WF310:
Wireless Security

John Schwartz
Technology Strategist

Agenda

- Security definition and terms
- 802.11 security and authentication
- 802.15.4 overview
- ZigBee smart energy security
- Q & A

Security Definition

"Any real-world system is a complicated series of interconnections. Security must permeate the system: its components and connections.

.....

In the real world, security involves processes. It involves preventative technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty. Security is not a product; it itself is a process."

-Bruce Schneier

Secrets and Lies

Encryption & Security

- Encoding
  - Uses a system or pattern to change information
  - Not specifically for security
  - Some encoding is public
- Encryption
  - Designed for security
  - Encryption algorithms are public: keys are not.
  - The best encryption can only be broken by a brute force attack

Encryption & Security

- Obscure
  - Kept hidden and secret
  - Limited access by a certain number of people
  - Only as secure as the secret

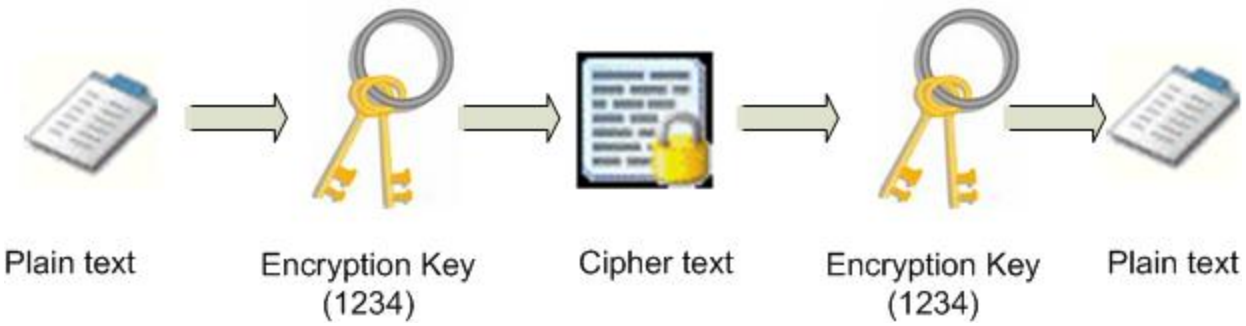
  Examples: Grandma's cookie recipe, Your ATM PIN number

- Secure
  - Public and Open
  - Still unbreakable by outside sources

  Examples: A good safe, Well designed computer systems

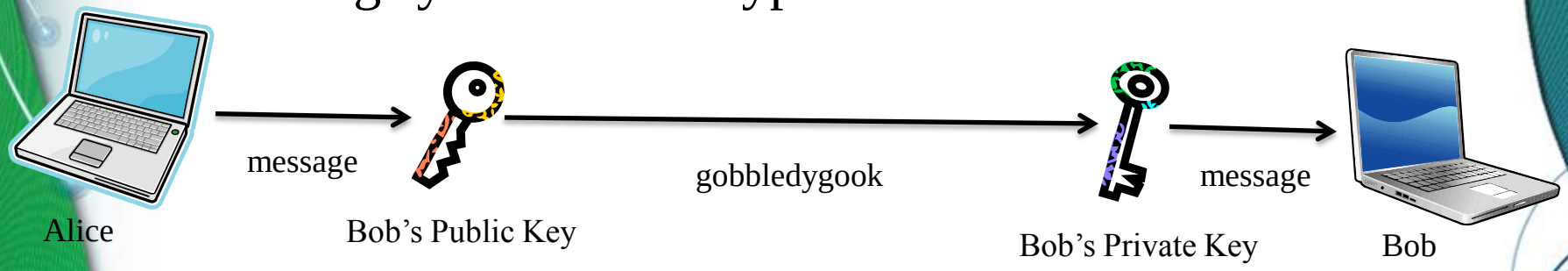
Encryption & Security

- Secret Key Symmetric Encryption
  - Same password (key) to encrypt & decrypt
  - Requires an algorithm and a key
  - Strength – very secure if used with a good algorithm
  - Weakness – key maintenance & transmission



Encryption & Security

- Public key encryption
  - Key to encrypt data called a public key
  - Key to decrypt data called a private key
  - Asymmetric encryption is very slow: symmetric is much faster
  - Often, asymmetric encryption is used only to exchange a symmetric key: further encryption done using symmetric encryption



