REDWALL
TECHNOLOGIES LLC

SMART CARDS IN THE IoT CHAIN OF TRUST

Smart Card Alliance

SECURITY OF THINGS
TRUST IN THE INTERNET OF THINGS

2016

October 18, 2016 - Chicago

Your presenter: Eric Üner

Get more coffee - I am an Engineer

CTO Redwall

Device security for mobiles, wearables, SCADA, and IoT

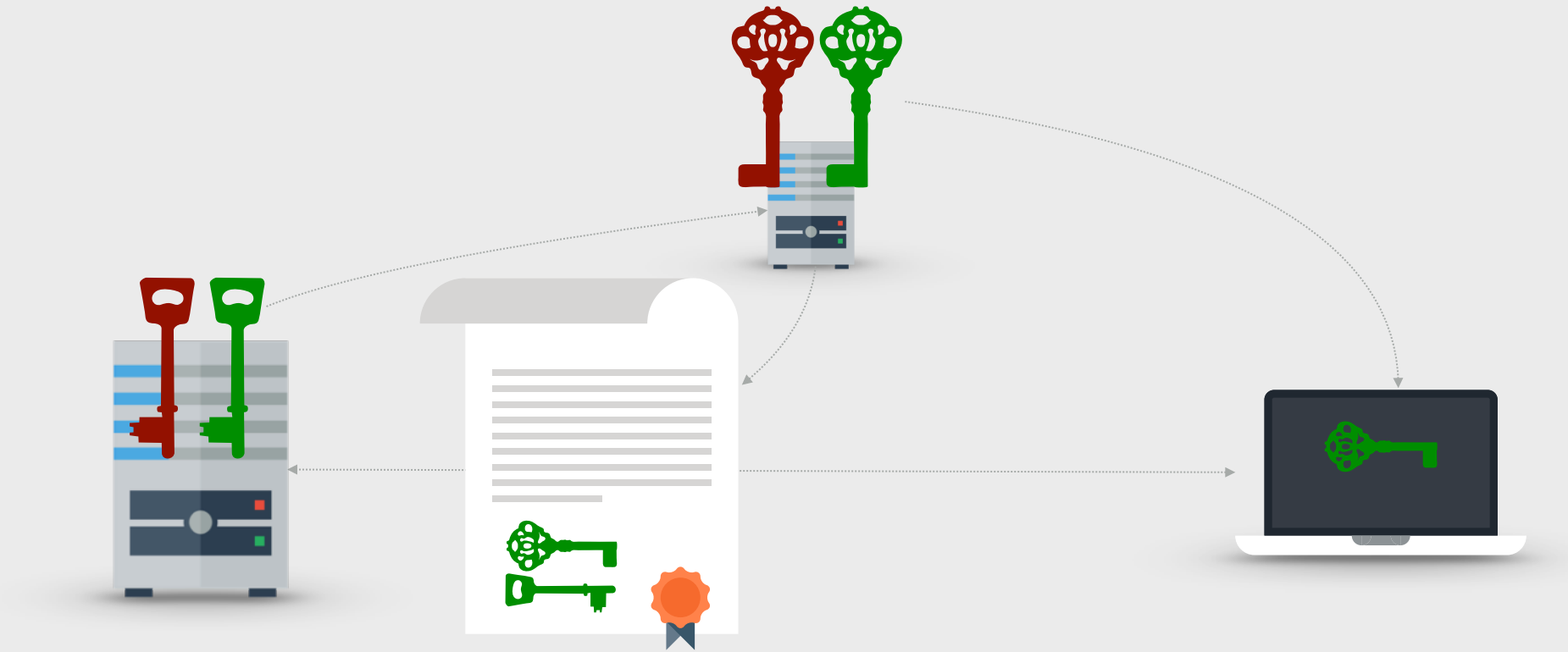
Integrity monitoring, root protection, DPA resistance and more

User base in include law enforcement, intelligence, defense, and regulated markets

