

Smart Grid Security

Selected Principles and Components

Tony Metke

Distinguished Member of the Technical Staff

IEEE PES Conference on
Innovative Smart Grid Technologies

Jan 2010

Based on a paper by:

Anthony R. Metke and Randy L. Ekl

Motorola, Inc., Schaumburg, IL USA

Tony.Metke@Motorola.com, Randy.Ekl@Motorola.com

Not Covered

- Encryption Algorithms / Key Lengths
- VNPs, Tunnels, IPSec, TLS, etc.
- Firewalls
- Secure Software Practices
- Virus and Malware Detection
- Intrusion Detection
- SNMP Security Issues
- SCADA Protocol Security
- Misconfiguration Issues
- Threat Analysis & Risk Management
- ...

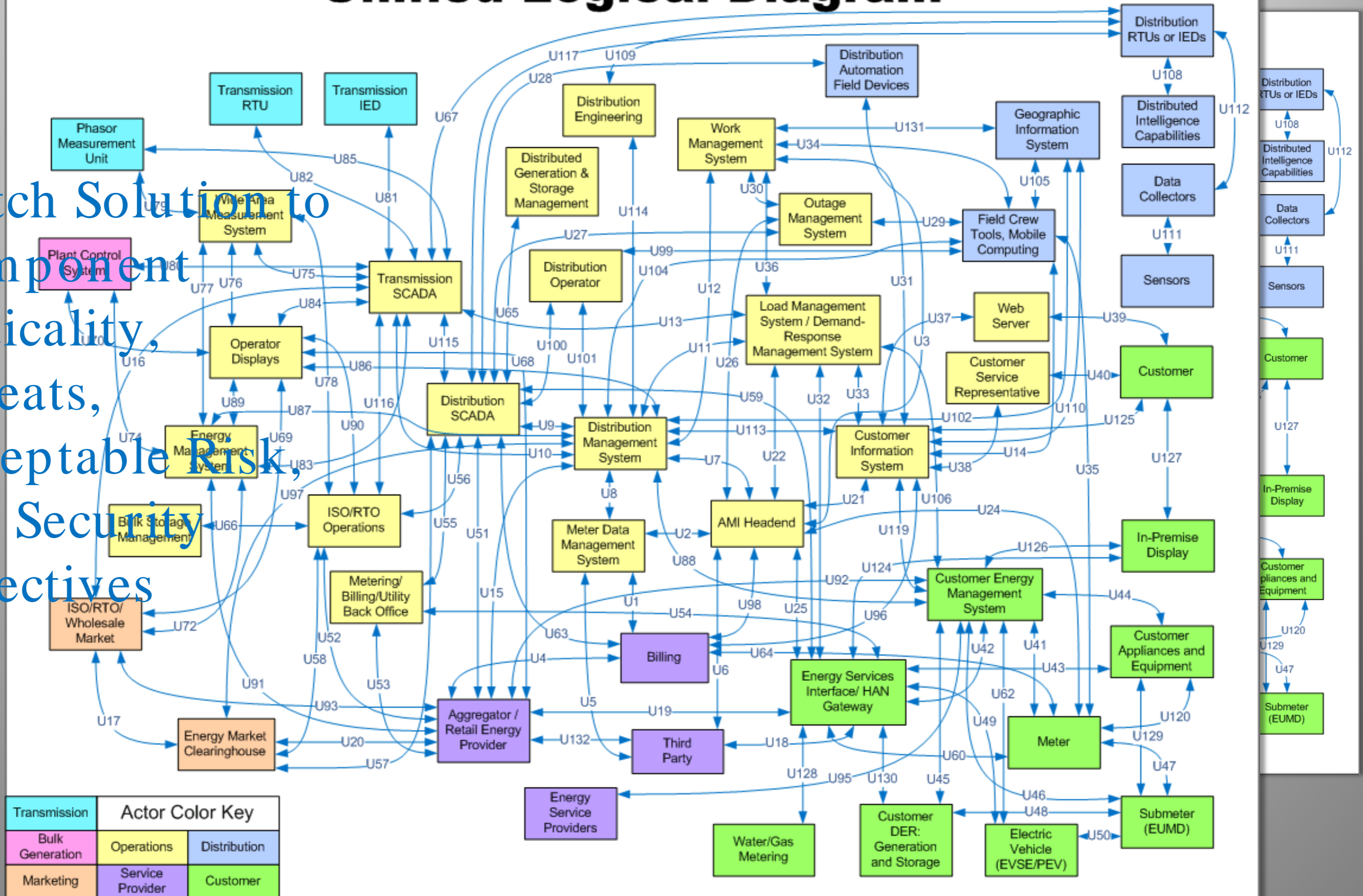
Topics Covered

- Scope
- Issues
 - Key Management
 - Trust Management
 - Authentication & Authorization
 - Device Attestation
 - High Availability
- A Holistic Solution

Scope

Unified Logical Diagram

Match Solution to Component Criticality, Threats, Acceptable Risk, and Security Objectives



Key Management

- **Common Symmetric Key /Shared Secret Use Cases**
 - Tunnels
 - IPSec/ IKE
 - Routing Security
 - OSPF & EIGRP message authentication
 - Management
 - SNMP

