Technische Universität München

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

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

Security and Trust

Motivation

Security in present home networks

- Neglected
- **Basically equals to WLAN security**
- **WLAN security is not solved nicely:**
  - Accecss is controled by using a shared password on WLAN AP and devices
  - Problematic when a guest needs access to the WLAN / when access needs to be withdrawn

➔**Better mechanisms for user authentication for WLAN access control are needed!**

Security in future home networks

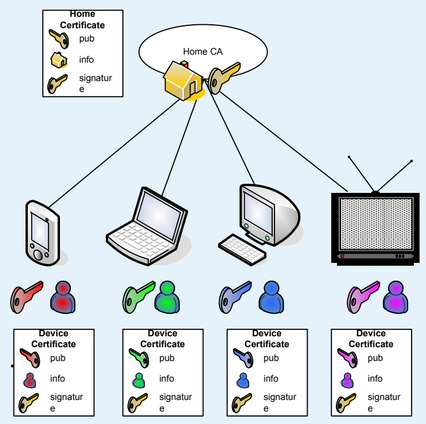
- **More devices** connect to the WLAN
- **More services** available in the Home Network
- Growing bandwith of home internet accesses → **Desire to share services with friends**

➔**Future home networks need a mechanism for user/device authentication**
➔**The gap between the demand for authentication mechanisms and existing solutions in HNs will widen even more in future**

Approach

Comparable solution in Enterprise Networks:

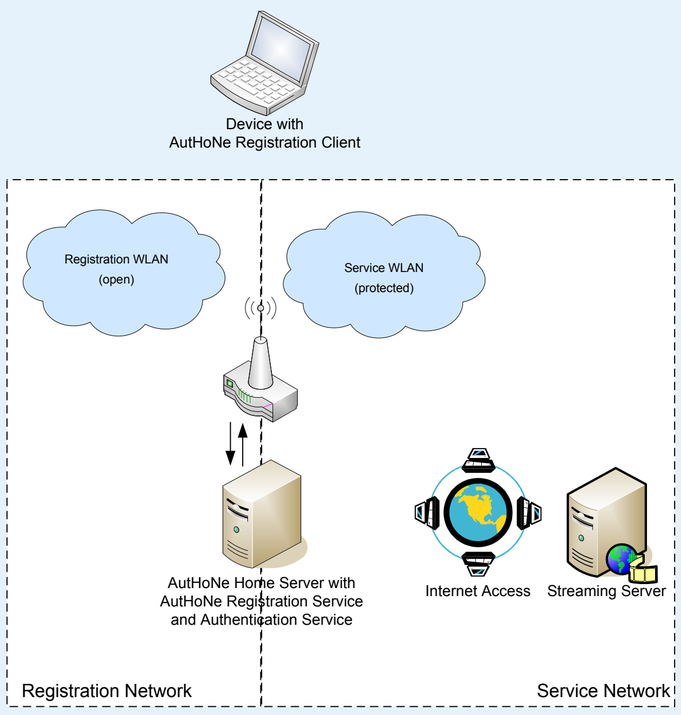
- **Authentication mechanisms based on Public Key Certificates**
  - Secure and flexible
  - Applicable to many use cases
- **Certification Authority required for certificate creation**
  - Operators are needed to setup, run and maintain the CA
  - Operators are needed to assist users with certificate creation



Assisted Device Registration System:

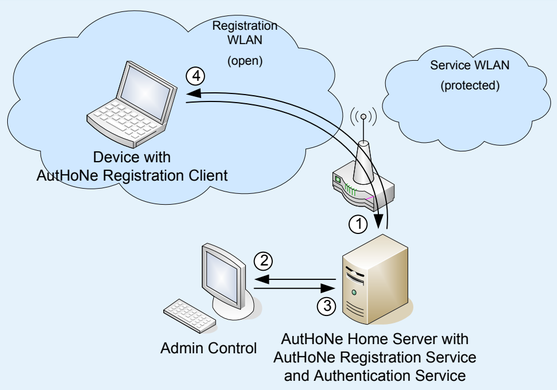
- Above approach can not be transfered directly to HN
  - No operators but inexperienced users
  - Users don't want to care about certificates, authentication, ...
- General idea:
  - Set up a **Home Certificate Authority**
  - Use **certificate based user/device authentication**
  - Assist home network administrator and users with **semi-automated certificate creation**
  - Hide difficult to understand details behind the easy to understand concept **Device registration**

Architecture



- Registration makes a device to a part of the home network
- **Registration Client**
  - Assists the user
- **Registration Server**
  - Assists the admin
- **Registration WLAN** enables Registration Client to connect to Registration Server
- Access to Registration WLAN is completely open
- After registration Registration Client can connect to Service WLAN
- **Service WLAN** gives access to services within the home network
- Access to Service WLAN requires authentication with certificates

