



OSGi™ Alliance

2005 Developer Forum & World Congress

*Paris,
France*





*Paris,
France*

Using OSGi for Secure Service Discovery

Slides available at <http://godot.be/slides>



Presentation Structure

- TEAHA
- TEAHA Approach for seamless interworking
- Using OSGi and Service Discovery
 - OSGi and TEAHA Features and Needs
 - OSGi vs. TEAHA Registration
 - TEAHA Security Modules
 - Architecture for Service Discovery and Security



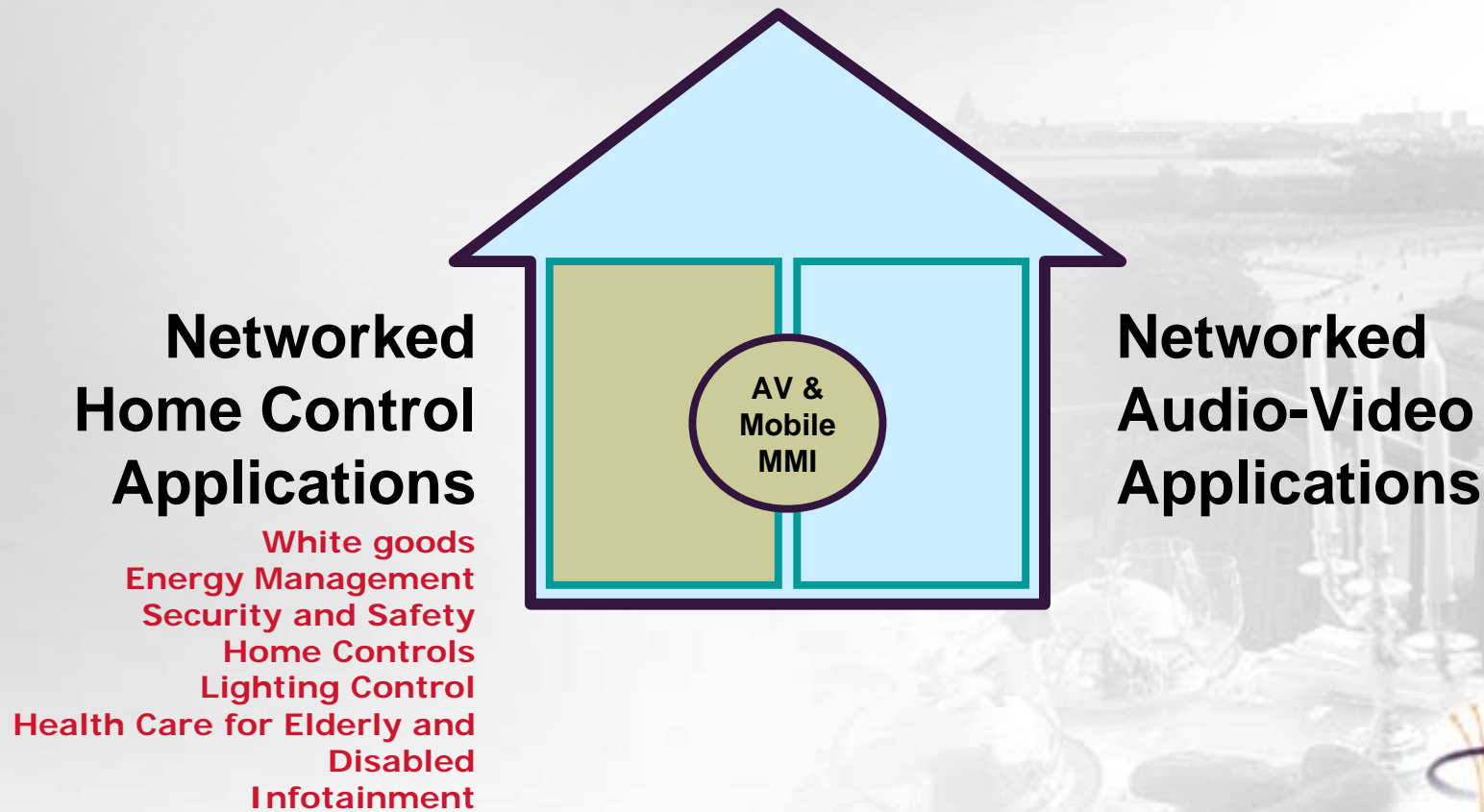
The TEAHA Consortium

- Leading manufacturers and service companies
- Technology and market research companies and Universities
- Industry groups

