I am Joe's Fridge: Scalable Identity in the Internet of Things

9^{th} IEEE International Conference on Internet of Things

Prashant Anantharaman [1], Kartik Palani [2], David Nicol [2], Sean W. Smith [1]

[1]Dartmouth College, USA

[2]University of Illinois at Urbana-Champaign, USA

December 2016

This Talk

Section 1

Introduction

The consumer-side smart grid

- Massive number of devices talking to each other.
- The talking has to be meaningful – so who is talking?
- Impersonation is always a threat!
- In the vision of consumer-side smart grid, every house would have a smart meter.

The smart meter as the gateway

- Meters know about occupancy of houses and can turn off devices.
- Real-time pricing.
- Demand-response signals to help ease stress on the grid.
- Communicate with gateway devices like Bidgely to get more detailed bills.

Auxiliary communication

- Receive software updates from its manufacturer.
- Send repair diagnostics to the manufacturer, to aid in quick fixing of the appliance.
- Devices communicate with the utility (through the smart meter) to receive commands.

Electric vehicles

- Charging station and car need to authenticate each other.
- Infrastructure needs to authenticate the car for billing.
- Charging can be scheduled in case of differential pricing.
- The electric vehicles draw more power than many standard households, and hence coordination is needed to help a meltdown.

Section 2

The Problem

Overview

- What attributes do listeners need to know?
- Who is in a position to witness these attributes?
- How would the binding of attributes happen?
- What happens when these bindings change?

Attributes

- A simple unique global identifier does not suffice to tell relying parties what they need to know. e.g. IPv6 address – we still need a DNS along with other semantics.
- When appliances talk to each other, does a peering (a communication channel) relationship exist between the appliances? Is the appliance of the correct type?

Lifetime

- An attribute can be formalized as a tuple (P, O, Δ).
- Property P holds for the object O, for time Δ.
- Someone present at the manufacturing location of the device, or the sales location of the device can make these assertions.
- **But how does a relying party know this witness is in a position to make this assertion?**

