KERI for Muggles

IIW #31
Day 1 - Session #2
20 October 2020

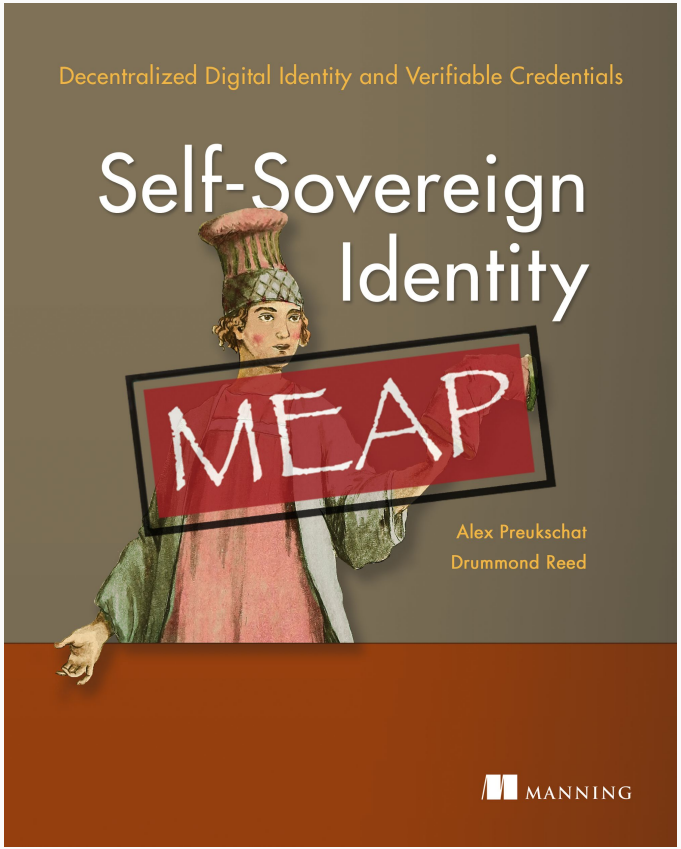
https://keri.one

KERI is a new approach to decentralized identifiers and decentralized key management that promises significant benefits for SSI (self-sovereign identity) and ToIP (Trust over IP) infrastructure

KERI is being developed and standardized in the Identifiers & Discovery Working Group at the Decentralized Identity Foundation

https://identity.foundation/working-groups/identifiers-discovery.html

I learned this while helping KERI inventor Dr. Sam Smith write a book chapter about KERI and decentralized key management



I volunteered to host this session to make these basic concepts accessible to anyone at IIW who wants to get the basic idea

Although the full technical architecture of KERI goes very deep (140 pages deep), the basic ideas are surprisingly straightforward

Format

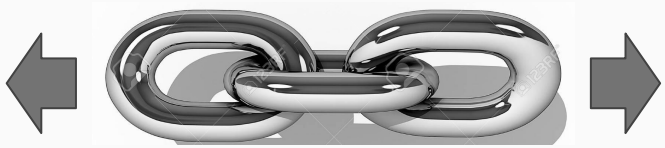
- First, a little background from Sam and Timothy Ruff
- Then 7 minutes for each of the 7 concepts
  - 3 minutes to explain the basic idea
  - 4 minutes for Sam to answer Q's about that slide
- A few more minutes for any additional questions
- Close with a quick summary of next steps for KERI

Meet KERI inventor Dr. Sam Smith

Meet Sam’s partner in Digital Trust Ventures, Timothy Ruff

KERI in Seven Easy Steps

Caveat: all of this depends on one fundamental concept:
public and private keys



Public key— MUST be shared

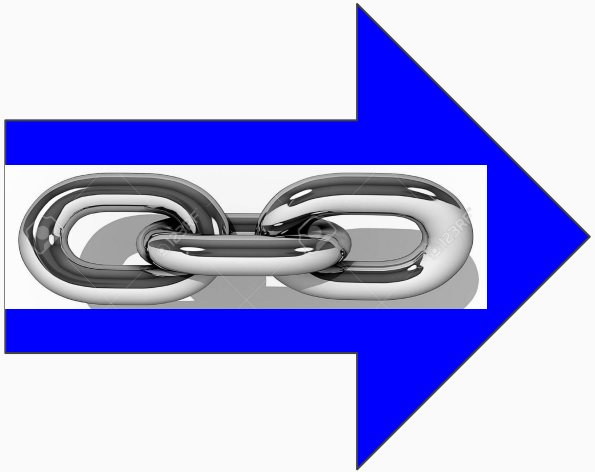
Cryptographic binding

Private key— MUST NOT be shared

#1: Self-Certifying Identifiers

A self-certifying identifier (SCID) is a identifier that can be proven to be the one and only identifier tied to a public key using cryptography alone*

