Technische Universität München

Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Holger Kinkelin, Andreas Müller
Contact: [kinkelin|mueller]@net.in.tum.de · http://www.net.in.tum.de

Security in Future Home Networks

Motivation

Security in today's home networks

- WLAN access protected by shared key
  - ➔ Flexibility? Usability? Security?
- Most other services are not protected, e.g. UPnP, DLNA, ...

Security in future home networks

- More devices
- More services
- Desire to share services with friends

➔ **Future home networks need mechanisms for user/device authentication and fine grained authorization that are easy to use and easy to understand**

The AutHoNe Security Architecture

Idea: Adapt enterprise solutions to home networks and make them easy to use

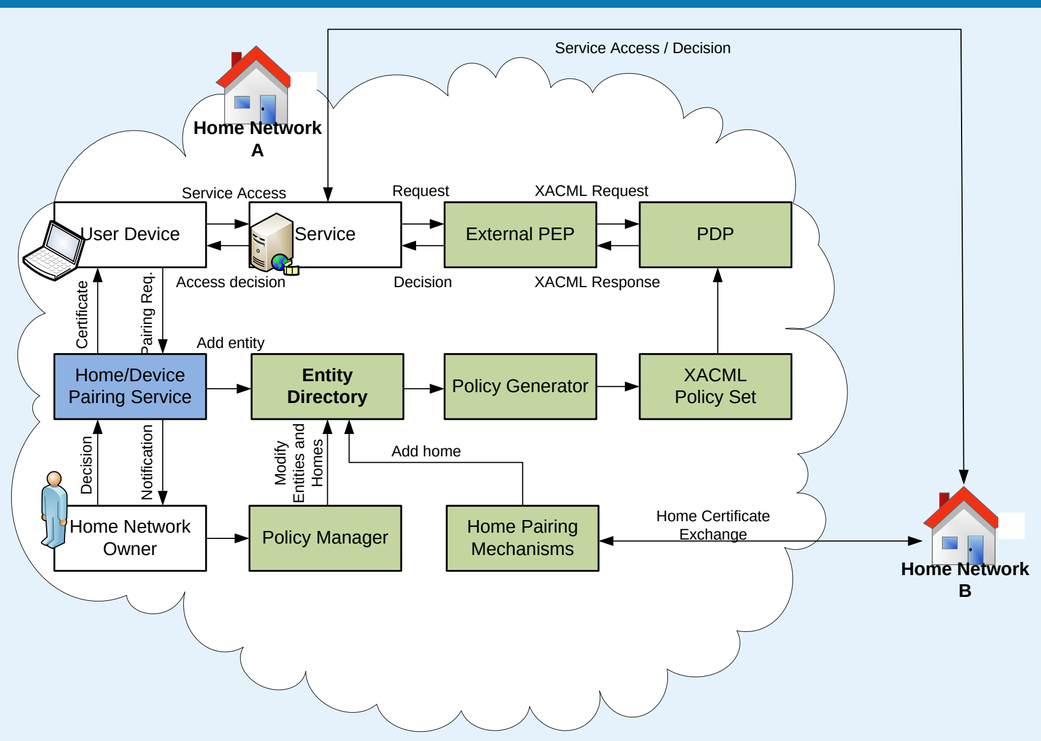
Identities:
- Each home maintains its own Certificate Authority
- Each home issues certificates to its users
- Unique IDs for users/devices/services are derived from their respective public keys

Device/Home Pairing
- Assist home network administrator and users with semi-automated certificate creation
- Hide difficult to understand details behind the easy to understand concept of the Device/Home Pairing mechanism
- The user „pairs" the device with his home network and obtains a certificate

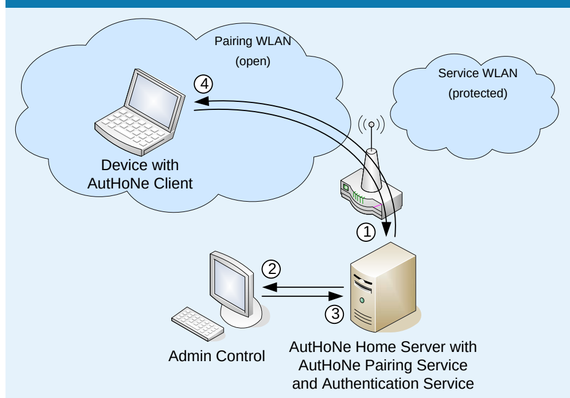
Authorization
- XACML Policies are used for defining fine grained access rights
- Policies and complex technical details are hidden behind GUIs and simple XML databases

Services
- Radius and EAP-TLS for network access
- TLS protected Devices Profile for Web Services (DPWS) for plug and play services
- https for all web based services

