

e-PASTA
e-Protection of **A**ppliances through **S**ecure and **T**rusted **A**ccess

Antonio Kung - Trialog
Mario Cipriani - Merloni Elettrodomestici



e-PASTA

◆ Consortium

– Trialog

The logo for Trialog, featuring the word "TRIALOG" in a stylized, red, sans-serif font with diagonal slashes through each letter.

– T-Systems

The logo for T-Systems, featuring a pink "T" inside a square with dots, followed by the word "Systems" in a grey, sans-serif font.

– Trusted Logic

The logo for Trusted Logic, featuring a stylized orange "TL" above the words "Trusted Logic" in a black, sans-serif font.

– Merloni Elettrodomestici

The logo for Merloni Elettrodomestici, featuring the words "Merloni Elettrodomestici" in white, sans-serif font on a dark blue rectangular background.

– Wrap

The logo for WR@P, featuring the letters "WR@P" in blue, sans-serif font inside a green circular border.

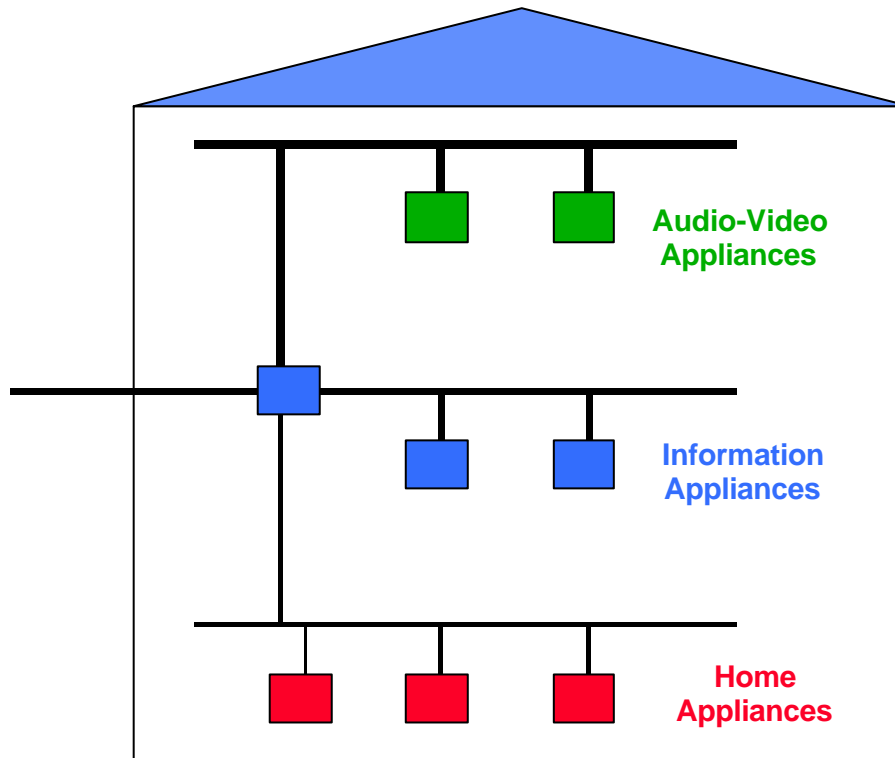
◆ www.e-pasta.org

Presentation

- ◆ Context of Home Connectivity
- ◆ Situation on Security
- ◆ Trust Value Chains
 - Example of Service on Demand Application (Pay-per-use)
- ◆ Trust through Evaluation and Certification
 - Common Criteria
- ◆ e-PASTA work
- ◆ Next steps

Presentation also applies to
vehicle connectivity

Smart Homes will be Connected



◆ Home control

- Lighting/shutters
- Heating Ventilating Air Conditioning (HVAC)
- Applications for Domestic Appliances
- Safety and Security
- Energy and Resource Management