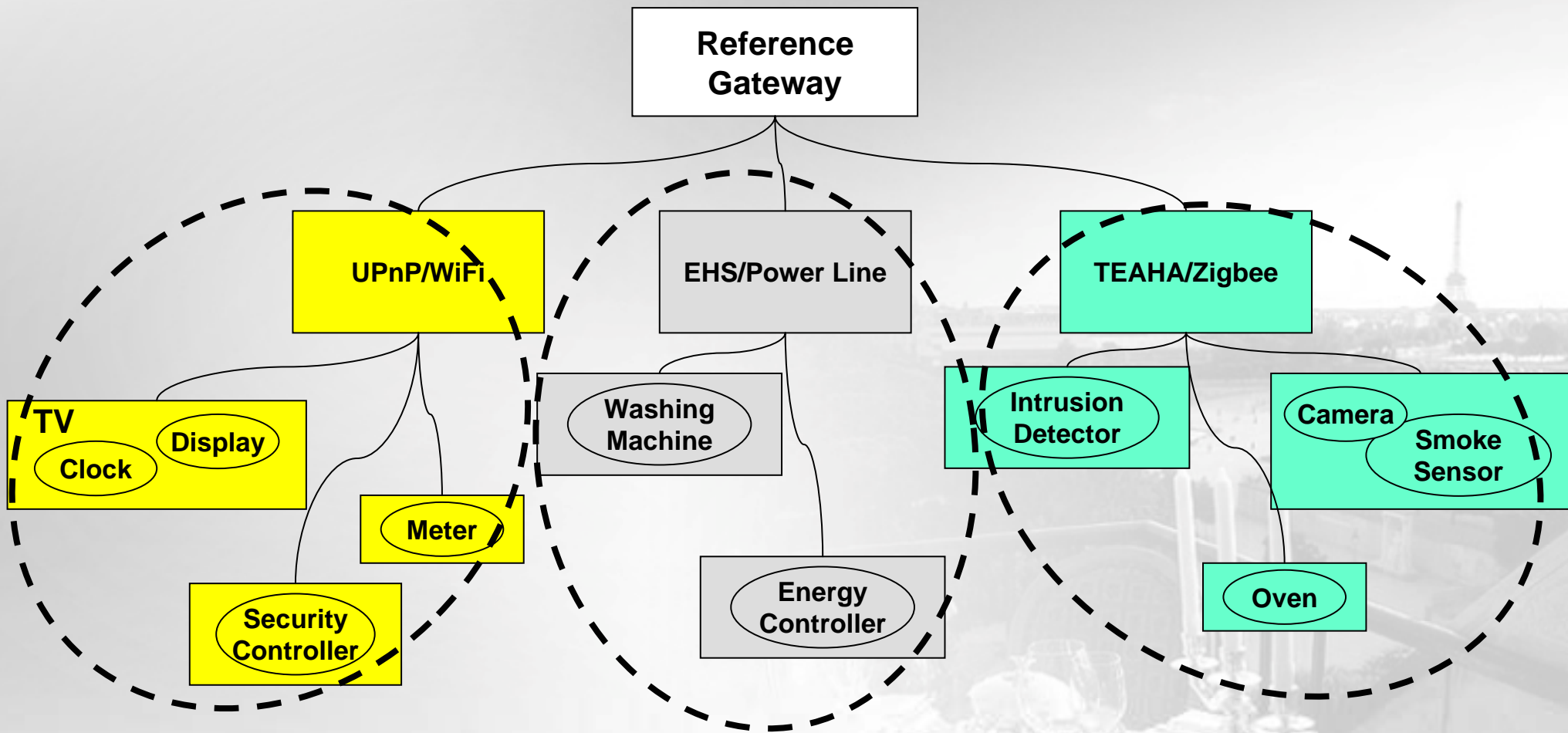


TEAHA Mission

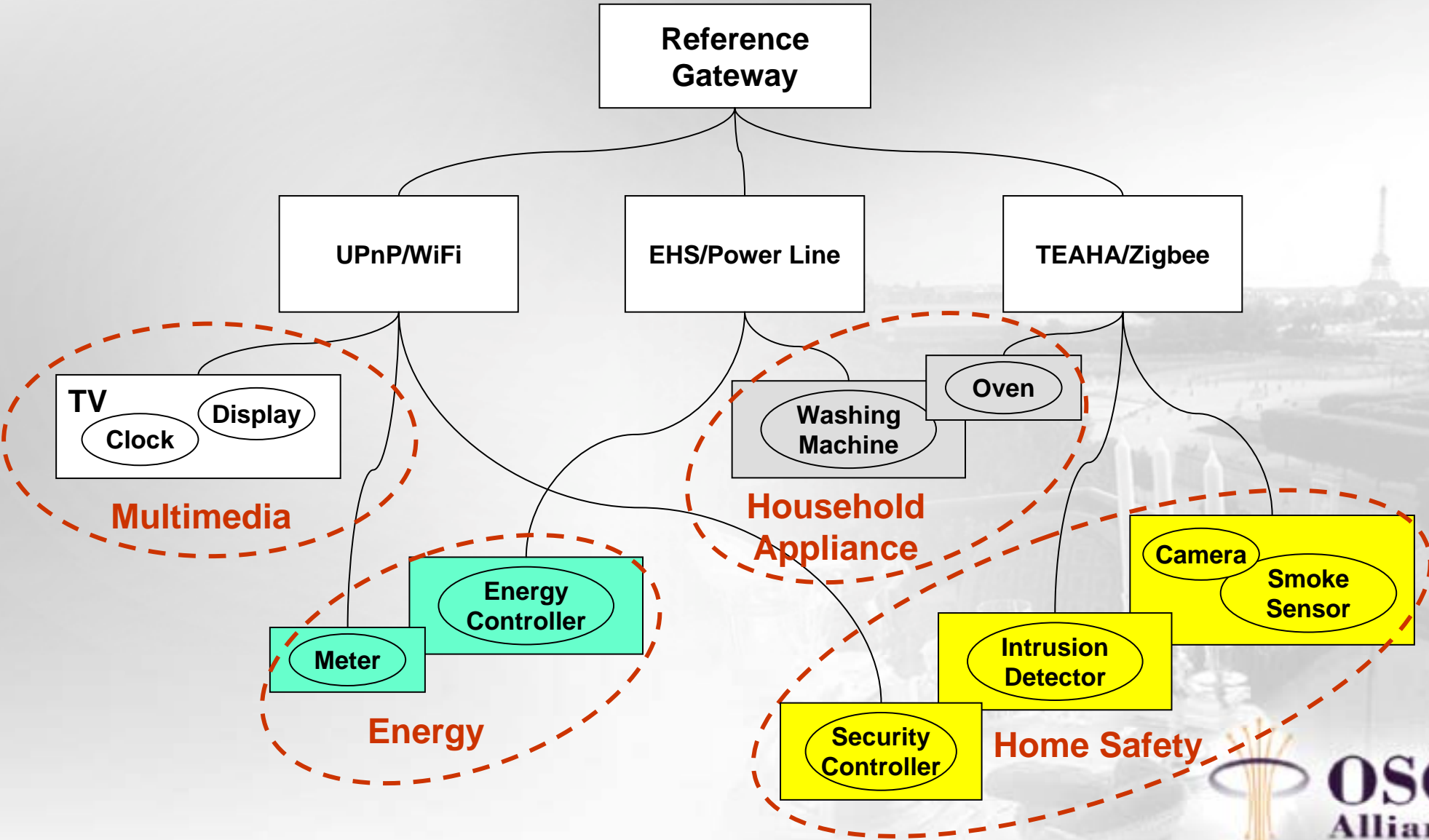
- Specify an open, secure framework for seamless interoperability and interworking



TEAHA Has Technology Clusters



TEAHA Has Business Clusters



Facts about Stakeholders

- Stakeholders in a business cluster
 - Are competitors
 - Share the same culture
 - Are involved in the same value chain
 - Would prefer to abstract away from technology clusters
- Stakeholders in different business clusters
 - Do not understand each other
 - Do not need to understand other clusters
 - Have different cultures, value chain, life cycle



Approach for Seamless Interworking

- There are issues in supporting the mixing of different types of clusters
 - Technology clusters
 - Business clusters
 - ...
- TEAHA focuses on solving those issues



Seamless Interworking Unsolved Problems

- **Service Discovery**

- Can a device in one technology cluster discover a device from another technology cluster?
- Can these devices use one another's services?

- **Secure Communication**

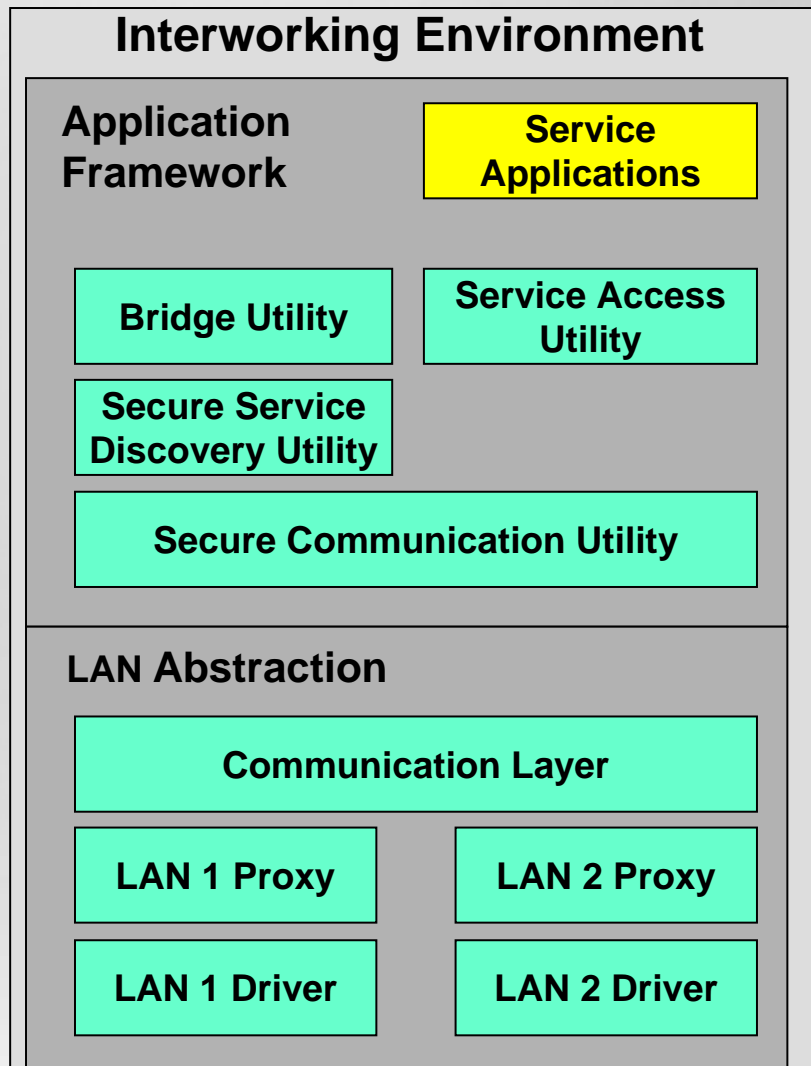
- Can a device in one technology cluster communicate securely with a device from another technology cluster?
 - Authenticity: No faked devices!
 - Confidentiality: No eavesdroppers!
 - Trusted/Registered devices: No intruders!

- **Security Policy**

- Can a business cluster be protected from other clusters?
 - Policy enforcement: is a multimedia application allowed to access security system information?