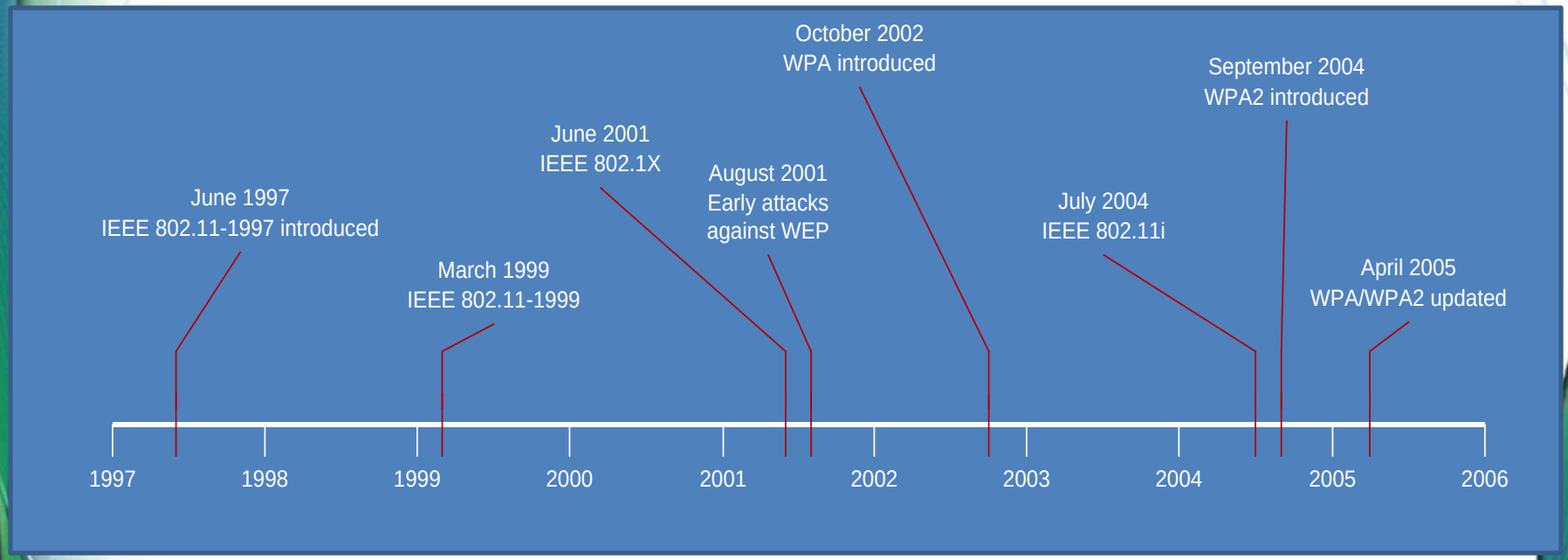
Three Pillars of Security

- **Encryption**
  - Data cannot be understood by someone without a key
- **Integrity**
  - Verification that the data has not been modified en route
  - Protects from attacker data corruption, replay attacks
- **Authentication**
  - Did the message come from the right source?
  - For true authentication, machine provides information that could only come from that machine. Often a digital signature (a hash of a digital certificate)

802.11 “Wi-Fi”

- Why 802.11?
- Most popular and well-established digital wireless communications standard
- Infrastructure is there – newer standards are either designed for specialized applications or are too new to have a settled specification (such as Bluetooth and ZigBee)
- Security is well-defined but highly confusing
  - Confusing jargon, tangled history