◆ Communication

- Messaging
- Chats and Bulletin Broadcast
- PDA

◆ Infotainment

- Information
- Entertainment

Several Types of Access

◆ Local

- owner access is direct
- owner access is through home network

◆ Remote

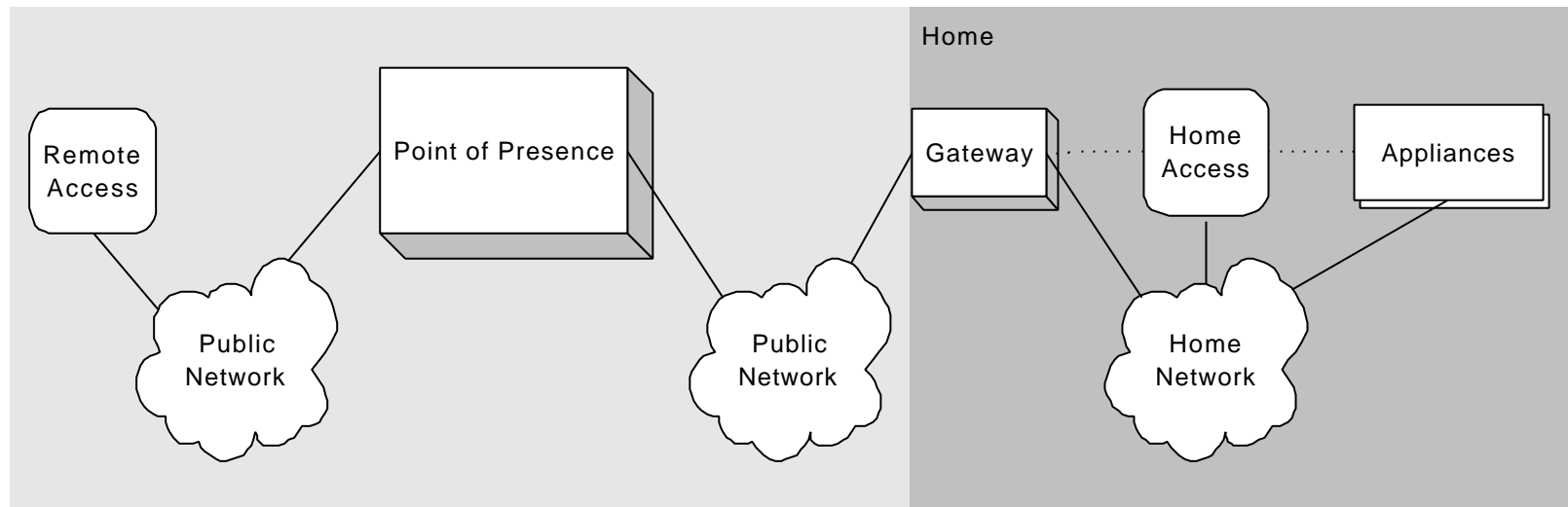
- owner access is through other network (e.g. ISDN)
- owner uses “virtual interface” (PDA, PC, etc.)

◆ Delegated

- third party access through other network

Typical Connectivity Infrastructure

- ◆ Remote Access
- ◆ Point of Presence
- ◆ Access Network
- ◆ Gateway
- ◆ Home Network
- ◆ Appliances
- ◆ Local / Home Access



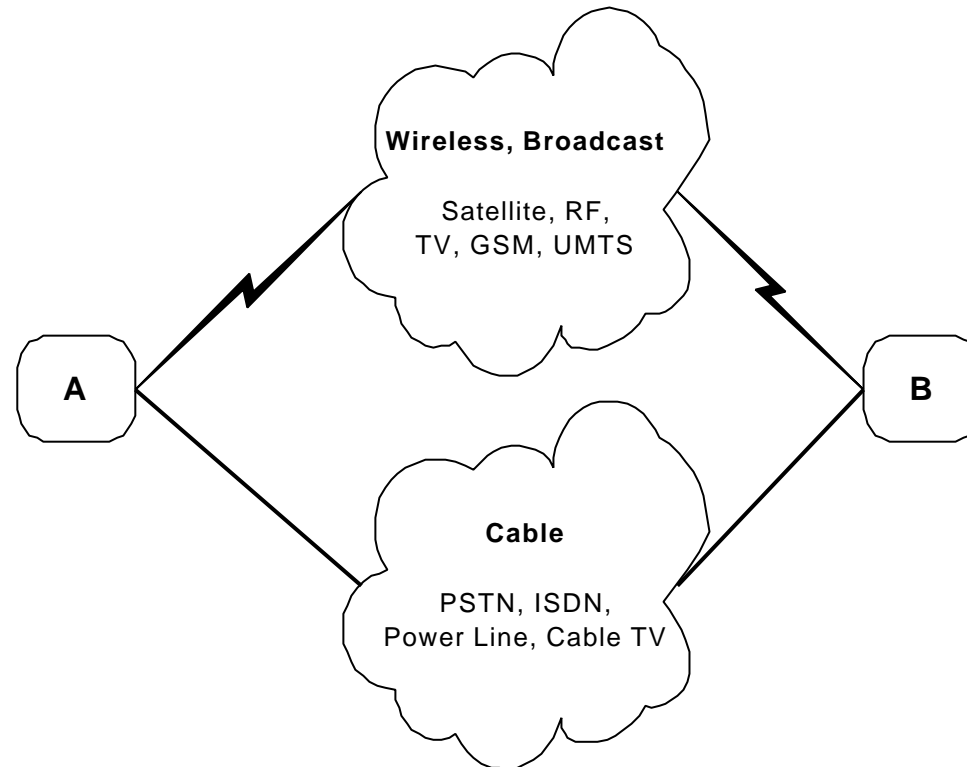
Typical Home Access

◆ Dial-Up

- PSTN
- ISDN
- GSM

◆ Permanent

- xDSL
- Cable



Situation on Security of Access

- ◆ Connectivity systems are complex
- ◆ No real approach for security of access
 - not enough experience on this
 - lack of awareness
 - not all or few networks provide cryptographic mechanisms
- ◆ We need a trusted value chain
- ◆ Which guarantees that the right level of security is deployed

Trust Value Chains

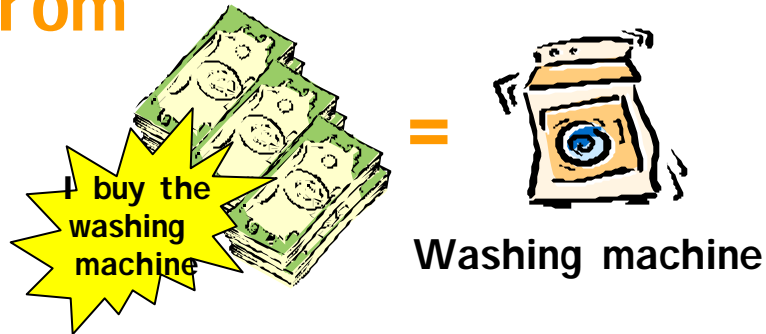
Example of Merloni Pay-Per-Use Application