* No blockchain needed

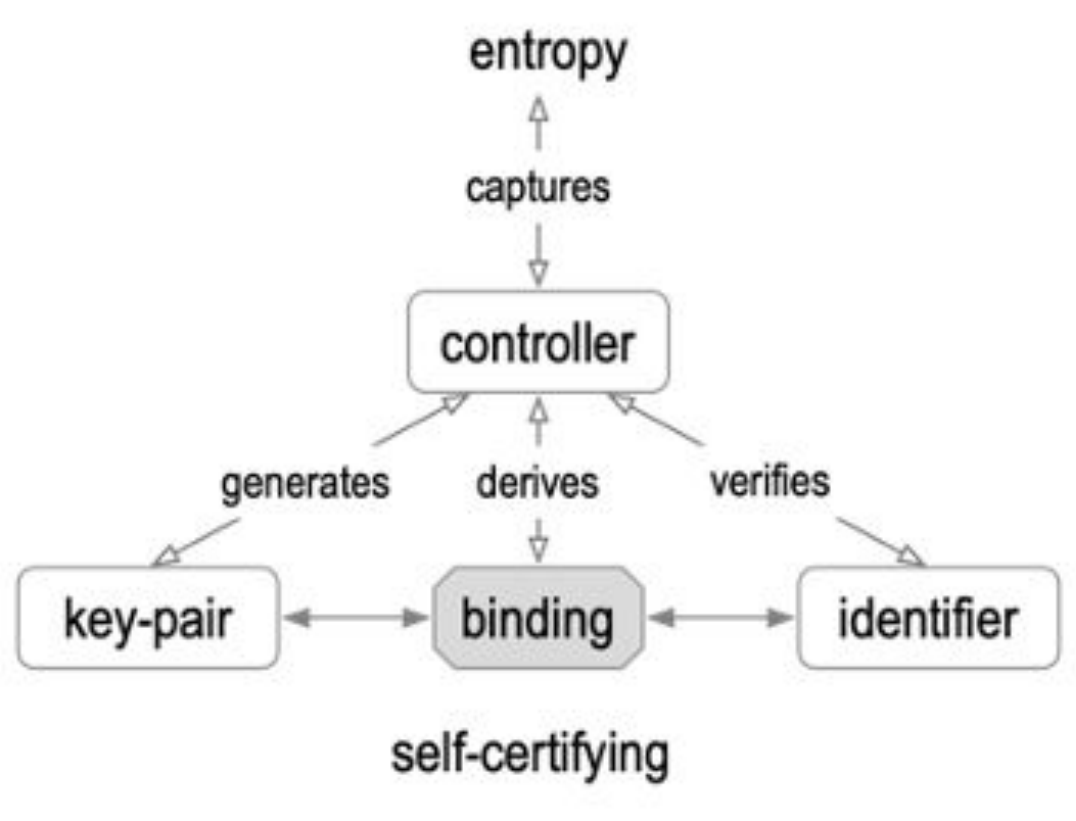


keri:21tD
AKCERh95u
GgKbJNHYp

Public key

Cryptographic binding

Self-certifying identifier


entropy
captures
controller
generates
derives
verifies
key-pair
binding
identifier
self-certifying

Benefit #1

You can prove you control a KERI identifier without needing to rely on ANYONE outside your control (even a blockchain)

#2: Self-Certifying Key Event Logs

Each time you change (“rotate”) your public/private key pair, KERI writes a new digitally-signed message to a log file so you can prove you made the change

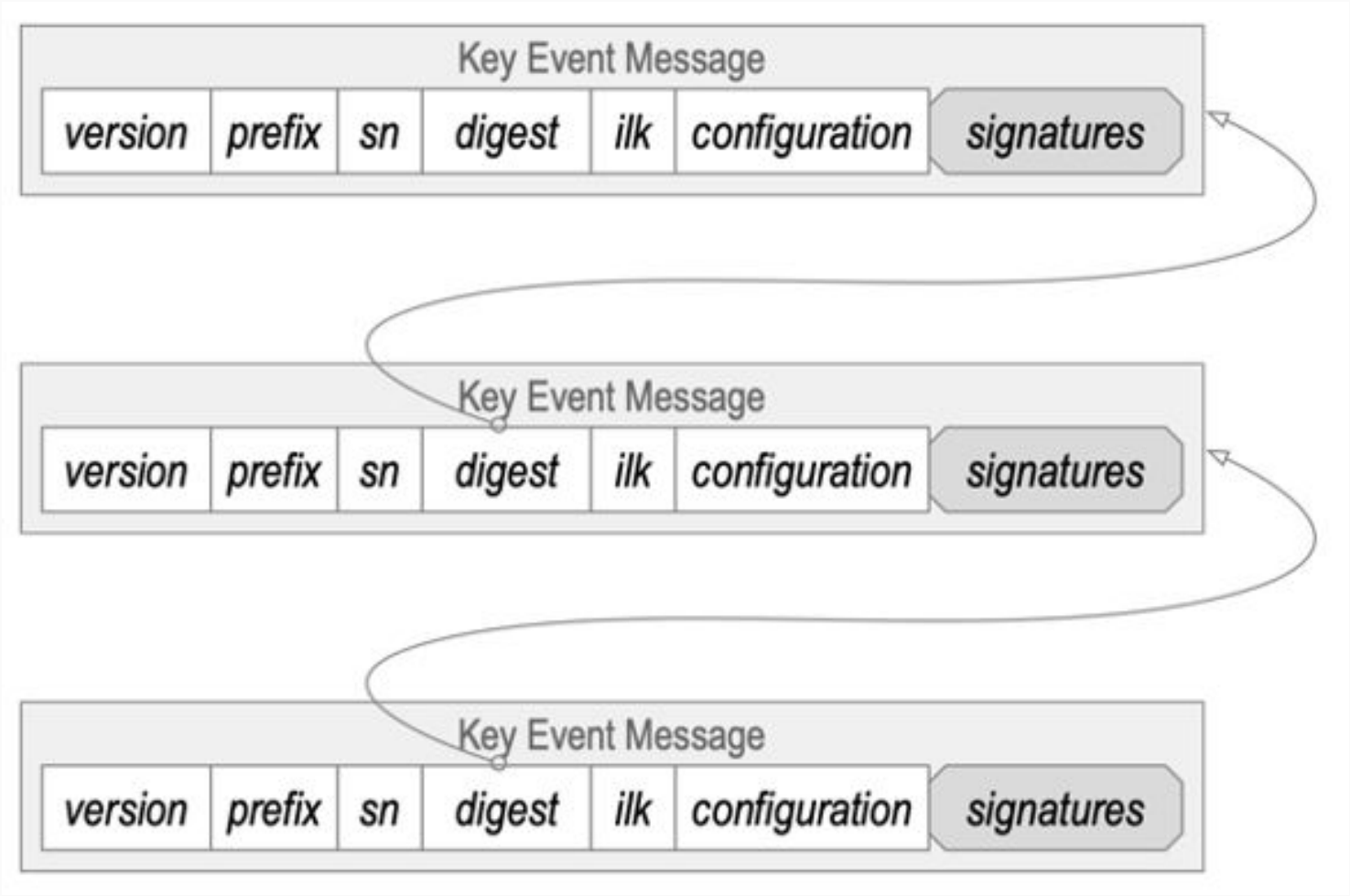
1)