Example

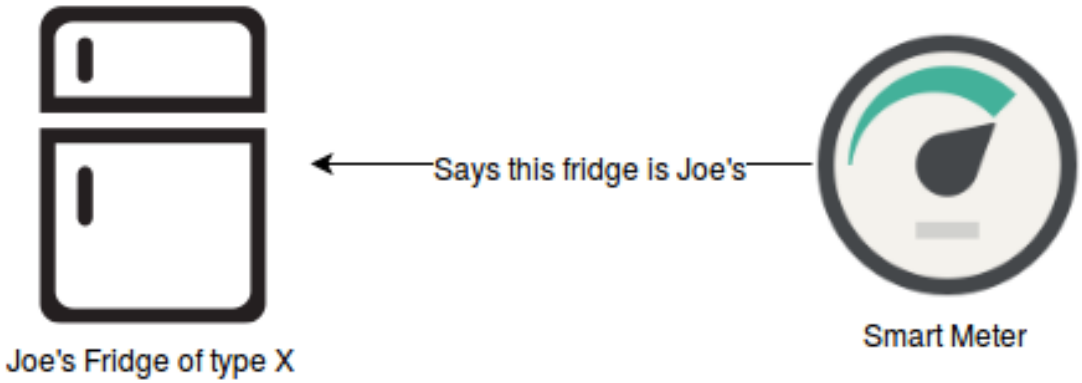
Joe's Fridge of type X

Example

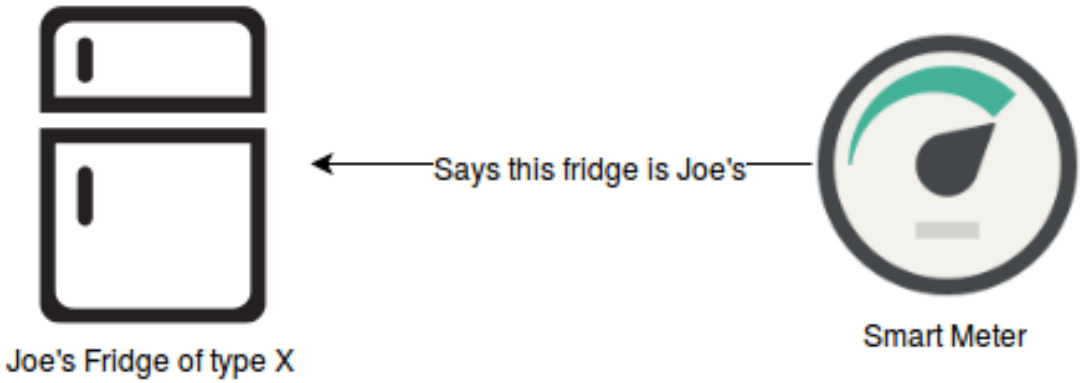
Joe's Fridge of type X

Who would be the witnesses here?

Example (contd.)

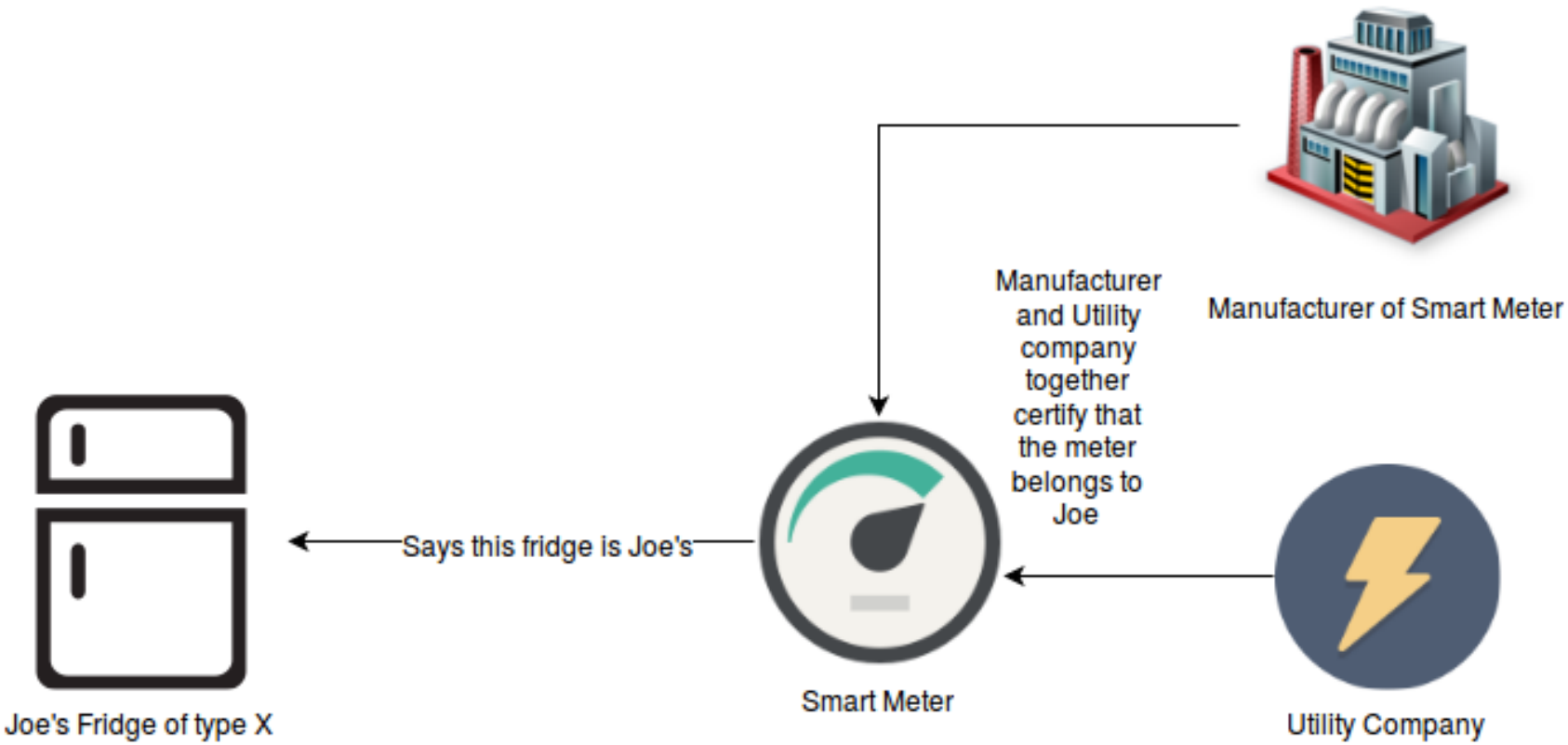


Example (contd.)