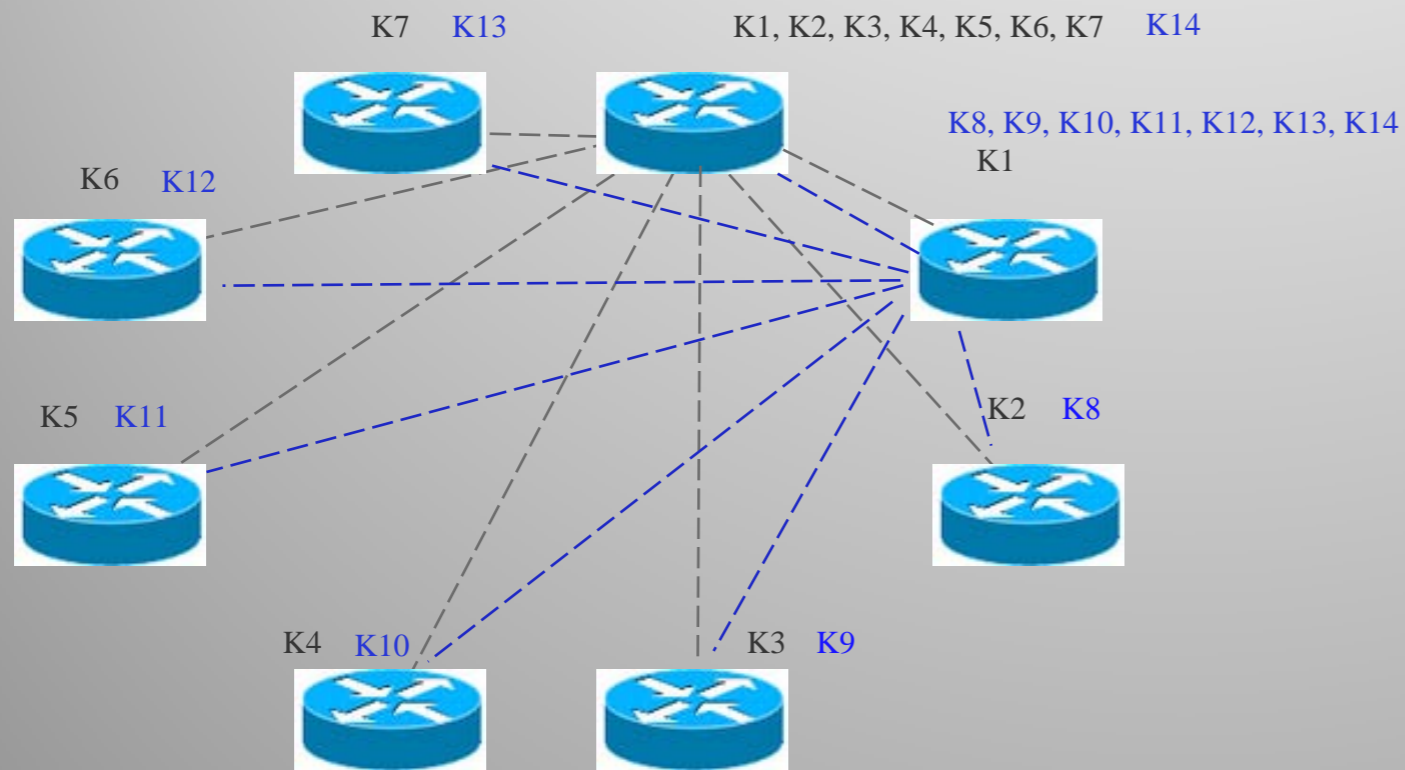
Key Management

- Key Management Issues
 - Scalability Issues
 - Coordination Problems
 - Inter-Organizational Complexities
 - Privacy/ Security Issues
 - High OPEX

Symmetric Key Management
Can be complex and expensive.