2)

3)

4)

Rotated public keys


Key Event Message
version
prefix
sn
digest
ilk
configuration
signatures
Key Event Message
version
prefix
sn
digest
ilk
configuration
signatures
Key Event Message
version
prefix
sn
digest
ilk
configuration
signatures

Benefit #2

Each time you change your keys, you can prove you control your new public key without needing to rely on ANYONE outside your control (even a blockchain)

#3: Witnesses for Key Event Logs

You can keep your own copy of your KERI key event log, but you can also have other witnesses keep and digitally sign their own copies

sound and disposing mind, memory and understanding, and in all respects competent to make a Will.

Mickey Hall
WITNESS

Mickey Hall
(Printed name)

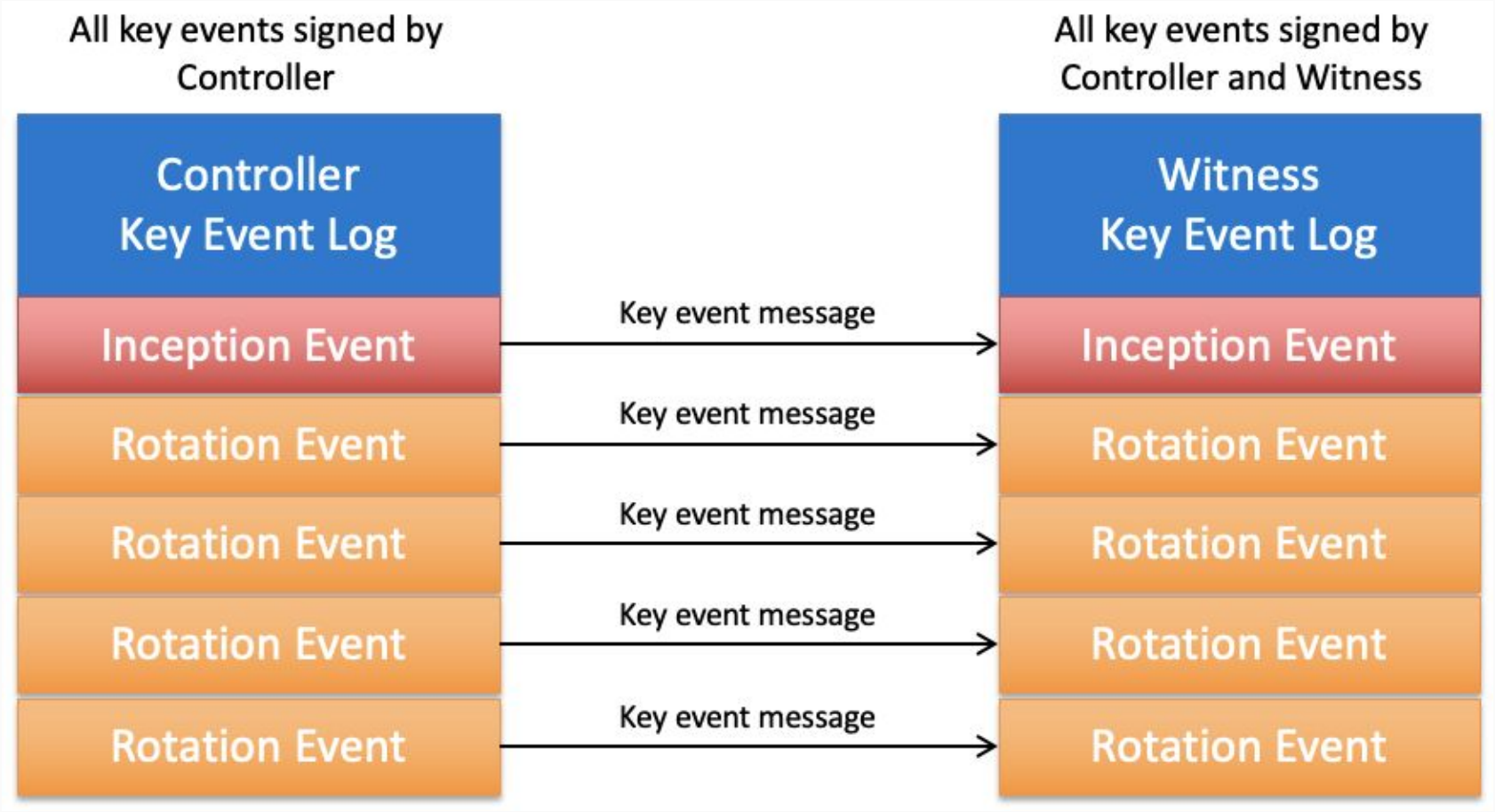
Kimberly K. Davis
WITNESSES

Kimberly K. Davis
(Printed name)

Sworn to and subscribed before me, this 10th day of October, 2008.