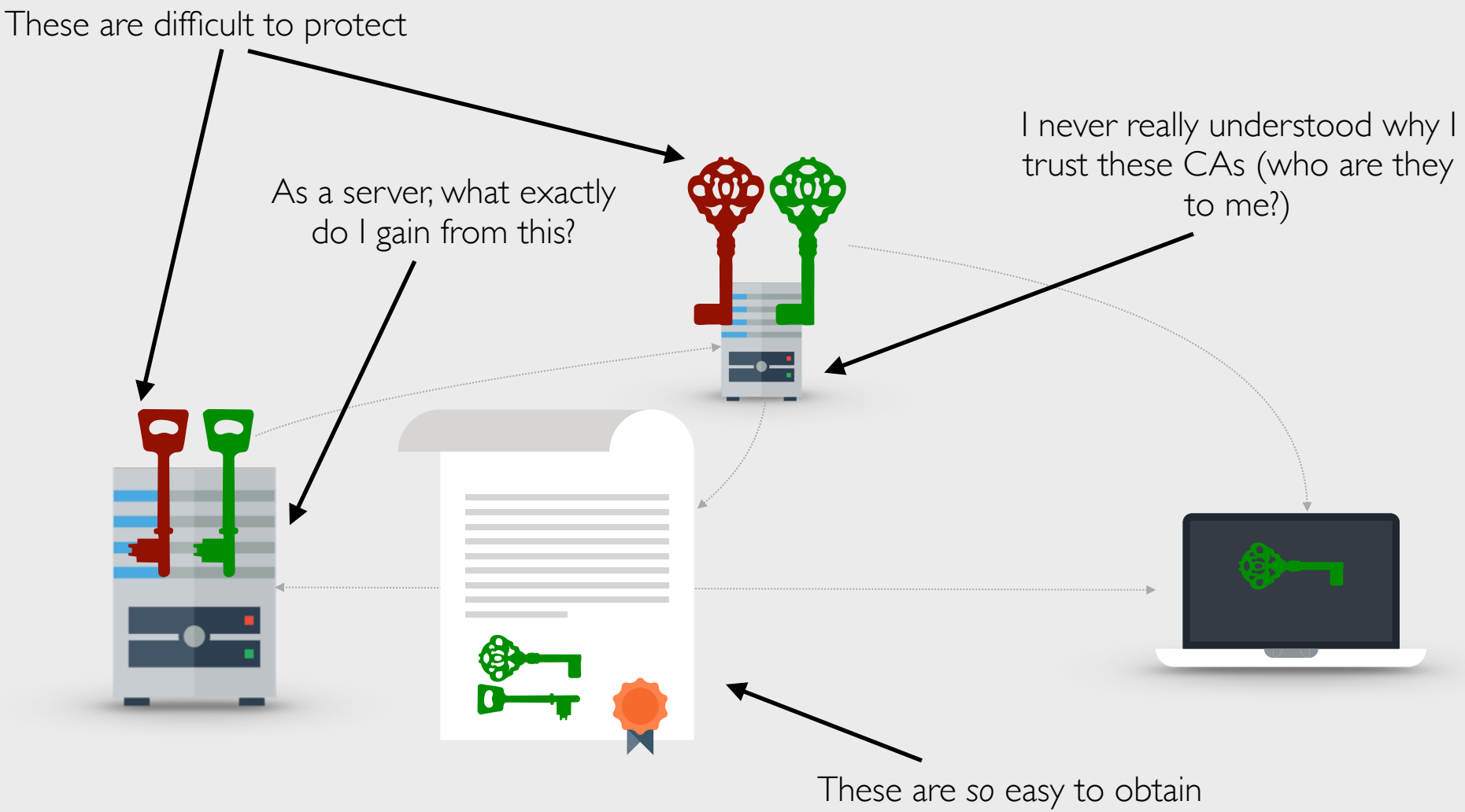
Deep background in offensive work, which includes many systems with smart cards

Trust chains

Most people think of "certificate chains"



Web certificates don't do what people think



The model isn't broken, the implementation is

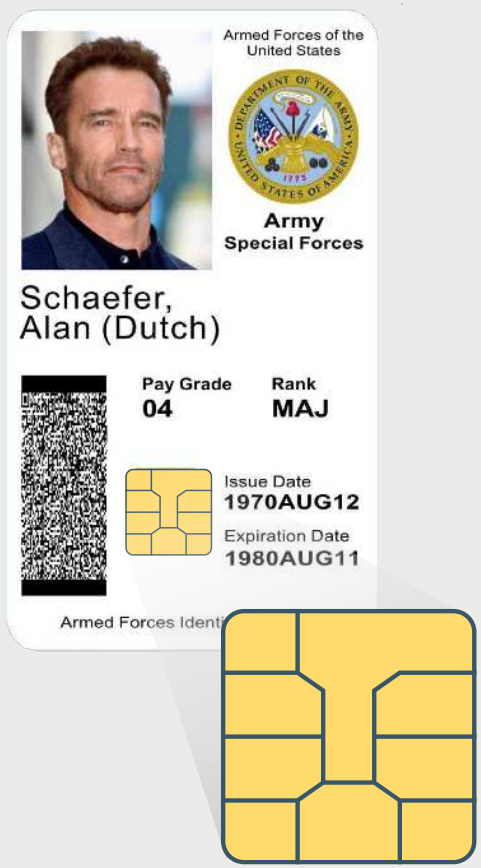
Smart cards are frequently used to address the most significant issues when mapping this from mobile to IoT architectures

Private keys can be stored more securely

Provisioning/enrollment adds trust

Authentication requires possession (multi-factor)

Consider - the CAC

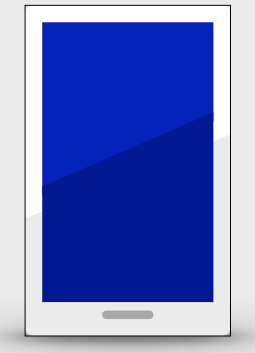


Common access card

Provides multi-factor, but also:

- Hierarchical
- Difficult to duplicate
- Only works for me
- Serves multiple purposes
- Keys and passcodes are local

Say…what else shares those characteristics?



