CREDC

Fast and Scalable Authentication in Energy Delivery Systems

Scalable Identity in the Smart Grid

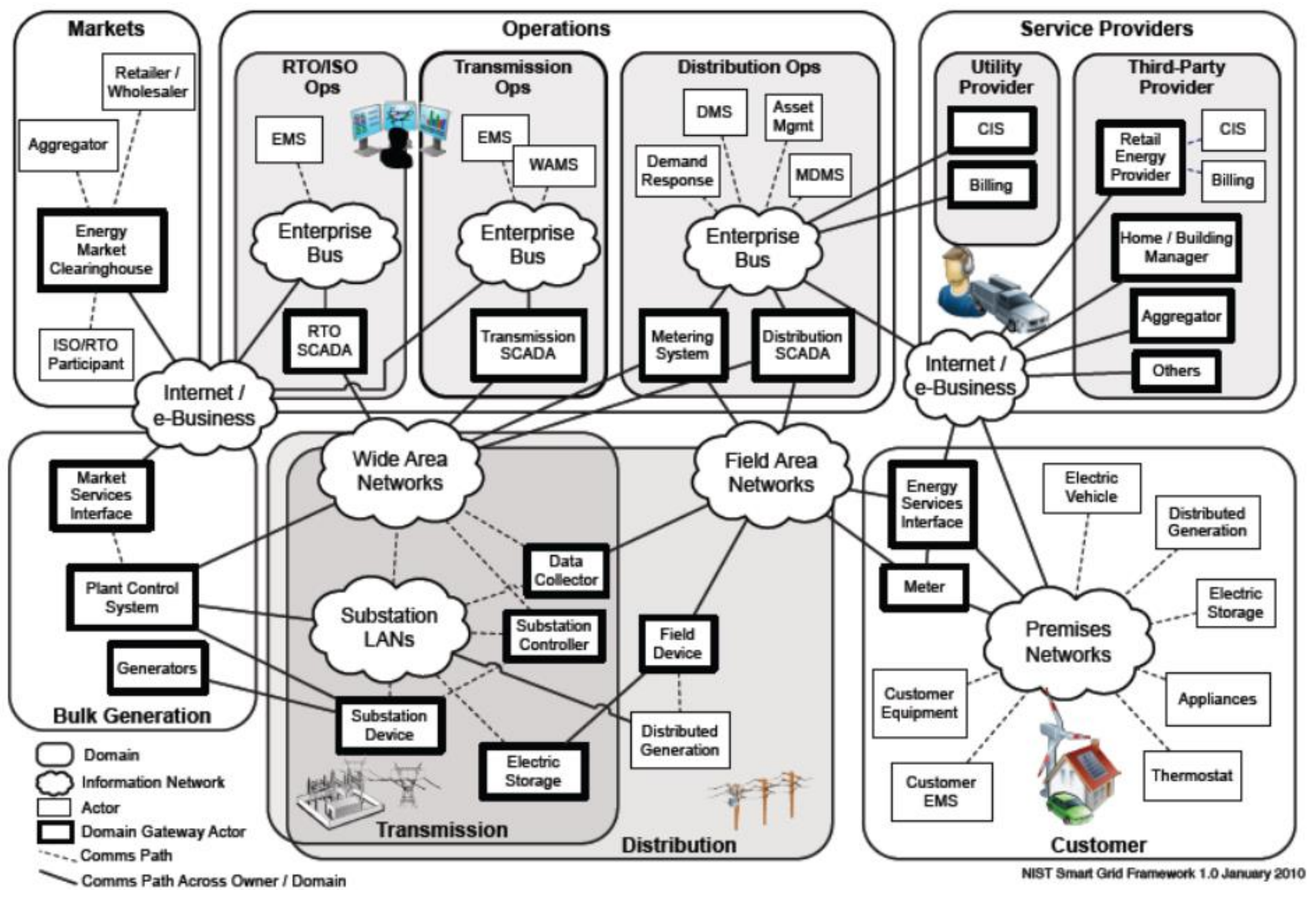
Prashant Anantharaman, David Nicol, Kartik Palani, Elizabeth Reed and Sean W. Smith

GOALS

With the power grid and other EDS becoming increasingly smart, we are seeing these systems being augmented with massive numbers of computational devices which will communicate with each other. These communications will be important to overall system security and reliability. Consequently, it is important to consider the security of these communications: e.g., authentication of senders and receivers; integrity of messages; and (where appropriate) confidentiality of messages.