Patricia K. Pearson
Notary Public

My Commission Expires: 10-18-11

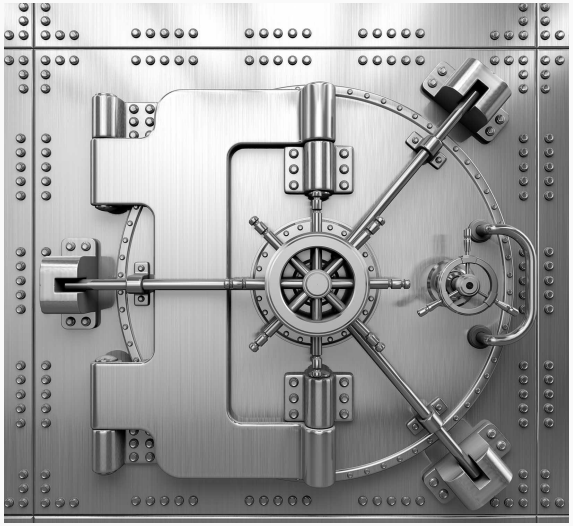

All key events signed by Controller
All key events signed by Controller and Witness
Controller Key Event Log
Witness Key Event Log
Inception Event
Rotation Event
Rotation Event
Rotation Event
Rotation Event
Key event message
Key event message
Key event message
Key event message
Key event message
Inception Event
Rotation Event
Rotation Event
Rotation Event
Rotation Event

Benefit #3

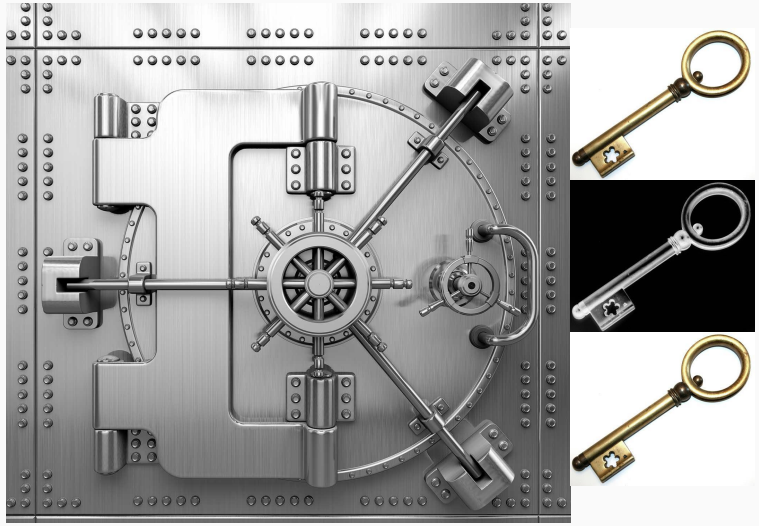
Although witnesses are not required, they provide additional evidence that you control your current public key(s) and are not cheating

#4: Pre-rotation as simple, safe, scalable protection against key compromise

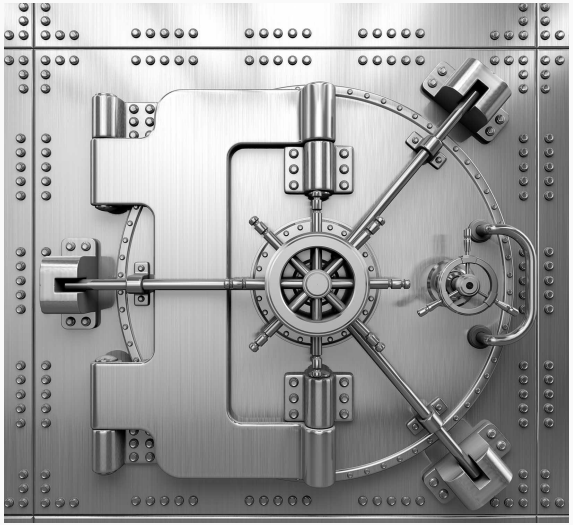
KERI can’t prevent theft of your current private key—but it has an ingenious solution for hiding your next private key that makes it nearly impossible to steal

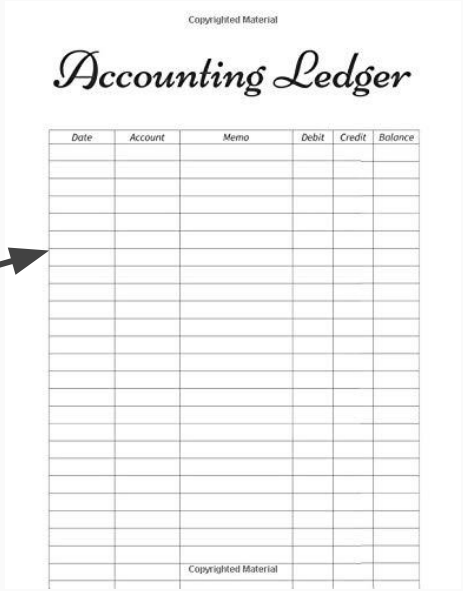


Step 1: Go inside your bank vault (digital wallet)