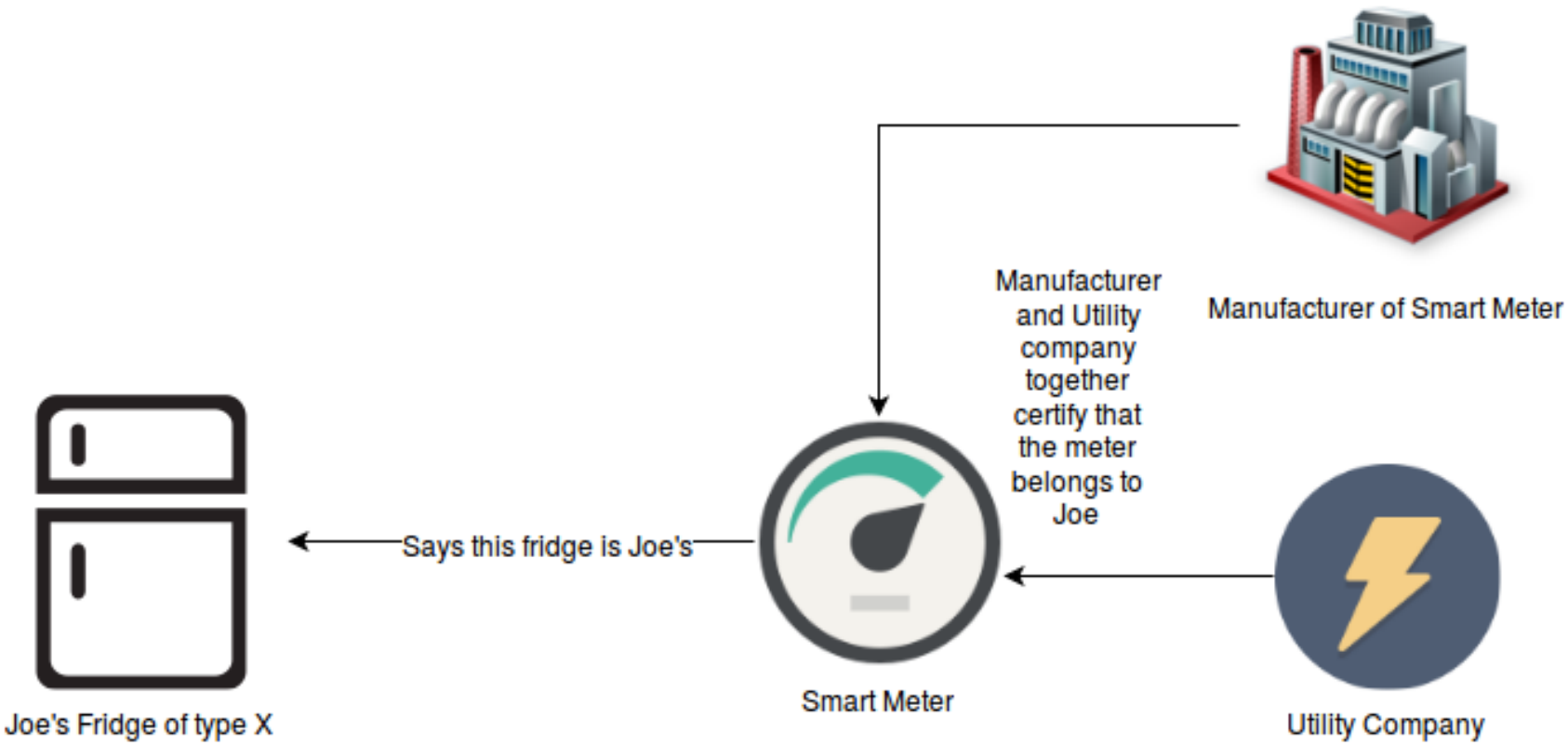


Who said it was the meter?

