Secure Service Discovery in Home Networks

Hans Scholten, Hylke van Dijk
University of Twente
Enschede, the Netherlands

Danny De Cock, Bart Preneel
Catholic University of Leuven
Leuven, Belgium

Michel D'Hooge, Antonio Kung
Trialog
Paris, France

***Abstract*— This paper presents an architecture for secure service discovery for use in home networks. We give an overview and rationale of a cluster-based home network architecture that bridges different, often vendor specific, network technologies. We show how it integrates security, communication, and service discovery to achieve a secure and trusted way of deploying services in a domestic environment.**

I. Introduction

This paper presents work done in The European Application Home Alliance (TEAHA) project [1]. TEAHA's objective is to develop an open, secure, interoperable, and seamless global home platform. TEAHA's approach is to define a suitable middleware platform that allows the seamless interworking of a wide variety of appliances found in a home environment. Industry sees a wide range of business opportunities when the platform supports legacy services and existing standards next to new TEAHA compliant services. Examples include UPnP, Bluetooth, SLP [2], Jini, and Salutation.

Security is a key component in TEAHA's design. If required, the entire process from the first discovery of a service in the network, through the use of that service, to the closing down of a service can be secured. Security is therefore an integral part of the architecture.

II. System Components

In this section we present the principal components of the TEAHA platform. We start with the articulation of its main requirements. Seamless interworking of services and technologies requires:

- The architecture to support heterogeneous technologies. Standardisation may help to reduce the diversity of technology but it is insufficient. Moreover legacy technology must be supported.
- The architecture to support "cluster cultures". Applications and services that reside in one cluster share the interests of a specific value chain. Necessarily, stakeholders of the same application area share the same culture; they use an accepted terminology, and must cope with the same set of industrial requirements, standards, and regulations.
- The architecture to provide a zero-configuration environment (touch and play). The end users of the TEAHA platform expect out-of-the-box operation.

This work is sponsored in part by the European Commission (IST-507029 priority 2.3.1.8)

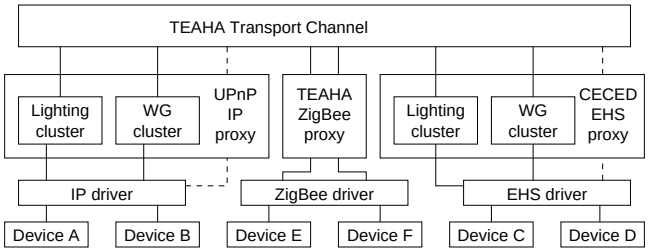


Fig. 1. TEAHA Transport System

A. Communication

Figure 1 shows the TEAHA transport system. At the bottom, as an example, four devices (A $\cdots$ D) are connected to two different types of network (IP and EHS). Devices A and B offer a service according to the UPnP protocol, while Devices C and D offer a service following the CECED protocol. In addition, the services of A and C belong to the Lighting cluster whereas the services of B and D belong to the White Goods cluster (WG). Clusters represent business alliances with a predefined application programming interface (API). In the example, the offered services of each cluster reside on devices that are connected to different network technologies, moreover each service uses a different protocol. We therefore must bridge the technologies (proxy) as well as the respective protocols (cluster).

The TEAHA middleware offers a rich set of technology *drivers* to connect to a wide range of devices. In order to access the offered services, the middleware provides a set of *proxies* that bind a specific protocol to a specific technology. Proxies, in turn, support a plug-in mechanism to specialise protocol transformations, i.e., the *clusters* of Figure 1. The default plug-in of a proxy is useful for inter protocol communication, e.g., between two UPnP services or between two TEAHA services.

Consider as an example Figure 1 once more. Device A connects to an IP driver. Since the service of Device A follows the UPnP protocol it will be handled by the UPnP/IP proxy, moreover the communication can be specialised to follow the protocol of the Lighting cluster. The service of Device A is now available as a Lighting/UPnP service, which can be used by other Lighting services as well as UPnP services. Suppose we have a Device X (not shown) that connects to the EHS cluster and its service follows the UPnP protocol then it would require UPnP/EHS proxy with a default cluster plug in to connect the service of Device X with the service of Device A.

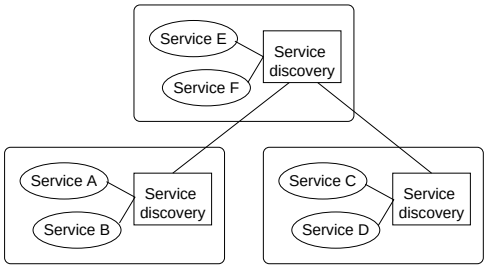


Fig. 2. TEAHA Service System

In the diagram of Figure 1 both Device E and Device F use the default cluster plug in of the TEAHA/ZigBee proxy. Services of Device E and F are thus connected through the TEAHA protocol, which allows them to communicate in a secure way (see hereafter). Note that all proxies are in fact TEAHA services and therefore security can be guaranteed between two proxies. The security between the proxy and the end service depends on applied technology, in case of a TEAHA/ZigBee network security is again guaranteed.