Abstract Architecture

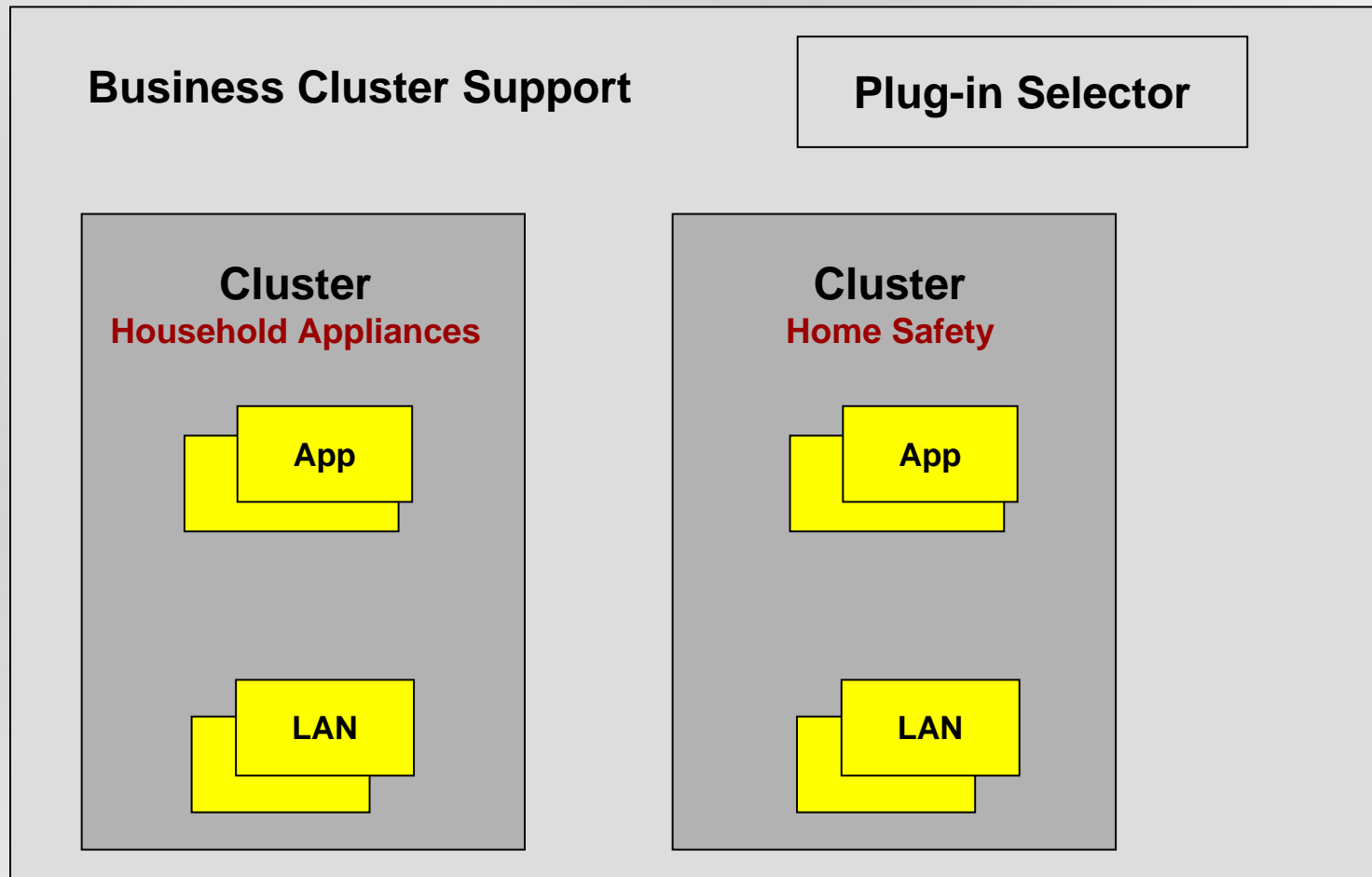


Business Cluster Support

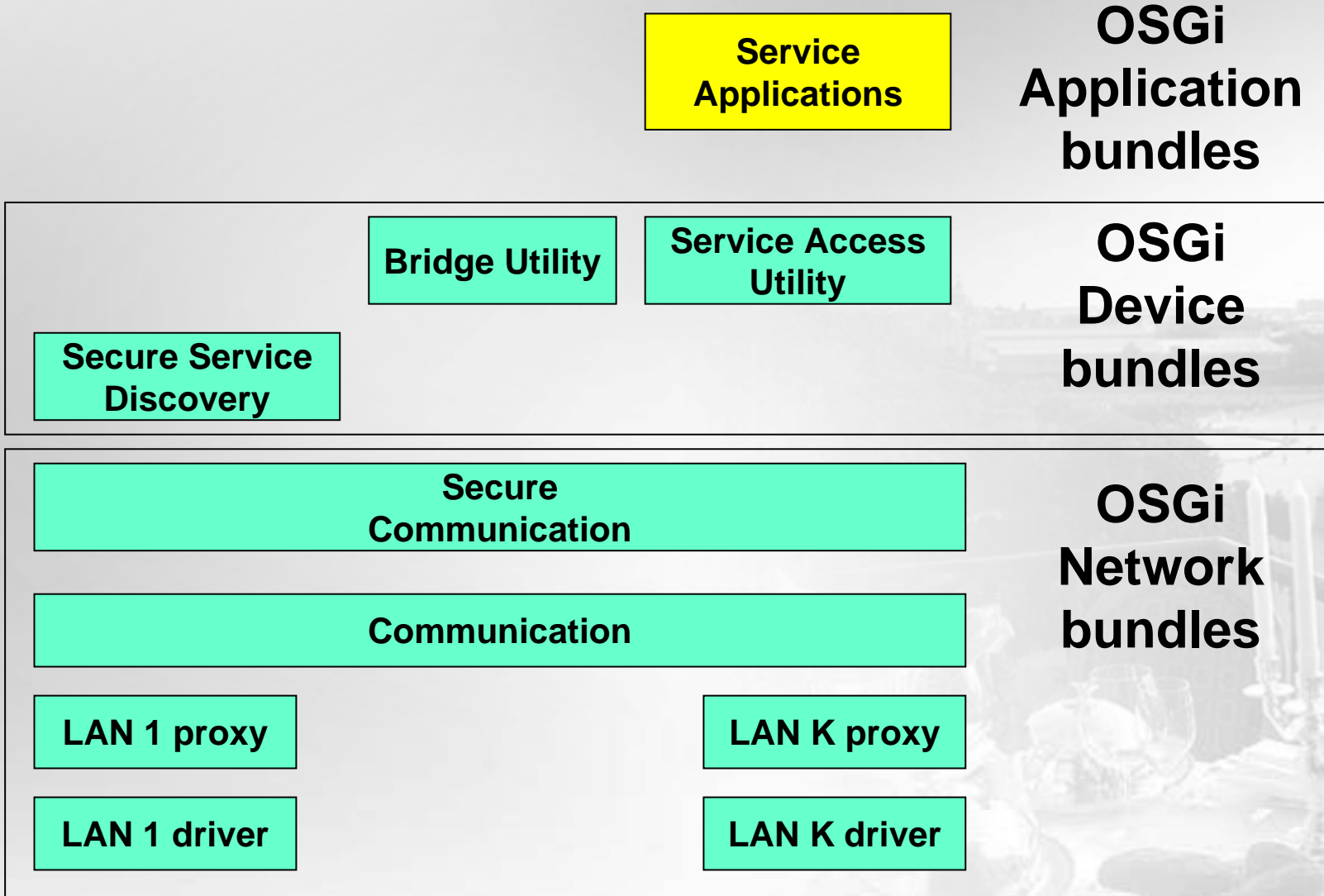
Security Support



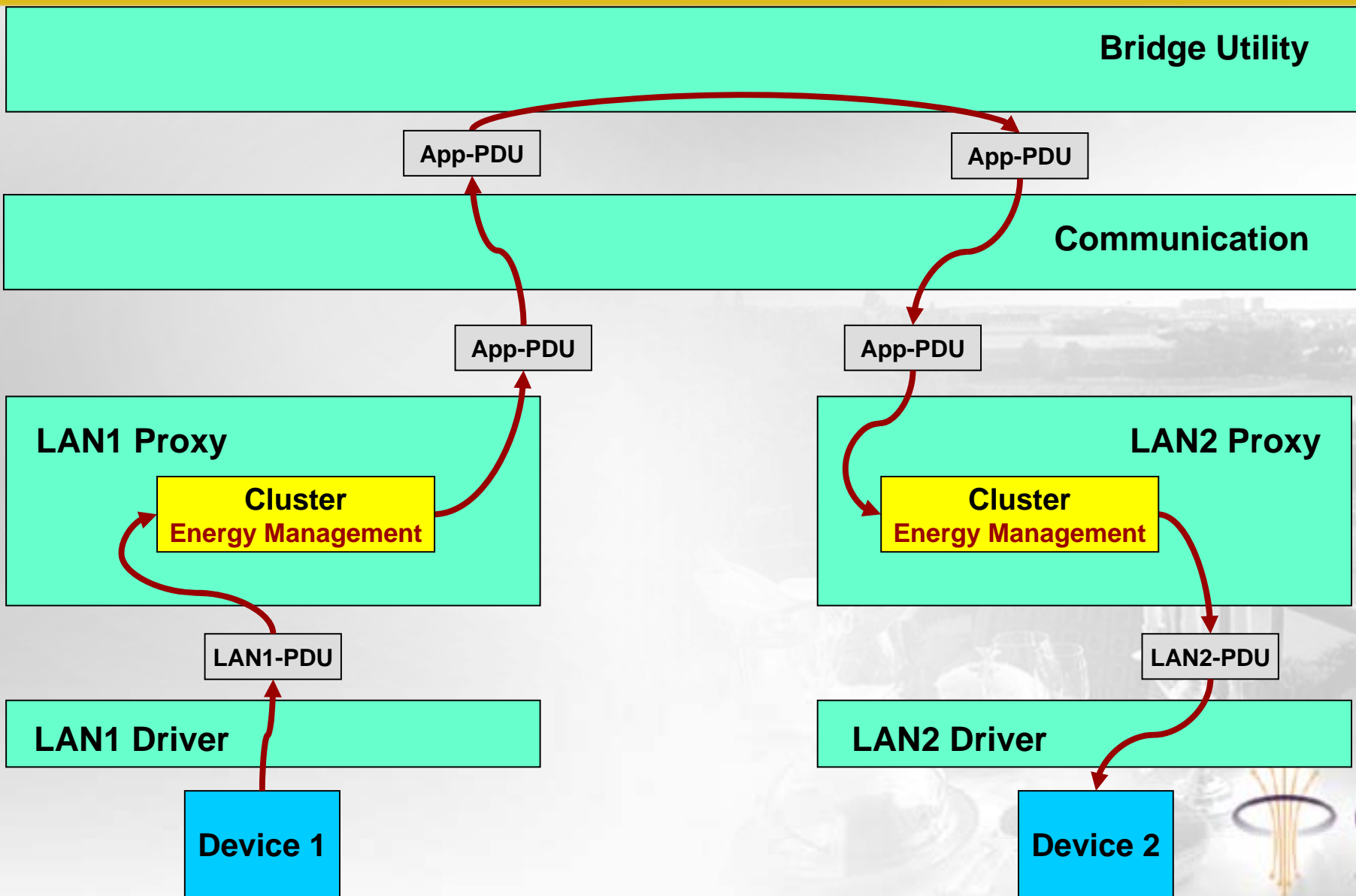
TEAHA Business Cluster Support



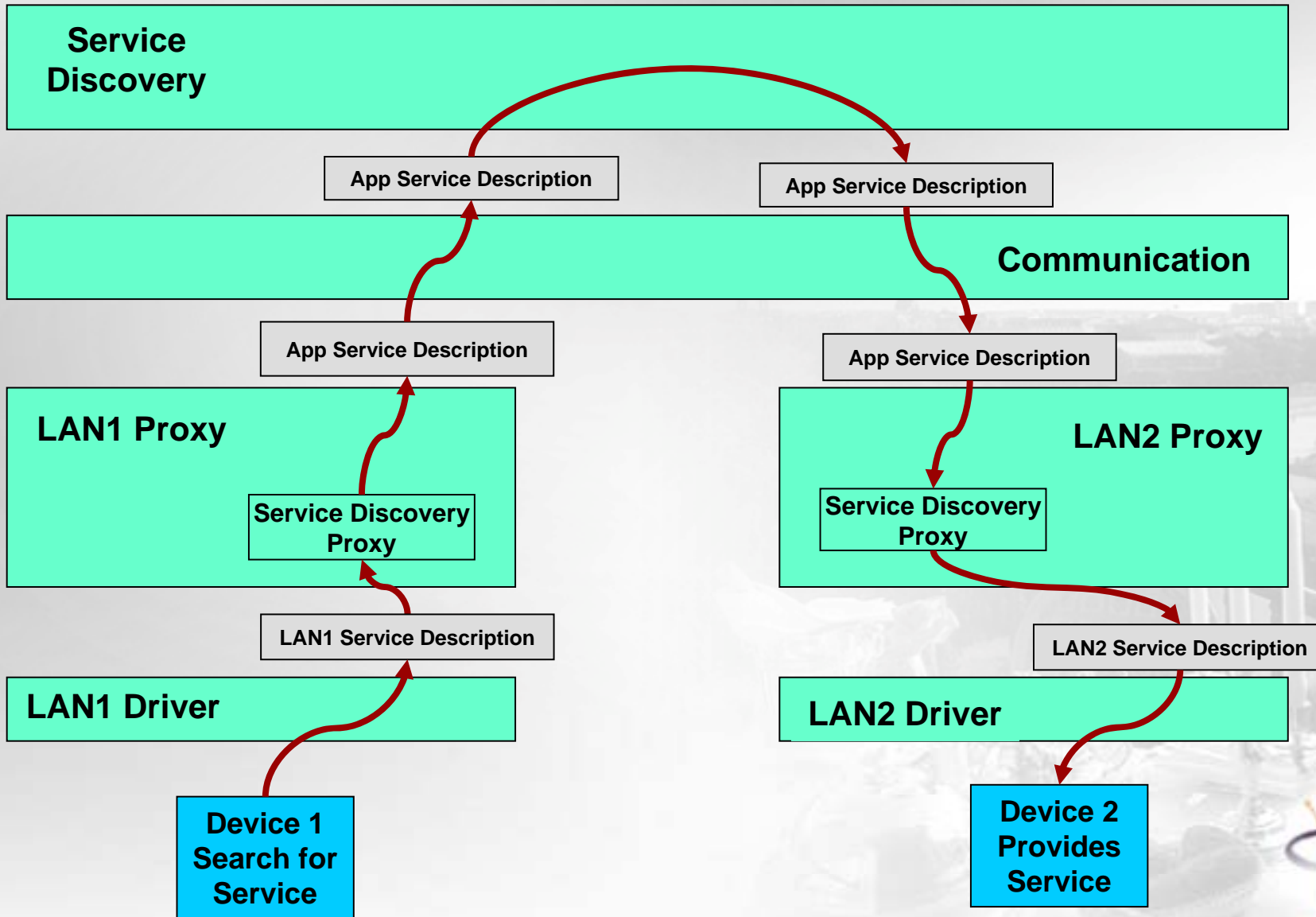
Mapping on top OSGi



Seamless Interworking in Action



Service Discovery in Action



OSGi and TEAHA Features and Needs

- OSGi

- Targets wide application area
 - Embedded and dedicated devices
- Provides *specifications* for a service-oriented architecture
- Defines a computing environment for *networked services* and is
 - Standardized
 - Component oriented
- Embodies into a *service platform* with secure execution environment
- Not supported
 - Device authentication
 - Platform management protocol

- TEAHA

- Targets
 - *Home applications* and
 - *Relationships* with A/V applications
- Provides specifications for a global home platform, focuses
 - Openness
 - Secure communications
 - Interoperability
- Defines a middleware platform for seamless interworking of
 - Wide variety of appliances available in the home environment
 - Heterogeneous networks
- Embodies into a logical TEAHA device
- No open issues ☺