Example (contd.)

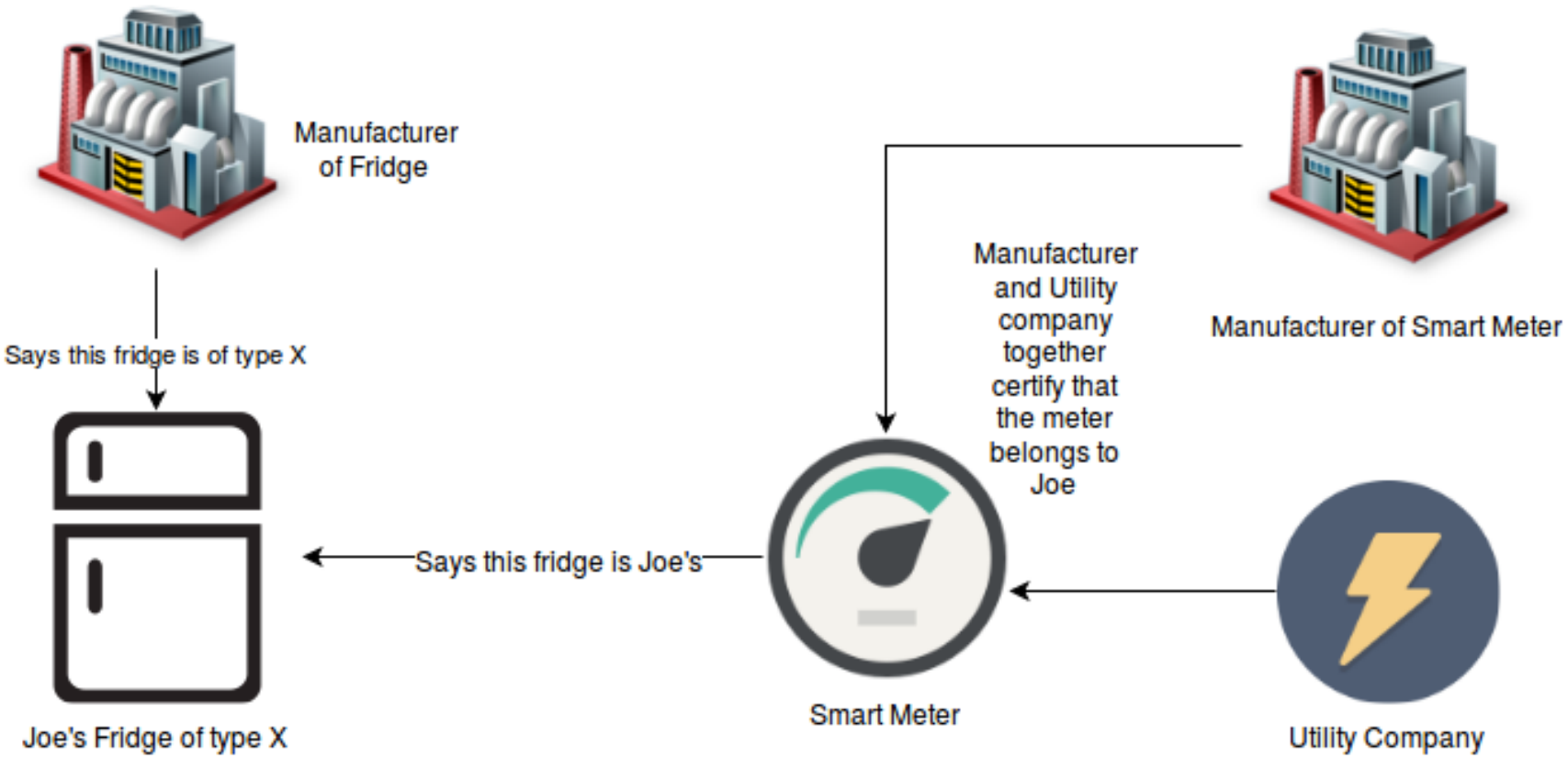


Example (contd.)