You phone:

- Hierarchical
- Difficult to duplicate
- Only works for me
- Serves multiple purposes
- Keys and passcodes are local

Except none of that is actually true

You phone:

~~Hierarchical~~

~~Difficult to duplicate~~

~~Only works for me~~

~~Serves multiple purposes~~

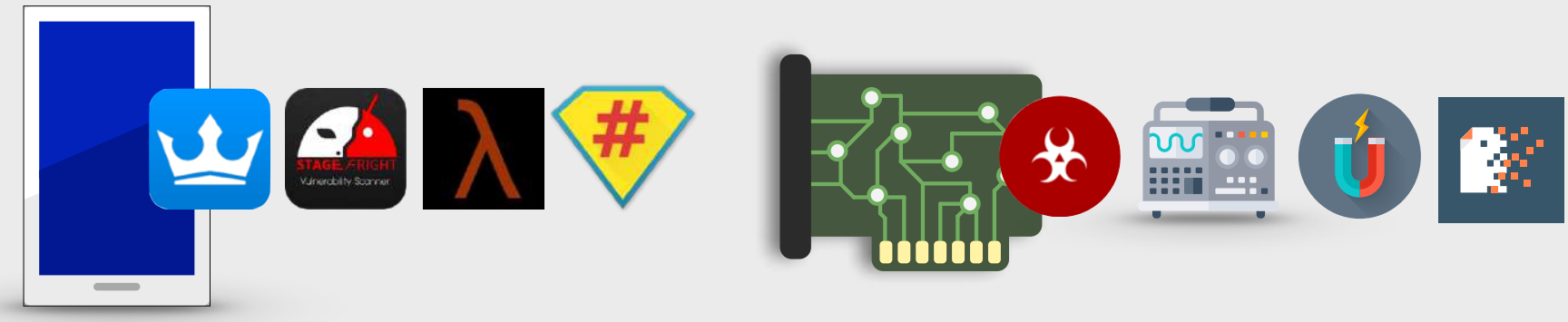
~~Keys and passcodes are local~~

Except none of that is actually true

Phones and IoT devices are ridiculously hackable

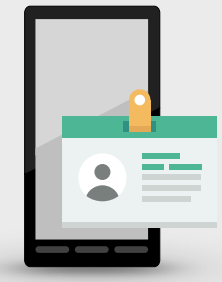
We've tried hypervisors, microvisors, virtualization, different operating systems, RTOSs etc. and they've all fallen

We create malware under contract, but don't take our word for it…



Unless your devices have Redwall of course, which makes them immune to all of this and more

There are some hybrid approaches

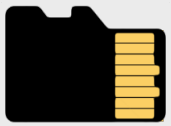


Derived credentials

- You may not have your PIV card, but you *did* have it
- Still leverages certificate and/or key from PIV card
- NIST guidelines are ready (see link at end of slides)

Alternative authentication

- Sekur Me - QR-code + biometrics or PIN
- Redwall separates authentication from HILOS



Smart card HSM in µSD and other small form factors

Smart card HSM you say?

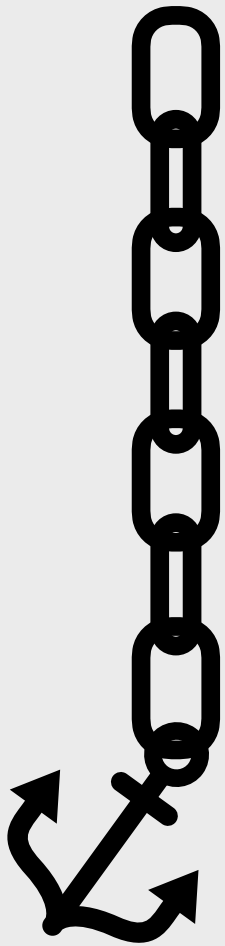
Available in different form factors applicable to IoT for different use cases and devices

Trusted, highly robust key storage with hardware protections and advanced defenses