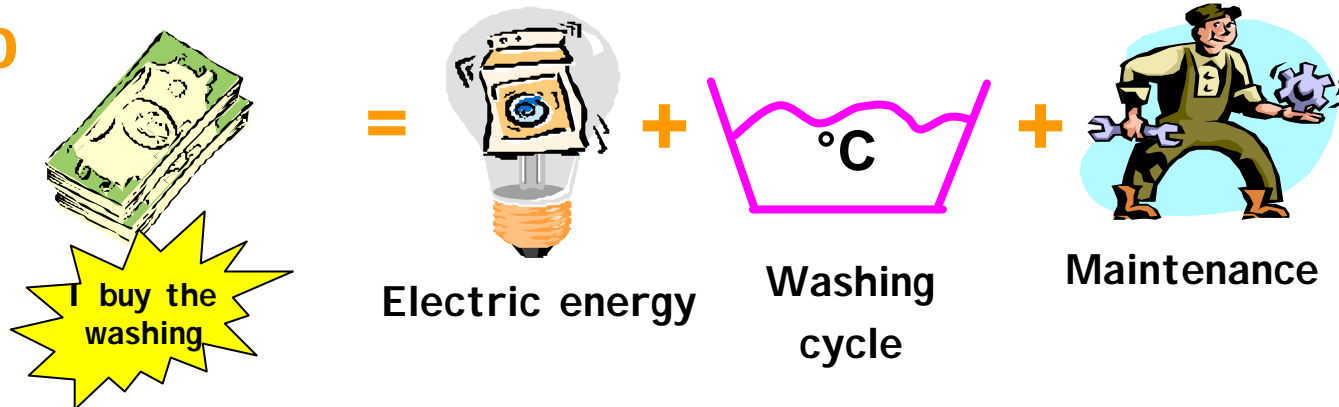


From the washing machine to the washing

From

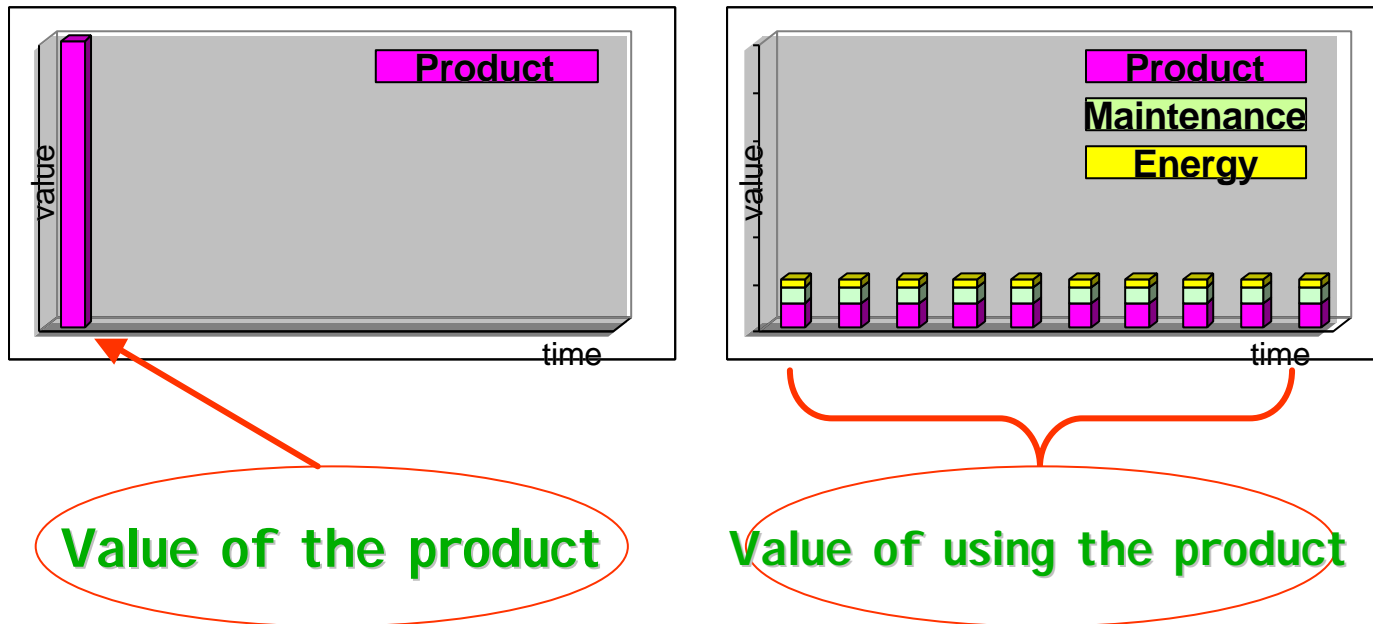


To





From the product to the use of the product



The traditional logic of purchasing a new washing machine is replaced by a modern and smart appliance rental that enables the consumer to pay for each use, i.e. per each washing load.