Key Management

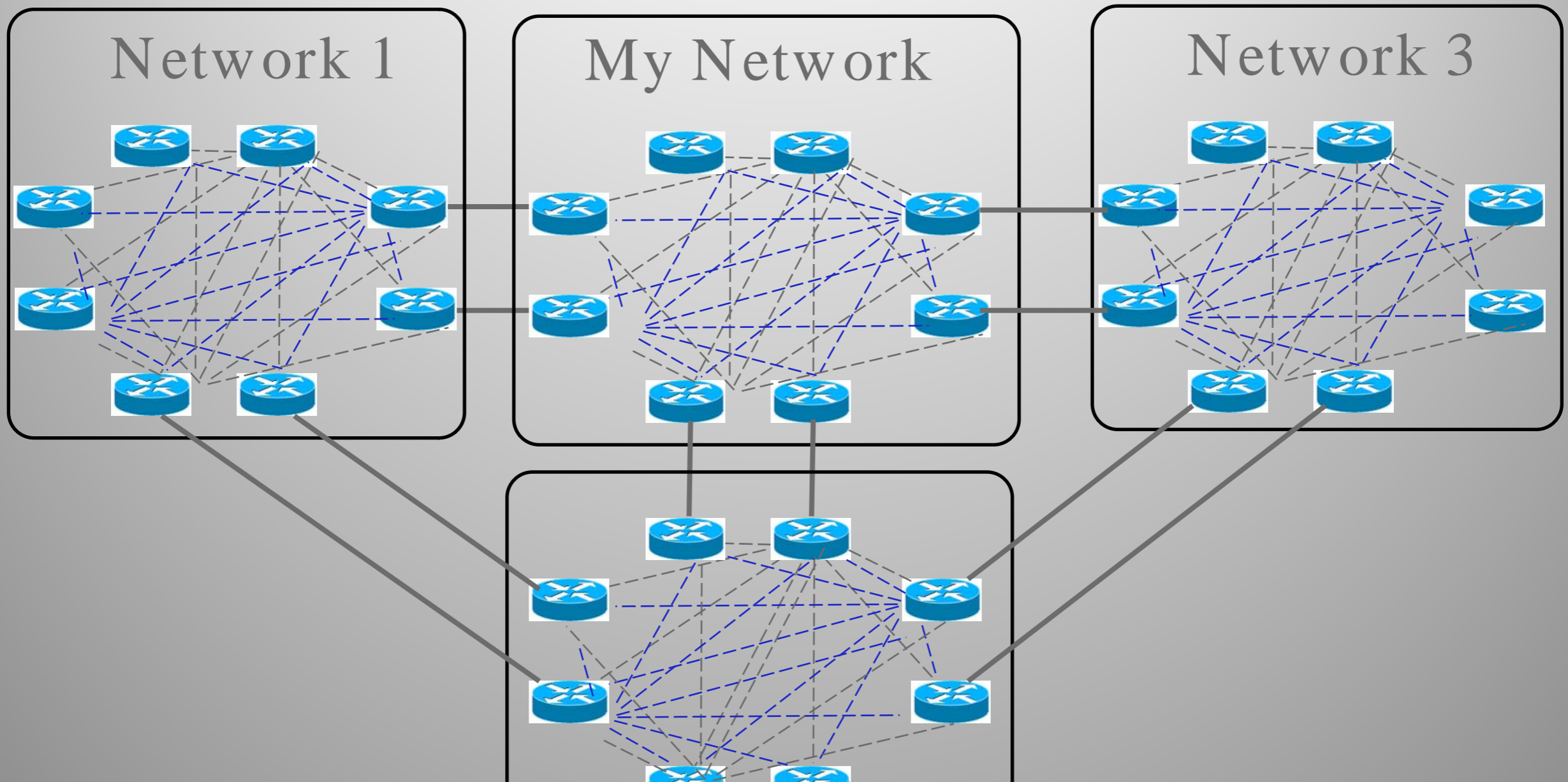
Device Provisioned Keys



- Several Key Management Strategies exist.
- KDC's can be used, but limit availability