OSGi vs. TEAHA Registration

- OSGi

- Registration of services in the OSGi platform
- Registration with the local OSGi registry
 - Code/Bundle signing
 - Policy-based
- OSGi services use one another's services in the OSGi platform

- TEAHA

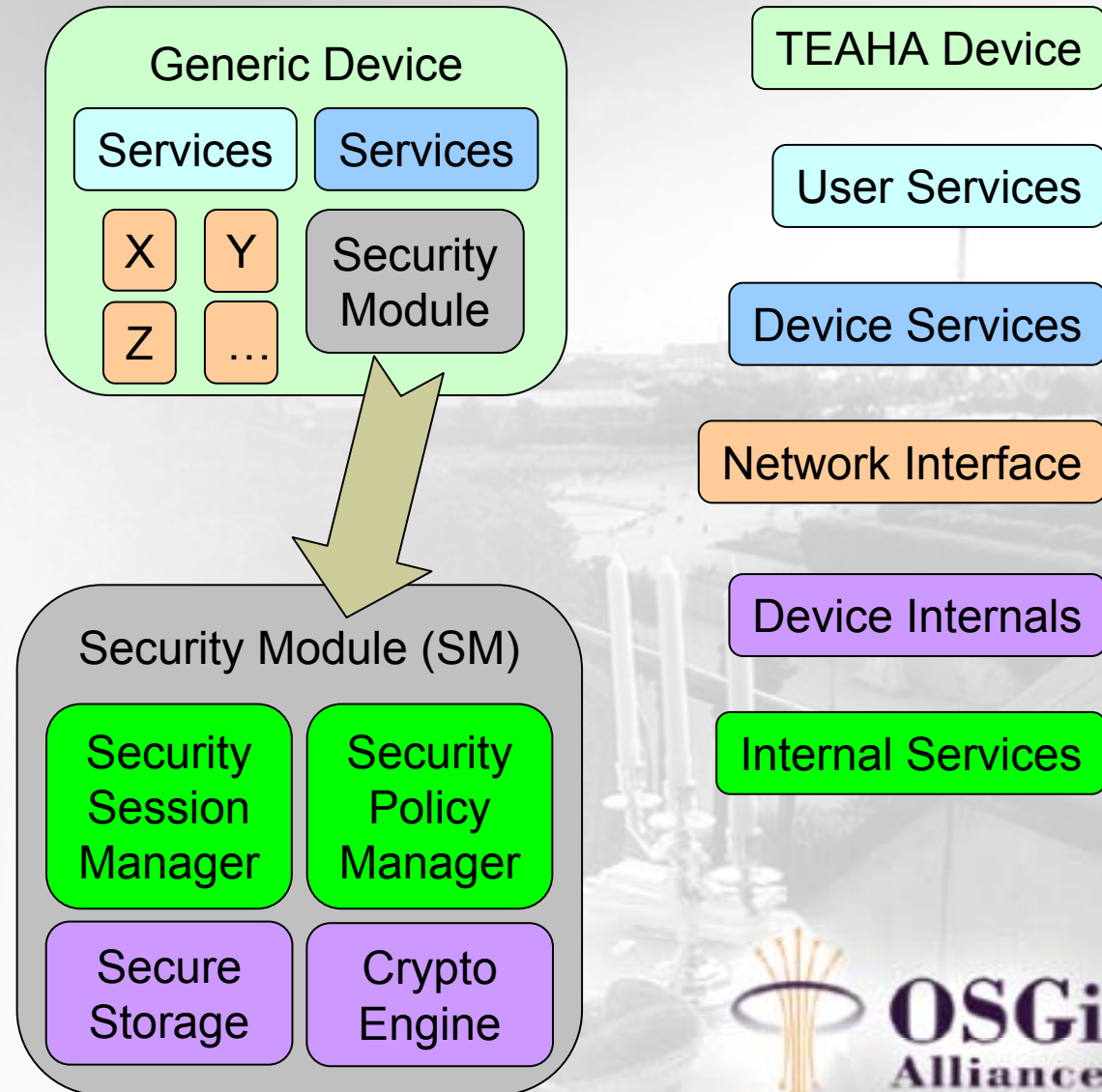
- Registration of TEAHA devices in the wide home environment
- Device registration requires touch & play
 - Secure zero configuration
 - Policy-based
 - Unregistered devices cannot use registered devices' services
- Device-Device service usage



TEAHA Devices and Security Modules

Key Features of a Security Module:

- One SM per Device
- SM = OSGi bundle
- SM offers services to other bundles
- SM initialized by manufacturer
- Initialized SM ready to be used
- Combination of hard- and software
 - Hardware → Non-cloneable
 - Software → Risk for cloning
- Provide true strong authentication
- Secure communications rely on SM
 - Insecure
 - Authenticity
 - Confidentiality
 - Secure = Auth. + Conf.



