ZigBee®
Control your world

Analysis of CEC Requirements
Requirements Engineering for AMI-HAN interface

Robert Cragie
Chair, ZigBee Security Task Group

ZigBee
Control your world

CEC Method

- Requirements Engineering techniques used to analyze OpenHAN documents and identify configurations
- The identified OpenHAN configurations were modeled
- The open market configuration was also modeled
- Model includes:
    - Context diagrams
    - Venn diagrams
    - Use case scenarios
- Process rights and obligations identified and validated
    - Customers
    - Vendors
    - Utilities

ZigBee
Control your world

Options

- Three options (configurations)
  - Two from OpenHAN
  - One developed by project team
- OpenHAN options:
  - Utility Program option
  - Utility Program Extended option
- Project team option:
  - Open Market option

ZigBee
Control your world

Rights

- Five main rights defined in this report
  - R1. Customers have the right to receive price (periodic and real-time) signals and reliability signals without enrolling in utility programs and without registering their equipment with the utility.
  - R2. Customers have the right to choose if and how they will respond to price and reliability signals.
  - R3. Customers have the right to purchase, rent or otherwise select from any vendor any and all devices and services used for energy management or other purposes in their premise.
  - R4. Vendors have the right to compete in an open market to sell HAN systems, energy management systems, security and entertainment devices and services to all utility customers.
  - R5. Utilities have the right to offer DR and energy management services to customers which utilize the informational and communication capabilities of their AMI system.

Assertions on Options with respect to Rights

- Utility Program option only promotes the utility right, R5 and limits or denies the customer and vendor rights, R1 – R4
- Utility Program Extended option provides additional support for customer right R3 and vendor right R4
- Open Market supports all customer rights R1 – R3 and vendor right R4

ZigBee
Control your world

OpenHAN Documentation

- Document cited as “Joint IOU HAN Use Case Definitions / Assumptions / Actors document (09/25/07)”
- Location of document as referenced no longer valid
- http://osgug.ucaiug.org/sgsystems/openhan/Use%20Case%20Contributions/Forms/AllItems.aspx appears to contain a number of documents but not the cited document
- “The project team recognizes that the OpenHAN document did not cover all of the configurations developed by the OpenHAN Task Force”

ZigBee
Control your world

Utility Program Option

- Developed purely on analysis of OpenHAN document
- Lack of clarity in OpenHAN document led to development of Utility Program Extended option
- Specific problems encountered resulted in interpretation issues
    - Overloading of the term HAN
    - Use of self-referential definitions
    - Inconsistencies between assumptions, definitions and actors

Utility Program Extended Option

- The model is more representative
- Two terms introduce in relation to the option
  - Translation Device
  - Communication Protocol
- These terms are too vague in the context to infer real meaning
- Interpretations may therefore differ and produce different scenarios
- Vague terms should not be used in obligations

Open Market Option

- Seems to have been independently developed in isolation from the other models
- Comparison to other models is idiosyncratic
  - Detailed specification of an RDS system for delivery of broadcast data
    - Wrong level of abstraction

Utility Program Option Venn Diagram

- Venn diagram shows overlaps
- Subset B'1 is shown as isolated from the Utility HAN however it is not clear how this conclusion was drawn
- If subset B'1 is considered part of set C, set B' disappears as it is wholly contained within set C
- Set D therefore abuts Set C and is able to receive AMI signals

Utility Program Extended Option Venn Diagram

- Venn diagram also shows overlaps
- Customer HAN Gateway device must implicitly be owned by a set
- Either Set C or Set B' is a suitable candidate
- Therefore fundamentally the same as reinterpretation of Utility Program option except for the ownership domain of the Customer HAN Gateway
- Gateway "with translation" is perhaps a too-literal interpretation of a specification which is in the process of major revision

Open Market Option Venn Diagram

- Sets A and B cannot fulfill the requirements for DR on their own
- The sets are shown without any intersection
- Therefore it is not clear how information produced from a device in set A is consumed by a device in set B

Rights and Obligations 3

- “R3. Customers have the right to purchase, rent or otherwise select from any vendor any and all devices and services used for energy management or other purposes in their premise.”
- “O3. Utilities are obligated to provide an AMI communication system that uses an open communication protocol and does not unduly restrict customer choice of customer equipment or services that support performing DR.”
- The activity model suggests the obligation is on the utility to fulfil via the purposes of "open AMI communication protocol". This seems rather specific. It is possible energy management information could brokered between utility and third party by other means. The customer should be able to select energy management equipment independent of a utility