Architecture



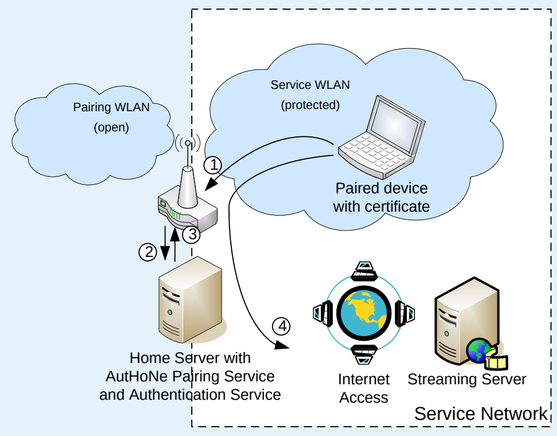
Device/Home Pairing



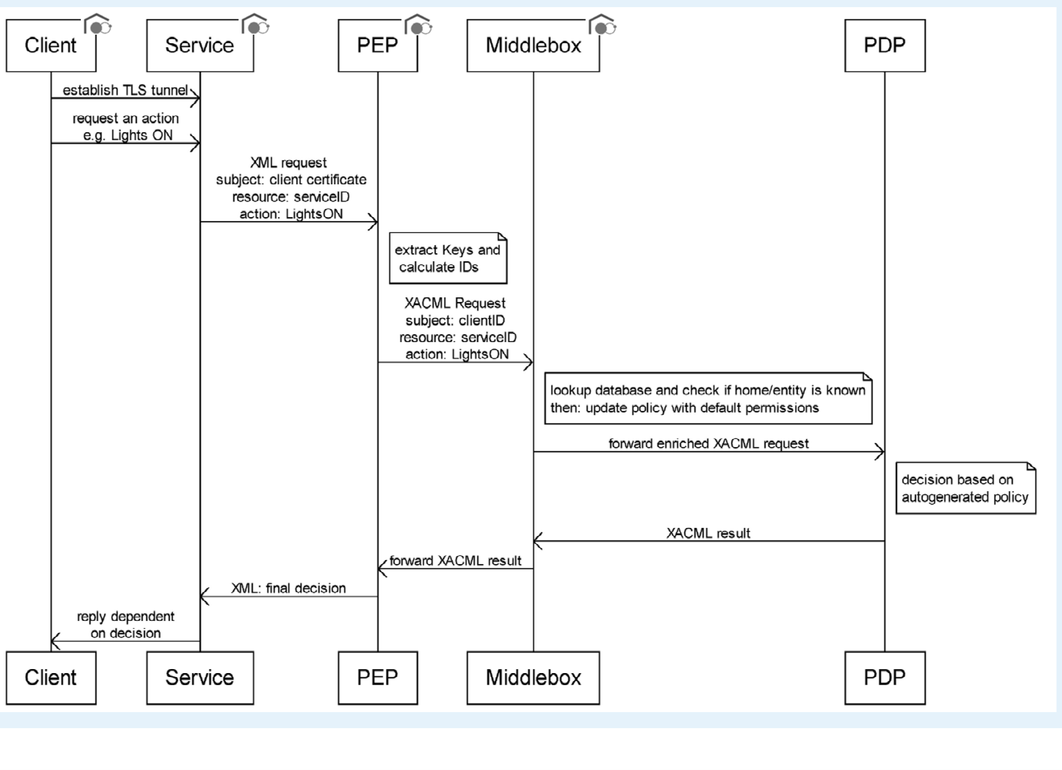
Architecture
- Open WLAN and a VM for pairing
- Protected WLAN and multiple VMs for the service network

Steps for a new client (open WLAN)
(1) pairing request is sent
(2)+(3) admin is notified and grants access
(4) certificate is delivered to client

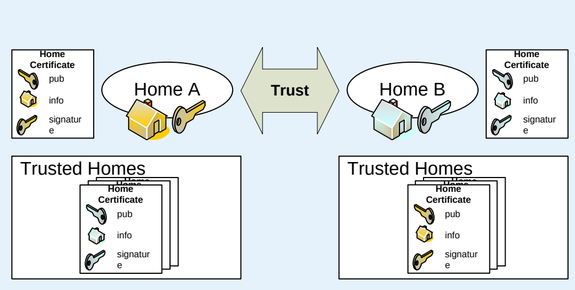
Steps after the pairing
(1) paired devices wants to access the service WLAN
(2) the authentication request is processed by the Authentication Server
(3) the Authentication Server's decision is sent to the AP
(4) Network access is granted



An example request



Home Pairing



- **Exchanged Home Certificates are stored in a repository**

→Home networks can identify devices that are paired to a friend's HN using the corresponding Home Certificate

→Policies for remote devices regulate access to services

- **A home network is able to authenticate its own users by validating their certificates**

To validate a user of another home, the Home Certificates have to be exchanged

Trust Exchange mechanism similar to exchanging business cards