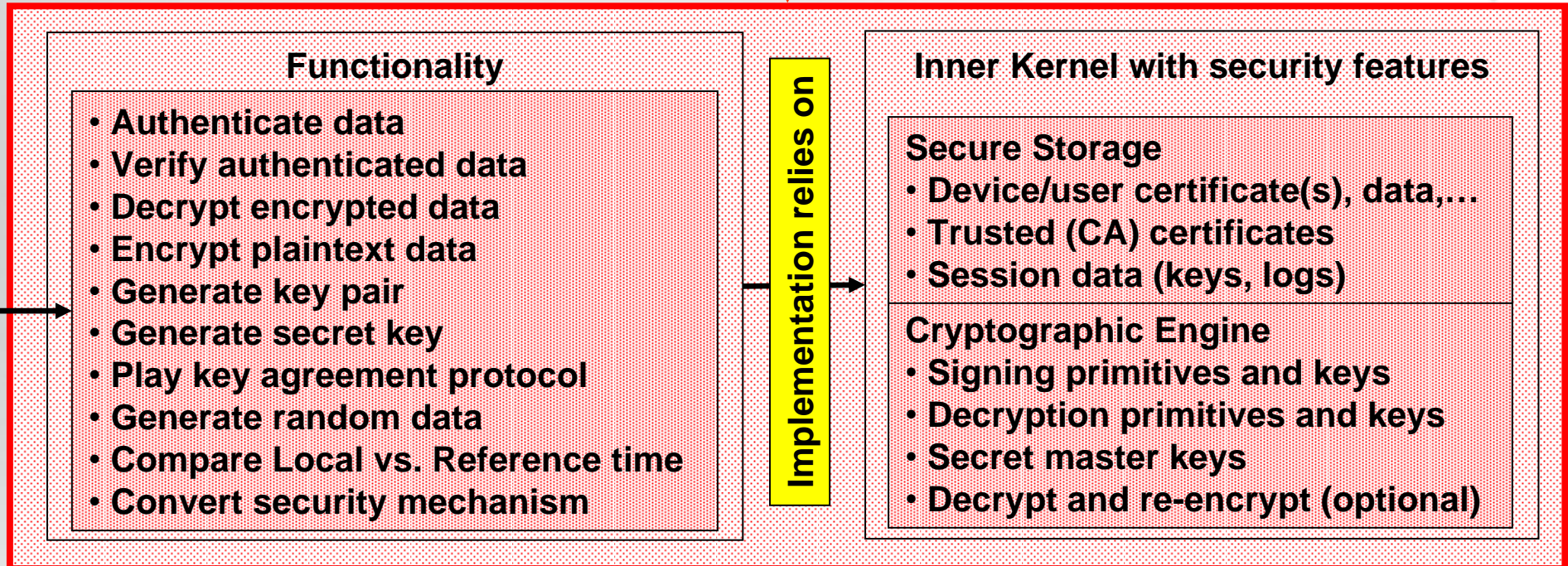
TEAHA Security Module Services

Can be used for

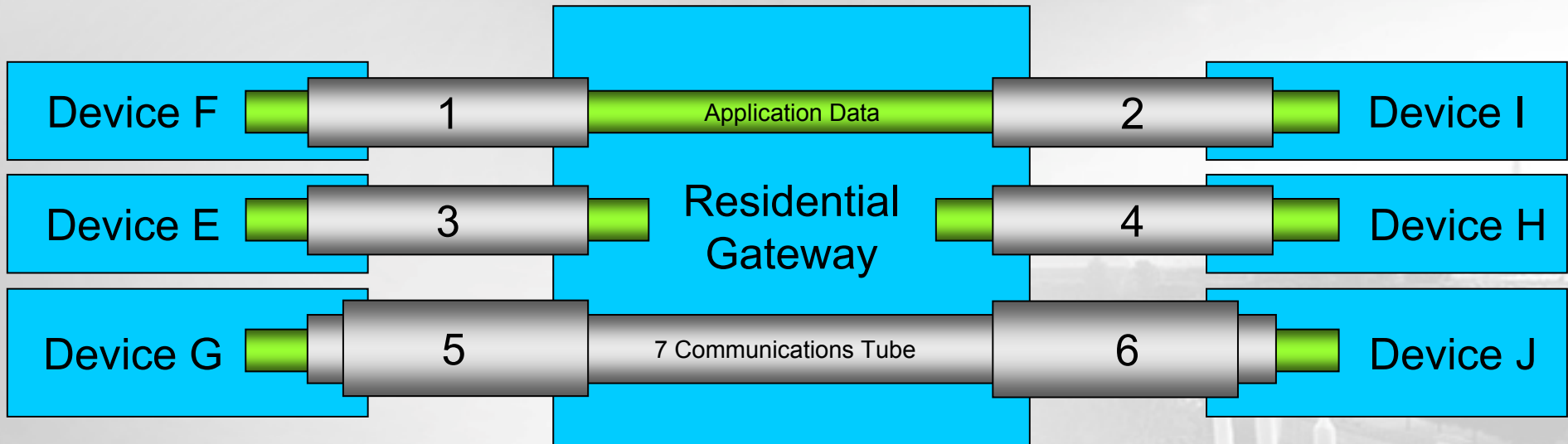
- Applications
- Secure Communications

API

Sealed in a tamper evident enclosure, e.g., Integrity-protected log file or database, hardware enclosure,...



TEAHA Secure Communication Types



4 Security levels:

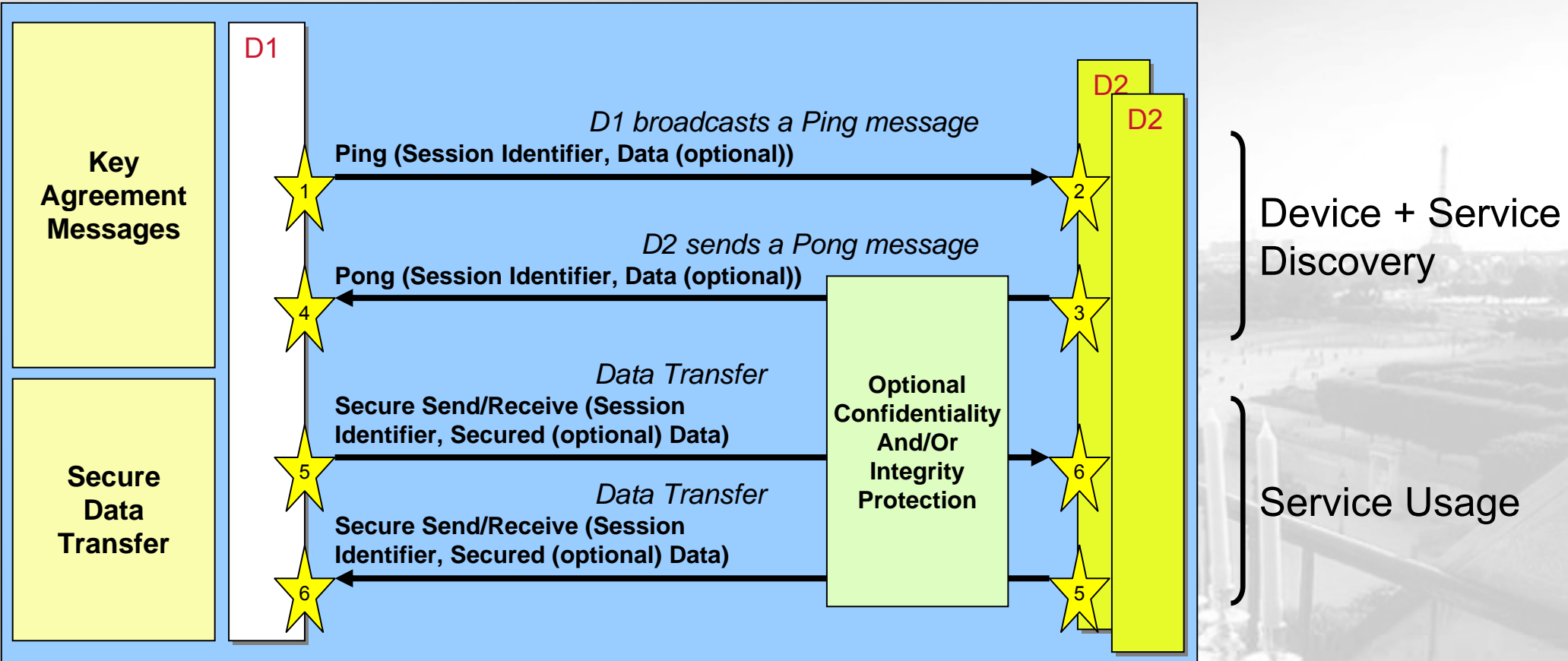
- Protecting Integrity and/or Confidentiality

Security parameters (keys):