- Secure Solutions with high availability present an N^2 provisioning problem

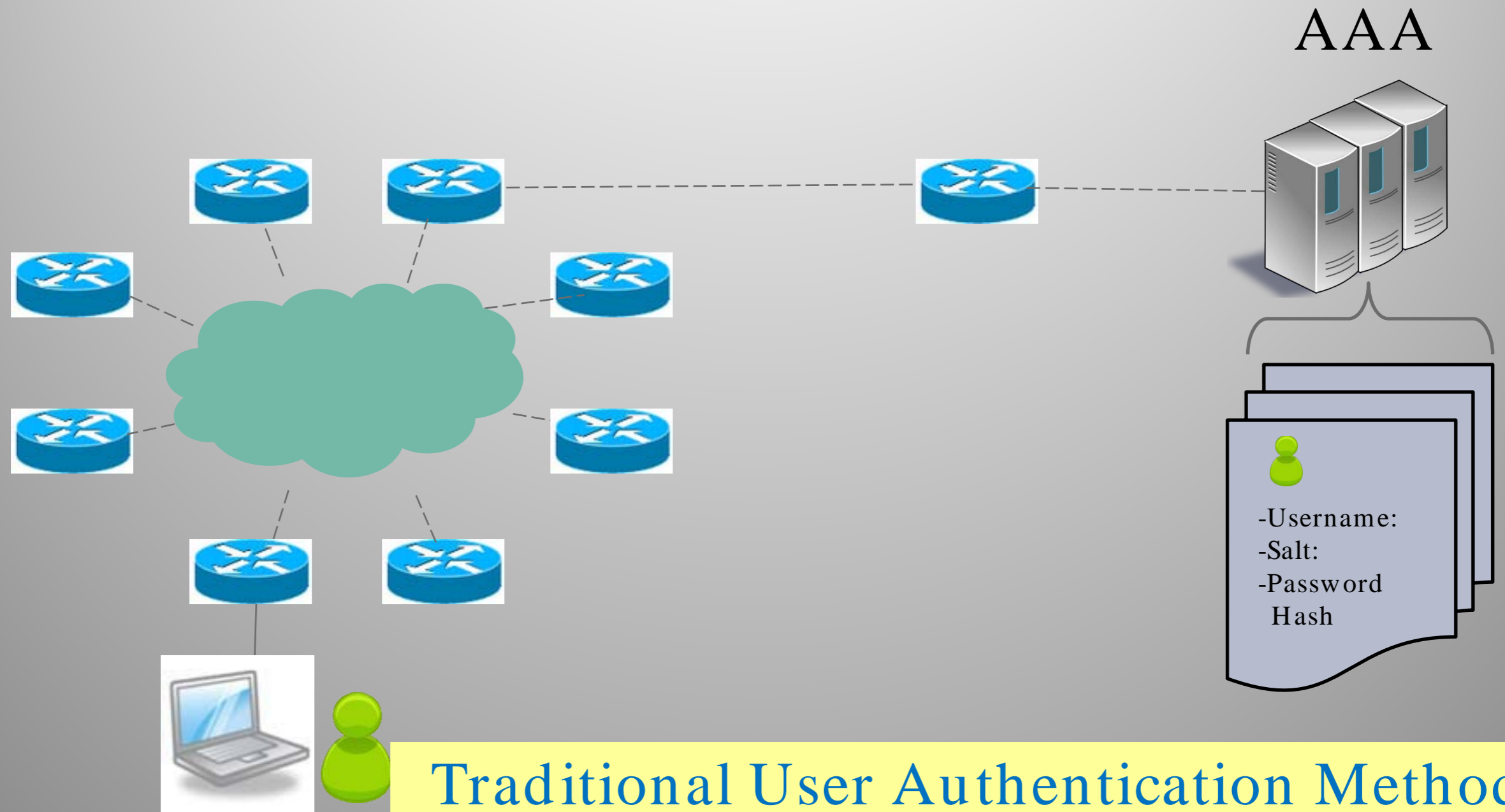
Provisioning Symmetric Keys can be Complex & Expensive.