B. Secure Service Discovery

The concept of service discovery is present in many systems. Examples are (without being exhaustive) Jini, UPnP, SLP, FRODO [3] and Salutation. In contrast to most other systems, TEAHA's service discovery and security are embedded in the architecture. The security features rely on the trustworthiness of the proofs of registration and the confidentiality of cryptographic key material. The security component handles all security-critical operations. It also stores the identity of the device in which it is installed.

In order to facilitate the zero-configuration of devices, we implement a touch and play paradigm. The touch is a physical registration process, which exchanges credentials among a gateway and a registering service; for instance by means of RFID tagging. We use a hierarchy of services as exemplified in Figure 2. Once registered a service is granted access to all services down the hierarchy.

Our service discovery process uses distributed directories, where each directory maps one-on-one to a pool of registered services. Discovering a service boils down to a query on the local registry followed with a tree traversal if the requested service cannot be resolved locally. In our initial design each directory only stores locally registered services, however if required for reasons of efficiency a directory could store more information. This does not change the design.

Our security mechanism relies on a security engine for storage of device credentials and a cryptographic kernel. We use a shared key protocol for the authentication and integrity proof of transferred messages. We chose the station-to-station protocol [4], which is an authenticated variant of the well known Diffie-Hellman key agreement protocol. This protocol has proven security properties, is simple, and allows piggybacking with a service discovery protocol.

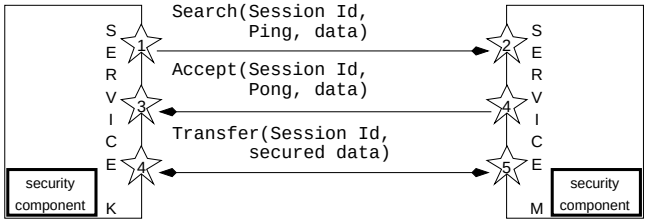


Fig. 3. Secure Service Discovery

III. System integration

As an example of the integration of the security component and the service discovery mechanism consider the following scenario. A Service K actively searches for Service M, which is willing to acknowledge the request provided Service K can be authenticated (is properly registered). Once accepted they decide to exchange messages in a secure way. The scenario is outlined in the diagram of Figure 3.

The steps are as follows: Service K sends a `Search` request that includes a so-called *Ping* message. The Ping entails the key agreement request of Service K and an authenticity proof, which allows Service M to verify that Service K posed the request. Once authenticated, Service M replies with an `Accept` message that includes a *Pong* message. The Pong entails the key agreement response of Service M and an authentication proof. After the (authenticated) receipt of the Pong message Service K and M share a secret session key, which can be calculated from the exchanged key agreement information. The session key is used to encrypt data messages in the further communication among Service K and M.

The architecture, while still under development, reached a state that makes prototyping expedient. We are developing a prototype based on commodity technology that includes seamless interworking, security, and service discovery. The technology of choice includes an OSGi platform and JXTA networking. It supports clusters for white goods and lighting, it supports protocols like UPnP, CECED, and Konnex, and it supports technologies such as ZigBee, Ethernet and EHS.

IV. Conclusion

In this paper we have presented an architecture for home networks that supports secure seamless interworking for heterogeneous networks and clusters. One of the main features is the integration of a flexible transport system, security, and secure service discovery. The quality of the architecture will be assessed through prototyping.

References

[1] "Teaha web site," http://www.teaha.org.
[2] E. Guttman, C. E. Perkins, J. Veizades, and M. Day, "Service location protocol, version 2," IETF Network Working Group, RFC 2608, July 1999.
[3] V. Sundramoorthy, H. Scholten, P. Jansen, and P. Hartel, "Service discovery at home," in *Proc. of the 4th Int. Conf. on Information, Communications & Signal Processing*, Dec. 2003, pp. 1929–1935.
[4] W. Diffie, P. C. Oorschot, and M. J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, vol. 2, pp. 107–125, June 1992.

TEAHA
The European Application Home Alliance

Secure Service Discovery in Home Networks

Hans Scholten
Hylke van Dijk
University of Twente
Enschede
the Netherlands

Antonio Kung
Michel d'Hooge
Trialog
Paris
France

Danny De Cock
Bart Preneel
Catholic Univ. of Leuven
Leuven
Belgium

Information Society and Media

European Commission

Overview

- Introduction
- Objectives & Requirements
- Technology and Business Clusters
- Communication and Service Discovery
- Integration
- Conclusion