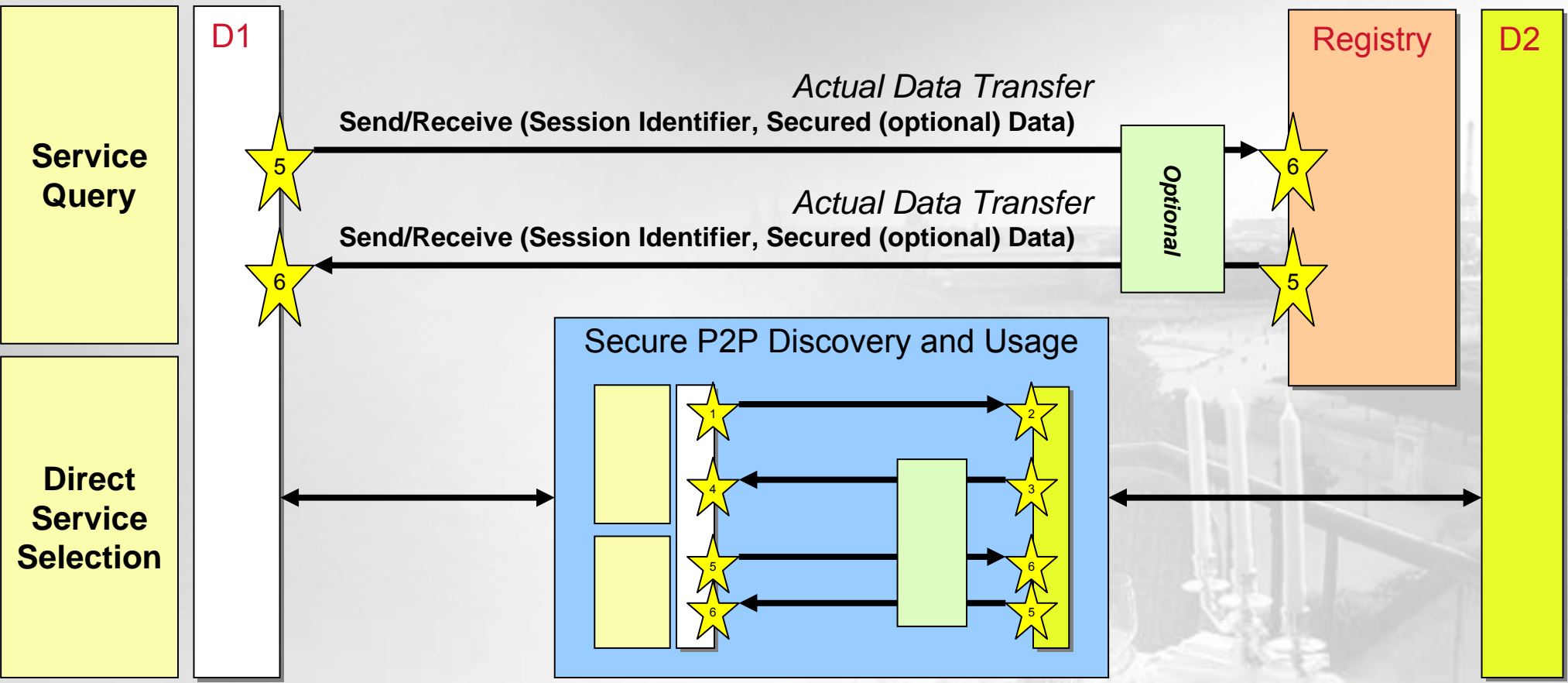
- Agreed on during device discovery



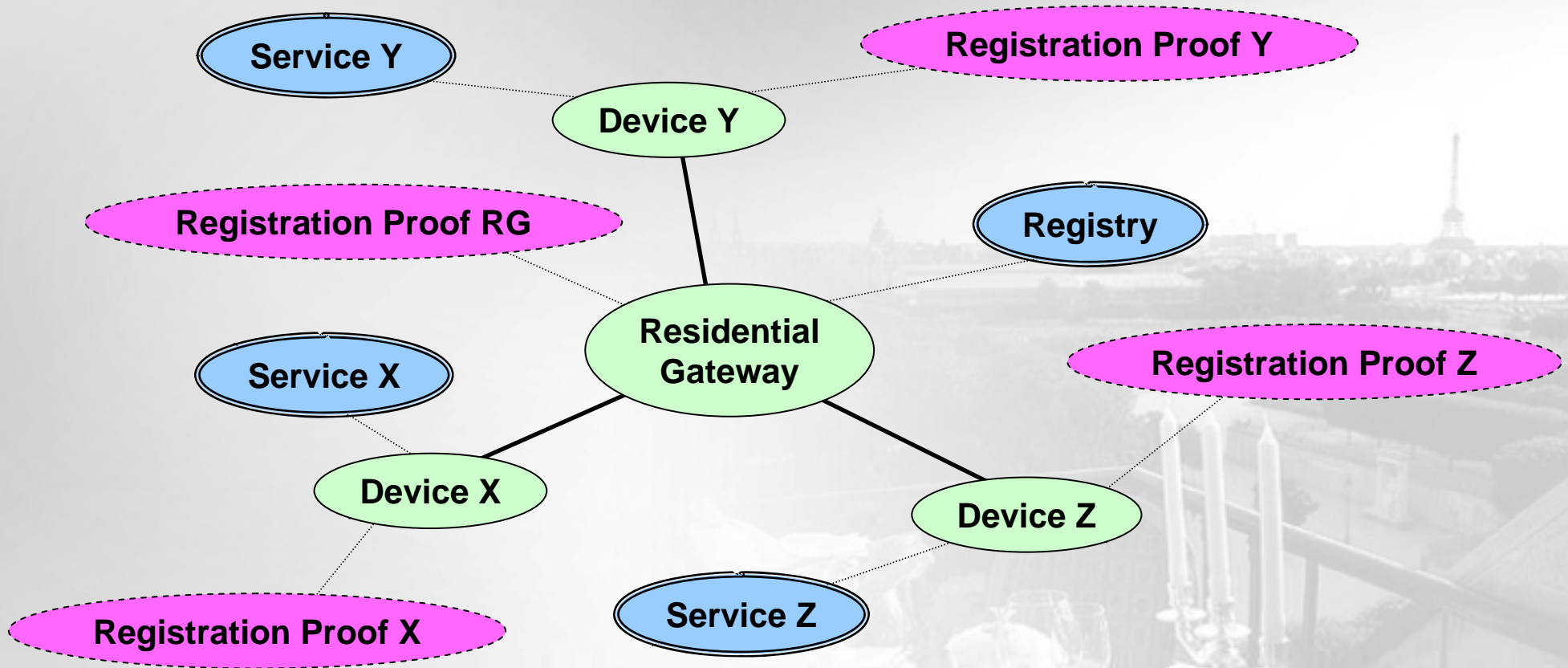
Secure Key Agreement with Station-To-Station



Secure Service Discovery and Use with Registry



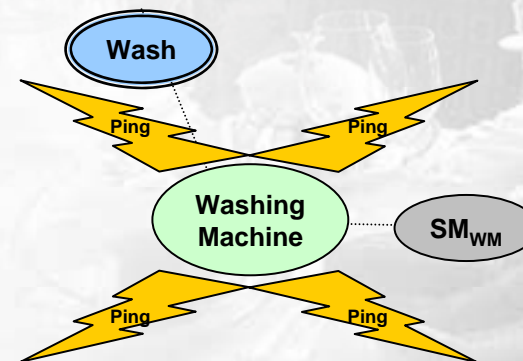
Registration of Devices



Master Registry issues Proofs of Registration
Strong Authentication (relying on Security Module) of Devices
Device-Device communication requires valid Proof of Registration