The **PayXUse** offer

Front door delivery

Recovery of the old appliance

Installation and full testing

5 years full warranty all included

Tele-diagnosis and Tele-allarm

48 hours technical assistance

Phone assistance 7 on 7 days

News letter with washing cycles and better use advices



First of all: a new generation of smart appliances



Capable to generate and memorize data:

- Diagnostics
- Consumption
- Historic
- Statistic

And ... ready to communicate with the outside world

The interface man - machine

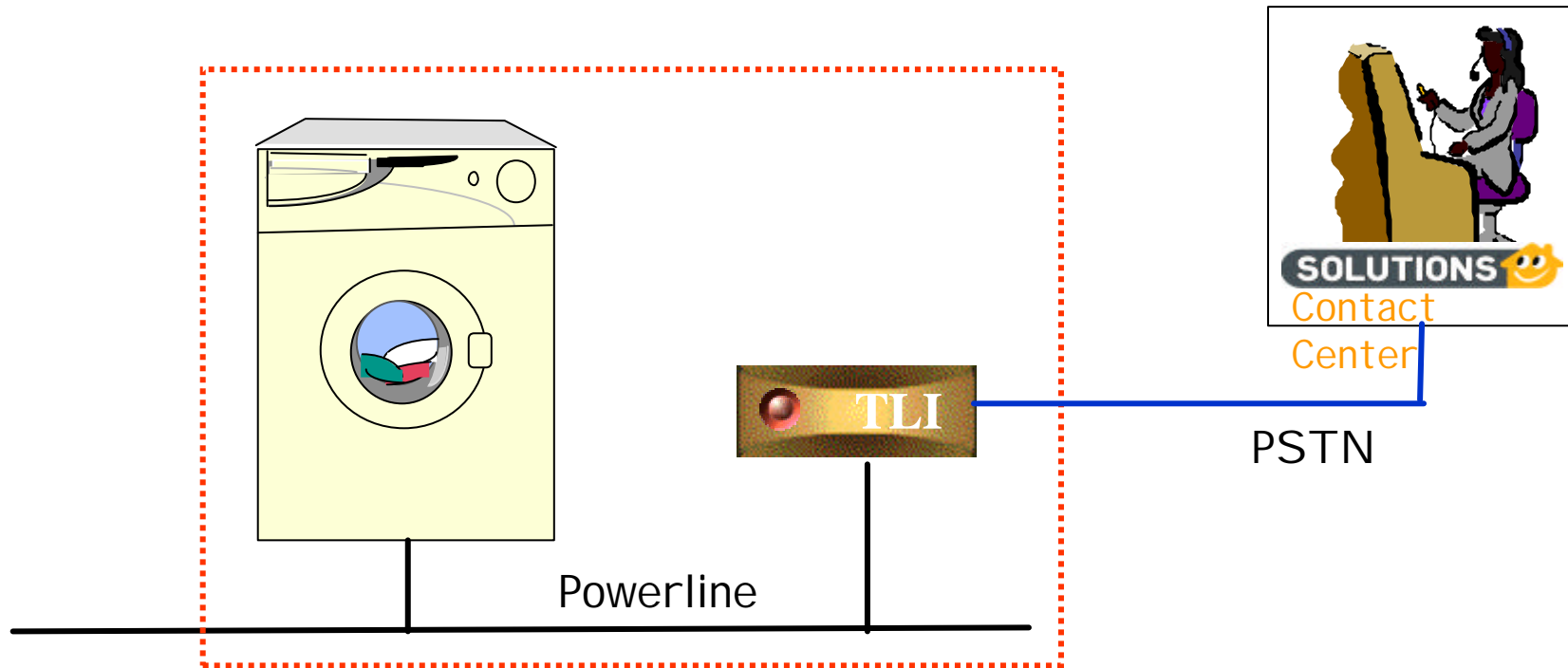
A multifunction display allows access to the PXU functions:

- Residual credit
- Cost of the last washing
- Access to promotion
- Date of the last recharge
- Messages



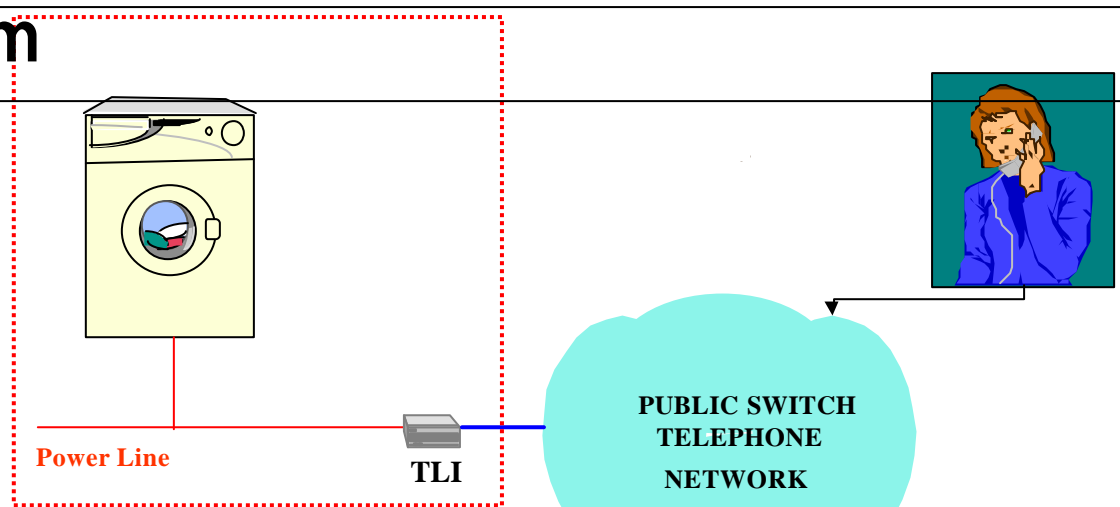
After each washing cycle the appliance display will inform the consumer about the amount of credit left. When the credit is finished, the appliance will connect automatically to the toll-free number for re-charge. The energy consumed for each load will be automatically deducted from the energy bill.