Rights and Obligations 4

- “R4. Vendors have the right to compete in an open market to sell HAN systems, energy management systems, security and entertainment devices and services to all utility customers.”
- “O4. Utilities are obligated to not restrict customers enrolled in utility programs to equipment that uses the AMI communication protocol.”
- This seems contradictory to O3. This makes more sense but even then the activity model places too much emphasis on the communication protocol.
- Suggest rephrasing O3

Rights and Obligations 5

- “R5. Utilities have the right to offer DR and energy management services to customers which utilize the informational and communication capabilities of their AMI system.”
- “O5. Customers participating in utility programs are obligated to maintain correct working of customer equipment that communicates with the AMI system and provide any communications translation device if needed.”
- There is an assumption on the method of delivery of such data, i.e. through the AMI system and AMI communications and the need for a translation device, which is a vague term which infers certain behavior

ZigBee®
Control your world

How SEP 2.0 and OpenHAN 2.0 satisfy CEC requirements

ZigBee
Control your world

SEP 2.0 Model

- Model developed in SEP 2.0 TRD and specifications is flexible
  - Allows for the HAN to be shared between
    - Utility-owned devices
    - Customer-owned devices
    - Third party-owned devices
  - Allows for federated security domains
    - HAN security domain distinct from AMI security domain
    - ESI acts as application gateway
    - Firewalling through application translation and decoupling
  - Allows for end-to-end security domain
    - Common security domain across HAN and AMI
    - ESI acts as network router
    - Firewalling through traffic policing and packet inspection

ZigBee
Control your world

OpenHAN Model

- Model developed in OpenHAN 2.0 SRS is a subset of SEP 2.0 model
  - Allows for the HAN to be shared between
    - Utility-owned devices
    - Customer-owned devices
    - Third party-owned devices
  - Allows for federated security domains
    - HAN security domain distinct from AMI security domain
    - ESI acts as application gateway
    - Firewalling through application translation and decoupling
  - Does not allow for end-to-end security domain

HAN Device Network Access (commissioning)

- Discovery
  - Finding the right network to join
- Joining
  - Getting onto the network
- Authentication
  - Transaction with Network Authentication Server to mutually check credentials and allow device onto network
- A device having network access *does not mean it is registered* as part of a utility or third party program
- Once a HAN Device is commissioned, it can communicate in the HAN
- Communication with registered HAN devices is either not allowed or strictly limited

HAN Device Authorization - Registration

- Registering HAN Device with utility or third party
- Performing transactions with Registration Server to mutually check credentials and authorize it to become operational in utility or third party program

HAN Device Authorization - Enrollment

- Enrollment is where a registered HAN Device joins a collection of other registered HAN Devices enrolled in the same group
- Group identity used to target all HAN Devices in same enrollment group
- Enables HAN Devices to communicate with each other in a specified manner for the purposes of fulfilling a particular program
    - DR messaging
    - Load control

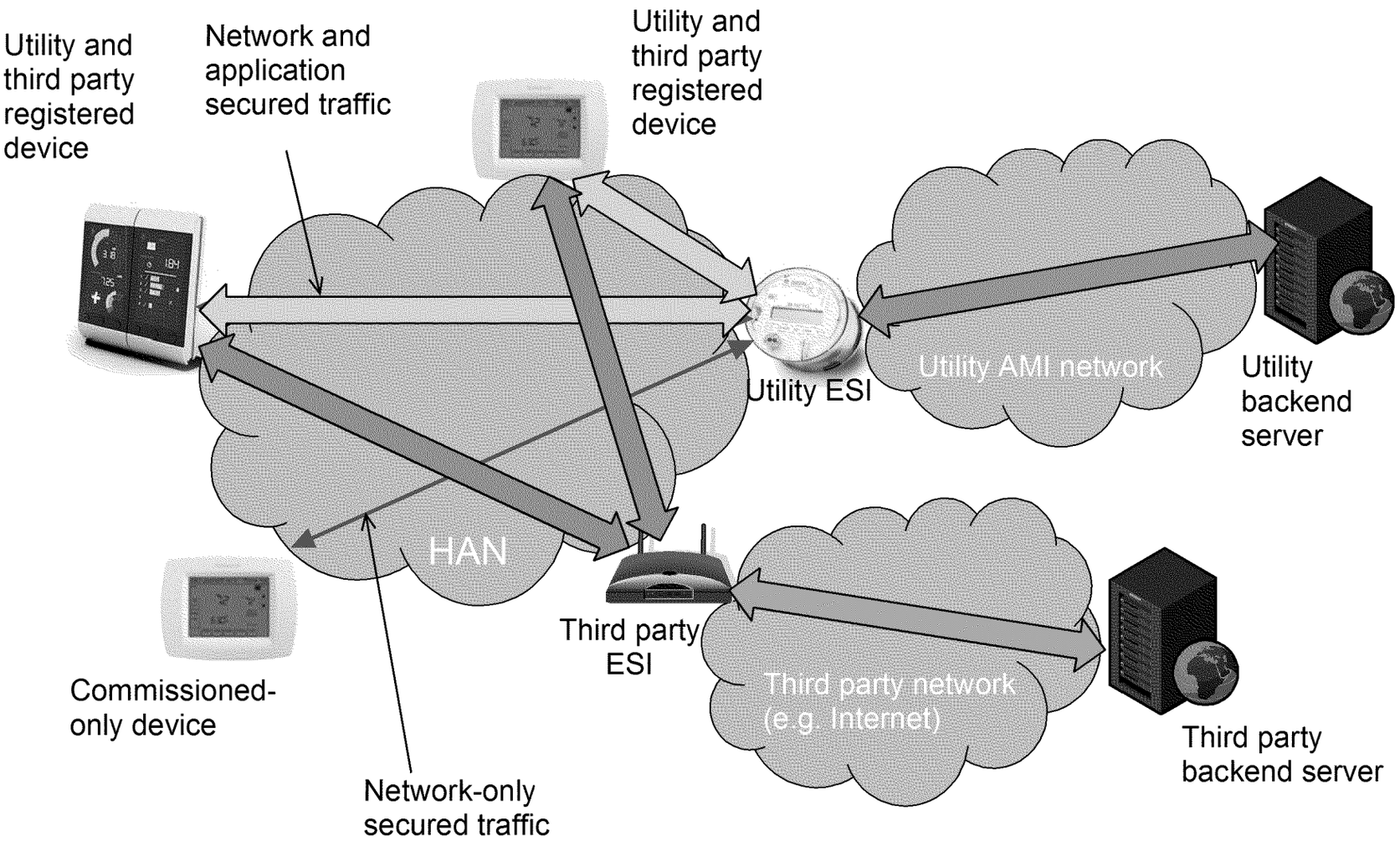
HAN Device Authorization – Access Control Lists