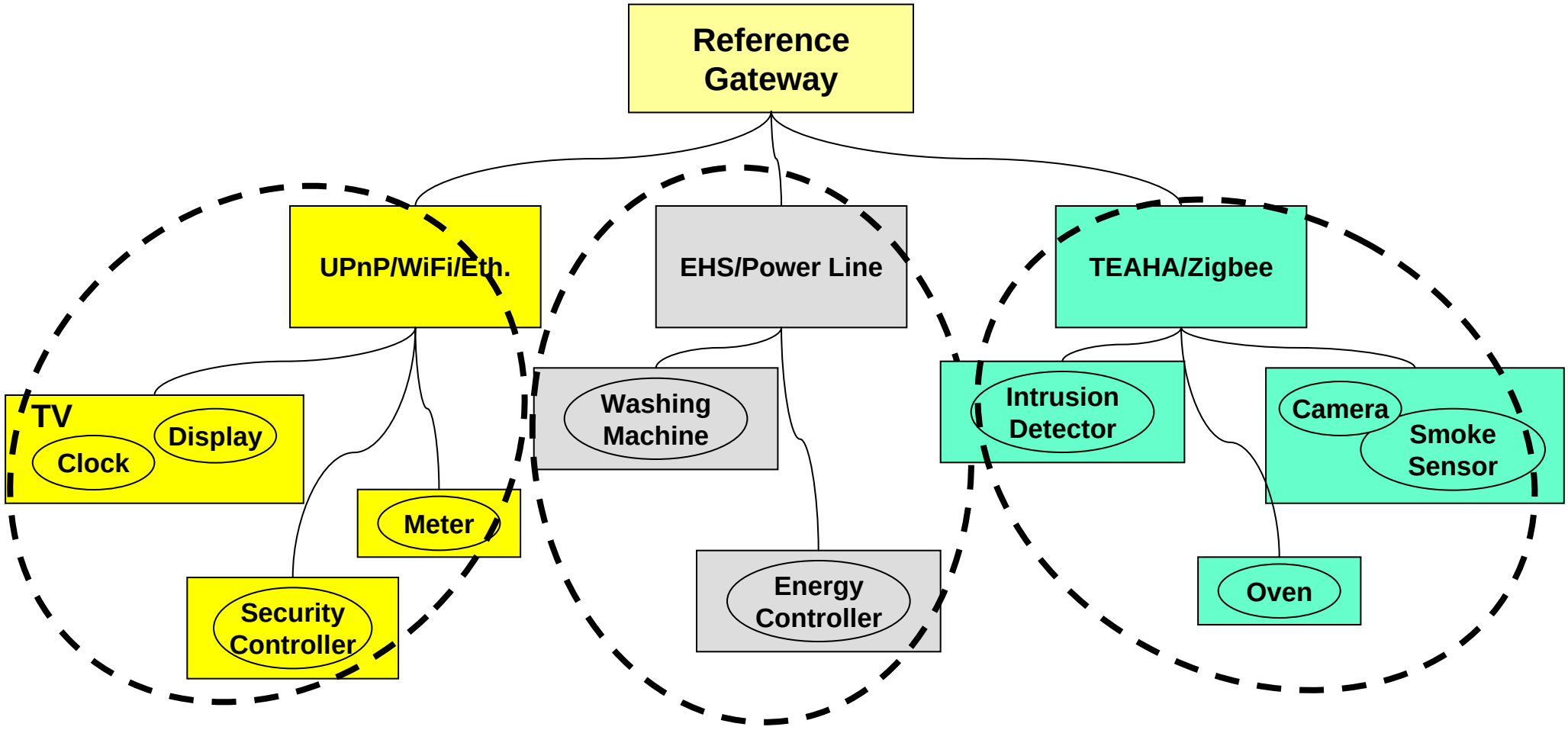
TEAHA Introduction

- **TEAHA: T**he **E**uropean **A**pplication **H**ome **A**lliance
  Sponsored by European Commission
  (IST-507029 priority 2.3.1.8)
- Partners: *(Spain, France, Belgium, Netherlands, Italy, UK)*
  - *Telefónica I+D*
  - *Electricité de France*
  - *Fagor*
  - *Ikerlan*
  - *Homega-Research*
  - *Konnex*
  - *Katholiek Universiteit Leuven -COSIC*
  - *Philips Applied Technologies (Apptech)*
  - *Sharp Laboratories of Europe Ltd (SLE)*
  - *TAHI represented by Advantica*
  - *Trialog*
  - *WRAP*
  - *University of Twente, CTIT*

