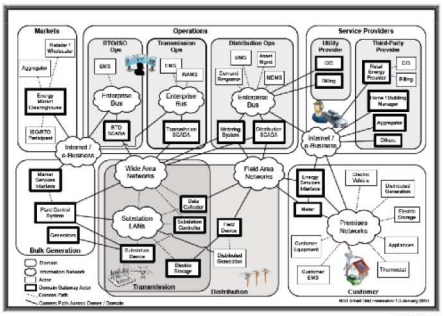
TCIPG Cryptographic Scalability for the Smart Grid

Tucker L. Ward, David A. Rice, Sean W. Smith

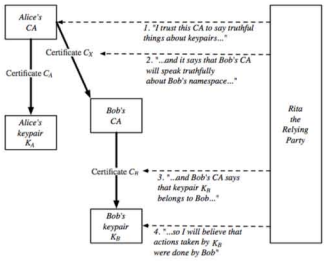
Smart Grid



- Spread over a big area with a large number of heterogeneous devices.

How Will Devices Authenticate?

- Communications between devices need to be authenticated.
- The community consensus seems to be PKI.



- PKI is expensive.
- Costs include bandwidth and latency.

Going Where No PKI Has Gone Before

Transmission Side	• Real-time is critical. • Didn't work on BGP with only 30k nodes. • Transmission side may have 1 million nodes in the US alone.
Consumer Side	• Revocation will be necessary. • But this didn't work with SSL servers, with 1 million correctly certified nodes worldwide. • There may be 1 billion consumer side nodes in the US. • And there may need to be attribute certification at the scale of the smart grid, which has never been done before.

DoD and Johnson & Johnson both had large (100,00 entities) PKI implementations; both had problems with large CRLs.

Anticipated Problems in the Smart Grid

- The electric grid is *context-dependent*. Certificates are not issued to a person, but rather to a device owned by a person in a specific facility.
- Certificate revocation lists (CRLs) may become prohibitively large.
- Bandwidth restrictions in rural areas may prevent effective communication; for example, transmission of CRLs may be impractical.
- Devices on the transmission side should be "plug and play," but on the consumer side there has to be some notion of ownership (what if I sell my fridge to a friend?).
- Devices tend to have low processing power and memory.

Research Plan

- Builds on work by Nicol, Smith, and Zhao.
- Scalable Simulation Framework (SSF): A set of tools that can simulate a generic network of entities, and their communications.
- SSFNet: A library built in SSF that provides ready-to-use internet protocols (such as IP, TCP, UDP). The communications in the smart grid will most likely resemble the kinds of traffic seen with these protocols.
- PRIME: An improvement to SSF, bringing greater parallel and distributed computing tools.
- With the above tools, we will define entities that exist in the power grid (generators, buses, meters, PMUs, etc.) and model their communication.
- Then we will build a library of authentication tools. These will simulate the typical behavior of PKI. We will start with X.509 as a baseline, and then experiment with variations of PKI.

Research Questions

- To start, we'll work with a smaller network size (resembling NH).
- We'll vary the kind of CA hierarchy used (one true root, tree, cross certified, bridge).
- We will also vary how revocation works (distribution of full CRLs, delta CRLs, or implementation of an Online Certificate Status Protocol).
- For all of these experiments, we are trying to get at the ***time*** it takes to validate devices and ***minimum required bandwidths.***
- We're looking for envisioned smart grid topologies!