- Access Control List is used to control HAN Device application transaction privileges and level of security required to access a resource
- Client on one HAN Device is allowed/denied access to a resource served on another HAN Device
- Permission granted based on HAN Device identity and its granted level of security
    - Commissioned only
    - Commissioned and registered

HAN Device Authorization - Operation

- Transactions between HAN Devices can occur when the privilege levels are consistent
- Scope of operation
  - Independent of any third party (commissioned)
  - In a utility program (commissioned and registered)
  - In a third party program (commissioned and registered)

HAN Device Authorization – Complex Registration Scenario



Abstraction of Public Pricing

- Need to abstract the concept of Public Pricing
  - Information
  - Transaction
  - Delivery method

Public Pricing Information

- Producer-oriented
    - Not specific to individual or groups of consumers
- Not confidential
- Should be authenticated

Public Pricing Transaction

- Public pricing producer
  - One or a few
- Public pricing consumer
  - Very many
- Relatively infrequent
  - Minutes to hours

Public Pricing Delivery Method

- True broadcast
    - Radio Data System (RDS)
- Through AMI/InterPAN
- Through AMI/HAN
- Through other network/HAN
    - Broadband internet
    - Maybe more than one “HAN”

ZigBee
Control your world

Radio Data System

- True broadcast
- Wide reach
- Data interface to broadcasters required
- Separate hardware for receiver
- Authentication would require signed data
    - Public key signature would require relatively expensive operation at receiver
- Potential to spoof information locally if unsigned

ZigBee
Control your world

AMI/InterPAN

- InterPAN is an unsecured 'side-stack' running on ESI and HAN Devices used in SE 1.0
- Allows unsecured broadcast of pricing information without having to be commissioned, i.e. no network access need be granted
- Need to be in radio range of ESI to obtain data
- No security at all as specified
    - Cannot authenticate message
    - Easy to spoof message locally
- Authentication would require signed data
    - Public key signature would require relatively expensive operation at receiver
- Use of same transceiver and network parameters as HAN can pose a security risk

ZigBee
Control your world

AMI/HAN

- HAN Devices only need to be commissioned, i.e. have network access granted, to be able to communicate in the HAN
- Need to have network connectivity to utility ESI to obtain data
- Network access mechanism and HAN communications provides layer of security
- Can authenticate message originating from utility ESI
- Difficult to spoof message
- Registered HAN Devices have additional layer of security

ZigBee
Control your world

Other Network/HAN

- HAN Devices do not have to be registered to a utility program
- They may be registered to a third party program
- Need to have network connectivity to third party ESI to obtain data
- Network access mechanism and HAN communications provides layer of security
- Can authenticate message originated from third party ESI
- Difficult to spoof message
- Registered HAN Devices have additional layer of security