

# Decentralized Identifiers, Verifiable Credentials

and the next phase of decentralization

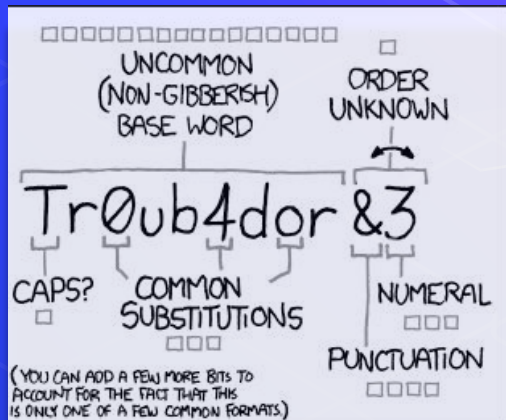
**Kim Hamilton Duffy**

MIT, Digital Credentials Consortium



“

Typical authentication systems in use today were designed for the pre-mobile-device internet.



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

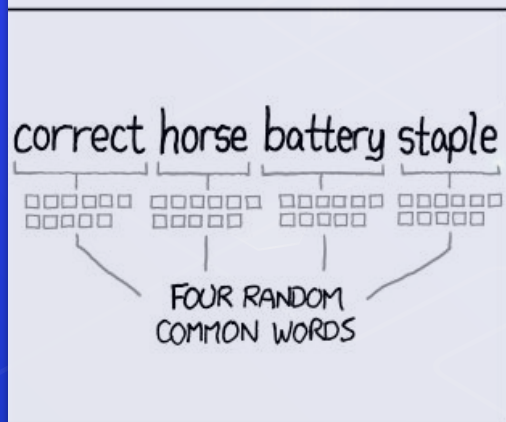
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

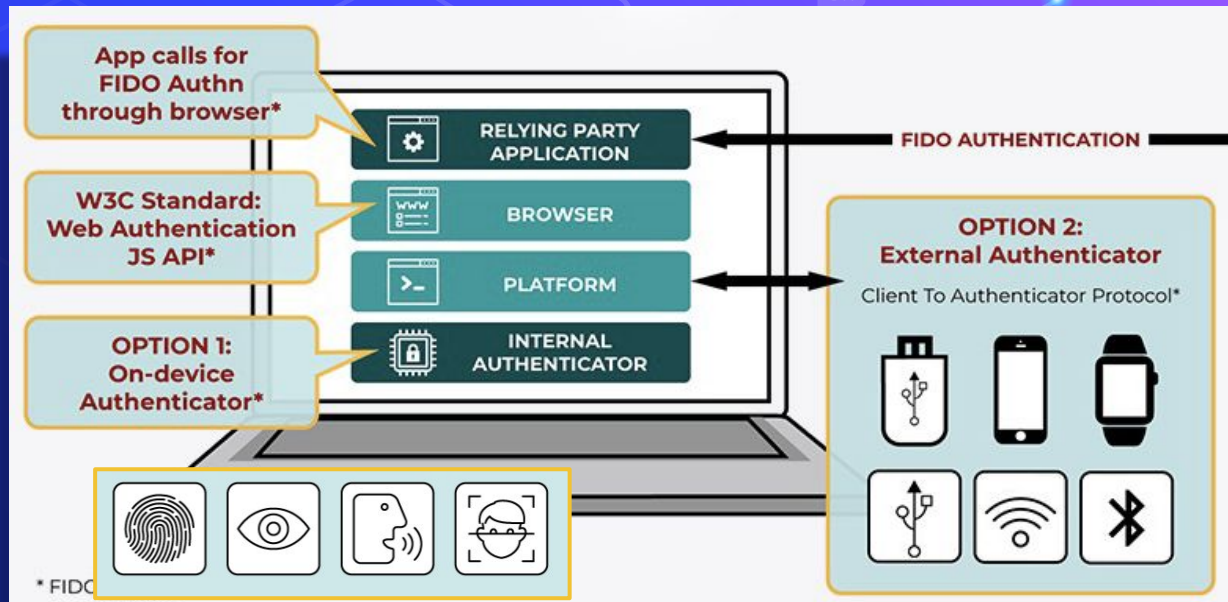
DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

