Android Bluetooth Credential Store

Camilla Reis, Dominik Ziegler

Institute for Applied Information Processing and Communications
Graz University of Technology

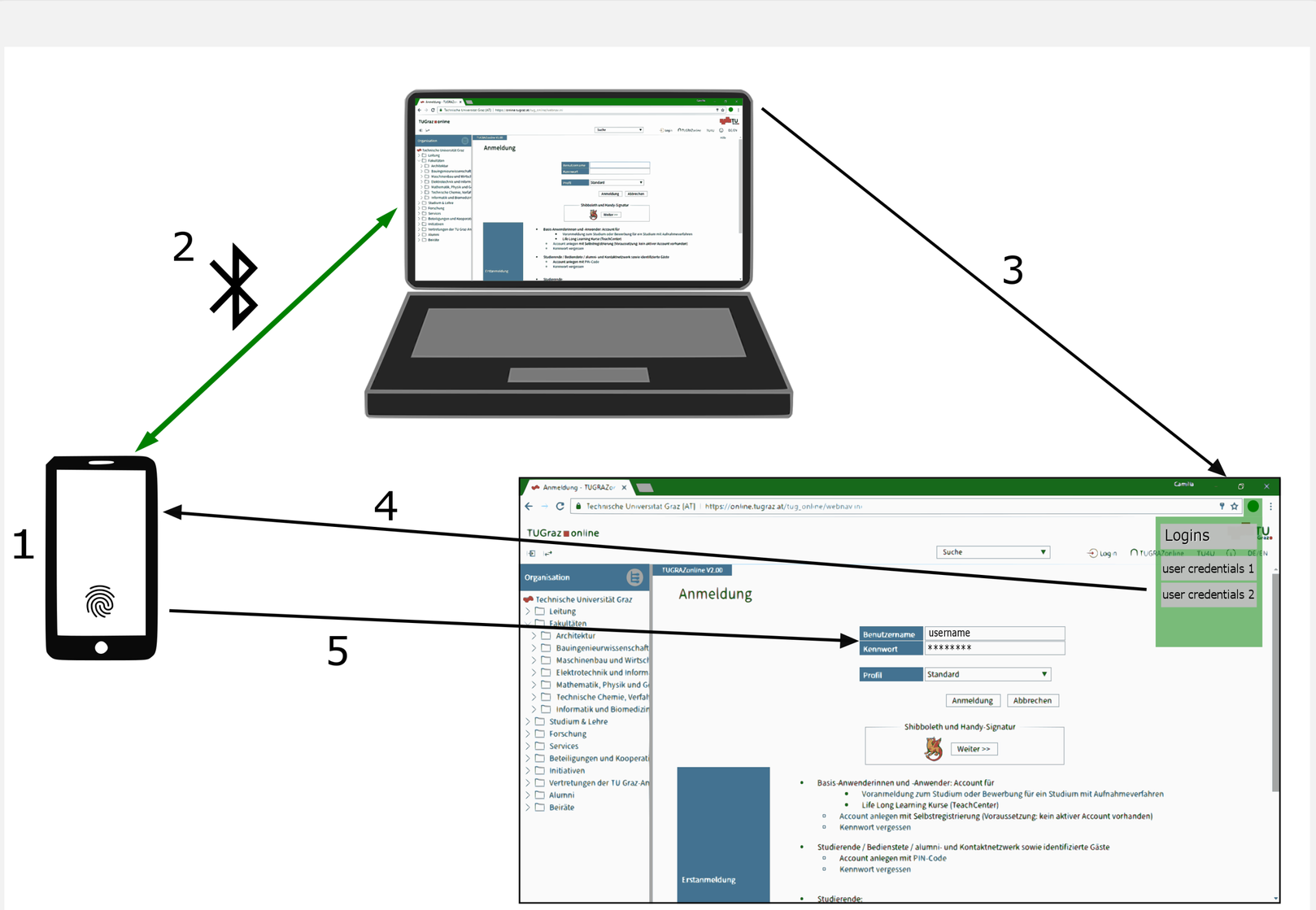
Motivation behind the Project

There exist a large amount of applications that offer a credential storage to synchronize data between multiple devices. They often rely on cloud services where data confidentiality cannot be guaranteed. Mobile phones offer a secure way to store data, for example through hardware backed key storage. By relying on this technology we can provide secure data storage.
The motivation of this project is to provide a safe possibility for mobile phones to store credentials that are available to the user on demand.

Goals of the Project

- Creating a new workflow to store and handle user credentials.
- Credentials are available to user on demand.
- No dependency on cloud services.
- Authentication through fingerprint scanning or master password.
- Easier and more efficient for the user to store credentials.

Procedure of the Login



1. Store user credentials on device
2. Establish Bluetooth connection between device and browser extension
3. Check all available logins for this website
4. User selects desired login account
5. Authentication on device with fingerprint or master password

Expected Solution

We will work towards a mobile credential store. The application will communicate via Bluetooth with a browser extension to provide device independent access to the stored data. Using a Bluetooth connection gives us a secure environment for transferring the credentials to the browser.
Before the credentials are stored in a database on the device, they are encrypted using a key, which is located in a hardware-backed keystore. This ensures that the key cannot be retrieved by unauthorized access for decryption of the data. This clearly reduces the attack surface. Therefore, confidentiality as well as availability of the data can be provided at the same time.