# KERI: 1
# Universal DKMI

# Decentralized Root-of-Trust

# *Last Mile*

Samuel M. Smith Ph.D.
IIW Fall 2019 2019/10/01
https://github.com/SmithSamuelM/Papers
sam@samuelsmith.org

# Background Reading

Girault, M., “Self-certified public keys,” EUROCRYPT 1991: Advances in Cryptology, pp. 490-497, 1991

https://link.springer.com/content/pdf/10.1007%2F3-540-46416-6_42.pdf

Kaminsky, M. and Banks, E., “SFS-HTTP: Securing the Web with Self-Certifying URLs,” MIT, 1999

https://pdos.csail.mit.edu/~kaminsky/sfs-http.ps

Mazieres, D. and Kaashoek, M. F., “Escaping the Evils of Centralized Control with self-certifying pathnames,” MIT Laboratory for Computer Science, 2000

http://www.sigops.org/ew-history/1998/papers/mazieres.ps

Mazieres, D., “Self-certifying File System,” MIT Ph.D. Dissertation, 2000/06/01

https://pdos.csail.mit.edu/~ericp/doc/sfs-thesis.ps

Smith, S. M., “Open Reputation Framework,” vol. Version 1.2, 2015/05/13

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/open-reputation-low-level-whitepaper.pdf

Smith, S. M. and Khovratovich, D., “Identity System Essentials,” 2016/03/29

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/Identity-System-Essentials.pdf

Smith, S. M., “Decentralized Autonomic Data (DAD) and the three R’s of Key Management,” Rebooting the Web of Trust RWOT 6, Spring 2018

https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/DecentralizedAutonomicData.pdf

**Smith, S. M., “Key Event Receipt Infrastructure (KERI) Design and Build,” arXiv, 2019/07/03**

https://arxiv.org/abs/1907.02143

# Human Basis of Trust

I know you

or

I know of you

therefore

I trust you

On the internet I can’t really know who you are.
therefore
I can’t trust you

# Decentralized Control Authority

Assymetric PKI: Public-Private Key Pairs with Digital Signatures

CSPRNG Cryptographic Strength Pseudo Random Number Generator

Collision Resistant Random Seed (Entropy) Available to Anyone

Seed -> Private Key -> One Way Function -> Public Key

Authority comes from collision resistance

Inherently decentralized

Sole Sovereign over random seed

Only one who can make verifiable signed statements associated with the Public Key

# Cryptographic Root-of-Trust

Trust *who said it* not *what was said*

Consistent attribution is the root-of-trust  (integral non-repudiable statements)

Duplicity detection

I trust that controller of private key made a set of statements

Build trust in *what was said* via consistent history of consistently attributable statements.

# Self-Certifying Identifier/Namespace

Use public key in identifier

Use public key as prefix in namespace

Decentralized Root of Trust

Signed Statements that include self-certifying identifier

Self-Certifying Namespace

Provenanced chain of transformations with verifiable control over transformation

End-wise Verifiable (primary root-of-trust)

Other roots of trust may add to but not replace self-certification

All decentralized infrastructure has self-certifying identifiers as primary root-of-trust

Decentralized key management is therefore essential to protecting infrastructure

# AUTONOMIC NAMESPACE

Self-Certifying

Self-Managing

Self-Administering

Extensible

# KEY MANAGEMENT

Rotation

Reproduction

Recovery

# KEY MANAGEMENT

Best Practice:

One-use: One-time One-place One-way

# BACKGROUND