Smart solutions.
Strong relationships.

Carles Pujol Soler
CG Automation BU. Barcelona, Dic 2014

AVANTIIA
GROUP COMPANY

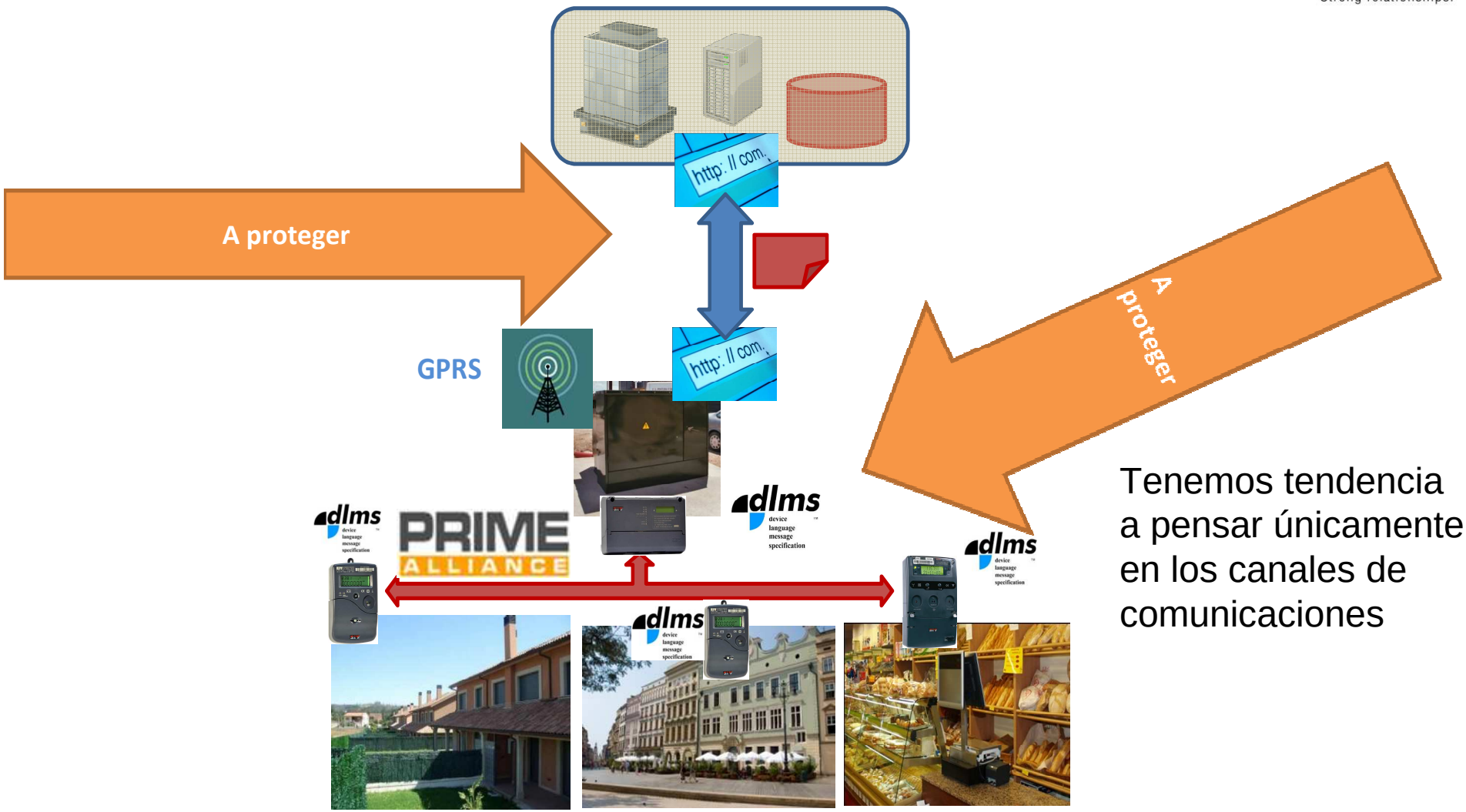
CIBERSEGURIDAD EN LOS SISTEMAS DE SMART METERING

Author: Carles Pujol

CG Automation

December 2014

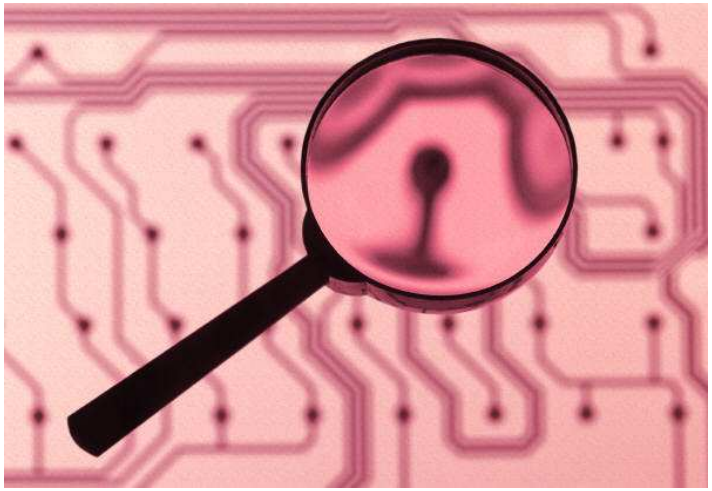
Arquitectura Smart Metering



Tenemos tendencia a pensar únicamente en los canales de comunicaciones

Author: Carles Pujol **CG Automation** **December 2014**

Ciberseguridad



Pero a la hora de la verdad, una auténtica política de ciberseguridad debe incluir:

-Seguridad en las comunicaciones
- Seguridad en los equipos
- Política a nivel de empresa

1.- SEGURIDAD EN LAS COMUNICACIONES

Author: Carles Pujol

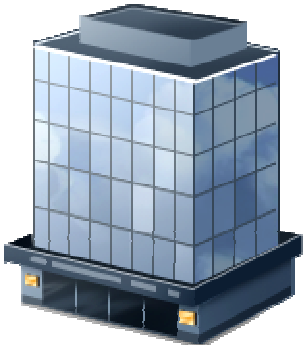
CG Automation

December 2014

Seguridad en las comunicaciones-1

Smart solutions.
Strong relationships.

Punto A



$$k_a; e^{k_a} \xrightarrow{e^{k_a}} e^{k_a}$$

$$e^{k_b} \xleftarrow{e^{k_b}} e^{k_b}, k_b$$

Punto B

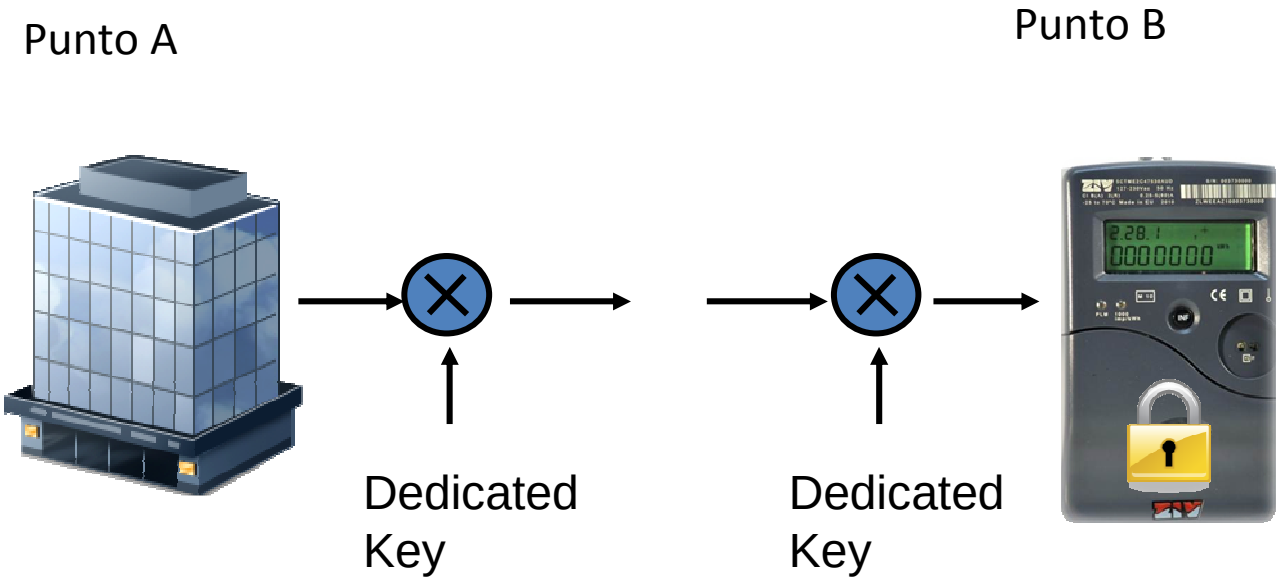
Clave asimétrica Diffie-Hellman

-Se escogen las claves de manera que el logaritmo neperiano de e^{k_a} o e^{k_b} sea extremadamente difícil de obtener

- Cualquier hacker que intercepte las comunicaciones sólo podrá obtener $e^{k_a+k_b}$

$$e^{k_b{}^{k_a}} = e^{k_b * k_a} \longleftrightarrow e^{k_a{}^{k_b}} = e^{k_a * k_b}$$

Seguridad en las comunicaciones-2



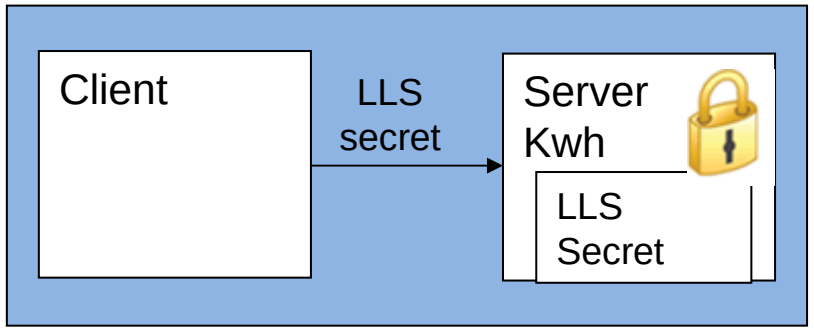
Clave simétrica AES Rijndael-128

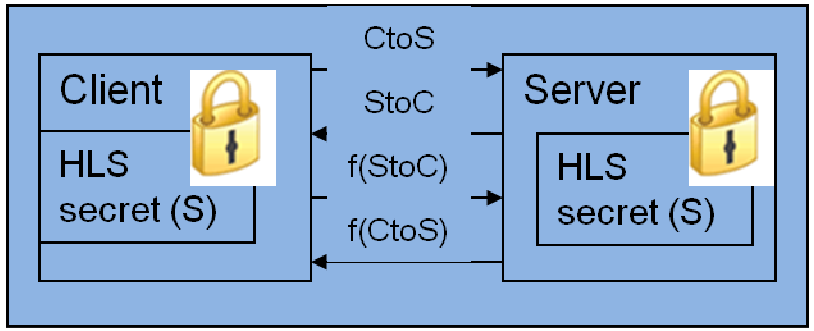
- Se puede escoger entre la versión AES-128 o bien AES-GCM-128 (más optima para la criptografía paquete a paquete)

- Proporciona protección criptográfica para los mensajes durante el transporte:
  - Autenticación para asegurar la integridad y autenticidad (fuente o origen legítimo)
  - encriptación para asegurar la confidencialidad
  - Encriptación autenticada

Seguridad en las comunicaciones-2

Control de acceso a los datos:



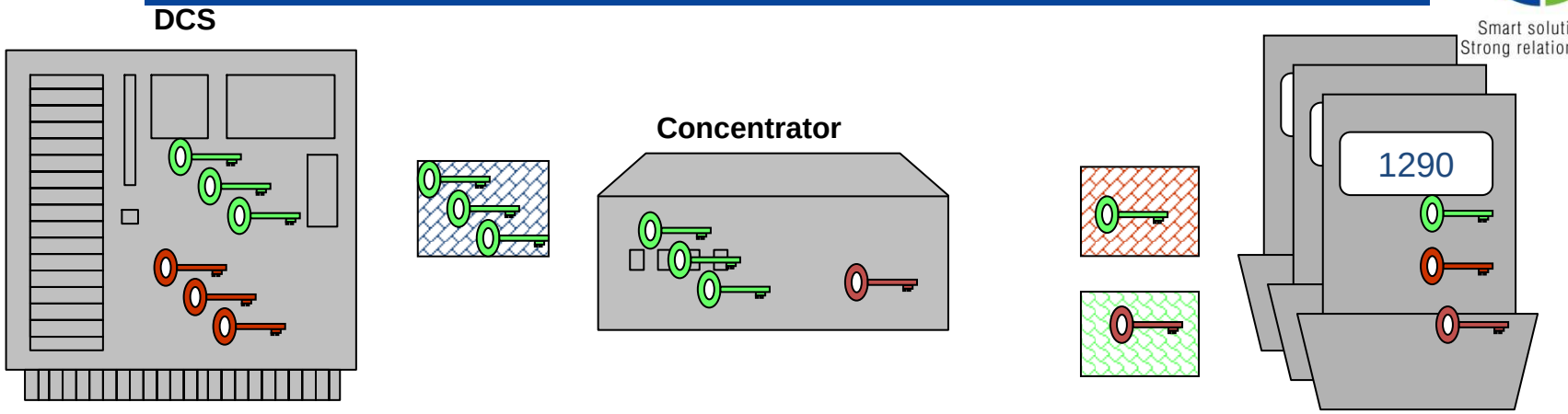


A new cibersecurity client has been designed for PLC:
-LLS (Low level Security), HLS (High Level Security)
-All traffic will be encrypted and authenticated using security_policy(3) and security_suite(0)

Seguridad en las comunicaciones-2

- DLMS proporciona mecanismos de seguridad
- Seguridad de acceso a los datos:
  - LLS and HLS
- Seguridad de transporte de datos:
  - Autenticación
  - Encriptación:
    - AES-GCM-128 para encriptación autenticada
    - AES-128 for key wrapping

Gestión de claves de seguridad



- Encryption keys:
  - Global key (es la que hace la parte asimétrica): usada en varias sesiones(AAs); unicast - broadcast
    - global unicast key encripta las dedicated key
  - Dedicated key (es la que hace la parte simétrica): será usada en una sóla sesión (Application Aassociation),y después destruida
- Authentication key (opcional con el GCM)
  - Global, unicast y broadcast
- Master key: preestablecida, usada sólo para envolver-proteger las global keys

Cryptographic material

- **MK-Master key:** Única por contador. Usada para el transporte cifrado del resto de claves. Es posible cambiarla
- **GUK-Global Unicast Key:** Única para cada cliente seguro y unica por contador. Usado para el dedicated key exchange.
- **GAK-Global Authentication Key:** Usado para autenticación GCM (cada paquete de datos es autenticado)
- **DK-Dedicated key:** Valido para cada sesión.

2.- SEGURIDAD EN LOS EQUIPOS

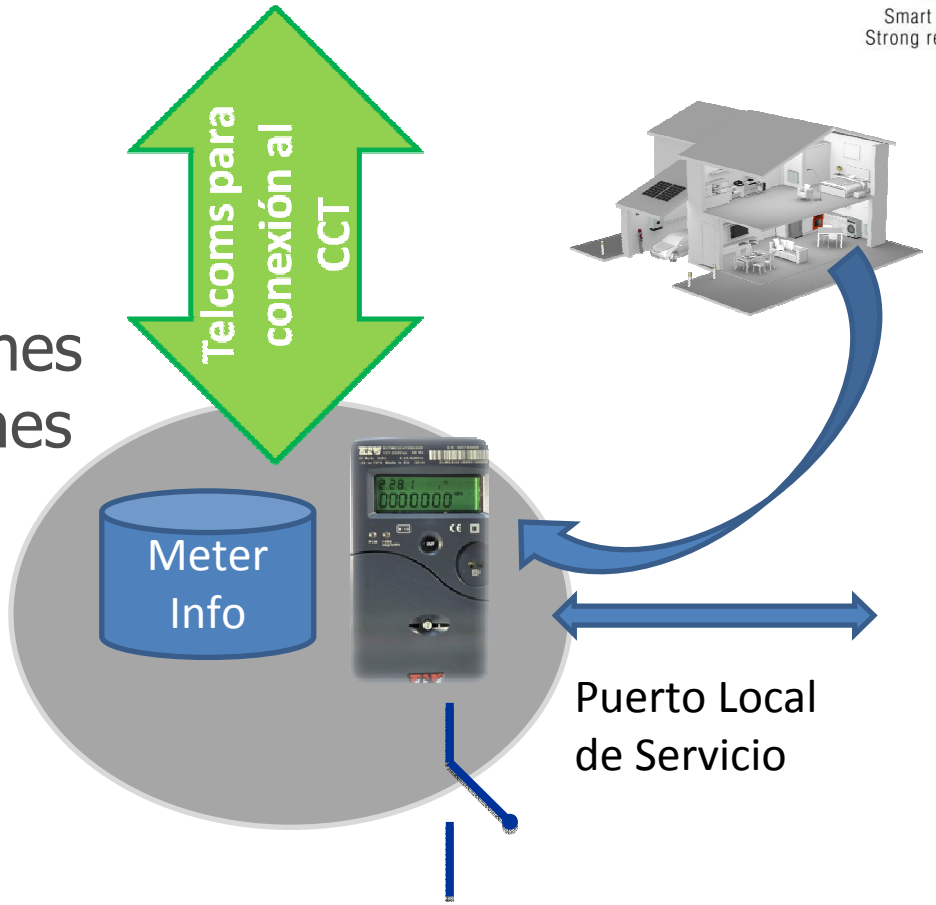
Author: Carles Pujol

CG Automation

December 2014

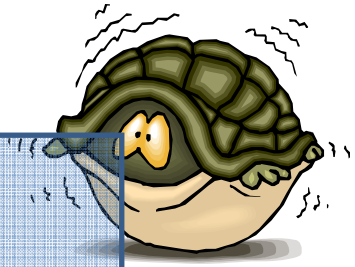
Seguridad equipos: Radiografía del contador

- Comunicación contínua con el concentrador (4CCT)
  - Variedad de soluciones de telecomunicaciones
    - Soluciones radio propietarias
    - Servicios celulares - TELCO
    - Comunicaciones via PLC de BT (PRIME)
    - IEEE 802.15.4g Zigbee
- Puerto local de servicio



Seguridad en los equipos – acceso físico

- Security by obscurity?
- Does not last forever



- Tamper detection
  +
- Communications

- Quick response

- Intrusion detection
  +
- Instant erase

- Valid for Smartmeters?

Seguridad en los equipos – acceso

Smart solutions.
Strong relationships.

Prestaciones ciberseguridad– acceso:

- **Se establecen roles claros para cada tipo de interfaz**
  - Acceso valores lectura de las medidas
  - Switch desconexión abonado
  - Configuracion
  - Actualización Firmware
- **Necesidad de auditar todos los accesos:**
  - Access logs
  - Alarmas de acceso erróneo

3.- POLÍTICA DE SEGURIDAD

Author: Carles Pujol

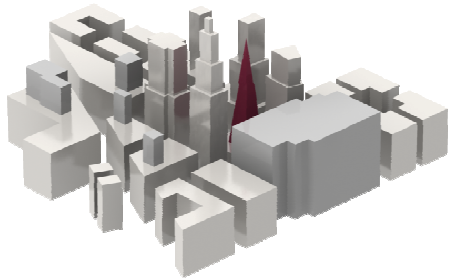
CG Automation

December 2014

Seguridad necesita ser gestionada

Smart solutions.
Strong relationships.

- Temas que se han de tener claros:
  - ¿Como deben entregar los fabricantes los detalles sensibles de las claves a las utilities?
  - ¿Como se gestionan los accesos de los subcontratistas?
  - ¿Como y cuando se refrescan las claves?
  - Que se hace en caso de una brecha de seguridad?
  - Gestión de acceso a los contadores



CG Automation B.U.

Gracias