Implementation of Cybersecurity testbed and Overseas Export Strategy for Smart Grid

2015.12. 9

Seungwon Lee, PhD & PE

KEPCO-KDN
I. Introduction to Implementation of Cybersecurity testbed

II. Certification technology in Smart Grid

III. Public Key Infrastructure

IV. Overseas Export Strategy for Smart Grid
I. Introduction to Implementation of Cybersecurity testbed (1/2)

- **Project**: Installment and demonstration of Cybersecurity testbed in smart grid
- **Current status and motivation**
  - Researched Cybersecurity system (year 2010~2012) and Developed key cybersecurity (year 2011~2015) in smart grid
  - A lack of experience needs to testbed on site in order to launch the commercial services
  - Implementation of cybersecurity Technology for Construction New Market Creation and expansion market in smart grid
- **lead agency**: NSRI
- **Participation agencies**: 13 institutions (KEPCO, KSGI, KISA, KEPCO-KDN etc)
- **duration**
  - 1st year (2015) : May ~ Dec (8 months)
- **Total Project Cost**: ₩5.09 billion
I. Introduction to Implementation of Cybersecurity testbed (2/2)

Implementation details and Participation agencies’ role

**(Lead Agency) NSRI**
- Vulnerability Analysis & Implementation Cyber-security testbed
  (AMI, DR, ESS, Weakness Analysis)
- Weakness Analysis & Attack Scenario Implementation
- Plan for SG security vulnerability

**KEPRI**
- Vulnerability Analysis & Implementation Cyber-security testbed (EVCI)
- Vulnerability Analysis based binary code

**KEPCO KDN**
- Testbed of Cryptography and authentication (AMI, DR, ESS, EV, PKI)

**KSGI**
- Testbed of Cryptography and authentication (AMI, EV in Jeju)

**Participants**
- Meter & DCU testbed (DONGEUN Instruments, PSTech, Tide, CNPloen)
- DR testbed (i-on communications)
- Security Module testbed
  - (KCS, CIOT, NHRC, UBIZCORE)

**Policy Development**
- Development of Security guideline
- Construction and Operation of SG Security Demonstration site.

**KISA**
- Personal Information Protection Guideline
- Strategies of SG Security Standardization
Ⅱ. Certification technology in Smart Grid (1/7)

Objectives

- Construct Certification testbed room at Jeju interoperability test center
- Design and Build cybersecurity devices of PKI for AMI, DR, ESS, EV Charger
- Construct testbed sites and Install cybersecurity devices in KEPCO-KDN Daejeon-chungnam branch office and Jeju interoperability test center
- Implement on-site testbed devices such as developed AMI, DR, ESS, EV Charger with PKI system
Construct Certification testbed environment

Construct Certification testbed room and SG PKI system at Jeju interoperability test center

- details: Implement on-site testbed devices such as developed AMI, DR, ESS, EV Charger with PKI system

An overview of Certification testbed room Architecture
II. Certification technology in Smart Grid (3/7)

- Implement encryption and authentication Test-bed
  - functional and performance test for AMI security
    - PKI based Field Application of AMI system using SW and HW cyber security module
II. Certification technology in Smart Grid (4/7)

- Implement encryption and authentication Test-bed
  - functional and performance test for DR security
    - PKI based Field Application of DR system using SW and HW cyber security module
Ⅱ. Certification technology in Smart Grid (5/7)

- Implement encryption and authentication Test-bed
- Functional and performance test for ESS security
  - PKI based Field Application of ESS system using SW and HW cyber security module
II. Certification technology in Smart Grid (6/7)

- Implement encryption and authentication Test-bed
  - functional and performance test for EV charger security
    - PKI based Field Application of EV charging system using SW and HW cyber security module
Schedule

- Construction PKI system (certification & verifying etc)
- Construction SG System with Security Module
- Construction PKI Certification center
- AMI, DR, ESS, EV Charger

Design and Build security systems (2014.05~2014.09)
Construct on-site testbed (2015.08~2015.09)
Implement on-site test (2015.08~2015.12)

Strategy and Methodology

- Construct Systematic cooperation with among Policy agencies (KISA, KSGI), Service agency (KEPCO), Research Institute (NSRI), and Business Company (KEPCO-KDN, PSTEK, Ioncommunications etc.) for becoming a success business in smart grid
- On-site testbed Validation of Smart Grid Cybersecurity by vulnerability analysis, encryption and authorization, security policy
- Conduct Step-by-step scheduling on the project and active publicity campaign for project result
- publish open architecture technologies as open standards, relation with local and overseas standardization organization

Ⅱ. Certification technology in Smart Grid (7/7)
III. Public Key Infrastructure (1/6)

- Implement encryption and authentication Test-bed
  - functional and performance test for PKI system
    - Certification Field Application of PKI system that installed on site
    - Locations Jeju
      - Root CA, Local CA - interoperability test center
      - Smart device: DR, ESS, EV - interoperability test center
        AMI - interoperability Smart Place test center
    - Location KEPCO-KDN Daejeon-Chungnam branch office
      - Standalone CA
      - DR, PV+ESS, EV
PKI (Public Key Infrastructure)

Definition: The sum total of the hardware, software, people, processes, and policies that, together, using the technology of asymmetric cryptography, facilitate the creation of a verifiable association between a public key (the public component of an asymmetric key pair) and the identity (and/or other attributes) of the holder of the corresponding private key (the private component of that pair) for uses such as authenticating the identity of a specific entity, ensuring the integrity of information, providing support for nonrepudiation, and establishing an encrypted communications section.