Key Management Issues



Key Management becomes much more complicated when
Multiple orgs need to interoperate.

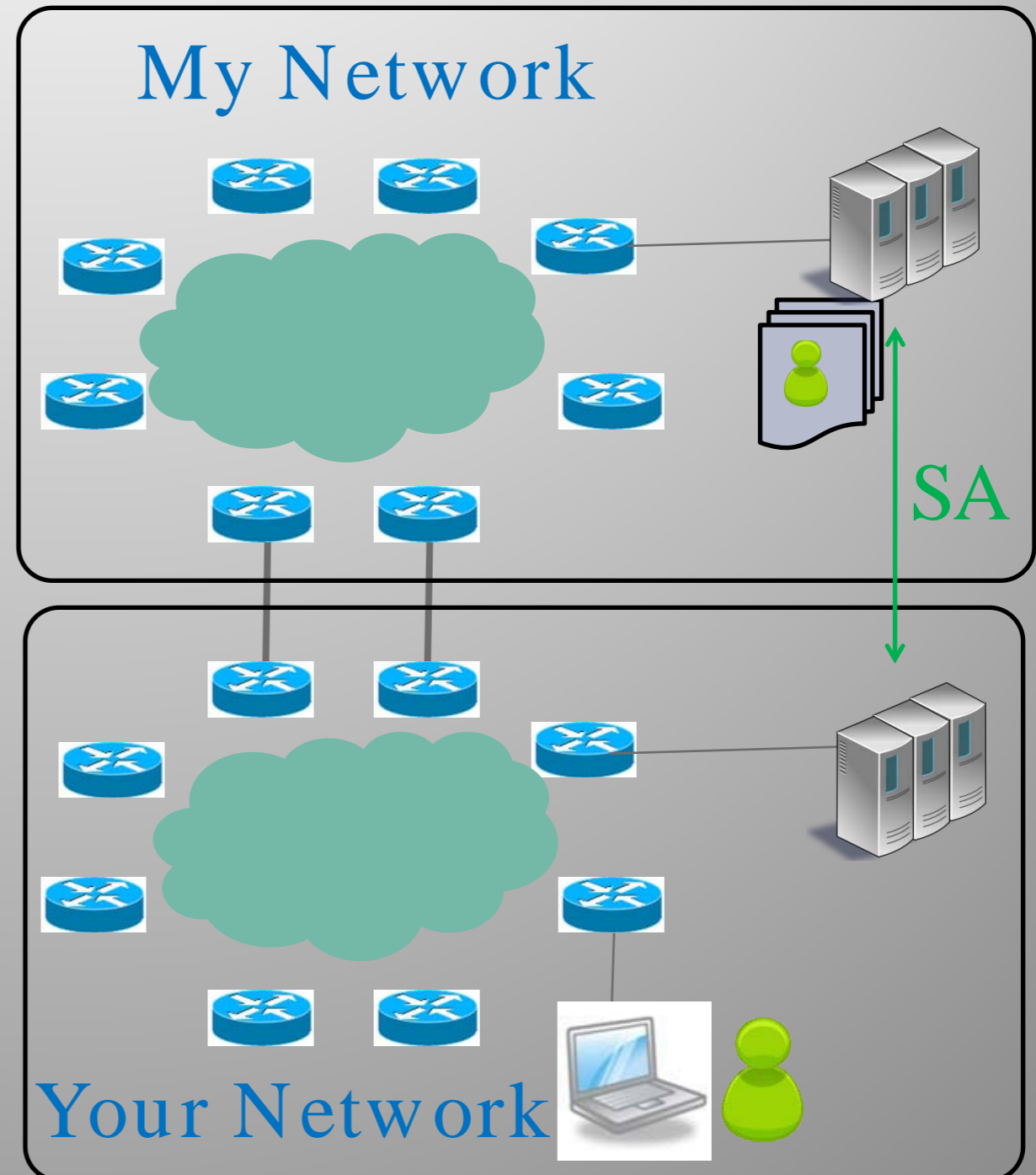
User Authentication



Traditional User Authentication Methods Rely on Central Authorization Database

Trust Management

- When accessing a remote system, user credentials can be referred to in the users local domain, if the domains AAAs have a security association.
- This requires an priori agreement across domains
- This requires network conductivity between systems