Indoor system



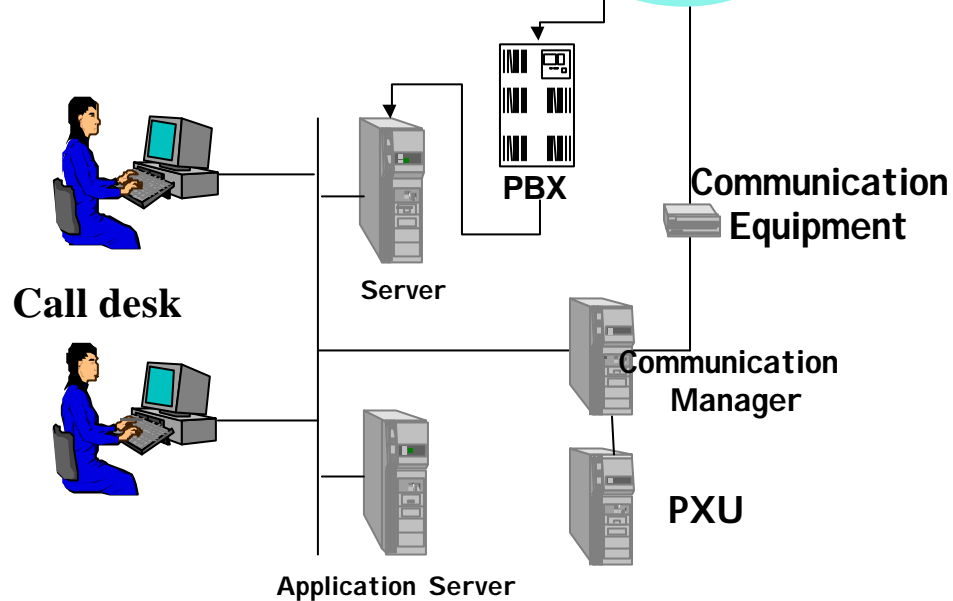
- Standard model: Ariston Dialogic AD 1600
- Node for power line communication assembled at the installation transform the WM in a PayXUse version
- Telelink: modem power-line / telephone-line

Outdoor system

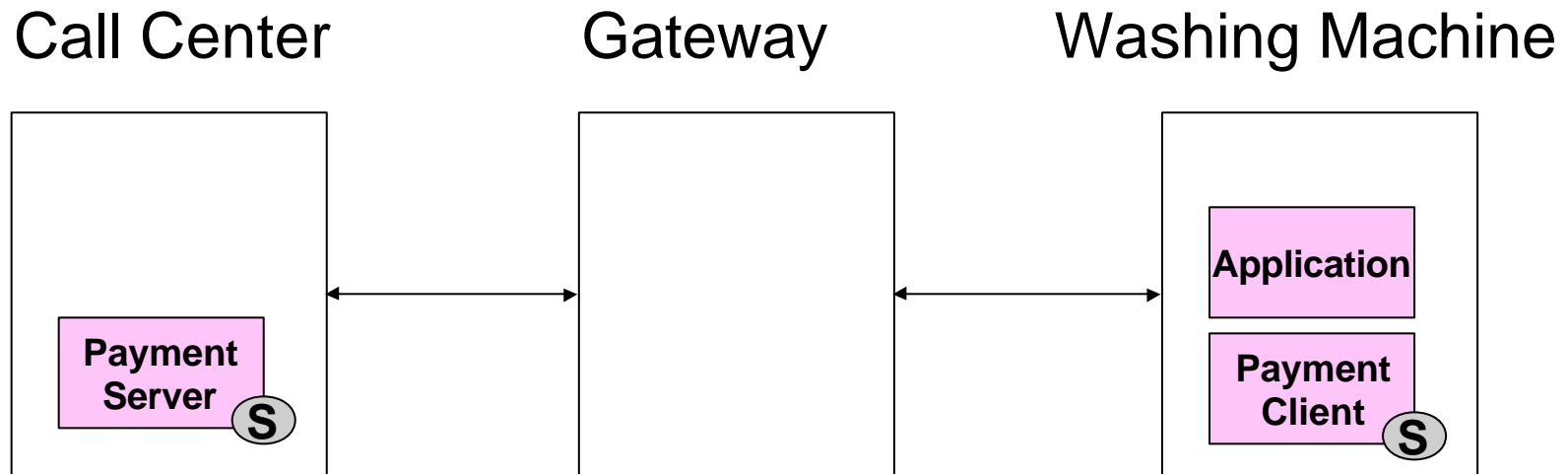


SOLUTIONS Contact Center

- Recharge management
- Promotion management
- Tele-diagnosis
- Tele-alarm
- SMS messages
- Statistical data recovery