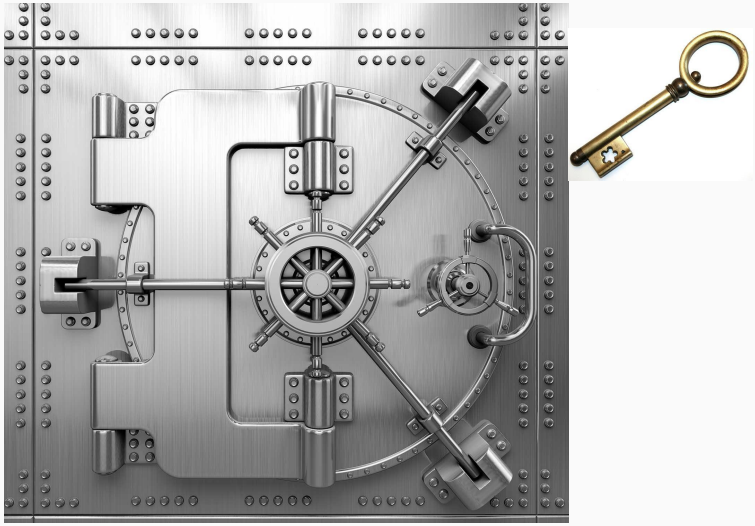
Step 2: Generate new key pairs for <u>future</u> use





Step 3: Digitally sign a proof of the next public key

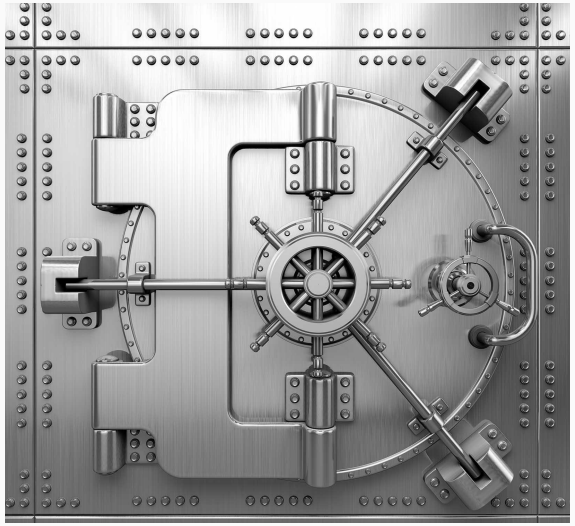
Step 4: Write that proof and signature to the event log



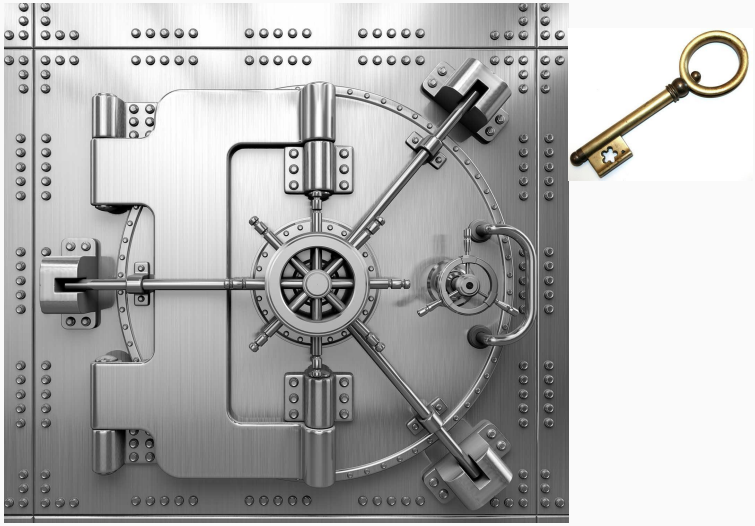
Step 5: Take out your current public key to share

Step 6: Use your current private key as needed

Step 7: ALERT! Private key compromised!