History of Wi-Fi security

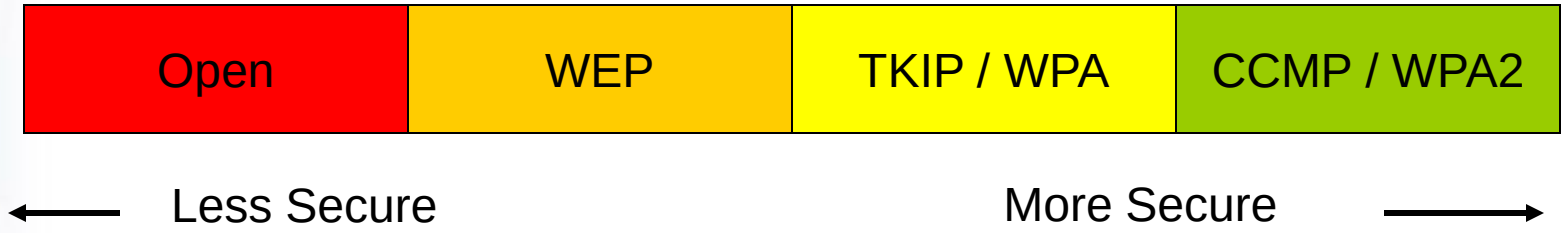


Wireless Security Organizations

- Two main organizations that specify Wi-Fi security
  - IEEE
    - 802.11 specifies WEP
    - 802.11i specifies TKIP, CCMP, 802.1X authentication
  - Wi-Fi Alliance
    - WPA specification based on draft of 802.11i (includes TKIP and 802.1X authentication)
    - WPA2 specification based on final 802.11i (includes TKIP, CCMP, and 802.1X authentication)

Wi-Fi Encryption Methods

- Wi-Fi has three major types of encryption:
  - WEP – Mostly obsolete, easily broken
  - TKIP – Often known as WPA encryption
    - Without authentication – WPA-Personal/WPA-PSK
  - CCMP – Often known as WPA2 Encryption
    - Without authentication – WPA2-Personal/WPA2-PSK
- Also, “Open” – no encryption



TKIP: Temporal Key Integrity Protocol

- IEEE recognized that WEP was broken: began work on replacement in the 802.11i Task Group
- New algorithm known as TKIP
  - Subsequently, the Wi-Fi Alliance adopted TKIP into their WPA (Wi-Fi Protected Access) standard, based on a draft of 802.11i
  - TKIP is often known as WPA encryption

TKIP Encryption, cont'd

- Improved integrity-checking
  - Developed algorithm called Michael
  - Supportable on low-resource devices
- TKIP/WPA does not provide "rock-solid" encryption
  - Can be considered practically secure
  - If security is of paramount importance, then TKIP/WPA is not an adequate solution

CCMP Encryption

- Designed from the ground up
- Uses best security practices
- Introduced in final IEEE 802.11i specification
  - Quickly adopted by Wi-Fi Alliance into WPA2 standard
    - CCMP is often known as WPA2 encryption

CCMP Encryption, cont'd

- Uses AES as its encryption engine
  - CCMP/WPA2 encryption often known simply as AES encryption
  - Considered very secure
  - Resource-intensive: throughput can be a problem on small embedded systems
- Many older devices do not support CCMP/WPA2 encryption
  - Support is increasing

Pre-shared Keys and Passphrases

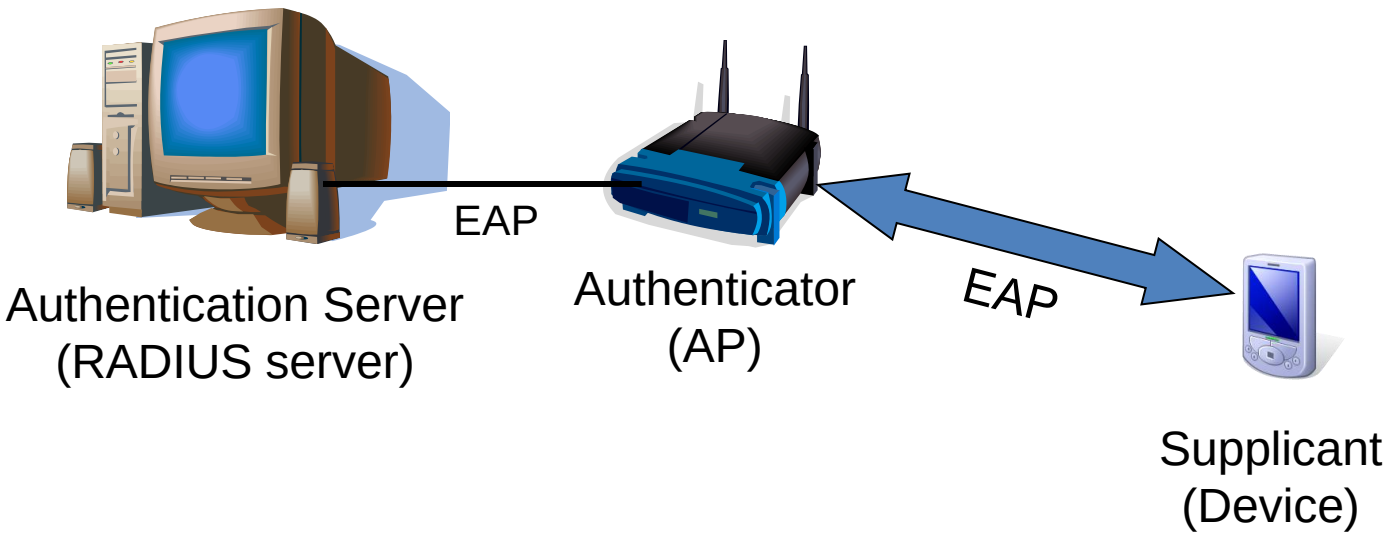
- All of these encryption methods require a master key
- Key can be pre-shared (PSK)
- TKIP/WPA and CCMP/WPA2 allow a passphrase
  - Passphrase is expanded into the PSK
- Alternatively, authentication can be used…