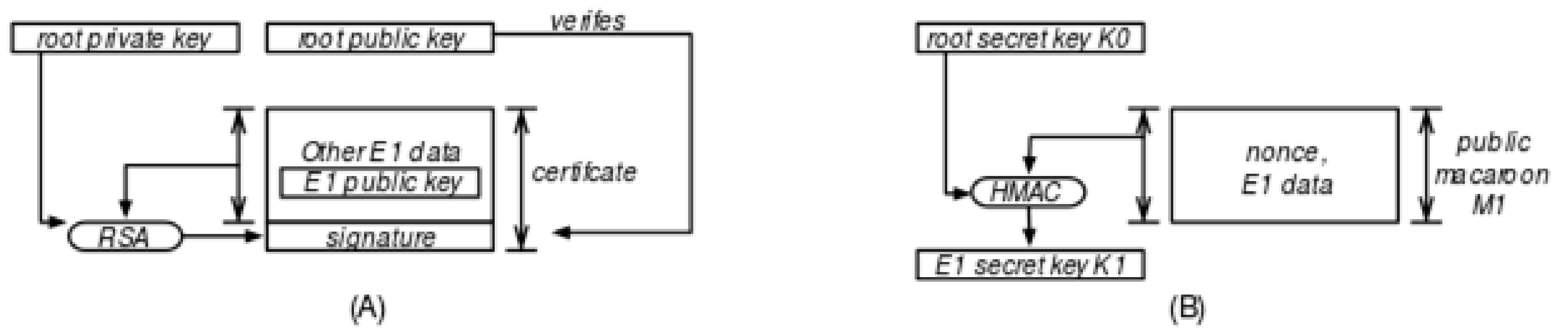
FUNDAMENTAL QUESTIONS/CHALLENGES

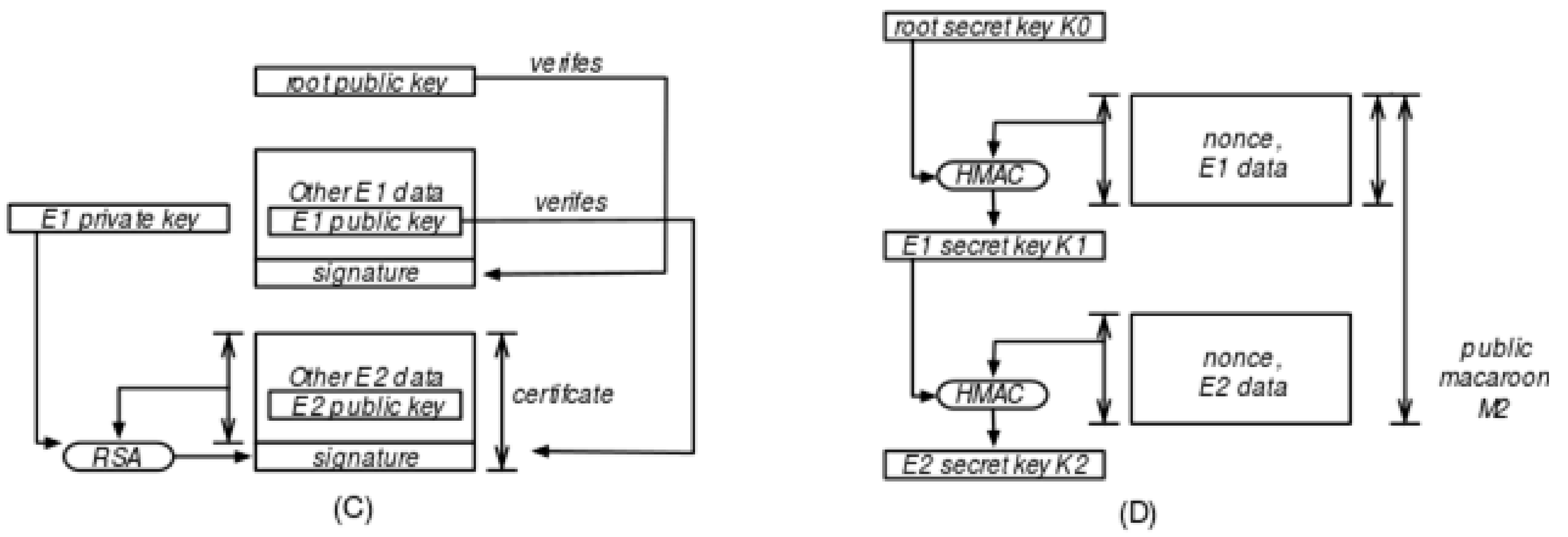
- How to assign **meaningful global identities** to a massive population of end-devices in the Smart Grid?
- How do we **revoke** these assertions?
- How do we test the **scalability** of a particular communication to a population representative of the Smart Grid?
- PKI is a natural solution but previous PKI deployments (all deployed on a much smaller scale than the envisioned smart grid PKI) have revealed several practical challenges/costs, including ***path discovery*** and ***revocation***.
- Consumer-side smart grid entities are **non-static**, and their assertions can change often. Electric vehicles keep moving, and need to be authenticated by a charging station for billing. Ownership of home appliances can change often. How do we keep track of these changes?
- What could go wrong even in the consumer side of the smart grid?
  - –What happens if the appliances all receive forged messages announcing near-zero electricity prices?
  - –or if 50% of the EV charging stations appear to simultaneously tell the grid they are about to start charging?
- What about other grid and EDS domains?