PKI Terminology and Concepts: Hashing functions, Symmetric encryption and decryption (Session key), Asymmetric encryption and decryption (Key pair), Digital signature, Digital certificate (X.509), Certification Authorities (CA), Registration Authorities (RA), Hierarchy of trust.
Who Uses PKI?

- Current demand for certificates

- Devices
  - Web Servers
  - Cable and Satellite
  - Domain Controllers
  - VPN

- Signed Code
  - PC
  - Mobile

- Wireless (WiFi) deployments
- Corporate Banking
  - Phishing Attacks
  - Identity Theft

- eCommerce
  - SSL

- Physical/Logical access
  - Windows Logon

Government and Industry Mandates

- Phishing Attacks
- Identity Theft

Sources: Perry Tancredi, VeriSign, Inc.
Key & Certificate Management

Key/Certificate Life Cycle Management

Identity ≠ Key. Focus on Key!

Stages

- Initialization:
  Key pair Generation (private key + public key)

- Issued (active):
  Issuance
  - Certificate Creation
  - Distribution (Certificate + private key)

[Usage]

- Cancellation:
  Certificate Expiration & Revocation
Smart Grid PKI Standards related

- NIST 7628 Guidelines for Smart Grid Cybersecurity Rev1 (2014.9)
- IEC 62351-5 Security for IEC 60870-5 and Derivatives (i.e. DNP3)
- IEEE Std. 1815-2012 Electric Power Systems Communications-Distributed Network Protocol (DNP3)
- IEC 62056 Electricity metering data exchange (DLMS/COSEM)
- DLMS User Association, DLMS/COSEM Architecture and Protocols v8, 2014.7
### III. Public Key Infrastructure (6/6)

#### SG devices certification systems
- LDAP
- CA
- RA
- OCSP

- Certificate signing request
  - Format (PKCS#10)
- Certificate (X.509v3)

#### SG devices certificate issuance system
- Key Pair generate
  - Issuing (PKCS#10)
  - [Private key] [device certificate] [server certificate]

#### H/W interface (USB/Ethernet/Serial)

#### SG device security module

#### Service (DR or xEMS) system
- Served-side KMS
- SG Service Management Server

#### AMI Server
- FEP

#### DCU
- HSM

#### OCSP
- Certificate signing request
  - Format (PKCS#10)
- Certificate (X.509v3)

#### SSL/TLS
- OCSP
- Android Device

#### Key Injection System
- USB Ethernet RS-232C

#### Certificate
- Format (PKCS#10)
- X.509v3

#### HSM
- DB
- HSM
- Served-side KMS

#### Certificate
- certificate
- Format (PKCS#10)
- Certificate (X.509v3)

#### Android Device
- SSL/TLS
- OCSP

#### Key Generation
- Key Pair generate
  - Issuing (PKCS#10)
- [Private key] [device certificate] [server certificate]
Smart Grid Cybersecurity Business Model

- EMS business: HEMS, BEMS, FEMS
- Construction, operation and control of Microgrid
- Construction of EV charging system
- Construction, operation and control of Renewable Energy system: PV, wind plant, ESS
- Construction, operation of AMI, AMR
- Construction, operation of SCADA
- Construction, operation of power generation
- DR and VPP (including DER) business
- Construction, operation of utility network
IV. Overseas Export Strategy for Smart Grid (2/4)

- **Export strategy**
  - Find out target market
    - highly-specialized
    - differentiation
    - segmentation
  - Selection and Concentration
    - successful business, avoidance risk of danger
  - Cooperation with a leading smart grid technology company
    - AMI case – Meter + DCU + utility company
    - small and medium-sized enterprises have the opportunity to participate
  - Form a domestic or foreign business group or consulting group
    - collect and exchange information
    - cooperate in business
  - Participate from consulting project
    - consulting->main project
    - consulting can be reduce risk
IV. Overseas Export Strategy for Smart Grid (3/4)

- **Infrastructure of smart grid cybersecurity**
  - Open standard
  - Compliance with national standards of various countries
    - devices side
    - security side
  - Software and hardware security modules
    - some cases of IOT
  - PKI system
    - Cryptographic Module Validation Program (CMVP)
  - Countermeasure for cyber and physical attacks
    - depend from attacks and tamper-proof
Propose to expand Export in smart grid security

- Collect export project information
  - transmit to highly-specialized enterprises
- Drive toward international cooperative testbed study
  - have opportunity to find out overseas market
  - small and medium-sized enterprises have the opportunity to participate
- Strengthen cooperation with foreign consultative networks
  - Collect and Exchange cybersecurity information and standards
  - Find out the technology changes
- Secure advanced cybersecurity technology
  - undertake a nationwide proliferation project in smart grid for spreading cybersecurity market and depending national security infrastructure
Thank you!

(Seungwon Lee : swlee@kdn.com)