This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2021-10424C

Sandia National Laboratories

Exceptional service in the national interest

Cybersecurity and Public Key Infrastructure for DER: Addressing a Global Challenge in the Australian Market

Jay Johnson, Sandia National Laboratories

Australia Workshop for Distributed Energy Resource Networks

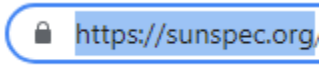
August 31, 2021

SAND2021-XXXX

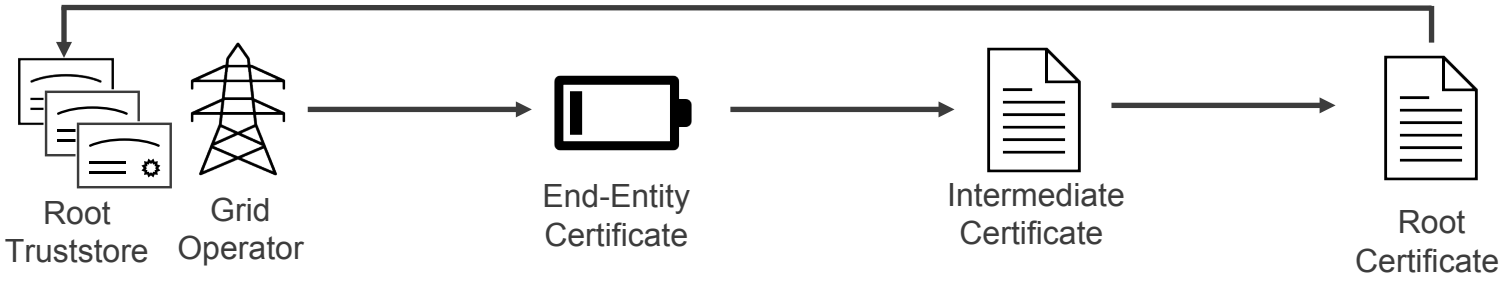
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Public Key Infrastructure for DER

- PKI is designed for *identify management* in a *many-to-many trust environment*
  - Asymmetric cryptography provides confidentiality, but how can we trust it's who we think it is?
  - PKI links an *entity* with a *key* and verifies that relationship with the *certificate* from an *authority*
  - Chains of trust are constructed by linking certificates—underpinned by a root CA.
  - Browsers come with dozens of trusted root CA certificates: 

- Challenges for the DER environment
  - Grid operator must communicate with (and trust) products from many manufacturers
  - Scalability/cost issues with many utilities/grid operators/aggregator
    - How many root CAs will be created for a given country/jurisdiction?
    - Nearly impossible for DER vendors to provision private keys at the time of manufacturer if there are multiple root CAs *unless* they know the PKI ecosystem where the product will be deployed