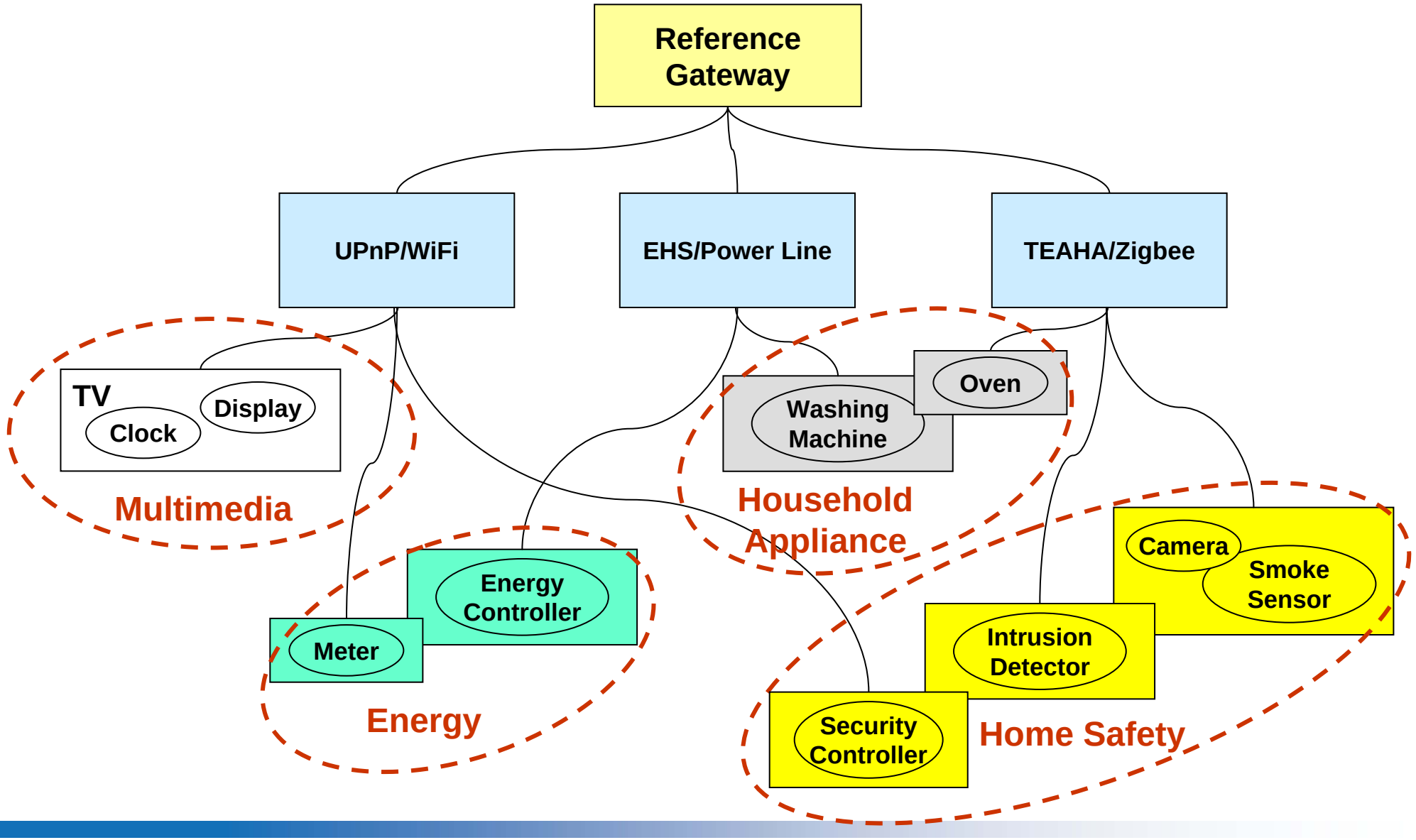
TEAHA Objectives & Requirements

- **Objective**
  - to develop an open, secure, interoperable, and seamless global home platform
- **Requirements**
  - support heterogeneous technologies
    - despite standardization
  - support legacy technologies and existing standards
    - Bluetooth, UPnP
  - support “cluster cultures”
    - technology clusters
    - business clusters
  - provide a zero-configuration environment (touch and play)
    - end users expect out-of-the-box operation

TEAHA Has Technology Clusters



TEAHA Has Business Clusters



Facts about Stakeholders

- **Stakeholders in a business cluster**
  - Share the same culture
  - Share the same value chain
  - Are competitors
  - Would prefer to abstract away from technology clusters

- **Stakeholders in different business clusters**
  - Have different cultures. Do not understand each other
  - Have different value chains
  - Are not competitors
  - Might see added value in cooperating

Mixing Technical and Business Clusters

- **Heterogeneous communication**
  - device tech A/cluster X **interworks with** device tech B/cluster Y
- **Service discovery**
  - device tech A/cluster X **discovers** device tech B/cluster Y

- **Secure heterogeneous communication**
  - device tech A/cluster X **communicates securely with** device tech B/cluster Y
    - Authenticity: No faked devices when this is a business requirement!
    - Confidentiality: No eavesdroppers when this is a business requirement!
    - Trusted/Registered devices: No intruders when this is a business requirement!
- **Secure service discovery**
  - device tech A/cluster X **discovers in a secure way** device tech B/cluster Y
    - Authenticity, Confidentiality, Trusted/Registered devices
    - Policy enforcement: A business cluster can be protected from other clusters
      - is a multimedia application allowed to access security system information?

Gateway Abstract Architecture

Interworking Environment

Application Framework

- Service Applications
- Bridge Utility
- Service Access Utility
- Secure Service Discovery Utility
- Secure Communication Utility