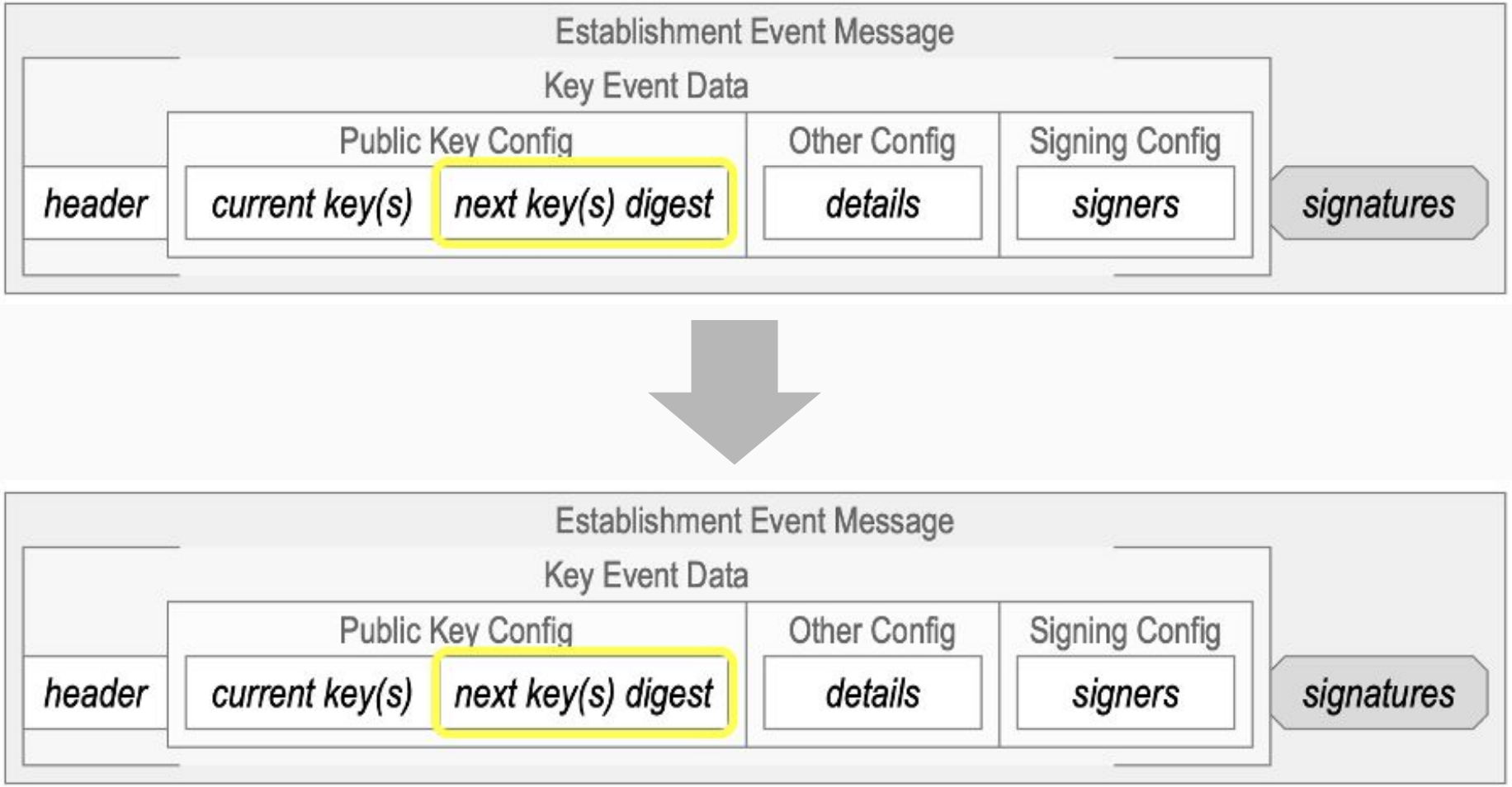


Step 8: Go back to your private vault (digital wallet)



Step 9: Take out next public key to share

Step 10: Use your next private key as needed


Establishment Event Message
Key Event Data
Public Key Config
Other Config
Signing Config
header
current key(s)
next key(s) digest
details
signers
signatures
Establishment Event Message
Key Event Data
Public Key Config
Other Config
Signing Config
header
current key(s)
next key(s) digest
details
signers
signatures

Benefit #4

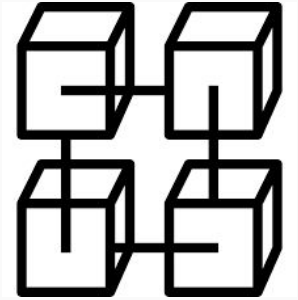
You can safely “lock away” your next private key so it it can’t be stolen from your current device—and protect yourself if your current private key is ever compromised

Bonus Benefit!

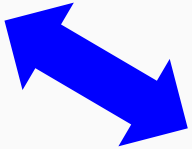
This key protection technique is post-quantum proof!

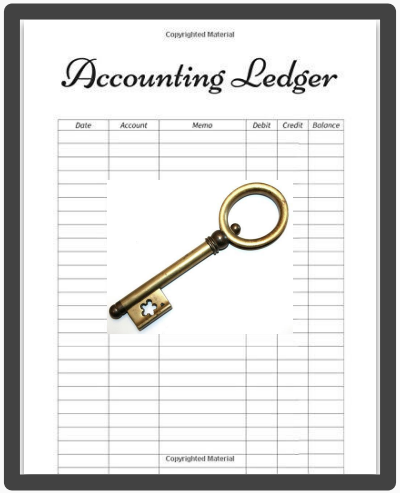
#5: System-independent validation

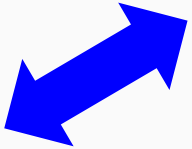
Because KERI identifiers and event logs are self-certifying, they can be witnessed by any system anywhere that can store and return data—and you can use all of them as witnesses