What about the type of the fridge?

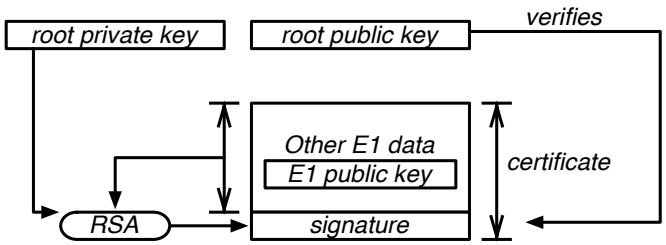
Example (contd.)



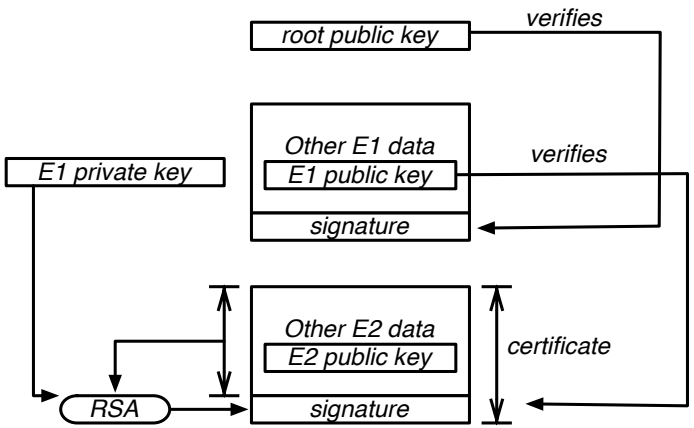
Section 3

Tools

PKI



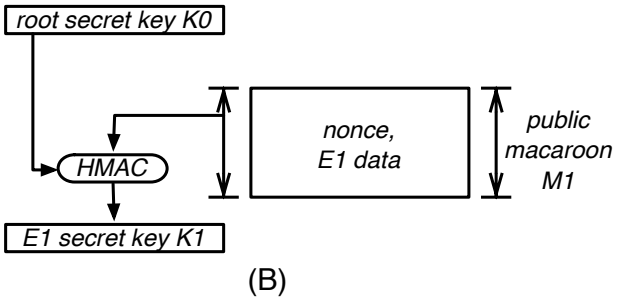
(A)



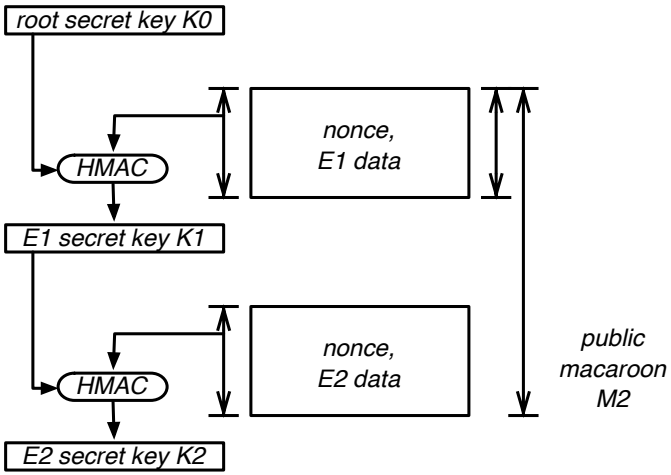
(C)

- Each entity would have matching public key and private key, and an entity can issue a digitally signed certificate asserting something about the public key of another entity.
- Any relying party who knows the CAs public key (trust root) can verify a certificate.