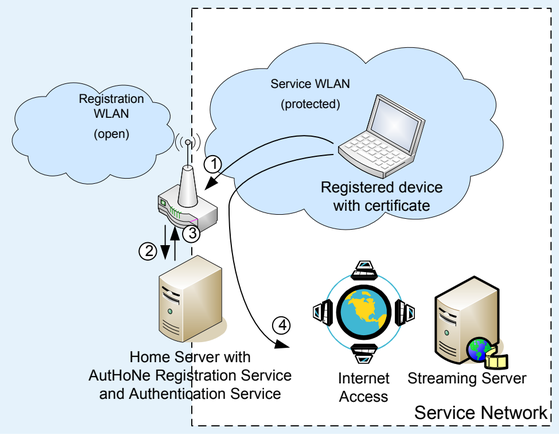
Registration / Service Access



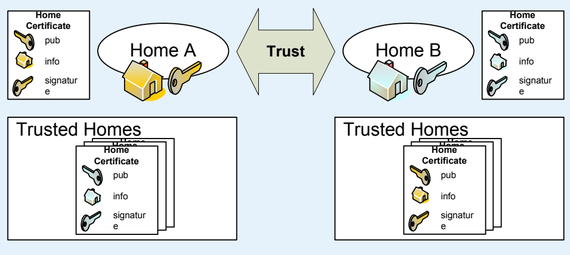
(1) Send registration request
(2) Admin is notified about pending registration
(3) Admin decides
(4) Certificate is delivered to Registration Client

→Device obtained a certificate
→The certificate enables the device to user WLAN and other services

(1) Registered devices wants to access the Service WLAN
(2) The authentication request is processed by the Authentication Server
(3) The Authentication Server's devision is sent to the AP
(4) WLAN Access is granted to the device



Interoperability between Home Networks

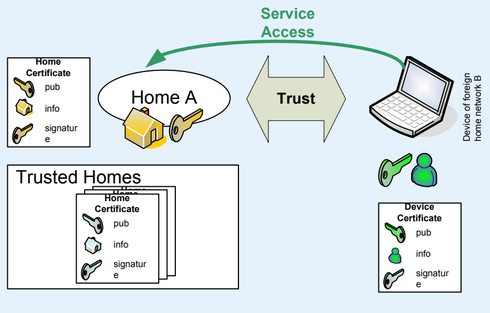


- **Trust Exchange:** exchange Home Certificates between friendly HNs
- Friends' Home Certificates are stored in a repository for future use

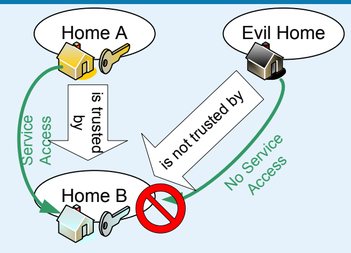
→Home networks can identify devices that are registered in a friend's HN using the corresponding Home Certificate

→Basis for HN trust relationships

- Services in a HN can be shared with a friend's HN
- Device registered in the friend's HN are able to prove their membership to the trusted HN
- The friend's device is for instance able to ...
  - access an other HN's WLAN
  - access a service in an other HN



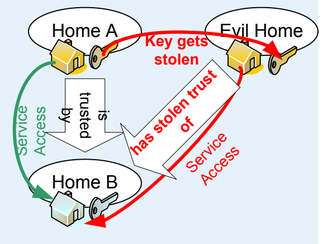
TPM-based Home CA



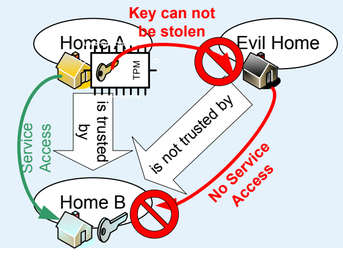
- Certificate based authentication offers high security and is a valuable basis for access control to WLAN/servies
- Major weakness: theft of a Home CA's secret key

→**Identity theft of a HN**

- If the private key of a Home CA got stolen, the attacker is able to register **own** devices inside the victim's network
- The attacker is now able to
  - use services inside the victim's home network
  - use services other people shared with the victim!



→**A trustworthy safeguard the Home CA's secret key is needed**



- Approach: Use a Trusted Platform Module (TPM) for secure key storage/usage on the HomeCA
- Keys are guaranteed to never leave the Home CA's TPM

→TPM makes Identity theft (almost) impossible
→**TPM can bring more trust into authentication**