IEEE 802.11i Authentication

- 802.11i introduced an authentication framework for Wi-Fi
  - Uses 802.1X specification authentication framework
  - Authentication methods are based on EAP, the Extensible Authentication Protocol
  - Does not specify any actual authentication methods, but rather the framework that they must conform to

802.11i Authentication

- 802.11i authentication typically requires a supplicant, authenticator (access point), and authentication server (RADIUS server)



EAP-TLS Authentication

- Uses Extensible Authentication Protocol (EAP) in conjunction with Transport Layer Security (TLS)
- Wi-Fi Alliance adopted EAP-TLS into WPA
  - Still the “preferred” authentication method in WPA2
  - Use of EAP-TLS is often known as WPA-Enterprise

EAP-TLS

- Authentication is certificate-based
  - Certificate contains public key of a device
  - Need a Certificate Authority (CA) for signing and authenticating device certificates
- To set up a device for authentication, you need:
  - Signed certificate for device
  - Private key for device
  - Certificate for Certificate Authority

PEAP Authentication

- PEAP, or Protected EAP, also uses TLS as a basis for authentication
- Different from EAP-TLS in that the authentication is provided by a separate authentication method within a TLS-secured tunnel

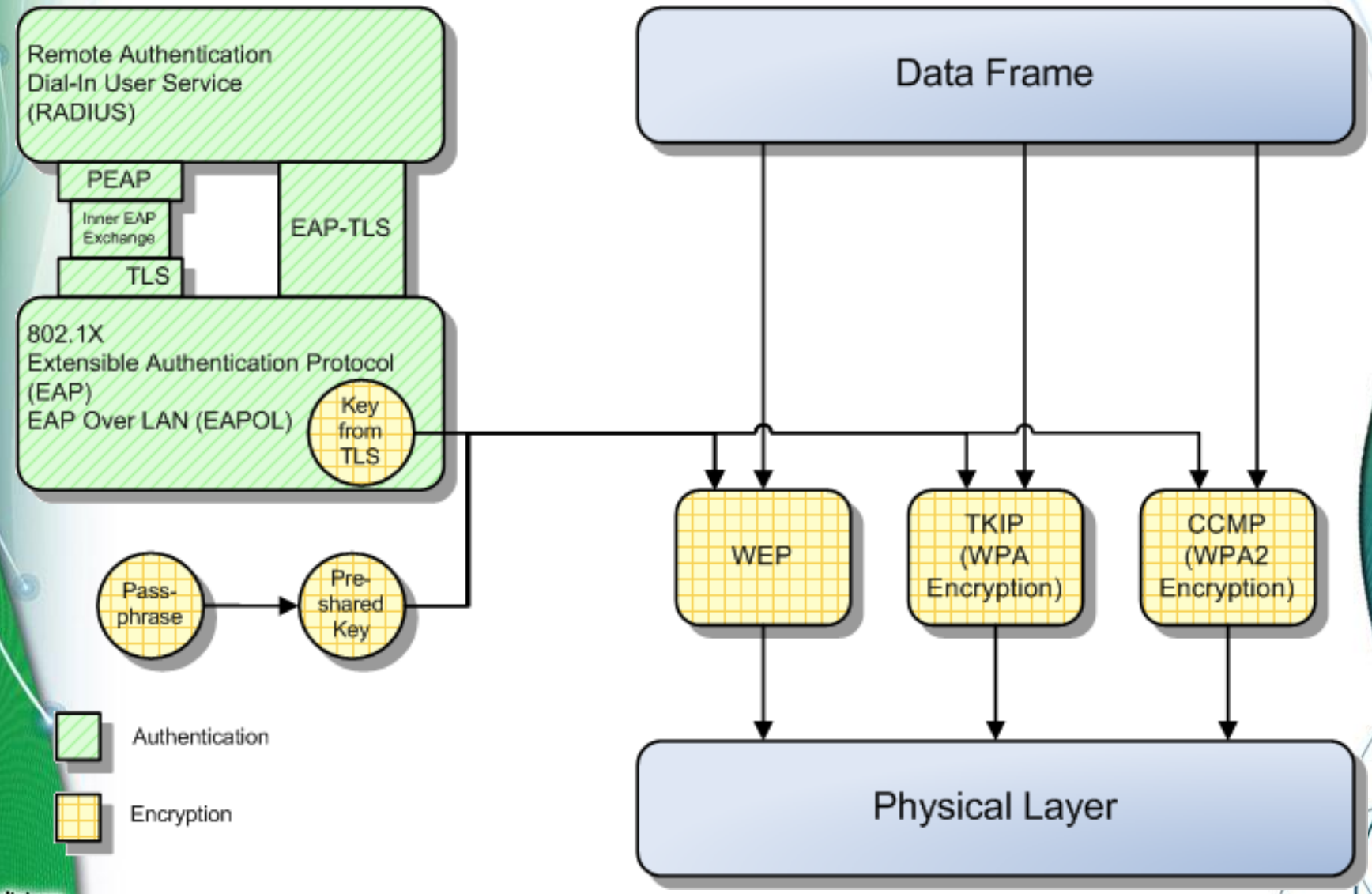
PEAP

- PEAP has one major advantage over EAP
  - Does not require a TLS certificate for clients/supplicants since authentication is a simpler username/password
  - This frees up resources on the client by reducing the storage required for the extra certificate
- Each device needs the following:
  - A Certificate Authority (CA) certificate for server verification
  - Username/password

Other Authentication Methods

- EAP-TLS and PEAP are the most commonly used methods, but there are many others
- WPA2 specifies 5 methods that may be used and should be supported for compliance