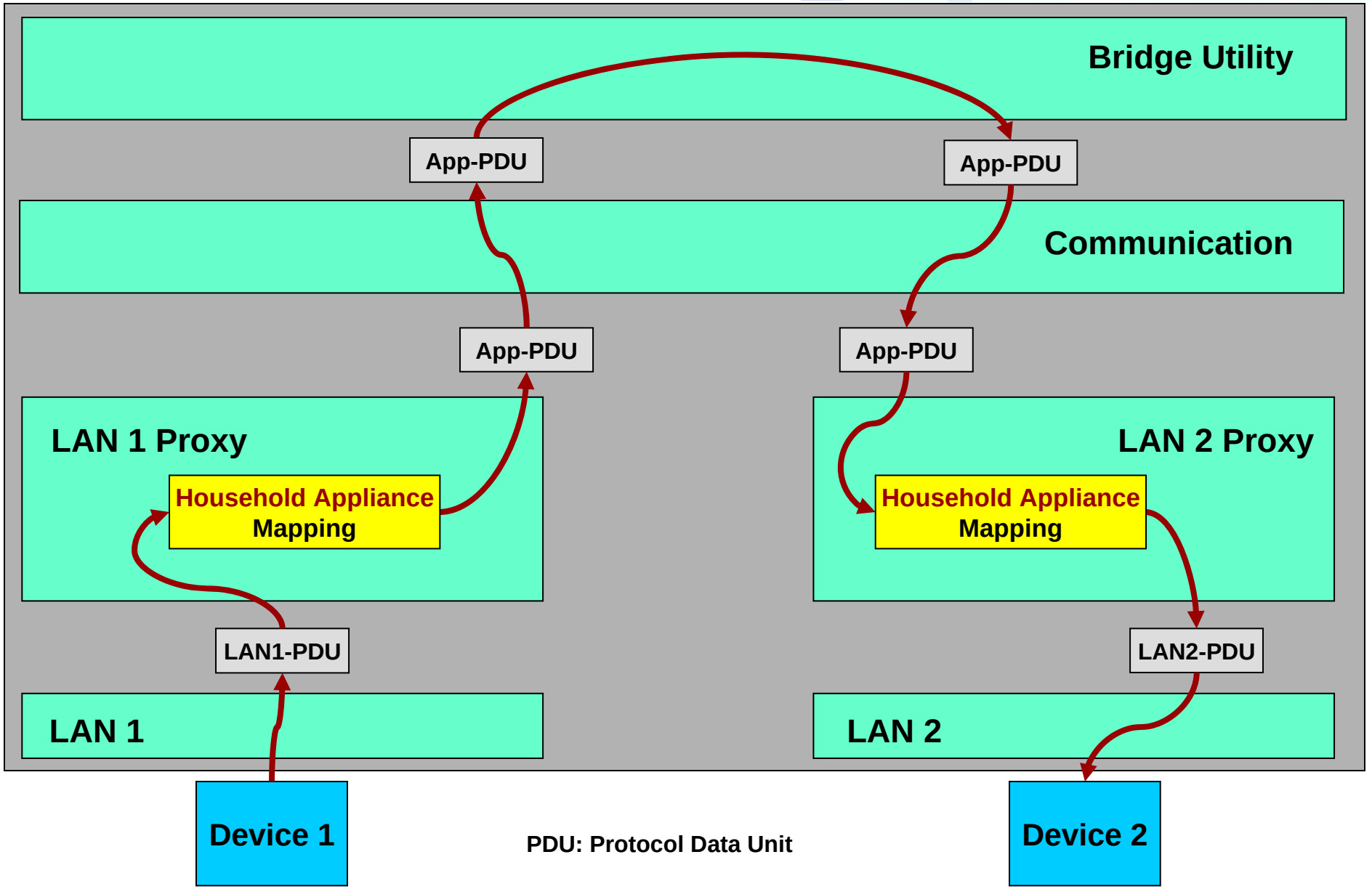
LAN Abstraction

- Communication Layer
- LAN 1 Proxy
- LAN 2 Proxy
- LAN 1 Driver
- LAN 2 Driver

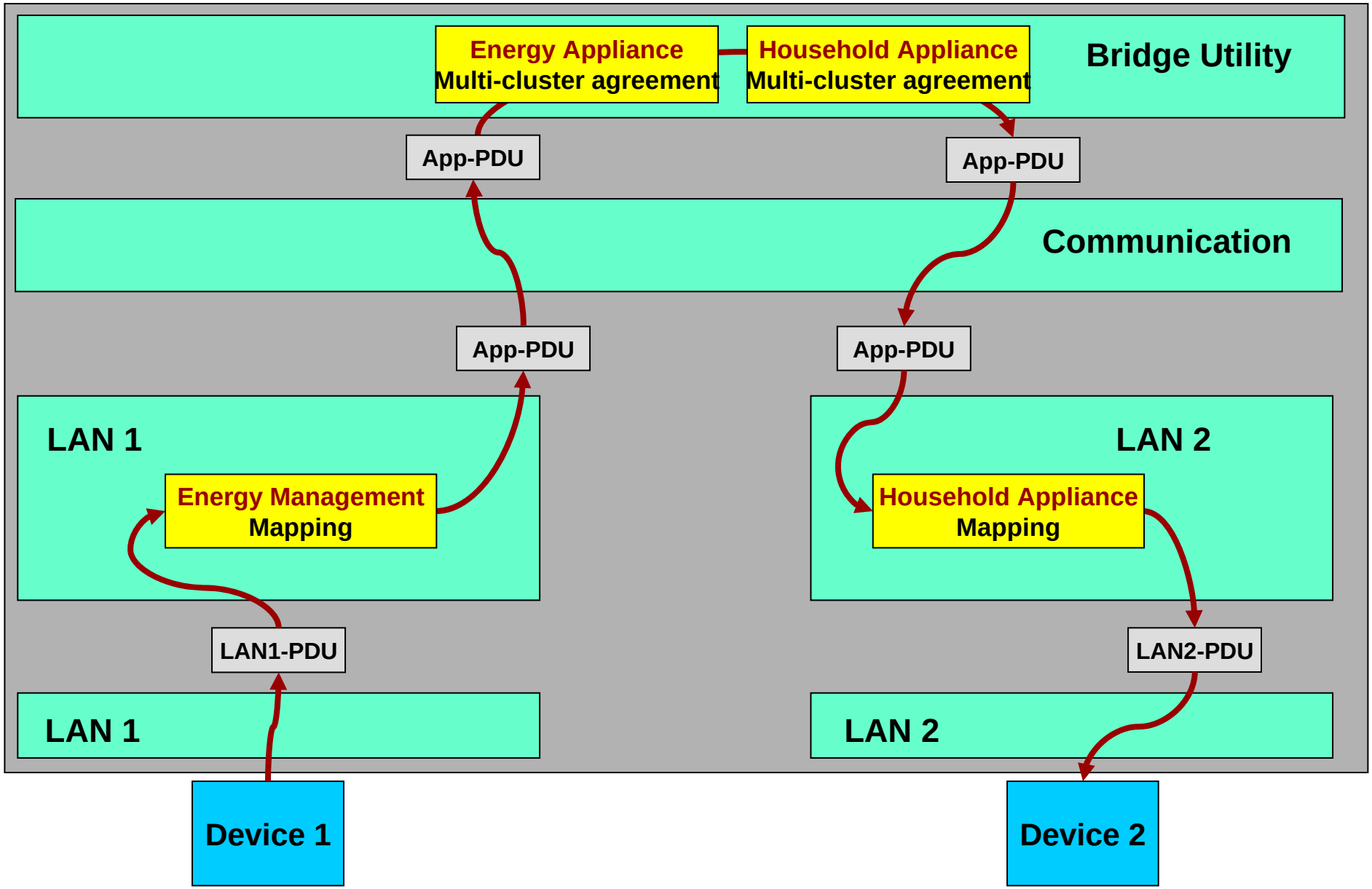