Blockchain

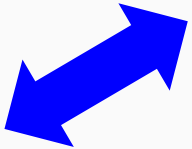


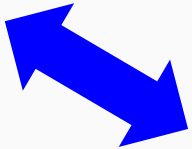


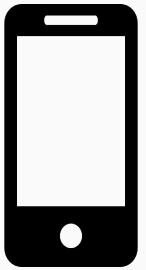


File system

Database







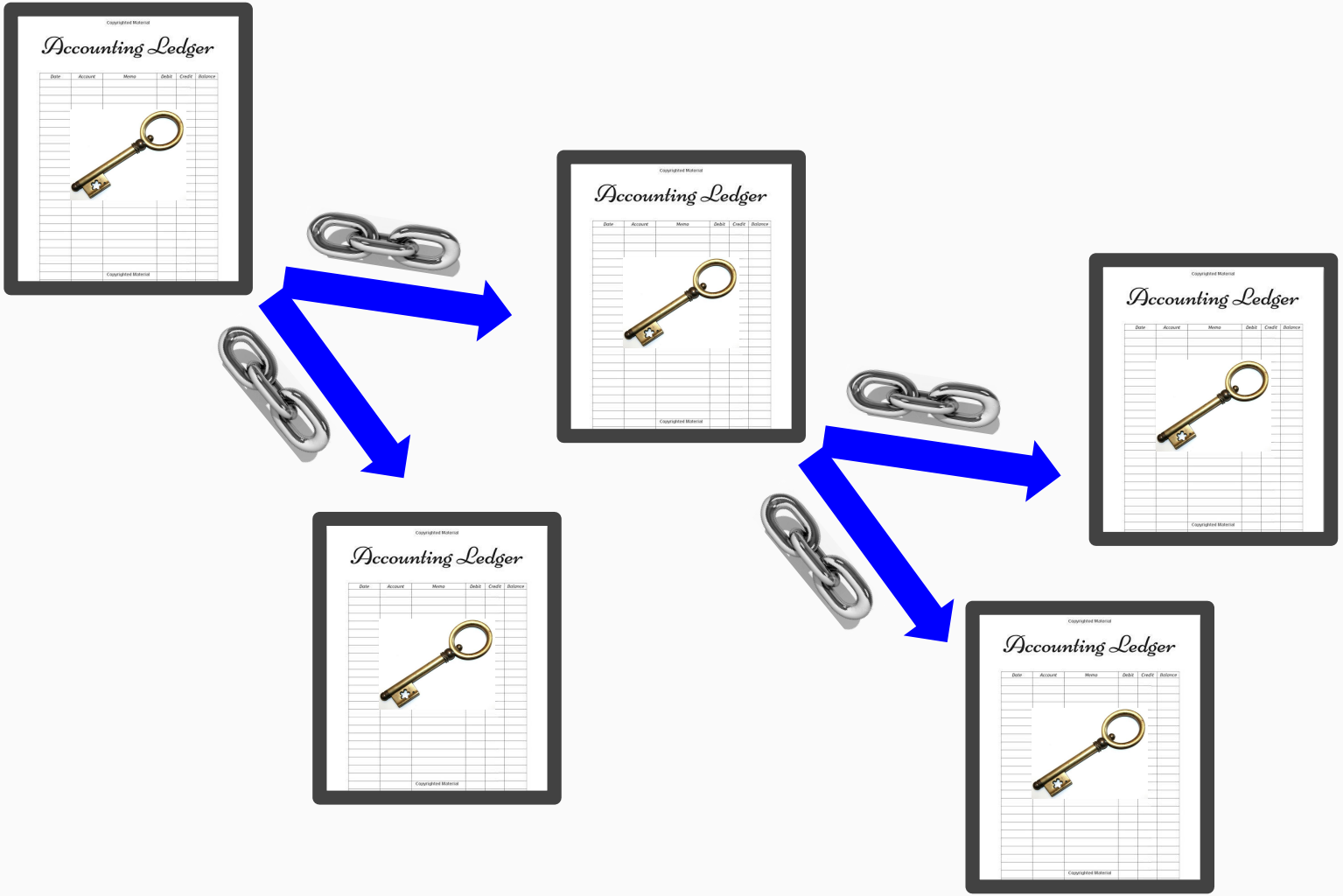
Local device

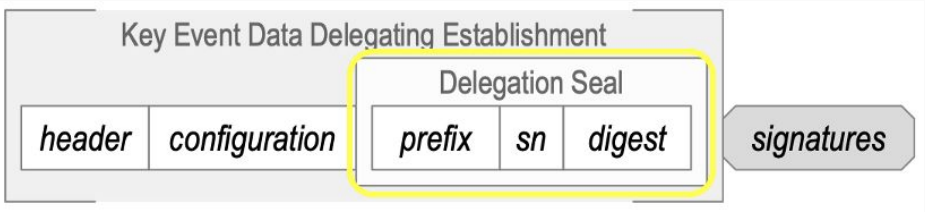
Benefit #5

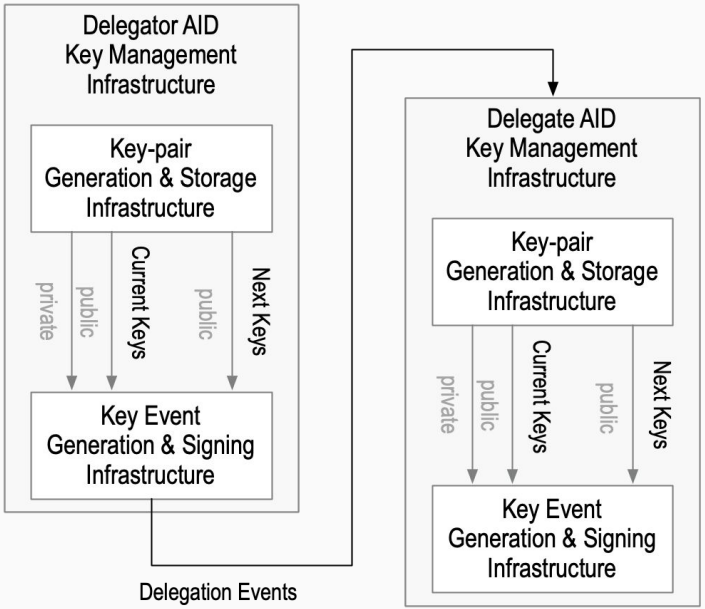
KERI identifiers and keys are not “ledger-locked”—they are fully portable and can be validated using any ledger, distributed database, or other verifiable data registry