- Other methods include EAP-FAST and LEAP (LEAP is now considered insecure) that are primarily used in Cisco products
- EAP-TTLS is another method that is less popular and decreasing in use

Wi-Fi Security Architecture

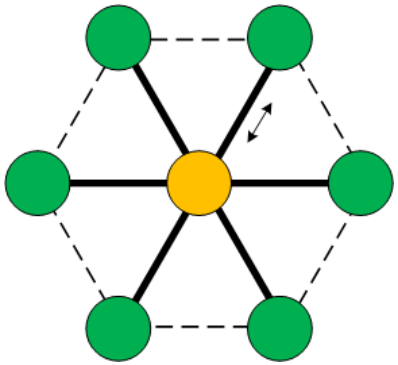


802.15.4 Characteristics

- Designed to be a PAN
  - Lower power than MAN, LAN technologies
    - Ability to sleep
  - Simple
    - MAC and PHY layers
    - Point to point, Point to Multipoint, Peer-to-pe
    - Coordinator possible, but not required
    - Broadcast and unicast modes
  - Low data rate
    - Not necessarily an “Internet” technology
  - Security
    - AES 128-bit
    - CRC for data integrity
    - No authentication defined

802.15.4 MAC

802.15.4 PHY



ZigBee

Key Characteristics

- Built on top of 802.15.4 – DSSS in 2.4 GHz
  - End points sleep, routers don't
  - Coordinator needed to start network
- 2006 vs. 2007
  - ZigBee 2006 had significant limitations
  - ZigBee 2007 includes frequency agility, message fragmentation, enhanced security
    - aka ZigBee PRO Feature Set
- Routing
  - AODV style route discovery
  - Cluster-tree routing – short routing time, but knowledge of lots of routes

ZigBee Smart Energy

- Uses ZigBee PRO Feature Set (2007)
  - Current revision (rev.15)
  - Security – authentication and encryption
- Seven supported device types
  - Energy Service Portal (ESP)
  - Metering device (electricity, water, gas, heat, etc.)
  - In-premise display
  - Programmable Communicating Thermostat (PCT) for HVAC control
  - Load control device
  - Range extender
  - Smart Appliance Device
  - Prepayment Terminal Device

ZigBee Smart Energy

- Device associates
  - Network key is sent via preconfigured link key
  - Certificates include MAC address and device TypeKey
- With network key, device requests key establishment endpoint
- Does public key exchange to send certificate for authorization
  - Uses ECC
  - MAC address part of the certificate
- New link key is exchange for subsequent command/control messages