High Availability Trust Management

The grid is not an enterprise.

Smart Grid requires special High Availability Solutions.

Typical enterprises may have 10, 20 or even 50 HA campuses, and hundreds of other locations. For example, Google has 12 server farms, 20 US offices and 51 international offices.

The entire grid has approximately 10 thousand transmission substations, and is estimated to have 50 to 70 thousand distribution substations.

We cannot depend on traditional Enterprise Solutions.

This is a different market, with different requirements.

Authentication and Authorization

What are we Authenticating?

- Device Type, Model, and Serial Number
- Ownership
- Assigned Location, Groups or Peers
- Role
- Operational Integrity of Platform



Device Attestation

Device Attestation Definition:

Proving to a remote party that the integrity of your system has not been compromised.

- Trusted Platform Module
- Secure Software Update
- Root of Trust
- Certificate Based Authentication

Issues Summary

- Symmetric key management is not a good solution, because it can be complex and expensive.
- Symmetric key management offers poor interoperability solutions.
- Traditional user authentication methods which rely on central databases will not provide the high availability solutions needed for smart grid.
- Smart Grid Requires Special High Availability Solutions

Solution Space

- A solution is needed which enables authorized remote entities, who have never been configured with credentials from my system, to access my system when I need them.
- This solution must work when the network is down and even when the grid is down
 - No Access to back end AAA, Identity Provider or KDC.
 - This eliminates Radius, SAML, and Kerberos
- PKI/ PMI meet the requirement of Smart Grid

A Holistic Solution (1)

- The SG Industry establishes a PKI Standard Model Policy
 - Define Standard Requirements for issuing, renewing and revoking SG certificates
 - Requirements on all PKI entities
 - Define Certificate Policies for all **Device Types**, all **Roles** and for all **Assurance Levels**.
(Include vetting rules for all certificate types)

A Holistic Solution (2)

- Define Cross-signing and Interoperability Standards
 - Define Standard Constraints and Policy Mapping guidelines for Cross Signing
- Define Bridging Standards and Guidelines.
- Establish Accreditation Criteria for SG PKI Providers.
- Establish Governing Body to oversee Accreditation.

A Holistic Solution (3)

- Critical Components should support Remote Device Attestation
 - This could require new hardware requirements such as support FIPS 140 Level 3 Hardware
- Relying Parties should have secure TA and Local Policy Storage
- “New” technologies such as OCSP Stapling should be supported.

Next Steps

- We need to continue identifying critical components and interfaces, evaluating threats and risk associated with these components, establishing security requirements on these components, and developing an appropriate security architecture.

- We need a real trust management strategy.
- We may likely need to develop a set of SG certificate policy standards and best practices. (this is no small task)

Extra Slides

Background

Digital Certificate



Issuer (Name)
Subject (Name)
Public Key
Certificate Policy ID
...

Certificates are used as a credential for security related purposes.

Certificates show that a specified Public Key (PK) belongs to a stated Subject, and that the PK can be used as per the specified Certificate Policy (CP).

Background

Digital Certificate

Issuer (Name)
Subject (Name)
Public Key
Certificate Policy ID
...

Certificates can enable efficient secure organizational interoperability.

But only if the fields in the certs are well defined.

Background

Digital Certificate

Issuer (Name)
Subject (Name)
Public Key
Certificate Policy ID
...

X.509 & RFC 5280 define the formats for these fields.

However these standards do not provide Naming Conventions or Certificate Policy definitions.

Background

Certificate Policy

The CP ID in a certificate identifies a Certificate Policy described in a CP document.

Certificate Policy Documents define the conditions under which the certificate was issued.

