Android Bluetooth Credential Store

Camilla Reis, Dominik Ziegler

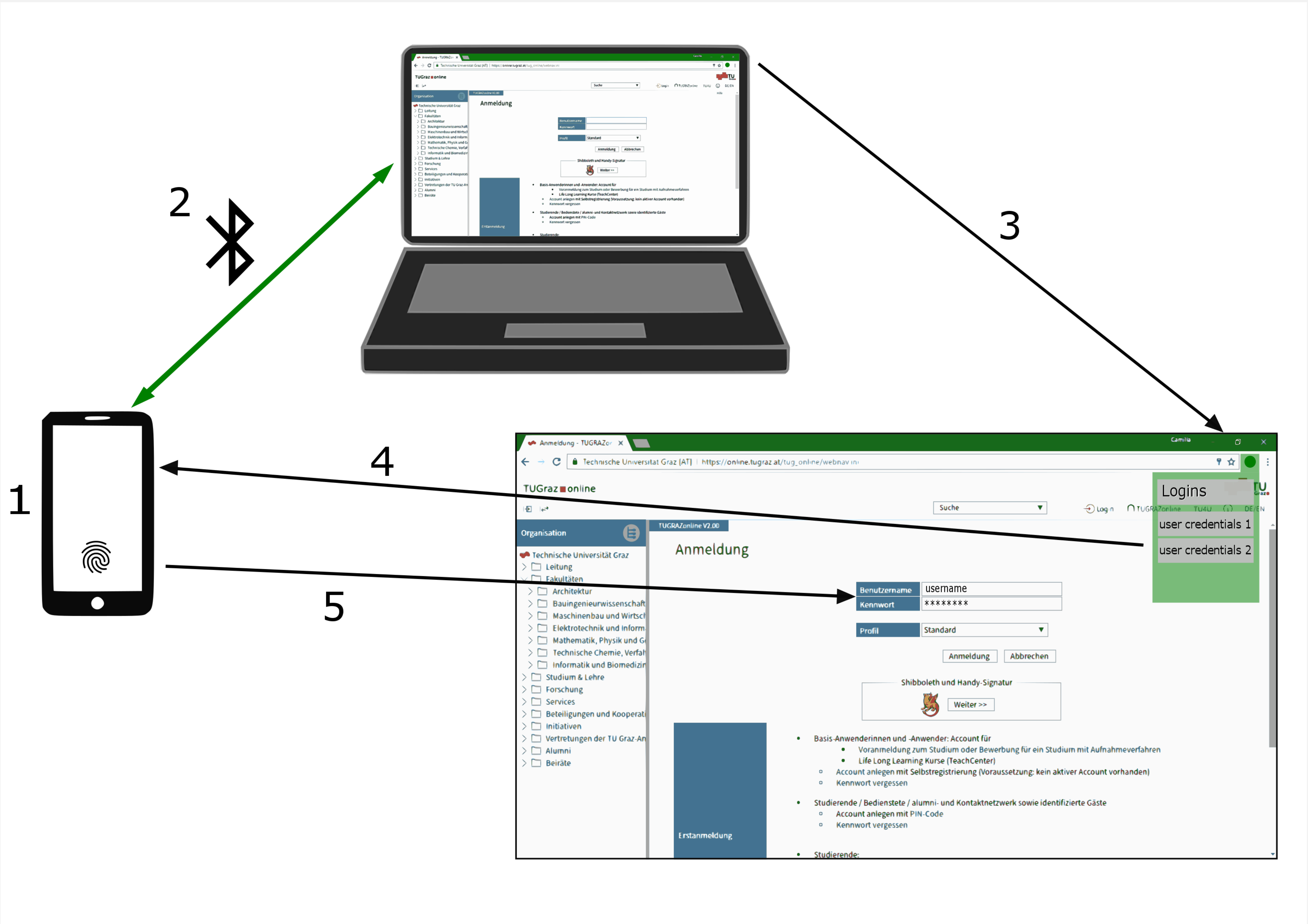
Institute for Applied Information Processing and Communications
Graz University of Technology

Motivation behind the Project

There are already lots of applications that offer credential storage. They often rely on cloud services where user confidentiality can not be guaranteed. Other applications assure confidentiality by not synchronizing data in any form but the availability of the data is restricted.
The motivation of this project is to provide availability and safety of user credentials by using a mobile password manager.

Goals of the Project

Creating a new way to store and handle our credentials.
No reliance on cloud services and secure transfer environment is provided through Bluetooth.
Aiming for a safer method of storing personal information, than the ones already available.
Authentication through fingerprint scanning or master password.
More easy and efficient for the user to store their credentials.



Procedure of the Login

1. Storing all user credentials on device
2. Establishing Bluetooth connection between device and browser plug-in
3. Checking all available logins for this website
4. User selects desired login account
5. Authentication at device with fingerprint or master password

Expected Solution

As mentioned we will work with a Bluetooth connection between device and browser plug-in. This gives us a secure environment for transferring the user credentials for the login procedure.
Before the credentials are stored in a SQLite database on the device, they are encrypted using a key, which is located in a hardware-backed keystore. This step differs from other already available credential stores. This ensures us that the key cannot be retrieved by unauthorized persons or devices for decryption of the data and the attack surface can be clearly reduced. Therefore, confidentiality as well as availability of the data can be provided at the same time.

LaTeX TikZposter