Can optionally be coupled to host hardware

Many, but not all, include smart card technology

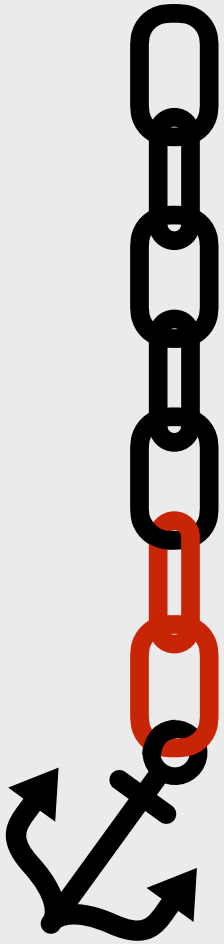
Trust chaining in IoT architectures



Not a detailed or complete picture, but in general:

- DIT
- Authentication from system
- Attestation
- DAR
- Authentication to system
- OS
- Bootloader
- Hardware keys and certificates

Some great places for smart cards in there



DIT ✓

Authentication from system ✓

Attestation ✓

DAR ✓

Authentication to system ✓

OS

Bootloader

Hardware keys and certificates ✓

Why not use (insert product name here)?

Trustzone (and wrappers that leverage it) - Several flawed implementations create serious weaknesses; ARM only

Your chip vendor's features - Maybe; not mutually exclusive with smart cards

Some container or virtualization someone keeps trying to sell you - Don't bother; high engineering overhead; poor defensive abilities

TPM - Depends on hardware needs; virtual smart card, anyone?

Smart cards are not a panacea

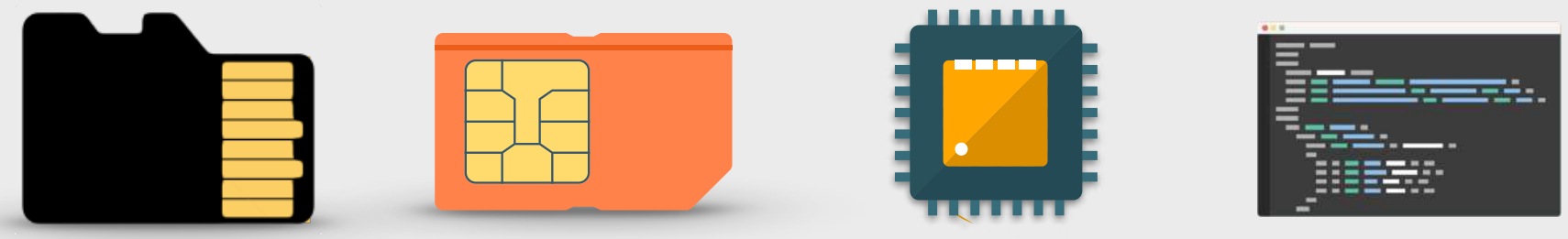
Actually nothing is - no single solution is perfect for everyone, and no magical security solution exists for anyone

Smart cards have some disadvantages:

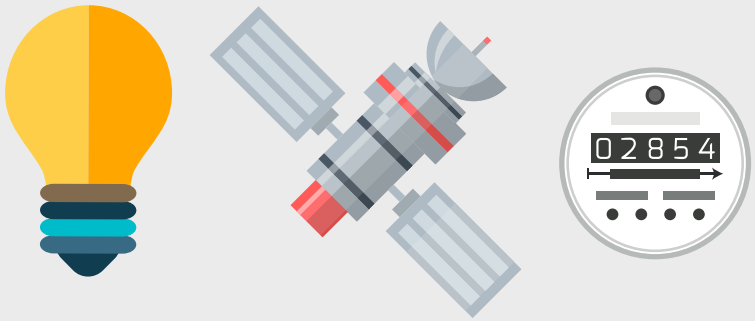
- Provisioning cost and complexity
- Additional hardware requirements
- Development and integration NRE

The Smart Card Alliance

One of the great things about the Smart Card Alliance - all of these are options are explored!



Because IoT is so diverse:



Think about smart cards in your design!

Reference links following these slides

Always feel free to contact me with questions, comments, and suggestions:

Eric Ridvan Üner
Chief Technology Officer
(847) 208-1077
eric.uner@redwall.us

HTTP://WWW.REDWALL.US

Some helpful links

Smart Card Alliance site has really impressive resources: http://www.smartcardalliance.org/

NIST guidelines for derived credentials: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

Redwall Technologies: http://www.redwall.us

Simon and Speck (Redwall has implementations of these available): https://en.wikipedia.org/wiki/Simon_(cipher), https://en.wikipedia.org/wiki/Speck_(cipher)

Relevant FIPS requirements: http://www.smartcardalliance.org/publications-government-id-fips-201/, http://csrc.nist.gov/groups/STM/cmvp/standards.html#02

Always feel free to email me with questions and suggestions - eric.uner@redwall.us