Business Cluster Support

Security Module

Mono-Cluster
Heterogeneous Communication



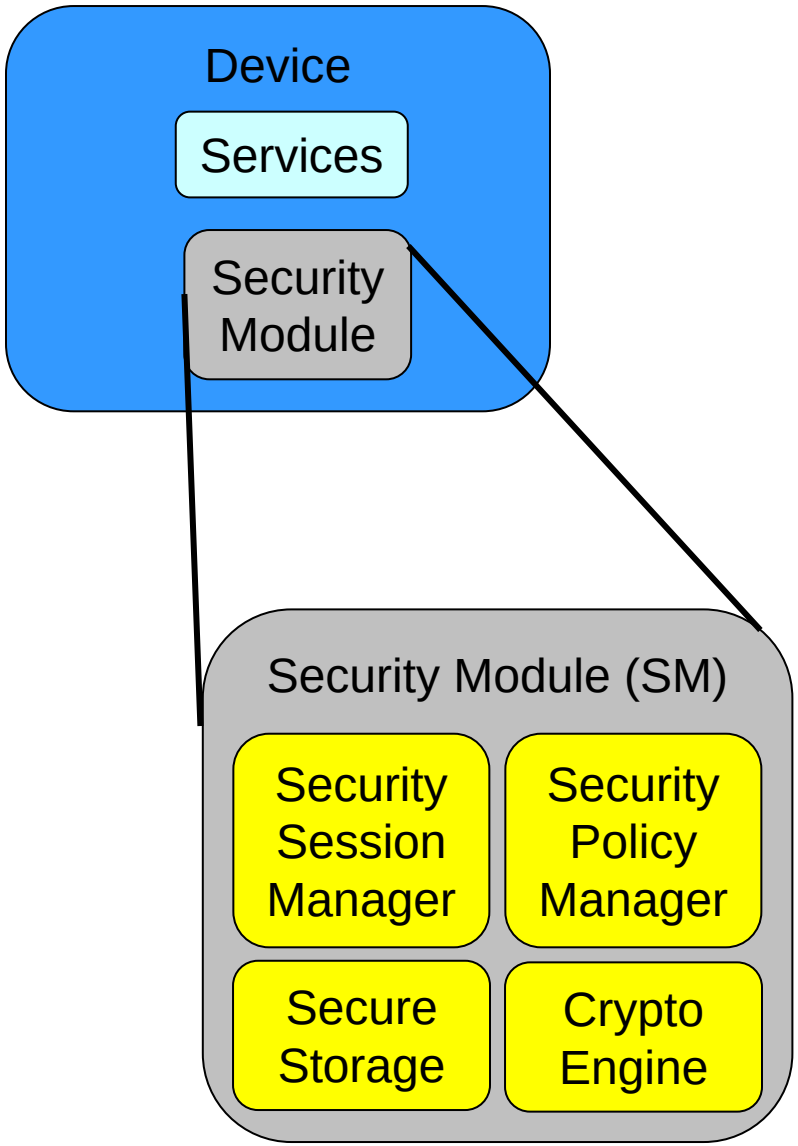
Multi-Cluster Heterogeneous Communication



