CAN BLOCKCHAIN ENABLE IDENTITY MANAGEMENT?

Kurt Lieber
VP, CISO of IT Infrastructure
Aetna

Prakash Sundaresan
Chief Technical Officer
Trusted Key
What we are hearing about Identity

1. A poor user experience
   Resulting from the need for multiple credentials and enrollments when a member:
   - Makes an appointment (Payer/Provider)
   - Sees a physician (Provider)
   - Files claims (Payer)
   - Picks up a prescription (Pharma, other ecosystem partners)

2. Duplicative IAM efforts and infrastructure costs
   NH-ISAC working group and other partners in the health ecosystem each maintain their own identity infrastructure (and bear the associated costs).

3. Dependence on for-profit entities for identity-proofing services
   Identity-proofing services in the market today are provided by a few commercial entities who can charge a premium price due to the lack of competition. This results in implied trust and “unchecked power” which may stifle innovation and increase health care costs for the member.

4. Provider credentialing is repetitive and time-consuming
   The credentialing process (e.g., requests for medical transcripts, state licenses, background check) is repeated each time a provider:
   - Joins a new facility as part of a float pool
   - Moves to a different health system

Leading to: Increased costs
Example: A member has to manage separate identities and NH-ISAC consortium partners have to manage separate IAM infrastructure

1. A member uses different credentials across the digital health life cycle.

2. A member provides personal information multiple times.

3. Payers, providers, other partners (collective NH-ISAC consortium partners) maintain separate IAM infrastructure.
A DAY IN THE LIFE OF A MEMBER
Our vision: Shared identity

Users own a portable identity which is accepted across the health ecosystem.

Relying parties use the portable identity to make access decisions.

Proofers vet attributes of a user increasing the fidelity of a user’s trust score over time.
The NH-ISAC Portable ID...

- Is an identity for members or providers
- Aims to improve the user experience and lower health care costs through efficiency gains
- Is built on open standards (e.g., NIST 800-63)
- Has a non-profit motive where the working group:
  - Establishes governance, leading practices and guidelines
  - Collaborates with other standard bodies (e.g., SAFE Biopharma), privacy working groups
  - Shares the cost of infrastructure
- Is in proof-of-concept stage
- Is a supplement to existing IAM infrastructure
What it is NOT

- Meant to store Personal Health Information (PHI).
- A replacement for electronic medical records (EMR).
- A replacement for industry frameworks (e.g., SAFE Bio-pharma Trust Framework, NIST).
- A replacement for existing individual NH-ISAC consortium IDs (e.g., Aetna ID, CVS ID etc.).
- A replacement for all existing IAM infrastructure.
- Set in stone. This is a proof-of-concept and we are continually incorporating feedback from the field.
- Meant to exist in a silo. Integration with other standards bodies, identity working groups is key.
An example of how the POC would work
On day 1 and ongoing basis

1. Member performs initial identity capture and form fill (with web form if needed)
   - Scan driver’s license and (take selfie for facial recognition)
   - Complete web form (import IDs from NHISAC partners as appropriate)
   - Verified identity
   - Blockchain-based ledger
   - Portable identity (blockchain)
     - FirstName
     - LastName
     - DLN (High trust level if selfie verified)
     - DOB
     - Address
     - Trust Level
   - Acquired user attributes
   - Attestations of attributes
   - Verified identity
   - Identity requestor and existing IAM infrastructure (NH-ISAC relying parties)

2. Providers verify a user (on day 1 and during regular touch points with members)
   - Verify last name
   - Verify DOB
   - Verify additional attributes
TECHNICAL DEMO
Introduction – How will the member get the app?

- Mobile friendly
- Something that will always be carried with the member
- Discoverable through app stores
- Member to be made aware of the app during the insurance enrollment process
Day 1 - Member Enrollment
On Day 1 - Enrollment

• Seamless enrollment on Day 1 by:
  • Importing existing IDs with NH-ISAC partners
  • Form fill thru driver’s license scan
  • Trust Level 1 verification with self asserted attributes
  • Trust Level 2 with remote driver’s license verification
Going to the provider
When going to the provider

- “Passwordless” login through biometrics (e.g., FaceID)
- Easy check-in at provider’s office by QR code scan
- Similar to a mobile boarding pass
Wearable check-in – for those with their hands full...

- Added convenience without having to reach for your phone
Checking the member in
Provider’s perspective – what the receptionist at the provider does...

- Provider has a companion app in the office
- On an iPad
- Provider verifies the ID concurrently with check-in
- Trust Level 3 – in-person verification with provider
- Usage / assertion history can be used by insurance provider for proofing (optional)
Can Blockchain enable Identity? – Sniff Test

- Are the answers to any of these “Yes”?
- Portability
  - Are there multiple parties that could benefit from sharing identity data?
  - Can we enhance the user experience by enabling a single identity at different places?
- Cost Savings
  - Is there a duplication of identity infrastructure across the ecosystem?
  - Is there a reliance on commercial entities for proofing services?
- Persistence
  - Is the use case "write once - read many"?
Lessons Learned

- Driving adoption from stakeholders is key, non-profit motives help
- Maturity of blockchain tools are still evolving
- Front-end, UI/UX design is key:
  - The end-user should not know that Blockchain was used
  - Don’t try to change consumer behavior
- PHI should not be put on the blockchain (tough sell)
- Co-existence with IAM tools is necessary
Identity + Blockchain = Portability

- Identity Management platforms (e.g., AuthN, authZ, directory)
- Decentralized, sovereign, immutable fabric
- Enable digital trust across untrusted parties.
Apply What You Have Learned Today

- Next week you should:
  - Identify identity issues related to portability, duplication and costly proofing

- In the first three months following this presentation you should:
  - Summarize your identity pain points, interested business partners
  - Explore a proof-of-concept
  - Socialize the vision with key sponsors, customers and gauge interest

- Within six months you should:
  - Expand the proof-of-concept to other business partners
  - Conduct a roadshow at industry consortiums to drive awareness and adoption