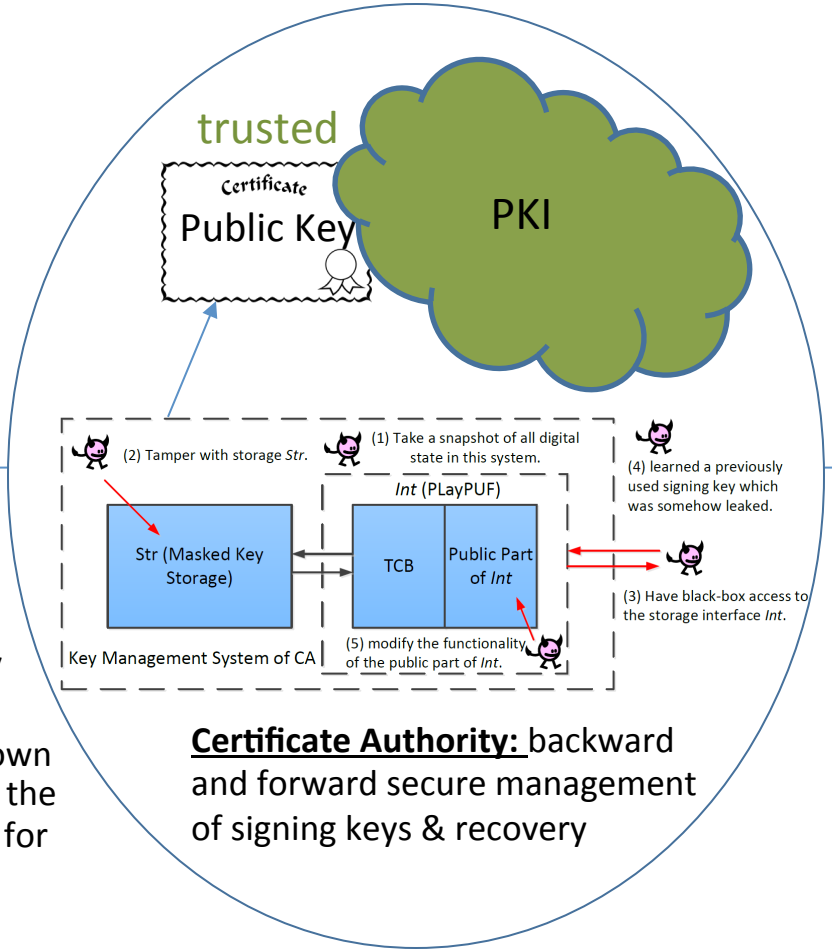
Self-Recovering Certificate Authorities using Backward and Forward Secure Key Management

Challenge:

- The current attack surface exposed by CAs makes trust in their issued certificates questionable
- An insider attack may allow an adversary to copy all digital state

Solution:

- Backward and forward security based on:
- Programmable Logically Erasable PUFs
- Revoke signing keys known to the adversary before the CA is going to use them for signing certificates



Scientific Impact:

- Self-recovering CAs promise strong security guarantees against the most powerful attacker who can read all digital state

Broader Impact:

- Enterprises and individuals will be able to trust CAs and will regain trust in PKI as a whole

NSF 1617774, Sept 2016 – Aug 2019

University of Connecticut
PI Marten van Dijk
marten.van_dijk@uconn.edu, http://scl.uconn.edu/