Device Architecture for Secure Communication

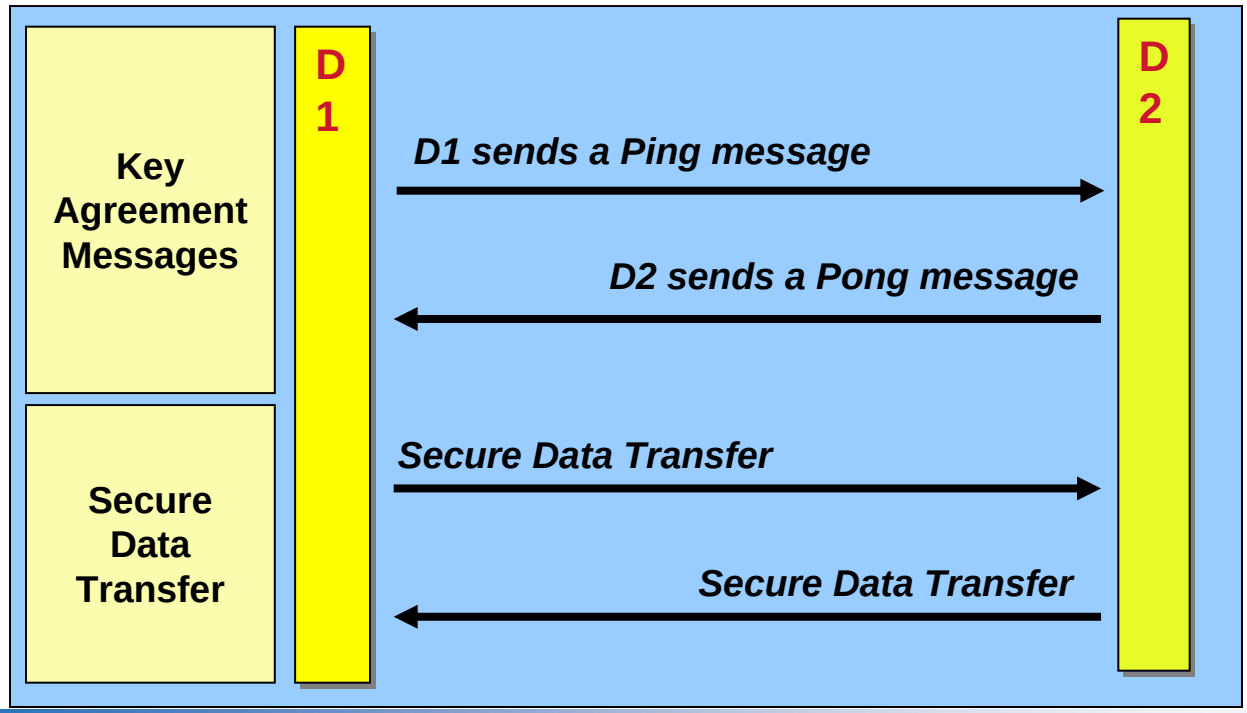
Key Features of a Security Module:

- **One SM per device**
- **Initialized SM ready to be used**
- **Combination of hardware and software**
  - Hardware ➔ Non-cloneable
  - Software ➔ Risk for cloning
- **Provide true strong authentication**
- **Secure communications rely on SM**
  - Insecure
  - Authenticity
  - Confidentiality
  - Secure = Auth. + Conf



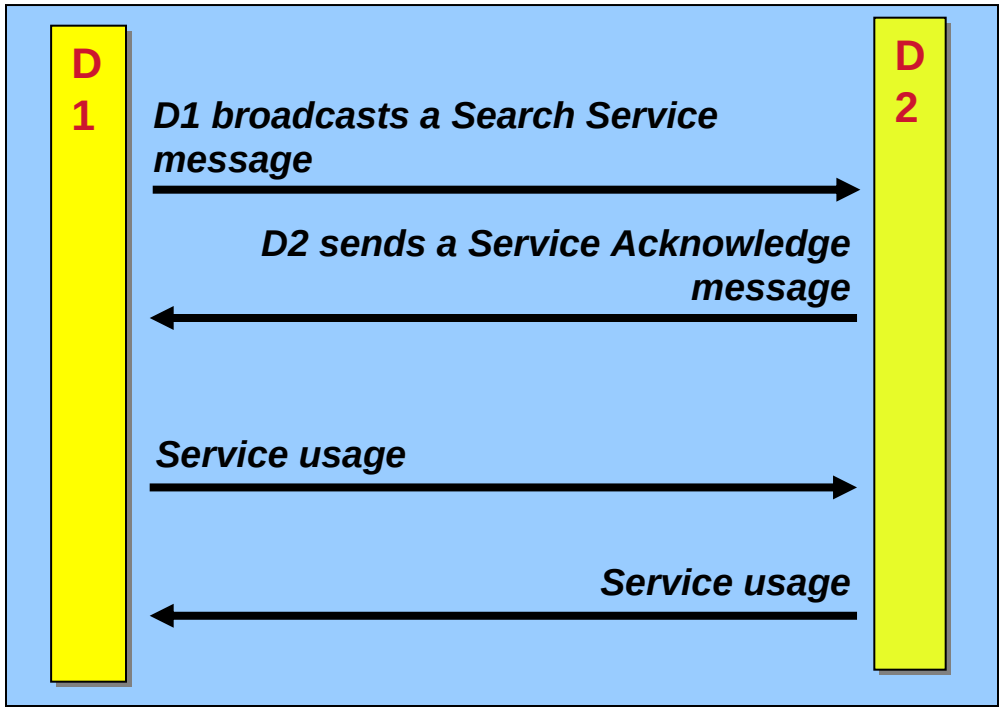
Secure Communication

- **Station-to-station protocol (authenticated Diffie-Hellman)**
  - establish shared key with mutual authentication
- **After Ping-Pong D1 and D2 share a common secret**
  - used to derive encryption and integrity-protection keys to protect the confidentiality and integrity of subsequent messages



