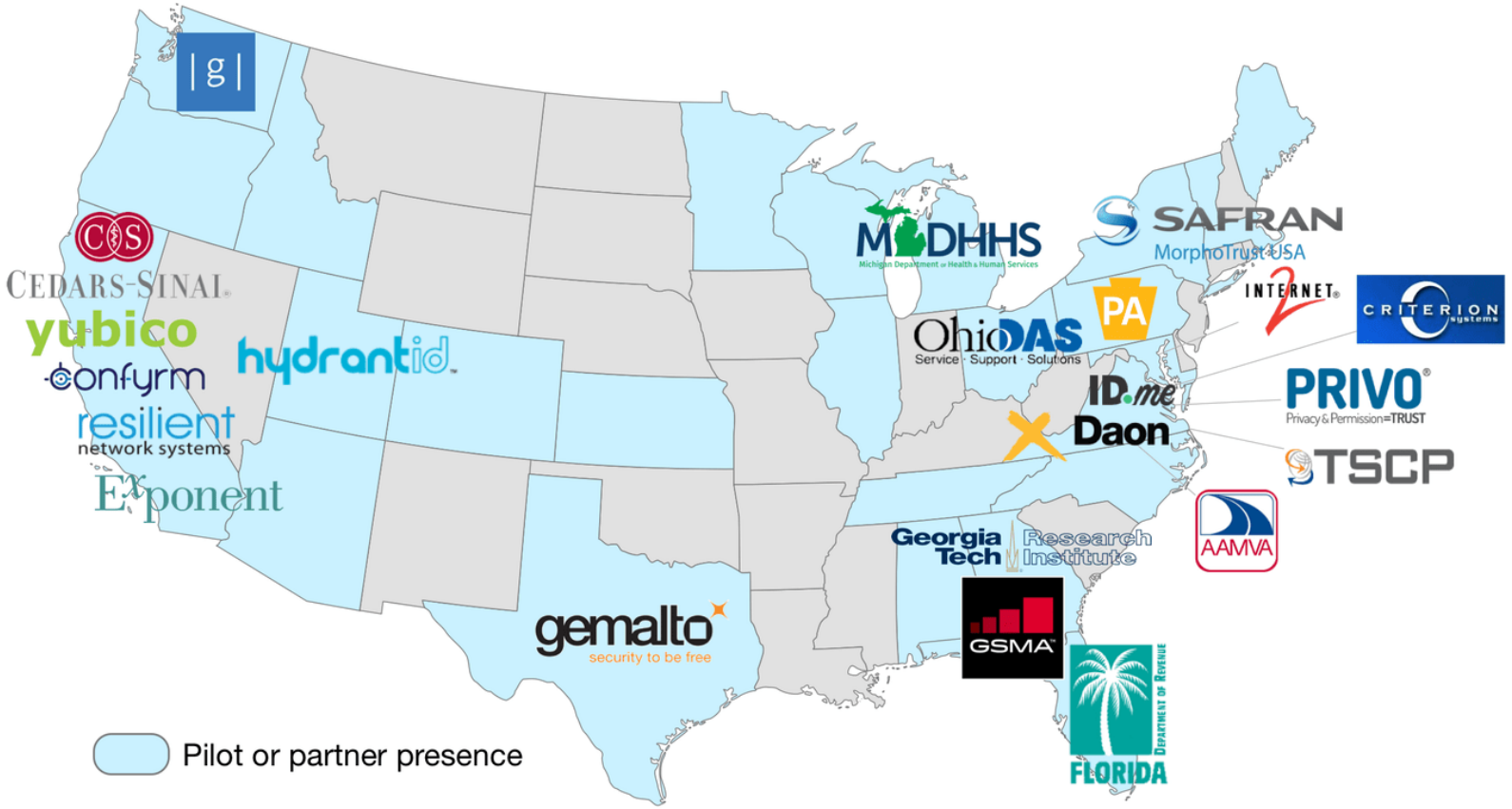
- SHALL be or maintains a relationship with, an authoritative source.
- SHALL only use information that is expected to be known only to the applicant and the source. Information accessible freely or for any fee in the public domain SHALL NOT be used.
- SHOULD be based on multiple data sources.
- SHOULD perform KBV by verifying knowledge of recent transactional history that the CSP is a participant in.
- MAY perform KBV by asking the applicant questions to demonstrate they are the owner of the claimed information. Provided that:
    - There are minimum of four KBV questions with each requiring a correct answer.
    - Responses should be free form. Any multiple choice question shall require a minimum of four answer options per question.
    - The service SHALL NOT use KBV questions for which the answers do not change regularly over a period of time (e.g., What was your first car?).
    - Additional restrictions in SP 800-63-3 A.

What does NIST SP 800-63-3 say about Remote Identity Proofing?

Remote ID proofing is allowed at Identity assurance level 2, in-person proofing is required for level 3. Remote ID Proofing requirements for the ID proofing service:

- Monitor the entire identity proofing transaction, from which the applicant SHALL NOT depart during the identity proofing session.
- Require all actions taken by the applicant during the enrollment and identity proofing process to be clearly visible to the remote operator
- Have a live operator participate remotely with the applicant for the entirety of the enrollment and identity proofing session. For example, by a continuous high resolution video transmission of the applicant.
- Require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors that are in the entire field of view of the camera and the remote, live operator.
- Require operators to have undergone a training program to detect potential fraud and to properly perform a virtual in-process proofing session.
- Employ physical tamper detection and resistance features appropriate for the environment in which it is located.
- Ensure that all communications take place over a mutually authenticated encrypted session.
- Send an enrollment code to the validated address of record of the applicant or may send the code to a mobile telephone (SMS or voice), landline telephone, or email that has been verified in records.

NSTIC Pilots with States



The NSTIC Pilots Program has **convened more than 170 organizations** to work together in advancing trusted digital identity solutions in more than 25 states. The pilots have **impacted over 6.7 million individuals**, with **advances occurring across 12 sectors** – including the **development of 14 multi-factor authentication solutions**.

NSTIC Pilots with States

Michigan Department of Health and Human Services (MDHHS)

https://www.rti.org/sites/default/files/resources/mdhhs_nstic_pilot_rti_evaluation_vf.pdf

Streamlined and secured citizen access to state services to reduce fraud

The Michigan DHHS piloted the use of KBV with MiBridges, Michigan's integrated eligibility system that supports online enrollment/registration for over 2.3 million Michigan residents seeking public assistance. The pilot project, in partnership with LexisNexis, aimed to help eliminate barriers citizens face in accessing benefits and services by streamlining the identity proofing part of the applications process.

Ohio Department of Administrative Services

The Ohio DAS will implement a range of identity-related capabilities including KBV and multi-factor authentication to provide stronger identity proofing, for three state services. These services include enterprise e-licensing, online filing and payments for businesses in the state, and tax-related transactions with the Ohio DAS.

MorphoTrust USA

http://www.morphotrust.com

MorphoTrust will extend the trust placed in state-issued driver licenses as a primary proof-of-identity document into the online world, enabling more secure transactions and delivery of state services to citizens. The pilot leverages identity proofing done in the drivers licensing process to create a digital credential (“eID’) for North Carolina.and Georgia.

Questions? Comments?

Contact:
David Temoshok
202-482-5475
david.temoshok@nist.gov