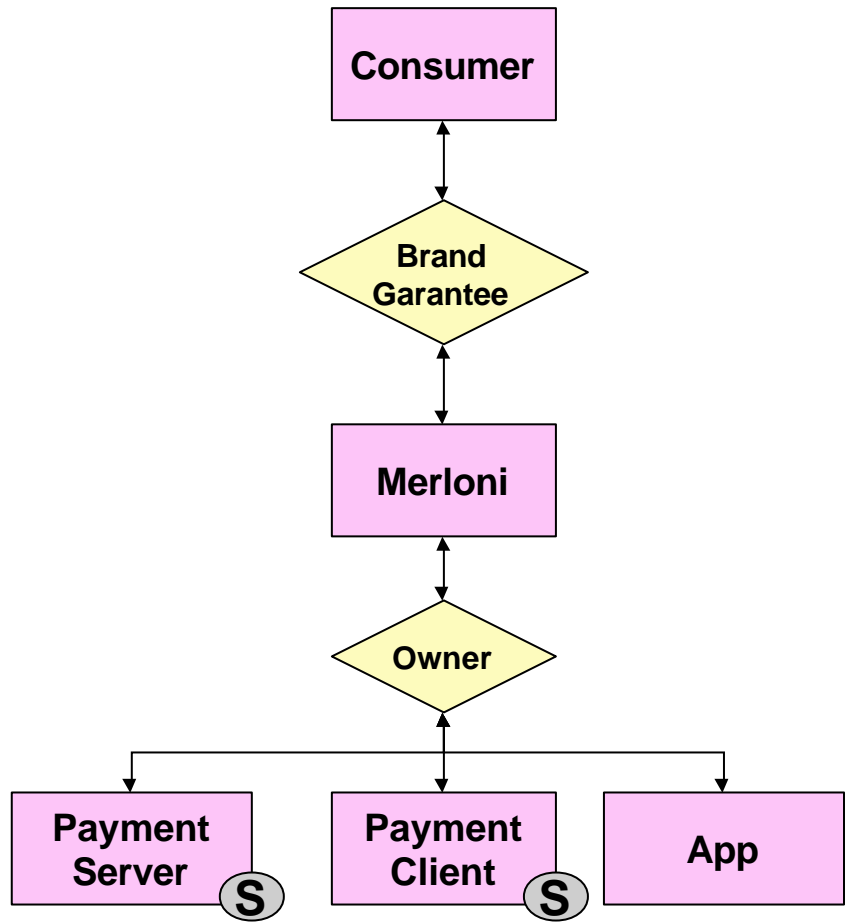


Merloni PPU Configuration



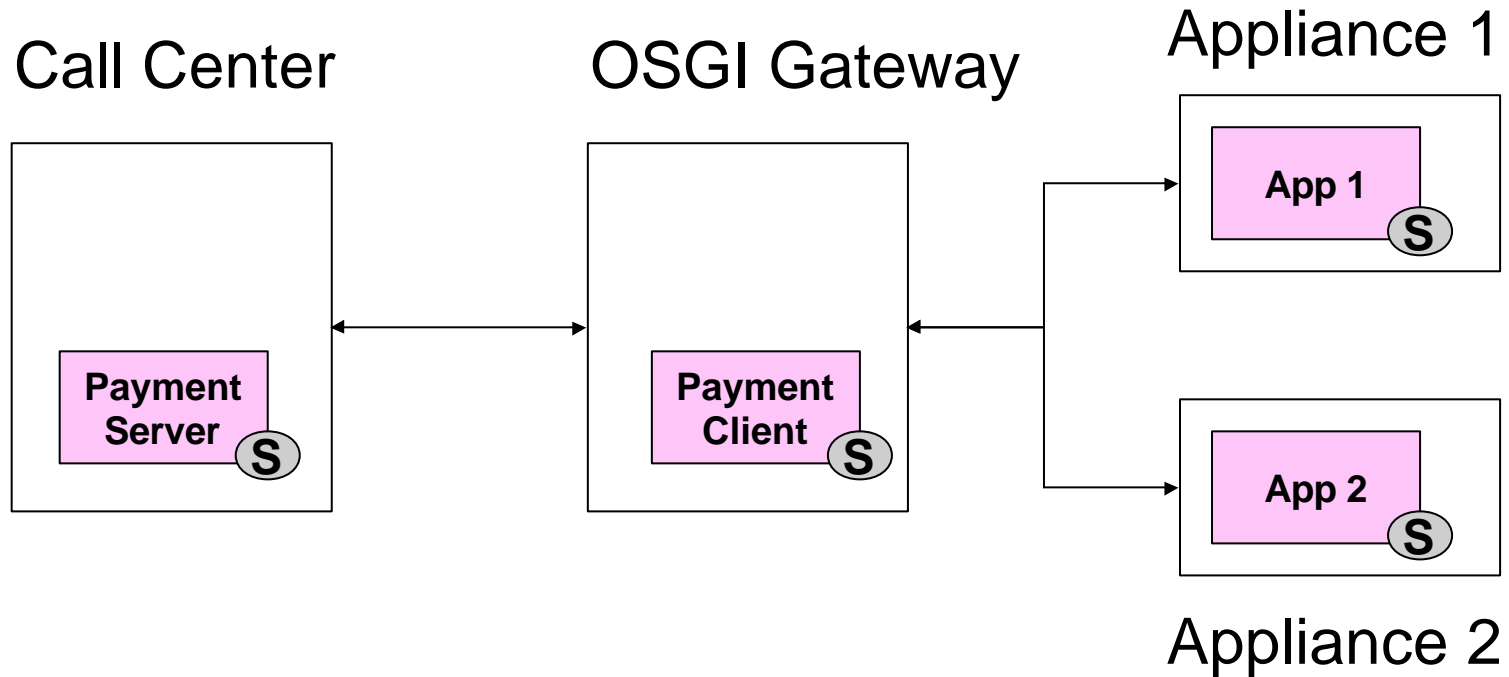
S Security component

Trust Value Chain



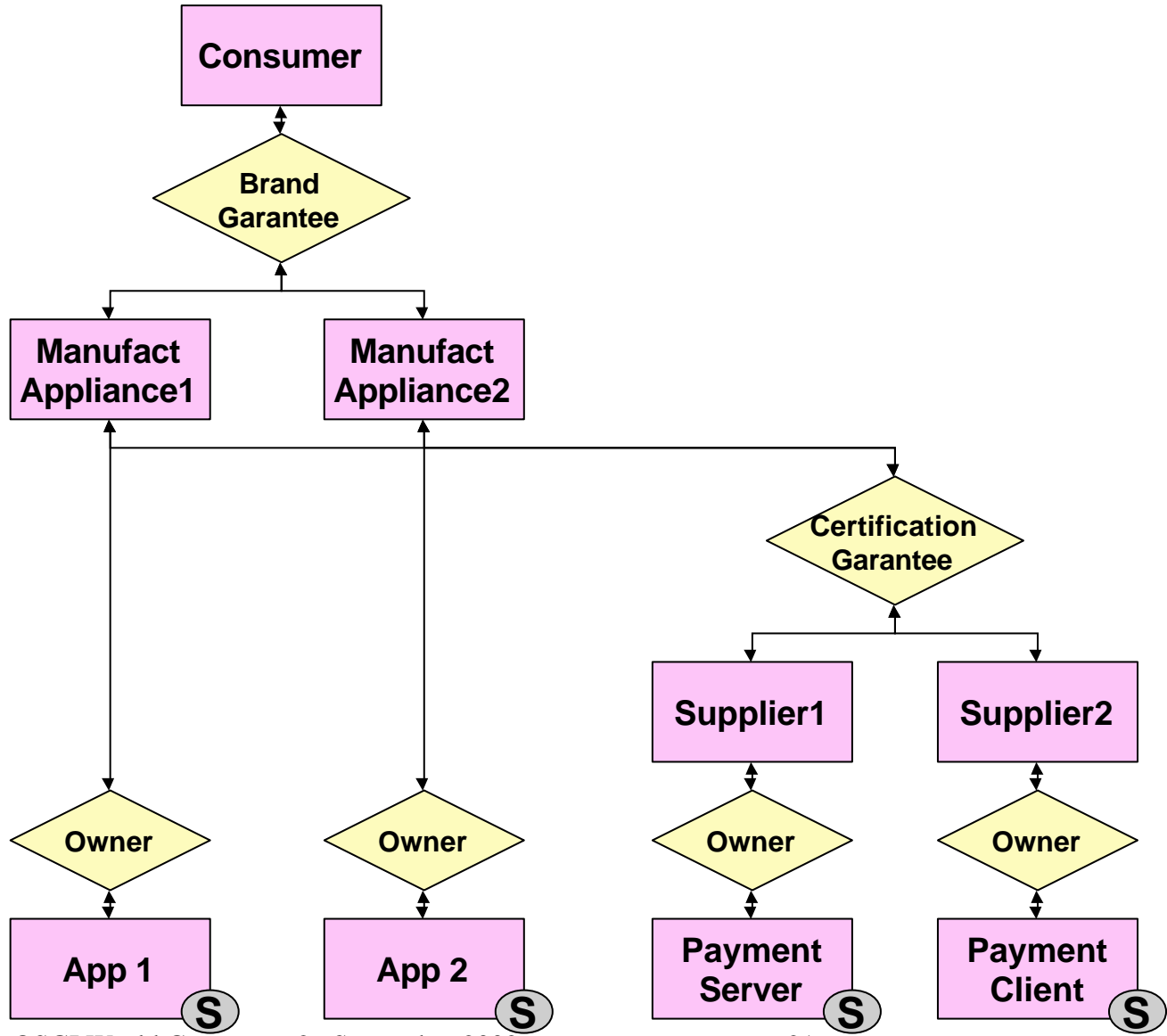
S Security component

Future Service-on-demand Applications



(S) Security component

Trust Value Chain



S Security component

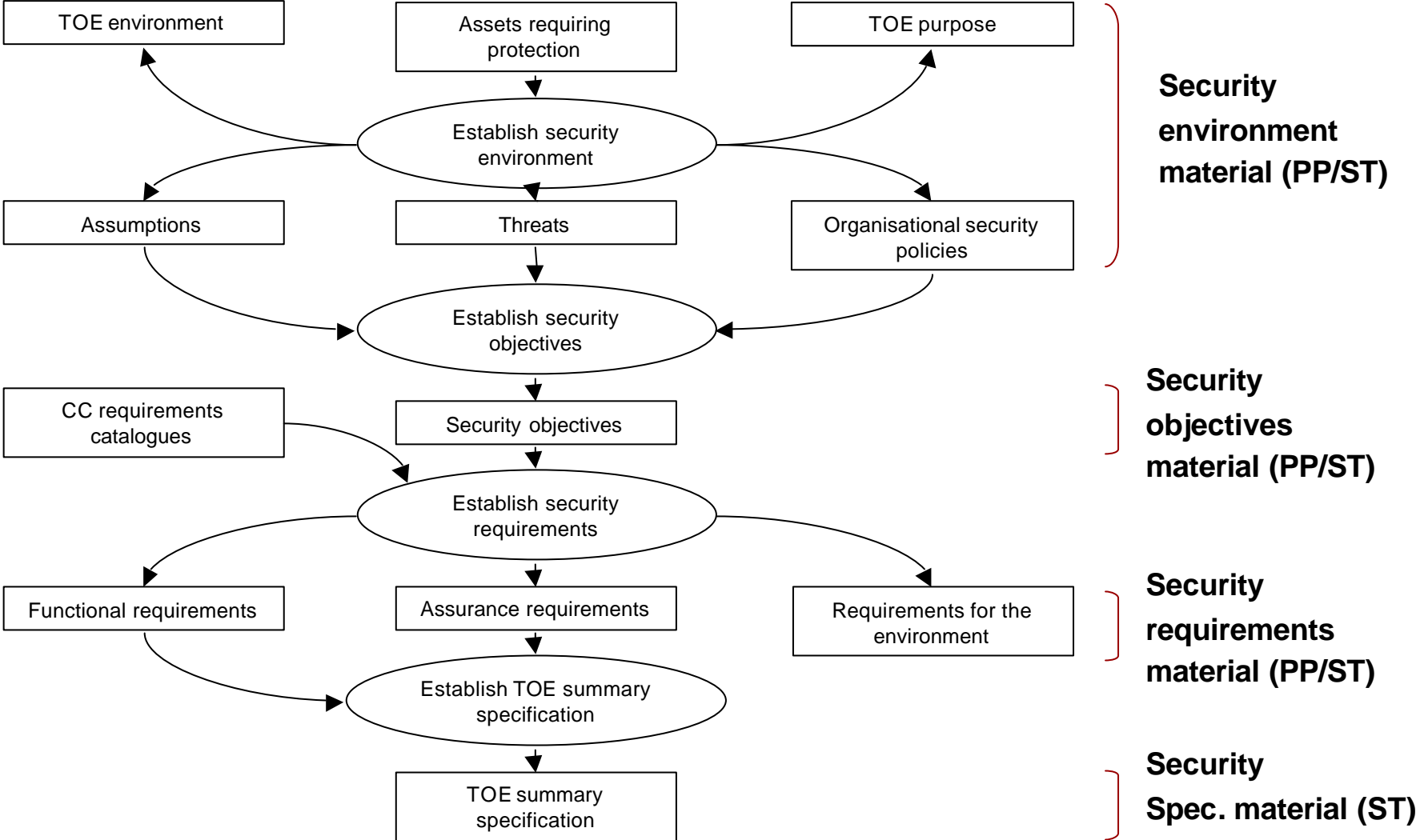


Trust through Evaluation/Certification

◆ Use Common Criteria

- ISO standard (ISO 15408)
- Standard for security evaluation
 - Used for an increasing number of products (e.g. smart cards, terminals, firewalls, ...)
- Evaluation Assurance Level
 - EAL1: functionally tested