“

The DFS ecosystem requires

standardized,  
interoperable,  
strong

authentication technologies to reduce risk and protect assets



# Data Centralization Risks Remain

- Centralized data stores are attractive targets
- Strong incentives for hackers
- Users have to trust data handling policies
- Steady flow of data breaches
  - Equifax: ~143 million US consumers exposed



# Enabling decentralized trust

## Verifiable Credential

- Claims about a subject
- Metadata
- Strong verification
- Decentralized Identifiers for issuer and subject





# Verifiable Credentials and DIDs



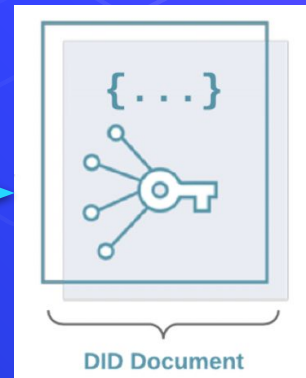
# What is a Decentralized Identifier?

- New type of identifier for verifiable, "self-sovereign" digital identity
- Fully under the control of the DID subject, enabling independence from any specific:
  - centralized registry
  - identity provider
  - certificate authority
- URL enabling trustable interactions with DID subject



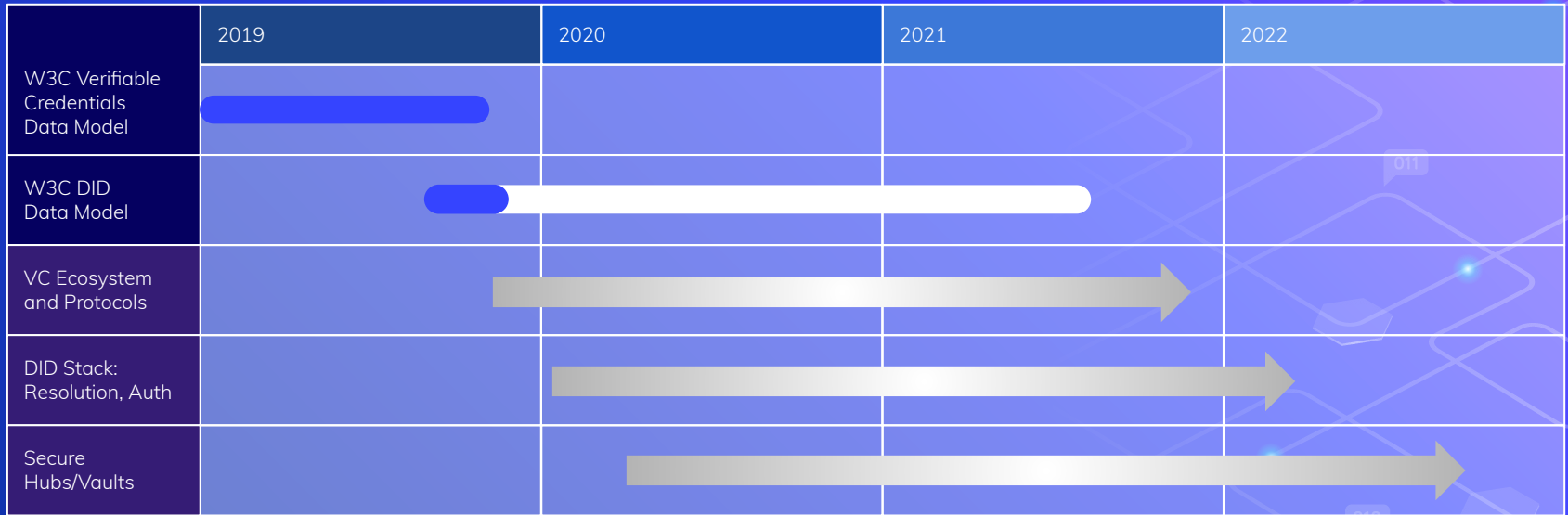
# DIDs resolve to DID Documents

- ⬡ DID Documents contain:
  - Verification methods
  - Service endpoints for interacting with the DID subject
- ⬡ Examples:
  - Authentication
  - Requesting a digital signature on a document





# Standardization Track



Pre-standards pipeline

# Thanks!

**Any questions?**

You can find me at:

@kimdhamilton

kimhd@mit.edu

Design Credits:

- ⬡ Presentation template by [SlidesCarnival](#)
- ⬡ Photographs by [Unsplash](#)