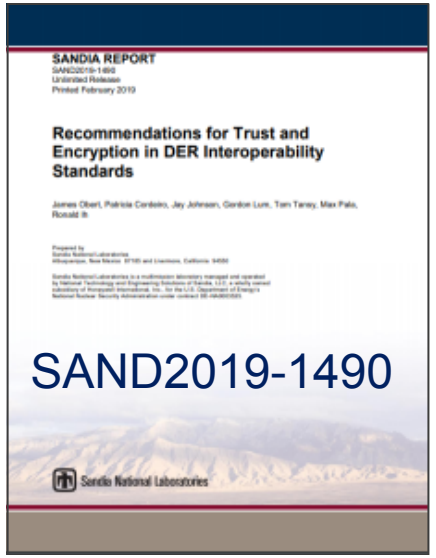


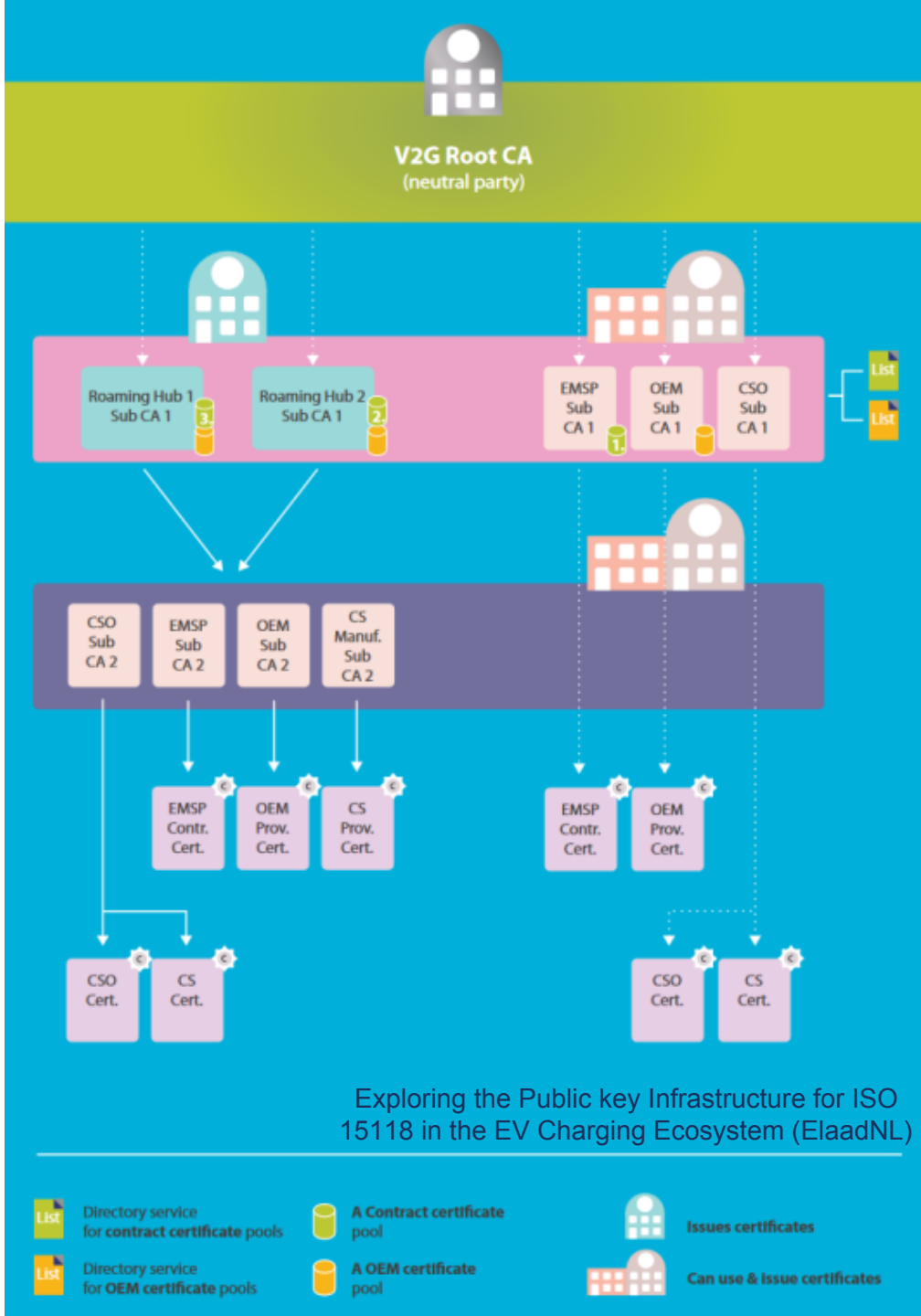
PKI Implementation Options

- Option 1: Create a **single** well-secured, offline, domestic root CA for IEEE 2030.5 communications in Australia
  - DER vendors and grid operators will operate intermediate CAs to provision clients and server certificates
  - Cost-effective and practical; all certificates are linked to neutral root CA
  - Aggregators/grid operators can manage whitelisted and blacklisted certificates/DERs locally
  - Manufacturers can provision certificate for Australian PKI during the manufacturing process
- Option 2: Create **multiple** well-secured, offline, domestic root CAs for IEEE 2030.5 communications in Australia
  - Grid operators have more leeway to control the environment and incorporate special cybersecurity features (e.g., certificate revocation, etc.)
  - Manufacturers can provision certificate during field commissioning when configured for interconnection (or potentially before if the root CA is known ahead of time)
    - DER may generate unique key-pair in field and send certificate signing request to appropriate CA (possibly via DER cloud system)
    - This capability is likely required for any DER company operating internationally since there will be multiple root CAs across the globe
- Option 3: Yet another approach!

IoT and Power System PKI Best Practices

- EV plug-and-charge PKI ecosystems in ISO 15118-2:2014 *Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Network and application protocol requirements* defines a PKI Infrastructure for electric vehicle ecosystem.
- PKI Key Lifecycle in IEC 62351-9 *Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment*
- Sandia Technical Reports
  - Recommendations for Trust and Encryption in DER Interoperability Standards
  - Recommendations for Data-in-Transit Requirements for Securing DER Communications





Questions?

Jay Johnson
Renewable and Distributed Systems Integration
Sandia National Laboratories
P.O. Box 5800 MS1033
Albuquerque, NM 87185-1033
Phone: 505-284-9586
jjohns2@sandia.gov