Example: Only one Washing Machine



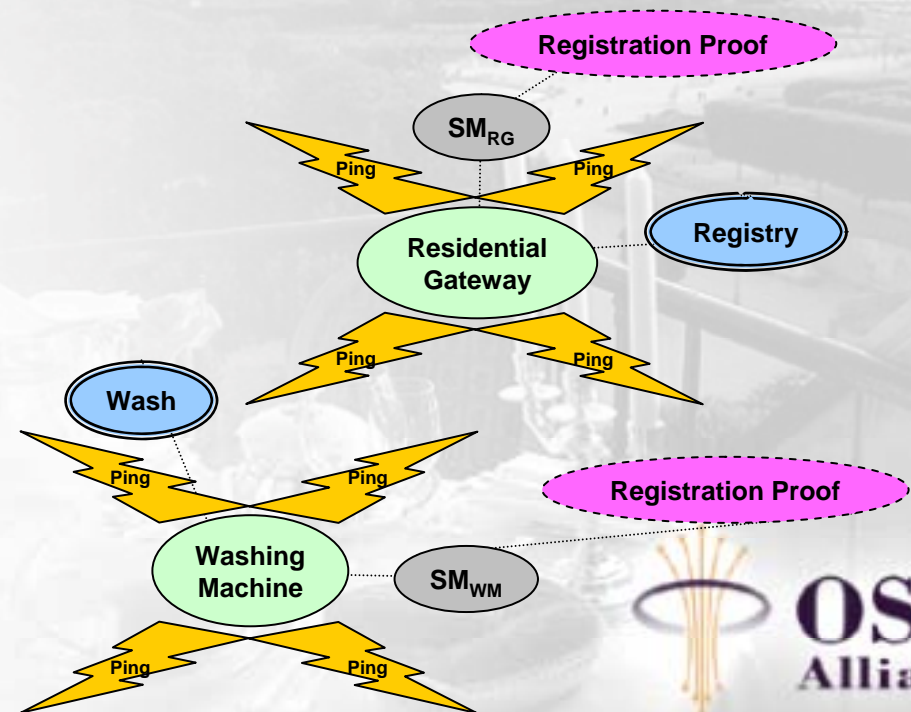
Example: Registry Device Comes Online

Residential Gateway (RG) assumes the role of a Registry Device

RG is personalized for the home

Issuing Registration Proof requires human interaction

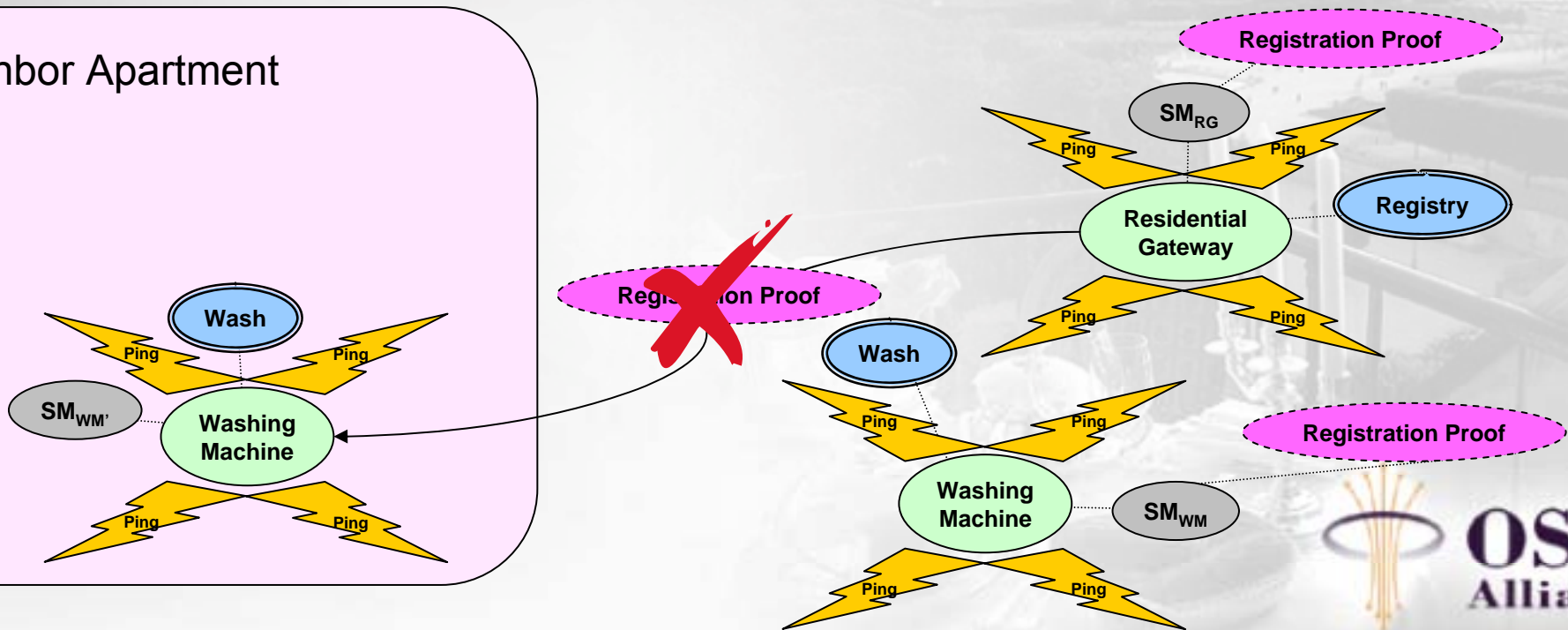
- Physical presence of the registered device
- Knowledge of activation code of the new device



Example: Neighbor Installs Washing Machine

Neighbor's device is not physically present → Cannot receive a Registration Proof

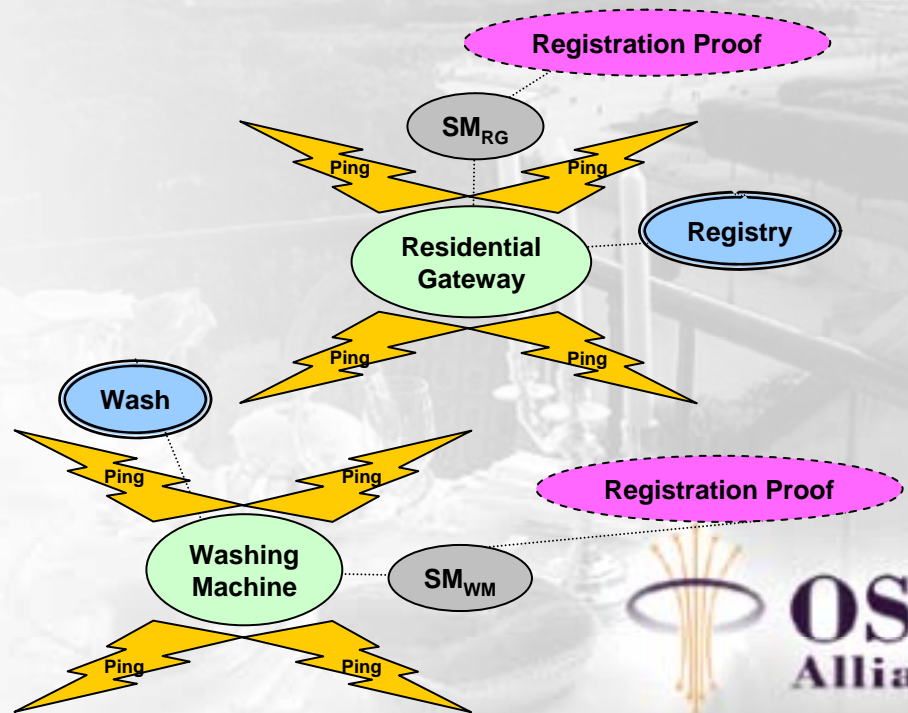
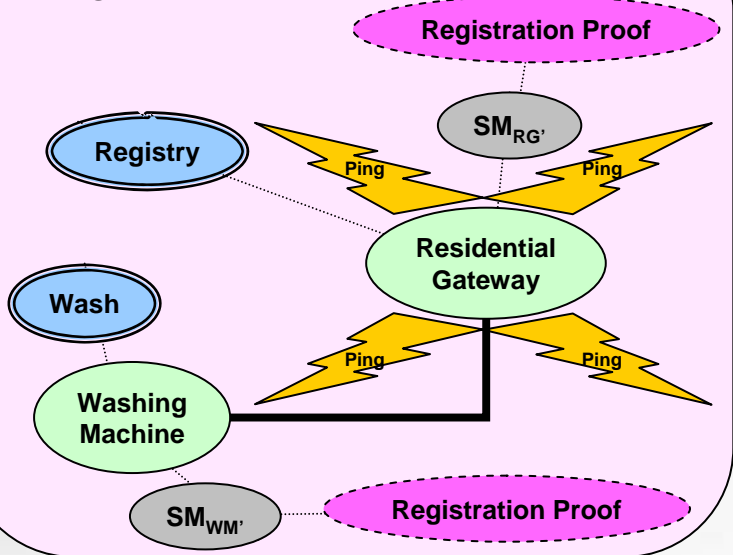
Neighbor Apartment



Example: Separate Registration Domains

Neighbor's devices receive Neighbor's Registration Proofs
Name space reflects where a device belongs to

Neighbor Apartment



Conclusions

- TEAHA provides a secure and interoperable architecture for networked home applications
- Security Module is an OSGi bundle that provides
 - Secure communications services
 - Protection against cloning of the device
 - Strong authentication of the device and services
- Initialization of security-related parameters embedded in the service discovery protocol





*Paris,
France*

Attend the 2nd TEAHA Open Forum

November 28, 2005

Le Méridien - Nice, France



Secure Key Agreement with Diffie-Hellman

Ping message sent from D1 to D2

- Computes secret x
- Calculates α^x
- Authenticates $\{data_1 || \alpha^x\}$

D1 Broadcasts the Ping message

- Broadcast of Authenticated $(data_1 || \alpha^x)$

1

D2 Receives a Ping message

- Checks Authenticated $(data_1 || \alpha^x)$
- Processes $data_1$

2

D2 Prepares a Pong message for D1

- Computes secret y
- Calculates α^y
- Calculates $K = (\alpha^x)^y$
- Encrypts data: $E_K(data_2)$
- Authenticates $\{E_K(data_2) || \alpha^y\}$

3

D2 Broadcasts Pong message for D1

- Broadcast of Authenticated $(E_K(data_2) || \alpha^y)$

D1 Receives a Pong message

- Checks Authenticated $(E_K(data_2) || \alpha^y)$
- Calculates $K = (\alpha^y)^x$
- Decrypts $E_K(data_2)$
- Processes $data_2$

4

D1 Prepares Secure Data Transfer

- Encrypts $E_K(data_3)$
- Authenticates $E_K(data_3)$

D1 Broadcasts Secured Data Transfer message for D2

- Broadcast of Authenticated $(E_K(data_3))$

5

D2 Receives a Secured Data Transfer message

- Checks Authenticated $(E_K(data_3))$

D2 Decrypts the information within a session with D1

- Decrypts $E_K(data_3)$

6

TEAHA Service Discovery