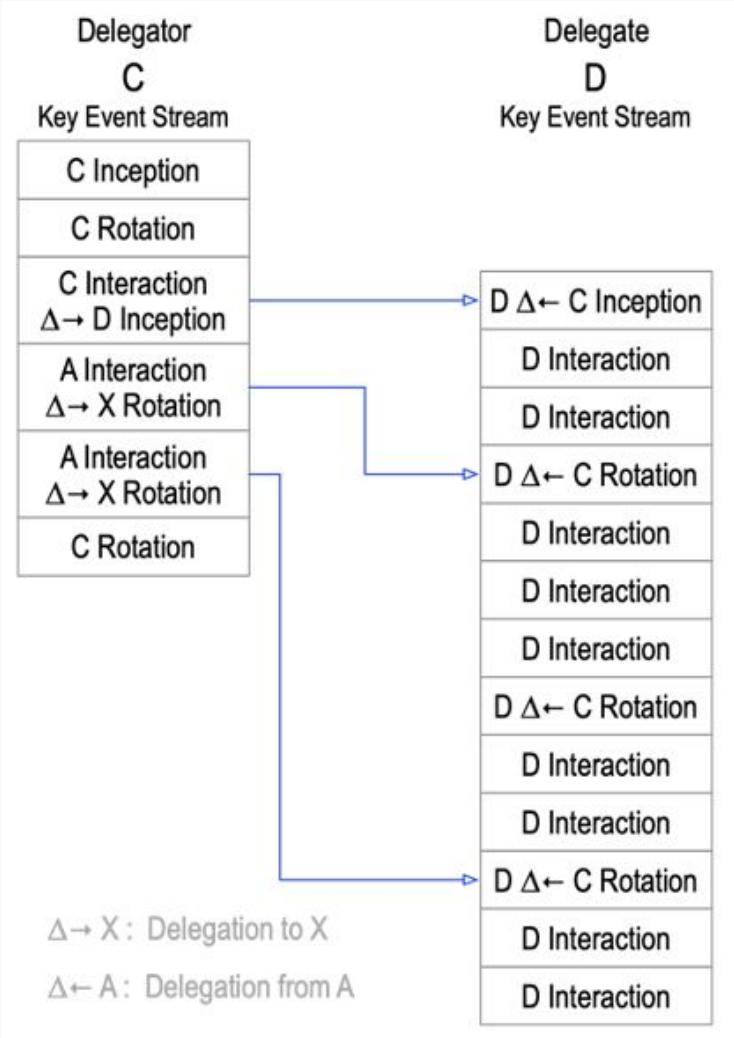
#6: Delegated self-certifying identifiers enables enterprise-class key management

KERI identifiers can be “delegated”, meaning one identifier can create another one that can prove its relationship with its parent—so you can create any hierarchy of identifiers & keys


Copyrighted Material
Accounting Ledger
Date
Account
Memo
Debit
Credit
Balance
Copyrighted Material


Key Event Data Delegating Establishment
Delegation Seal
header
configuration
prefix
sn
digest
signatures


Delegator AID
Key Management
Infrastructure
Key-pair
Generation & Storage
Infrastructure
private
public
Current Keys
public
Next Keys
Key Event
Generation & Signing
Infrastructure
Delegation Events
Delegate AID
Key Management
Infrastructure
Key-pair
Generation & Storage
Infrastructure
private
public
Current Keys
public
Next Keys
Key Event
Generation & Signing
Infrastructure


Delegator
C
Key Event Stream
C Inception
C Rotation
C Interaction
Δ→ D Inception
A Interaction
Δ→ X Rotation
A Interaction
Δ→ X Rotation
C Rotation
Delegate
D
Key Event Stream
D Δ← C Inception
D Interaction
D Interaction
D Δ← C Rotation
D Interaction
D Interaction
D Interaction
D Δ← C Rotation
D Interaction
D Interaction
D Δ← C Rotation
D Interaction
D Interaction
Δ→ X : Delegation to X
Δ← A : Delegation from A

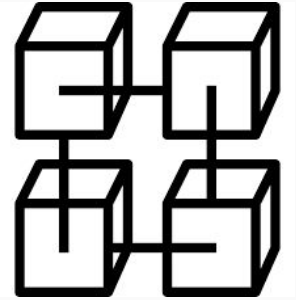
Benefit #6

With KERI identifier and key delegation, enterprises can scale and manage delegation hierarchies of any size and complexity

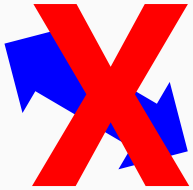
#7: Compatibility with the GDPR* “right to be forgotten”

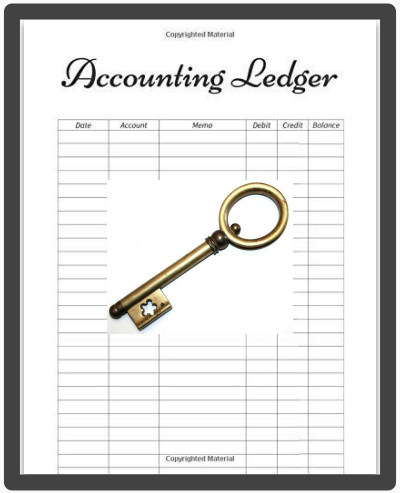
* EU General Data Protection Regulation

When a decentralized identifier for a person is written to an immutable ledger, it can creates a privacy issue because it cannot be erased—but KERI identifiers can use witnesses that permit erasure

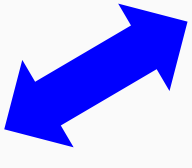


Blockchain



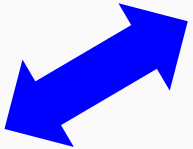


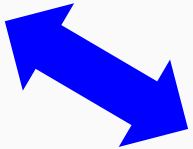
Person

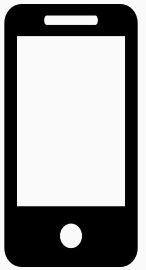


File system

Database







Local device

Benefit #7

KERI infrastructure can be GDPR-compliant because it does not require the use of immutable ledgers—KERI event logs can be deleted without compromising security

More questions for Sam?

Next steps for KERI:

https://identity.foundation/working-groups/identifiers-discovery.html

https://keri.one

Thank you!

May your keys be with you!