The CP can be used by an Relying Party to determine the applicability of the certificate to a given application.

Certificate Policies can be very complex.

PKI Issues, X.509 is not Specific Enough.

- Inconsistent Use of the Subject Field
 - Standards present inconsistent rules for using the CN, OU, or SubjectALTNName fields
 - Even if consistent rules existed, local naming conventions are not consistent.

The following two DNs are not compatible.

DN1: O=NYPD, OU=root ca, ST=New York, C=USA

DN2: O=NYPD, OU=root ca, ST=NEW YORK, C=US

- Inconsistent Certificate Policy Extensions

You Say

SWAT

Incident Commander

Unified Command

I Say

Emergency Response Team

Chief of Emergency Operations

Emergency Operations Center

X.509 is not Specific Enough.

- Inconsistent PKI Practices
 - Certificate Enrollment / Vetting
 - CA and Public Key Protection
 - Certificate Verification Procedures
 - Auditing Procedures
 - Cross-signing Requirements
 - ...
- Inconsistent Generation of Key Identifiers
 - Subject Key Identifier & Authority Key Identifier fields are used to ensure correct chain construction.
 - Different CA implementations use different methods to calculate these values.
- Inconsistent Use of Extension Criticality
 - 9 of 16 Standard Extensions do not specify criticality
 - If criticality is not agreed on between domains, cert chain validation may fail.

X.509 Certificate Format

◦ *Certificate ::= SEQUENCE {*

<i>tbsCertificate</i>	<i>This is the certificate Body. See Next Slide</i>
<i>signatureAlgorithm</i>	<i>This field identifies the cryptographic identifier used by the CA to sign this certificate</i>
<i>signatureValue</i>	<i>This field contains the digital signature of the ASN1, DER encoded tbsCertificate</i>

◦ TBSCertificate

version	<i>For Version 3 Use Value 02</i>
serialNumber	<i>A unique positive integer assigned by the CA to each subject</i>
signature	<i>This field identifies the cryptographic algorithm used by the CA to sign this certificate. It is a duplicate of the signature field in the header.</i>
issuer (name)	<i>The issuer field identifies the CA which issued this certificate. This field must contain a non-empty distinguished name (DN).</i>
validity	<i>This field contains 2 dates between which the certificate is valid. {Not Before, Not After}</i>
subject (name)	<i>The subject name MAY be carried in the subject field and/or the subjectAltName extension. If the subject is a CA, then the subject field MUST be populated with a non-empty distinguished name <u>matching the contents of the issuer field in all certificates issued by the subject CA</u>. If subject naming information is present only in the subjectAltName extension then the subject name MUST be an empty sequence and the subjectAltName extension MUST be critical. Where it is non-empty, the subject field MUST contain an X.500 distinguished name (DN).</i>
subjectPublicKeyInfo	<i>This field contains the Public Key and the associated algorithm identifier (e.g. RSA, DSA, DH)</i>
issuerUniqueID	<i>As per RFC 2380 these fields are intended for future use to handle the reuse of subject and issuer names over time.</i>
subjectUniqueID	
extensions	<i>EXPLICIT Extensions</i>