RESEARCH PLAN

- There are two types of identities tied to each end-device. One is the **core identity**, which is long term, and could be assigned by the manufacturer of an appliance or an end device.
- The other identity would be the **association attribute.** This tells us who or what a device is associated with. This is a short term assertion and can change frequently.
- *PKI with attribute certificates* -- In the case of a smart home, the smart meter could act as a gateway. The smart appliance would have a core identity from the manufacturer, and receive an association attribute from the smart meter.
- *Macaroons* -- Macaroons could be used in a way similar to the PKI scheme with attribute certificates. In the figure below, we show how PKI certificates and macaroons are analogous to each other. Both PKI and Macaroons make use of a root key, the PKI one being a private key and the macaroon one being a secret key for construction of an initial HMAC.





INITIAL REPORTS

- S. W. Smith, "Cryptographic scalability challenges in the smart grid." *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*. IEEE, 2012. http://www.cs.dartmouth.edu/~sws/pubs/gridpki.pdf
- P. Anantharaman, K. Palani, D. Nicol, and S. Smith, "I am Joe's Fridge: Scalable Identity in the Internet of Things," in *IEEE International Conference on Internet of Things*, Chengdu, China, December 2016. http://www.cs.dartmouth.edu/~sws/pubs/apns16.pdf

RESEARCH RESULTS

- We provide results of our experiments with a Raspberry Pi 2 to generate *attribute certificates* and *macaroons*.
- We note that macaroons take comparatively lesser time to generate and verify.

Protocol	Key Length	create AttrCert	verify AttrCert
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
Ed25519	256 bits	25.79 ms	29.34 ms

Hash Algorithm	*create Macaroon*	*verify Macaroon*
Raspberry Pi 2		
MD5	650 μs	473 μs
SHA-1	662 μs	513 μs
SHA-256	761 μs	566 μs
TCIPG Research Platform		
SHA-1	900 μ s	780 μs
SHA-256	1.2 ms	870 μs

BROADER IMPACT

- Our study of scalability can later be extended to any cryptographic scheme for the Smart Grid, and may be applied to understand the cost in terms of revocation of certificates and keys and delays due to verification of certificates.
- In constrained devices with very little memory, symmetric encryption has proven to be much faster in comparison to asymmetric encryption, and we provide a scheme demonstrating the use of hashes and symmetric encryption.

INTERACTION WITH OTHER PROJECTS

- Builds on previous PKI simulation work by Nicol (Illinois), Meiyuan Zhao (now at Intel), and Smith (Dartmouth).
- This work also builds on previous TCIP/TCIPG work on "Low Latency Authentication for Legacy Scada" by Patrick Tsang and Smith (Dartmouth), "Attribute-Based Usefully Secure Email for blackout recovery coordination" by Christopher Masone and Smith and on Smith's work with Zhao and Marchesini on "PKI semantics and scalability".
- The smart meter research platform was developed as a part of the hardware intrusion detection project by Nathan Edwards (Illinois).

FUTURE EFFORTS

- Explore the application of these schemes for practical protocols like **MQTT (**which is presently being widely deployed in ICS with poor security).
- Explore SSP21
- Define formal requirements for the namespace problem, and satisfy the requirements with the two proposed schemes.
- Investigate network topologies and the number of messages being passed in the proposed schemes.
- Perform a queuing theory based evaluation, taking into consideration that legacy serial lines make time costs higher.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY