

# Securing and extending the functionality of smart meters with smart card technologies

PROJECT+HYDRA

e-Smart 

**Charles Palmer – Onzo Limited**

# It's all my fault...



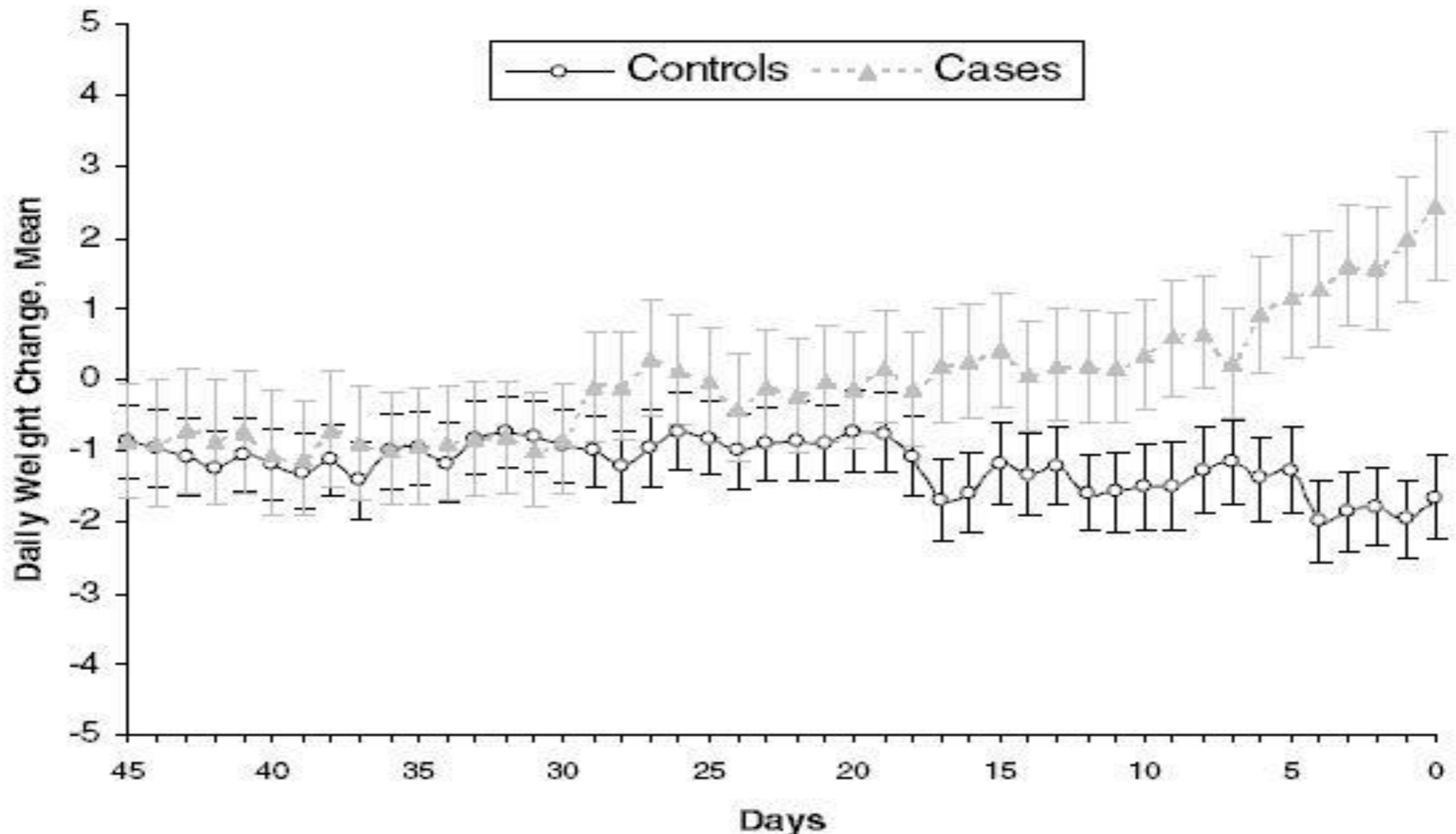
## ...me and the baby-boomers...

# How to care for an aging population?

- World healthcare systems are struggling with ageing populations.
- Number of people aged 85+ to increase 75% by 2025.
- 9/10 of older people want to live at home but in UK 1/2m live in care homes.
- Over 15m UK people have long-term health needs.

How can technology keep people at home and reduce the burden on health workers and carers?

# Weight change pre hospitalisation for heart failure \*



**Solution:** patient measures weight daily at home, so a doctor can intervene early. But, how to handle comms?

\*Patterns of Weight Change Preceding Hospitalization for Heart Failure - Sarwat I. Chaudhry et. al. <http://tinyurl.com/3xwaq78>

# Project Hydra is moving health data through the smart meter communications network.

A collaborative R&D project part funded by the UK Technology Strategy Board. Partners are:



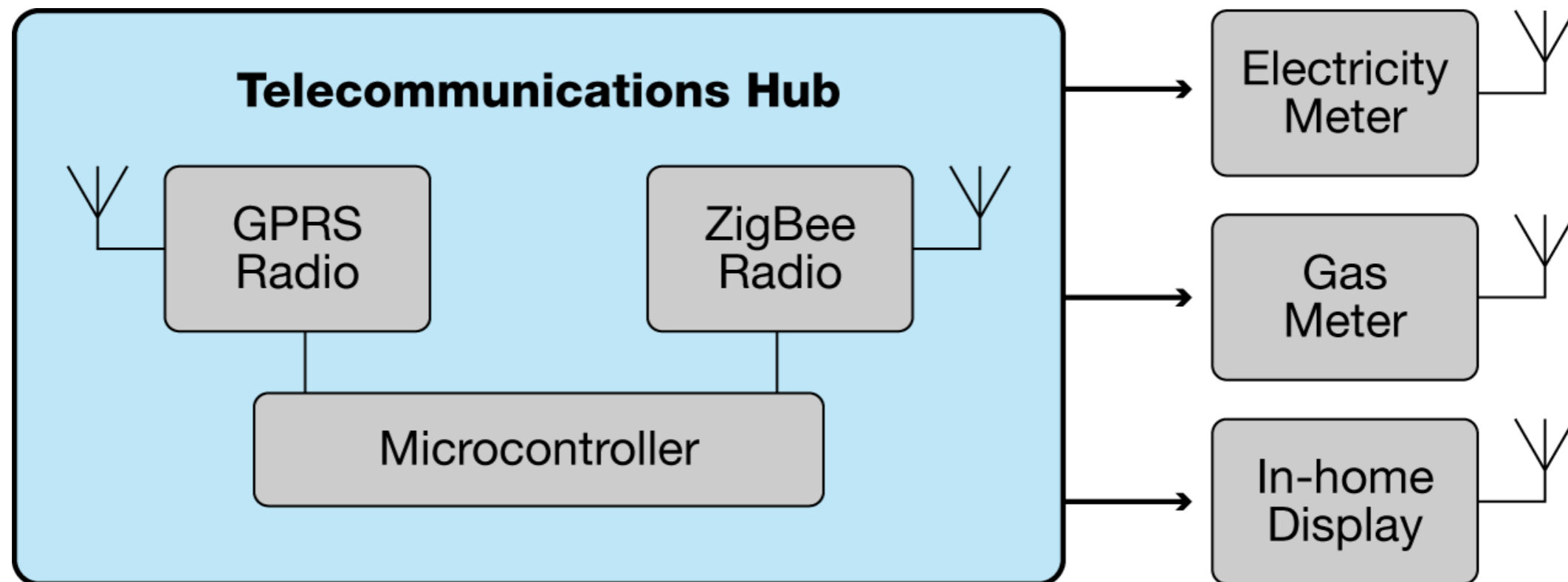
- Being deployed in UK homes now.
- Daily weight and blood pressure measurements.
- Standard Echelon smart meters and NES server.
- Standards-based, ZigBee and health data protocols.

# Why value-added services on smart meters?

- Reusing ubiquitous, always-on smart meter comms avoids new investment by home owners.
- Non-core services improve the ROI of smart meter rollout.
- Compelling in deregulated energy markets like the UK where attraction, retention and user revenue are key for energy retailers.
- Many energy and non-energy services are possible, e.g:
- Onzo and SSE's next project is HAWCS: Heating and Hot Water Control over Smart Meter Infrastructure.

# Conventional view of the UK smart meter arrangement:

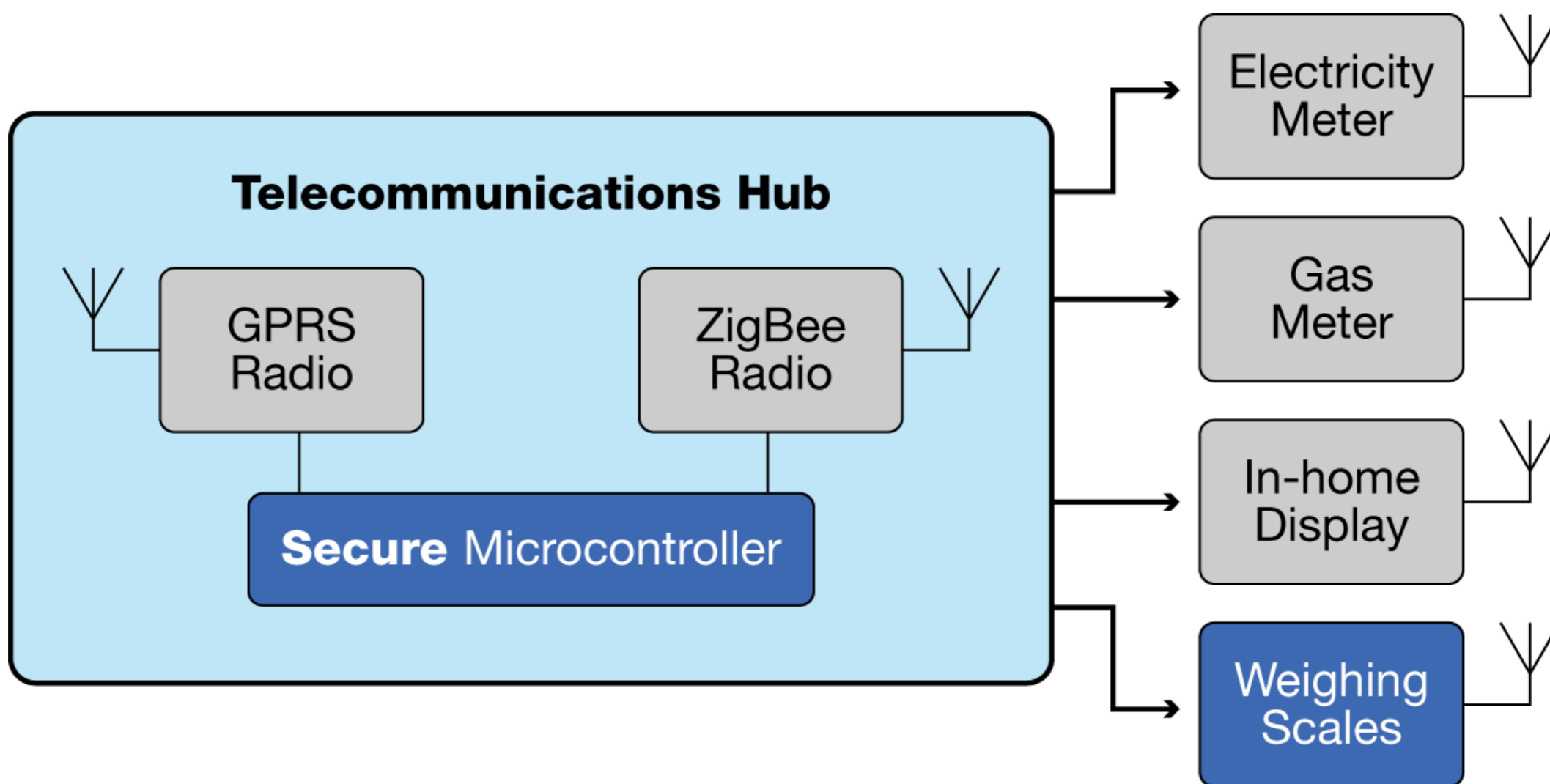
Home area network links meters, display, comms module.



**Typical Smart Meter Setup**

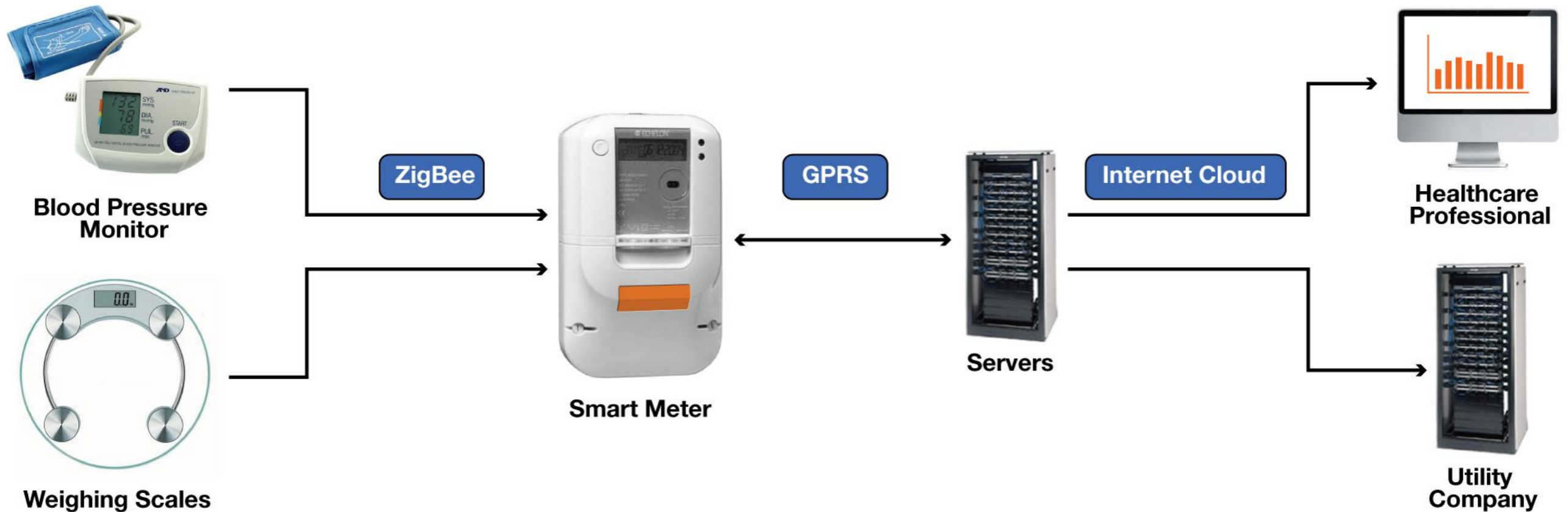
# Project Hydra view supports value-added services:

Other devices can be supported at almost no extra cost.



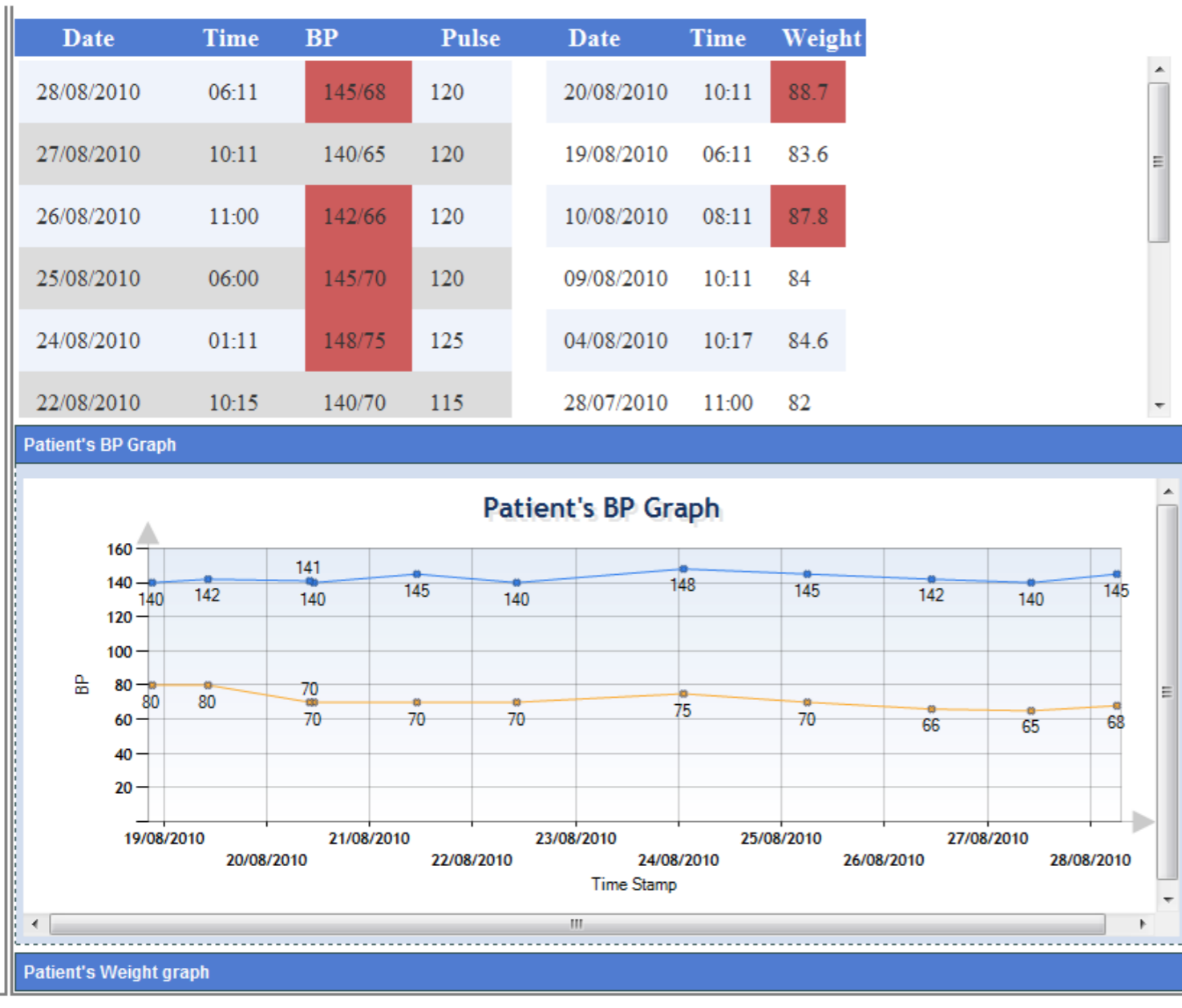
Smart Meter Setup Supporting Value-Added Services

# Project Hydra proof of concept demonstration



- Health data is transmitted to smart meter by ZigBee.
- Meter transmits data to server by GPRS.
- Health data and energy data delivered separately.

# Weight and blood pressure sent to doctor's offices.



Data is viewed by nurse, who spots trends that need investigation.

Patients send data from home – no travel.

Only worrying data needs following up, saving resources.

# So what does this have to do with smart cards?

To support value-added services we would need:

- Ability to add support for new devices and applications over time.
- This includes remote software updates.
- Separation of each application:
  - + applications can't interfere with each other
  - + data kept private
- Good cryptography, of course.

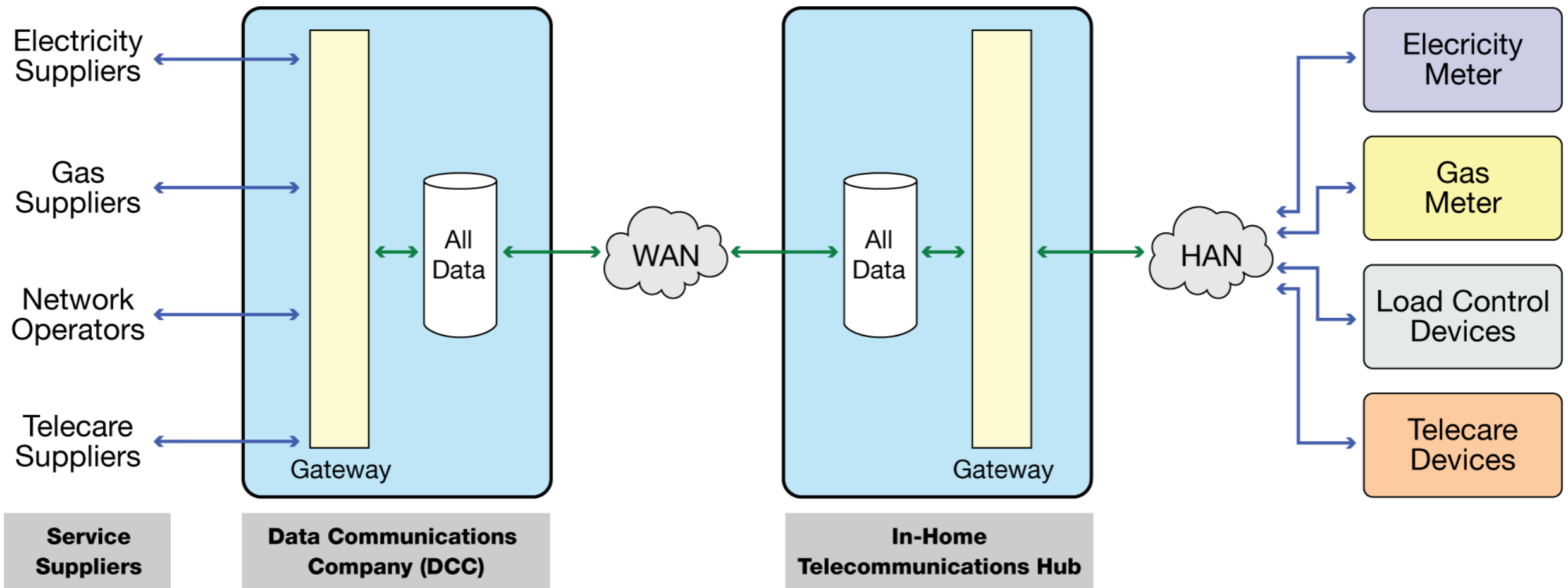
**But aren't these issues for smart meters already?**

**Sounds a bit like what smart cards do...**

# Similarities: smart meters and smart cards

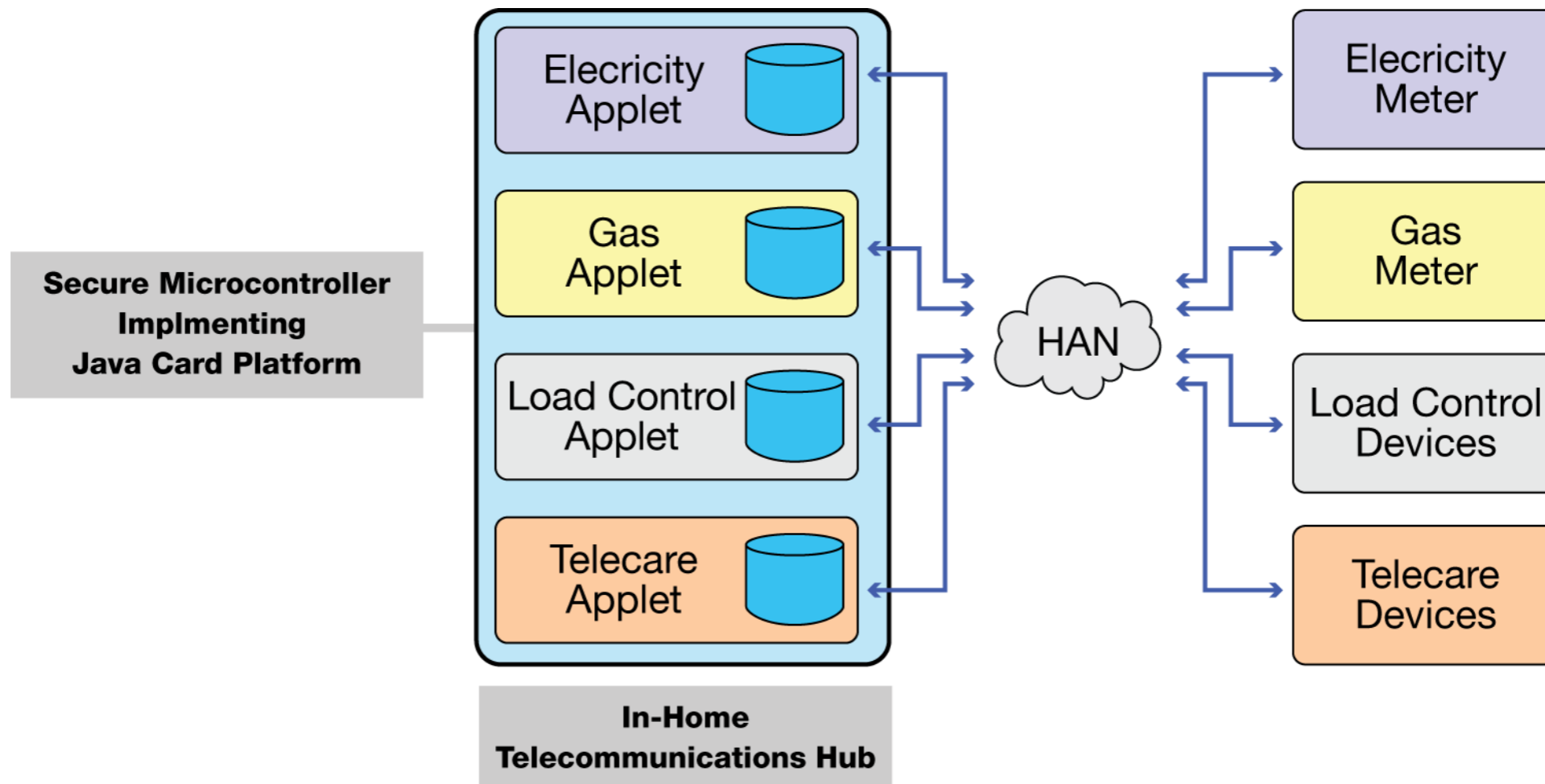
- The smart card industry has solved problems the utilities industries are now starting to ask about.
- Similarities:
  - ✚ Protecting valuable assets.
  - ✚ Devices are widely distributed in an uncontrolled environment full of Mallories motivated to defeat security.
  - ✚ Personalisation occurs as systems are deployed
  - ✚ Protecting assets of **multiple** stake-holders.
  - ✚ Post-Issuance software updates required.
  - ✚ High volume, low cost.

# Problems with the simple model:



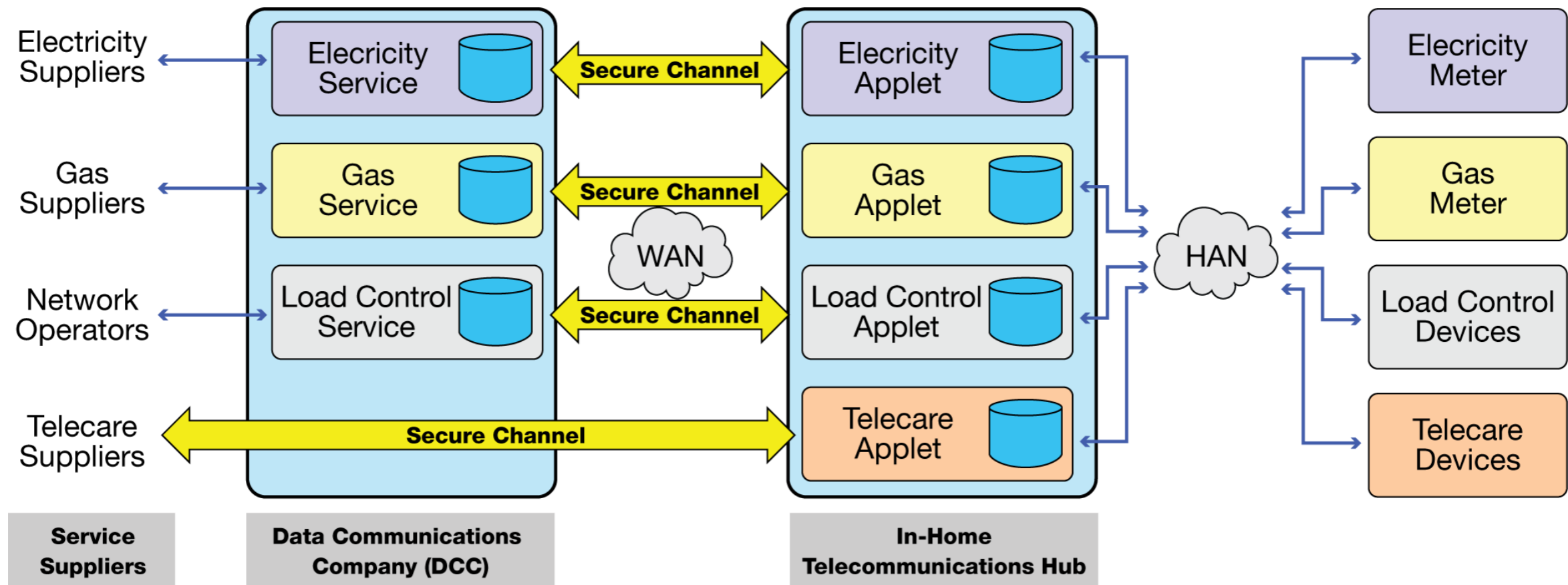
- No separation of data on the in-house equipment.
- No separation of data at the server.
- Server has huge database of half-hourly energy use.
- How to manage access control for different stakeholders?
- Who writes the security software?

# Alternative model uses secure micro, Java Card



- Secure micro adds first-line physical protection for keys, certificates, code and data.
- Java Card model separates applets data internally.
- A well-established platform – strong, tested crypto.

# GlobalPlatform adds software life-cycle management, secure communications channels



- Secure, dynamic management of applets.
- Separate cryptographic keys for each applet.
- Provides secure communications channels between applets and “off-card” entities.
- So each service can be separated from others.

## Reminder: why Java Card could help

- Designed for security.
- Secure operating environment.
- Application isolation with firewalls.
- Resists common hacking attacks - buffer overflow etc.
- Support for object persistence and atomic transactions is designed in.
- Platform-independent: virtual machine and hardware abstraction. Write once, run anywhere.
- Object oriented programming paradigm.
- Good development tools, good developer base (Java).
- Mature crypto libraries (don't reinvent the wheel).

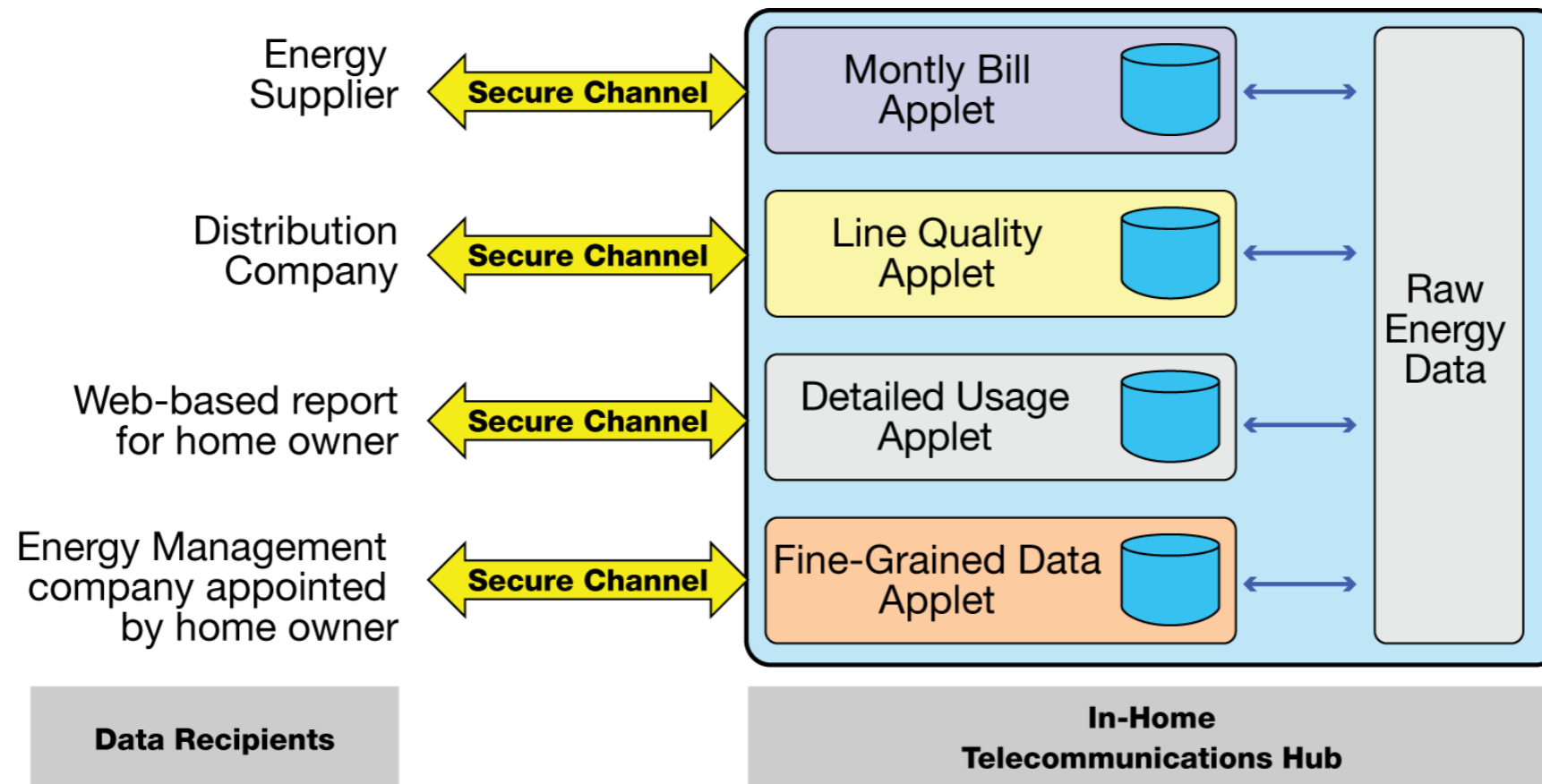
**Is the alternative for each meter manufacturer to implement their own security in C?**

## Reminder: why GlobalPlatform could help

- Designed to manage software on smart cards.
- Deploys multiple applications from multiple suppliers.
- Applications can be pre-loaded or added post-issuance.
- Manages life-cycle of card and applets (loaded, installed, selected, locked, deleted).
- Multiple security domains with separate crypto material.
- Supports independent secure communications channels between applets and corresponding off-card entities.
- Crypto protocols designed, evaluated, **certifiable**.

**Is the alternative for each meter manufacturer to implement their own security in C?**

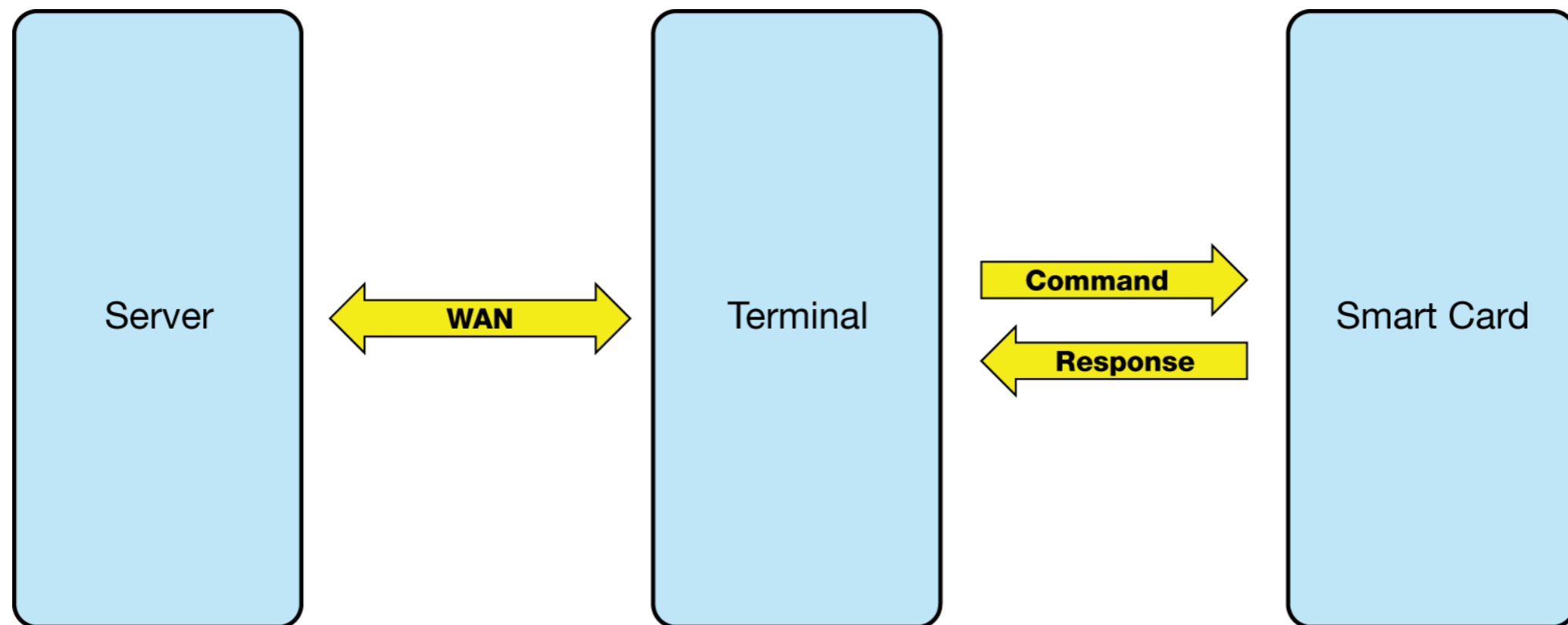
# Applets also solve privacy problems



- Multiple applets process data in the home.
- No need to export raw data to a central database.
- Applet knows tariff, can calculate monthly bill (this functionality needed for pre-pay meters anyway).
- Each recipient gets data on a need-to-know basis.
- Fine-grained data exported only if householder agrees.

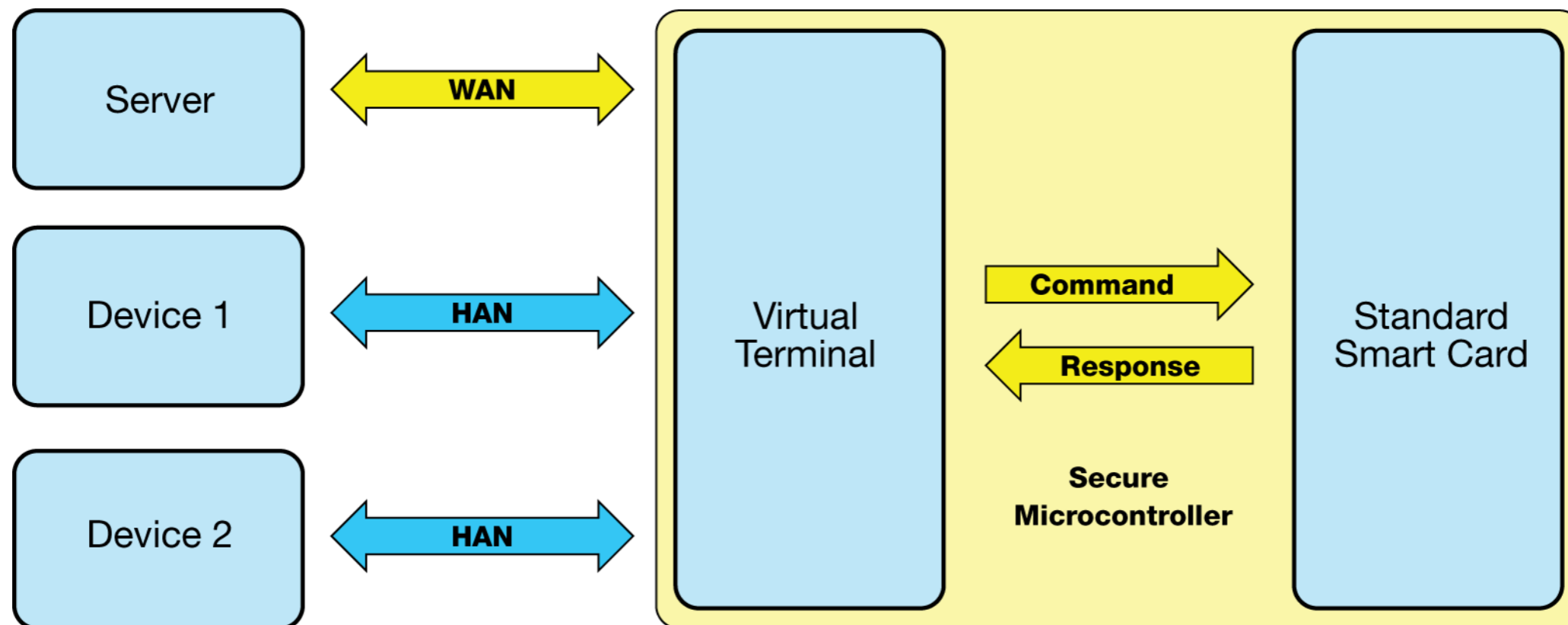
# Adapting the traditional smart card model (1/2)

- How to extend smart card interaction model to include messages from devices?
- Conventional smart card interactions are initiated from a terminal:



## Adapting the traditional smart card model (2/2)

- Add a Virtual Terminal that routes messages, using logical channels. Adds timer events.
- VT performs mapping between device, applet, AID.
- Applet's response may request other VT activities.



# Beyond Hydra:

## Using Java Card 3 Connected for Smart Meters

### Key features:

- Native IP network-oriented connectivity facilitates end-to-end integration
- Embedded web server
- Support for both Client and Server comms models
- Multithreading
- Enhanced security and cryptographic framework

### Key Benefits:

- Simplify overall hardware architecture on the smart meter
- Provide richer software development platform
- Facilitate end-to-end integration with backend servers
- Facilitate concurrent interaction with multiple devices
- Supports GlobalPlatform Networked Specification

# Some thoughts on the UK smart meter programme

- 27 million electricity meters, gas meters – *all with an off switch.*
- Political and commercial pressure for rapid roll-out.
- A committee will establish the technical specs (then disband).
- Privacy and Security Advisory Group is closed to industry and academics. Risk analysis not public.
- Will the technology be ready? Tested?
- Will the privacy and security issues be properly thought through?
- Where does the security liability lie?
  - ✦ Government regulator Ofgem?
  - ✦ Data and Communications Company (DCC?)
  - ✦ Distribution companies?
  - ✦ Energy suppliers?
  - ✦ Telecoms operators?
  - ✦ Equipment manufacturers?
- DCC is to oversee security, but:
  - ✦ Suppliers required to start roll out 1 year before DCC exists.

# Food for thought?

## Thank you.

Charles Palmer  
Onzo Limited, London  
charles.palmer@onzo.com