Optional

4.2.1 Standard Extensions

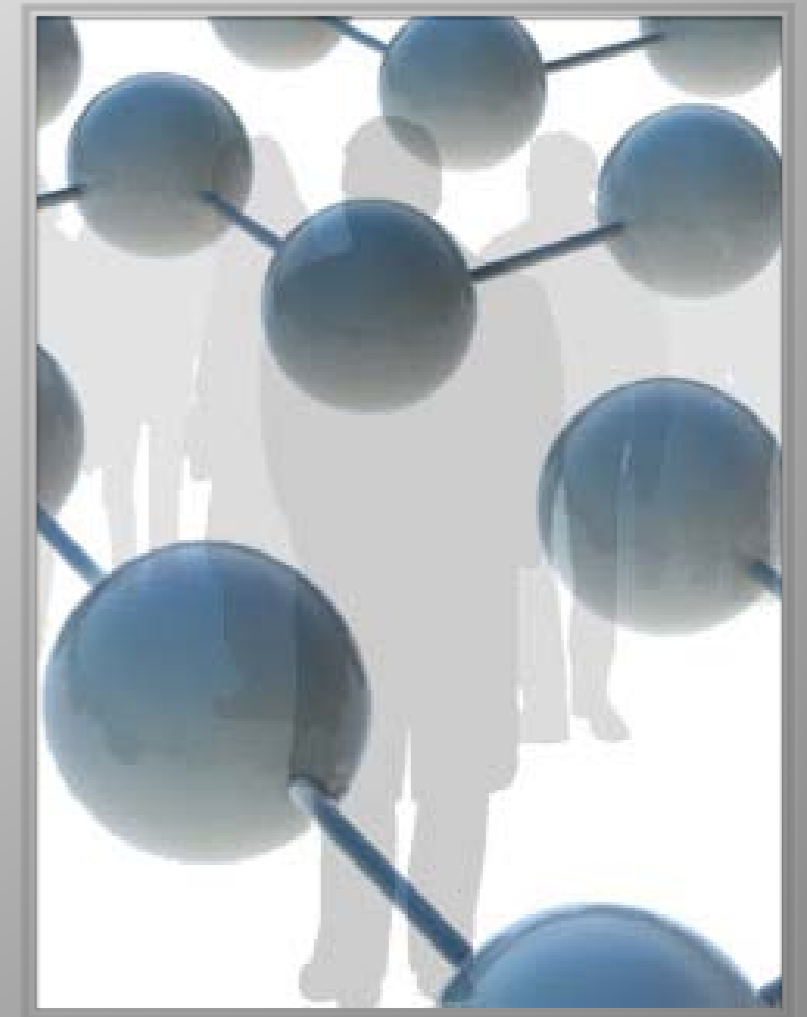
4.2.1.1	Authority Key Identifier	M non-critical
4.2.1.2	Subject Key Identifier	M non-critical
4.2.1.3	Key Usage	S critical
4.2.1.4	Private Key Usage Period	open
4.2.1.5	Certificate Policies	open
4.2.1.6	Policy Mappings	M non-critical
4.2.1.7	Subject Alternative Name	open
4.2.1.8	Issuer Alternative Names	S non-critical
4.2.1.9	Subject Directory Attributes	M non-critical
4.2.1.10	Basic Constraints	open
4.2.1.11	Name Constraints	M critical
4.2.1.12	Policy Constraints	open
4.2.1.13	Extended Key Usage	open
4.2.1.14	CRL Distribution Points	S non-critical
4.2.1.15	Inhibit Any-Policy	M critical
4.2.1.15	Delta CRL Distribution Point	M non-critical

4.2.2 Private Internet Extensions

4.2.2.1	Authority Information Access	<p><i>The authority information access extension indicates how to access CA information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and CA policy data. (The location of CRLs is not specified in this extension; that information is provided by the cRLDistributionPoints extension.)</i></p>
4.2.2.2	Subject Information Access MUST be non-critical	<p><i>The subject information access extension indicates how to access information and services for the subject of the certificate in which the extension appears. When the subject is a CA, information and services may include certificate validation services and CA policy</i></p>

Proposals

- The Smart Grid Community standardizes a standard set of Smart Grid CPs.
- The Smart Grid Community established accreditation organizations for PKI service providers who would like to provide PKI service to the SG community.



Advantage of Certificate Standards

Advantages to Utilities

- Interoperability
- Simplifies Deployment
- Protects System Integrity
- Lowers Costs

Proposed Solution

- The Creation of a Smart Grid or Critical Infrastructure “Model Policy”

What’s a Model Policy?

Institutionalization of Common Processes and Standards Related to PKI Operation for SG Systems

What does it include?

- Standard set of Certificate Templates
- Standard Rules for Certificate use for SG Applications
- Standardize Rules for PKI Operation

Proposed Solution continued

- Smart Grid “Model Policy” Continued:
 - Detailed Definitions for Smart Grid Registered Certificate Policies
 - Rules for When to use Each Policy
 - Definitions and Rules for Proper use of Constraints
 - Standardized Explicit Certificate Syntax
(e.g., DN Naming Convention, Consistent Certificate Extension Usage)
 - Standard Rules for Setting Validation Periods and other Parameters