Macaroons



(B)



(D)

A macaroon consists of a

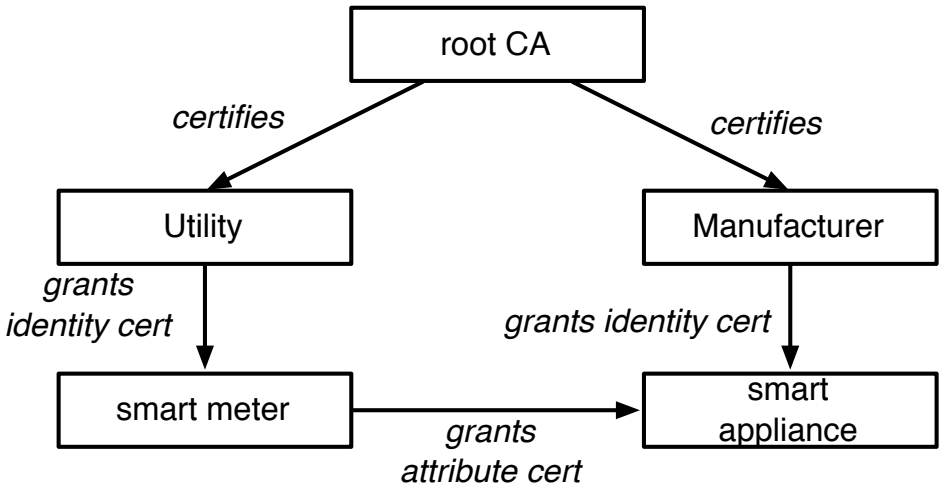
- public parta random nonce and a set of additional data elements called caveats.
- private partthe HMAC value generated with a symmetric key on the public part.

Overview

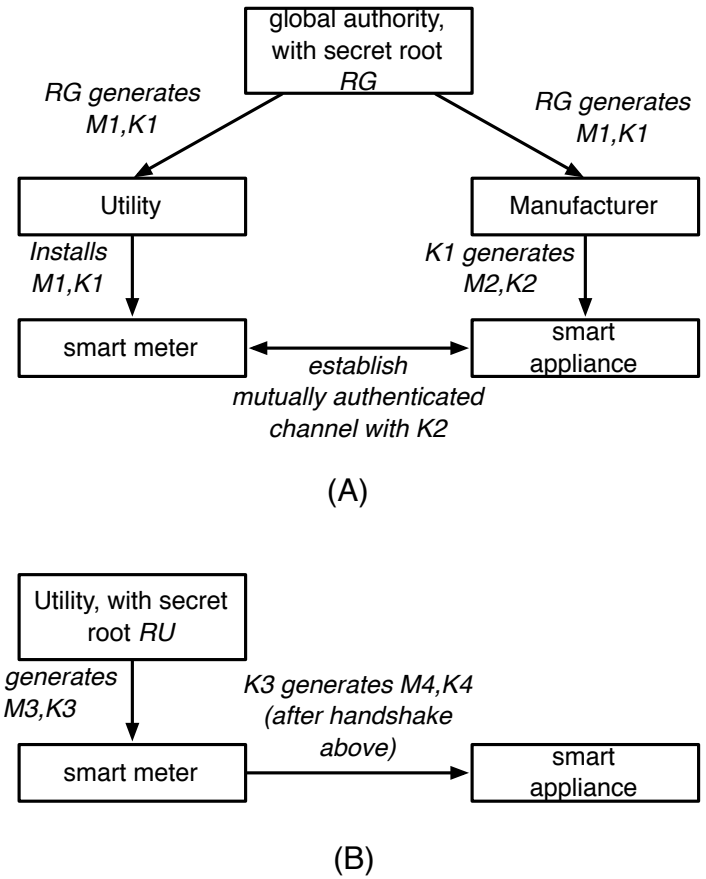
- Each entity would need two kinds of identity.
  - Core identity — This would tell us that an appliance is of a particular type.
  - Association attribute — This would tell us who or what an appliance is associated with.

PKI-based Approach

- A trust root certifies a CA at a utility and a manufacturer.
- Utilities issue certificates to the meters, and manufacturers to the appliances.
- Smart meters issue attribute certificates to co-located appliances.
- An appliance shows up in a house, presents a certificate and proves its knowledge of the private key.
- The smart meter checks the validity, and grants an attribute certificate to associate it with the meter.