 - EAL2: structurally tested
 - EAL3: methodically tested and checked
 - EAL4: methodically designed, tested and reviewed
 - EAL5: semiformally designed and tested
 - EAL6: semiformally verified design and tested
 - EAL7: formally verified design and tested

Common Criteria Implies an Analysis Methodology



Common Criteria Imply Templates

- ◆ Notion of Protection Profile
- ◆ Reuse of Security Analysis

e-PASTA Work

- ◆ Validate approach
- ◆ Work on 3 generic configuration
 - local operations
 - e.g. start the washing machine in the home
 - remote operations
 - e.g. remote diagnosis
 - service on demand
 - e.g. pay per use
- ◆ Demonstration of security components. Technology used
 - ISO15408 for security analysis
 - Simple gateways and OSGi gateway
 - EHS home networking

Example of Conclusions on Local Operation

- ◆ Impact on underlying home network
 - Authentication needed
 - Encryption not needed (but could serve as authentication)
 - Denial of service protection not needed
 - Non replay needed
 - Secure initialization of keys needed

Conclusions

- ◆ Analyse Security Needs
 - e.g. using Common Criteria
- ◆ Define Security Architectures
- ◆ Standardise Security Components when Needed
- ◆ Create Trust Value Chains

Conclusions apply for vehicle connectivity