

ANDROID BLUETOOTH CREDENTIAL STORE

Camilla Reis, Dominik Ziegler

Graz University of Technology

Motivation behind the Project

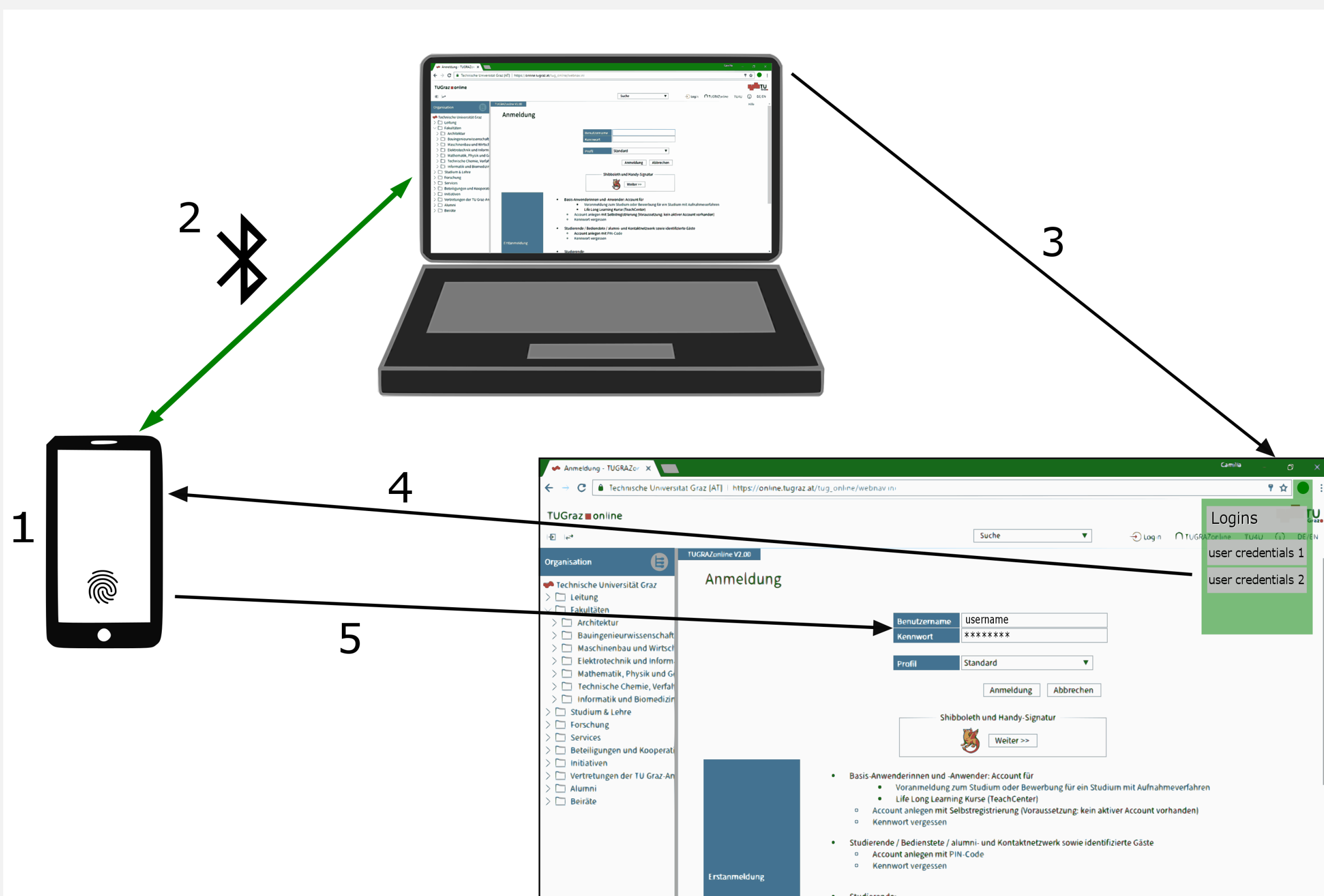
Revolutionizing the way we store and handle our passwords and other credentials.
Aiming for a safer method of storing personal information, than the ones already available.
Making credential storage more easy and efficient for the user.

Advantages and Goals

Assuring a more secure method of logging into accounts on user's PC or laptop.
No reliance on cloud services and secure environment through transfer via Bluetooth.
No need for typing in and remembering user credentials anymore.
Authentication through fingerprint scanning or master password.

Procedure of the Login

1. Saving 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

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 ensures us that the key cannot be retrieved by unauthorized persons or devices for decryption of the data.