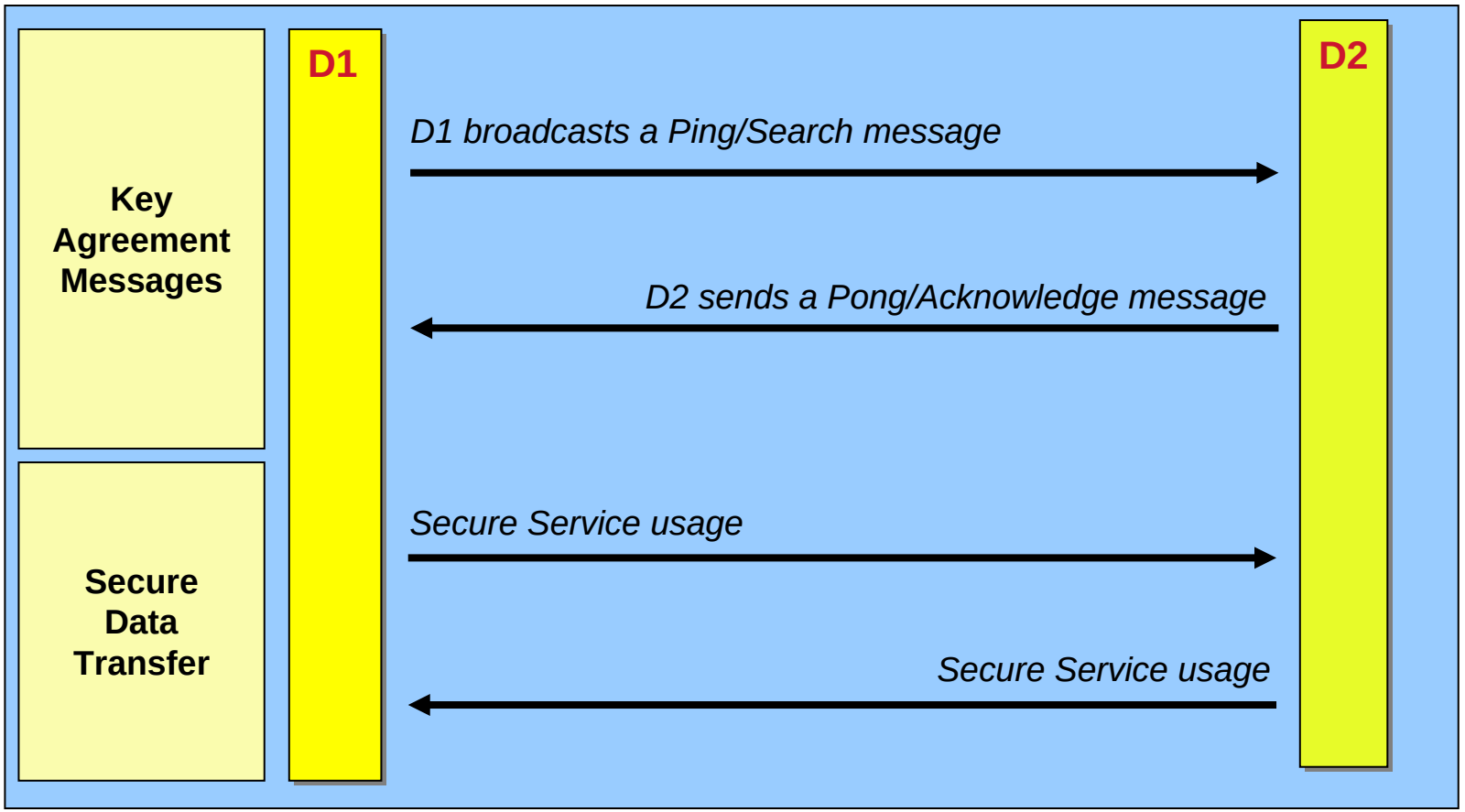
Service Discovery

- **Peer-to-Peer or Registry based**
  - Search Service is followed by Service Acknowledgement
  - If service is found it can be used



Secure Service Discovery

- **Combine Discovery and Key Agreement**
- **Combine Security and Communication**



Conclusions

- **TEAHA has defined an architecture for secure seamless interworking featuring**
  - Heterogeneous Secure Communication
    - Protecting integrity and/or confidentiality
    - Strong authentication of the device and services
  - Secure Service Discovery
    - Key agreement during service discovery
    - Secure communication
  - Protection against cloning of devices
    - Security modules
- **Prototype:**
  - seamless interworking, security, and service discovery
  - OSGi platform and JXTA
  - clusters for white goods and lighting
  - support for protocols like UPnP, CECED, and Konnex
  - support for technologies such as ZigBee, Ethernet (IP) and EHS

More Information

www.teaha.org

or

hans.scholten@utwente.nl