Macaroons-based Approach

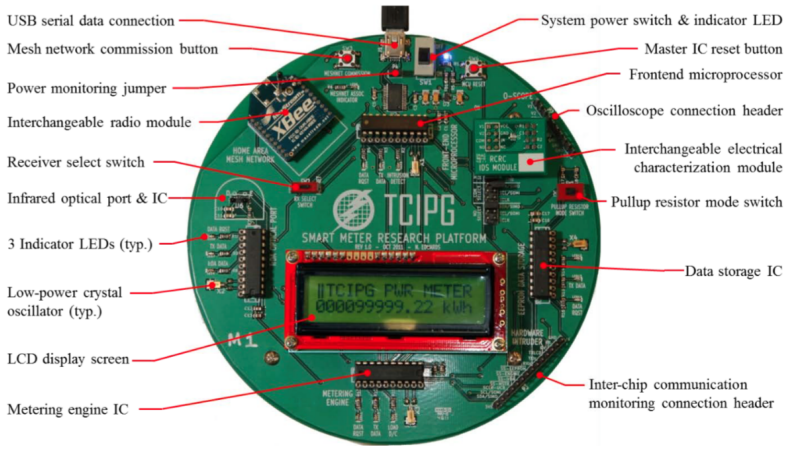


- A trust root issues an *introduction macaroon* to both the utility and the manufacturer.
- Utilities and manufacturers issue macaroons to the smart meters and appliances respectively.
- Smart meters issue short lived macaroons to the appliances in the same house.

Experiments

We performed our experiments on –

- Smart Meter Research Platform – TI MSP430 with Zigbee RF chip.
- Raspberry Pi 2 – 900 MHz 32-bit quad-core, 1GB RAM (shared with GPU).
- GNU/Linux Server with a 3 GHz Intel Xeon CPU running at 1GB of RAM.



PKI-based Approach

Table: Varying RSA modulus length, Elliptic Curve Ed25519 key size and DSA key size for PKI Attribute Certificates on the Server – 3GHz with 1GB RAM.

Protocol	Key length	*createAttrCert*	*verifyAttrCert*
RSA	1024 bits	40.26 ms	0.10 ms
RSA	2048 bits	253.61 ms	0.40 ms
RSA	4096 bits	1635.65 ms	1.43 ms
DSA	512 bits	19 ms	100 μs
DSA	1024 bits	82 ms	310 μs
Ed25519	256 bits	197 μs	226 μs

PKI-based Approach

Table: Varying RSA modulus length, Elliptic Curve Ed25519 key size and DSA key size for PKI Attribute Certificates on the Raspberry Pi 2.

Protocol	Key length	*createAttrCert*	*verifyAttrCert*
RSA	1024 bits	4.85 s	1.91 ms
RSA	2048 bits	24.06 s	8.33 ms
RSA	4096 bits	189.07 s	30.91 ms
DSA	512 bits	1.01 s	7.86 ms
DSA	1024 bits	1.34 s	10.36 ms
Ed25519	256 bits	25.79 ms	29.34 ms

Macaroons-based Approach

Table: Varying cryptographic hash functions for an implementation of Macaroons on the Server – 3GHz with 1GB RAM.

Hash Algorithm	*createMacaroon*	*verifyMacaroon*
MD5	98 μs	79 μs
SHA-1	100 μs	80 μs
SHA-256	110 μs	85 μs

Macaroons-based Approach

Table: Varying cryptographic hash functions for an implementation of Macaroons on Raspberry Pi 2 and Smart Meter Research Platform.

Hash Algorithm	*createMacaroon*	*verifyMacaroon*
Raspberry Pi		
MD5	650 μs	473 μs
SHA-1	662 μs	513 μs
SHA-256	761 μs	566 μs
TCIPG research platform		
SHA-1	900 μs	780 μs
SHA-256	1.2 ms	870 μs

Section 6

Conclusion

Conclusion

- We explored identity issues in the smart grid.
- We proposed two possible schemes for this problem.
- We noted that a macaroons based scheme is expected to scale more reliably for the number of data points in the envisioned smart grid, by putting decentralisation and symmetric key ciphers into practice.

Next Steps

Much of our future work includes exploring the following.

- For what population sizes and revocation patterns would X.509 stop working?
- Would Macaroons still suffice in such situations?
- How would resource-constrained devices fair with respect to generating strong keys in terms of entropy?

Thanks!

pa@cs.dartmouth.edu
http://cs.dartmouth.edu/∼pa

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.