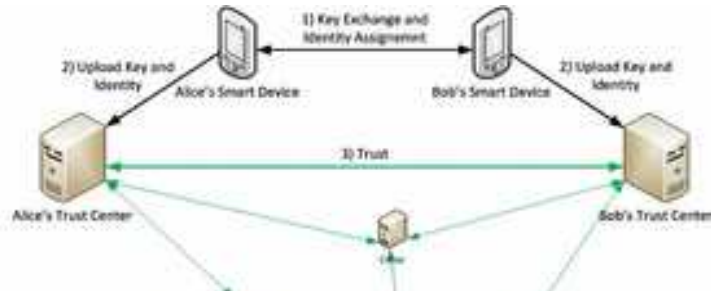
Technische Universität München
Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

BA

Establishing a Web of Trust between home networks

Introduction



The intermediate to advanced computer user is able to set up a home network which provides services like file sharing, music streaming, home automation, as well as communication channels like own mail or chat servers. In previous work we have discussed various mechanisms for establishing trust between such home networks (so called “Domains”), so that authenticated and authorized service sharing becomes possible.
The core idea of one mechanism is to exchange cryptographic material (public keys) between friendly Domains over a secure near-field network connection (NFC, Bluetooth, Ad-hoc WLAN connection, etc.) and assign the identity of the key owner to the received key. The exchange is performed when participants of two Domains meet in person. Later, received keys and learned identities can be used for the authentication of messages exchanged between Domains.

Problem

The overall concept and the administrative infrastructure, like a domain manager, which is able to handle authentication requests, has already been developed and analyzed. Nevertheless a client-side concept of interaction and a user-oriented client application which allows actual clients to use the developed mechanisms is still missing.

Task Description

Your task is to get to know with the current state of the prototype and develop a user interaction concept. Afterwards the goal of this work is develop a concept of how this system shall interact with the user and to create a working and easy to use prototype that implements this concept on a state of the art mobile platform, e.g., Android.

Requirements

You should have basic knowledge concerning X.509-PKIs as well as GPG and its realization of a Web of Trust. On the technical side, experience in programming android applications is necessary. Furthermore we expect you to cooperate with other students and members of the chair working on problems related to this thesis.

Miscellaneous

This thesis can be performed in German or English.

Further Information: Dr. Holger Kinkelin und Marcel von Maltitz
(lastname@net.in.tum.de)
Chair for Network Architectures and Services