# Digidow's Biometric Sensor

Proposal for Master Thesis

Michael Preisach BSc

December 2018

## 1 Motivation

Digital Shadow (Digidow) is a research project of Prof. Mayrhofer, head of the Institute for Networks and Security (INS). The project is aims to be a secure and privacy-friendly solution to identify or authenticate a person to a requester. Figure 1 shows a graphical overview of the proposed identification process in this project.

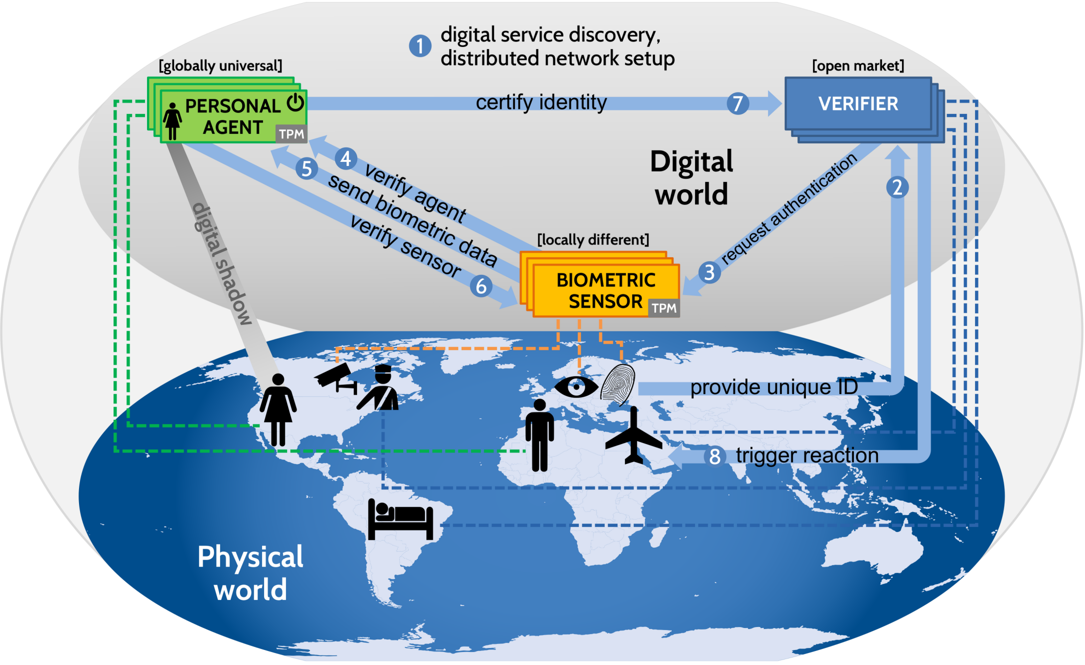

Figure 1: Overview of the Digidow Project

The illustrated distributed system works as follows: In the first step, the service discovery (1), each devices need to find each other over a distributed network. When a person requires to be verified by that system, he or she initially should provide a globally *Unique Identifier* (UID) (2). This could be Name, date and location of birth, address and so on. Given this information, the *Verifier* asks the *Biometric Sensor* (BS) to gain biometric data of this person (3). In fact, one can gain any form of data which uniquely identifies a single person. Once, this data is retrieved, the BS has to find the user's *Personal Agent* (PA), by using the provided unique ID. Only the PA is able to identify the user, because it is the only instance holding personal and biometric data of the corresponding person. The steps (4) and (6) are required to create trust between the PA and the BS. Only in a trusted environment, the biometric data payload is submitted. With this data the PA is able to decide whether the claim is correct or not. This result has to be signed by the PA and sent to the Verifier which itself proves whether this authentication message is valid (7). Based on that decision and the content of the message, the Verifier can then trigger an adequate reaction (8). This system is designed to implement the *Need-To-Know* principle and thus privacy for the user.

# 2 Scope of the Thesis

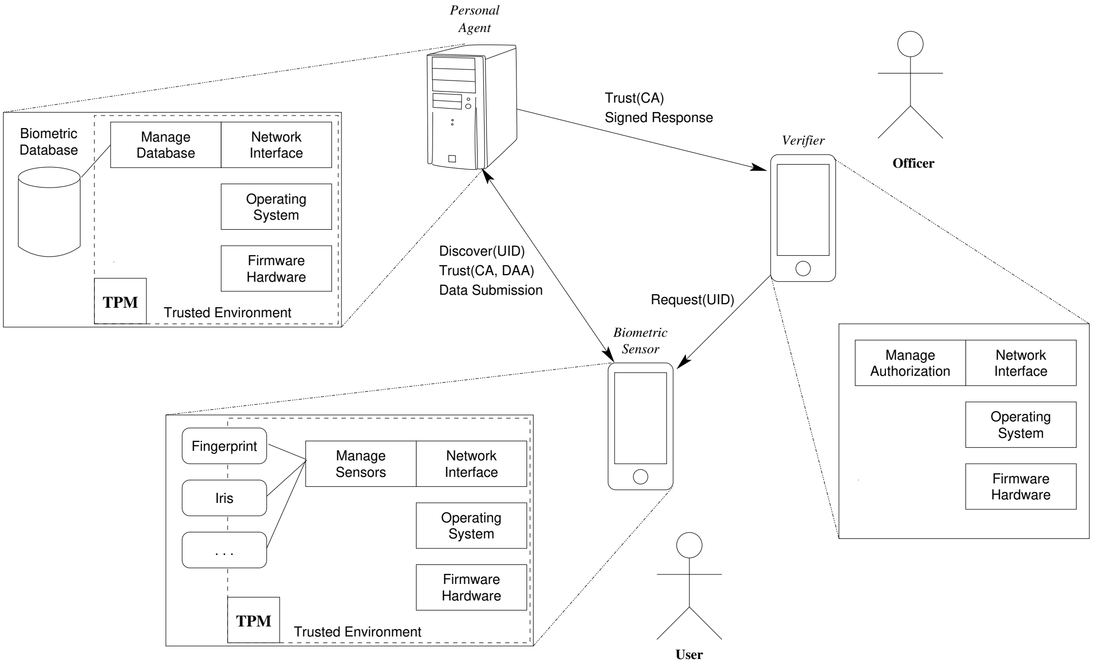

Figure 2: Physical view of the three instances

This master thesis will cover a major part of Digidow's BS. Figure 2 shows an example scenario where three physical devices are involved to explain the tasks of the BS.

The Verifier sends a request to the BS containing an UID of the user to be verified, signed with the organization's private key. The BS then gains the needed biometric data and finds the corresponding PA with the provided UID. Although Verifier and BS are usually reachable within the local network, the PA is available only via a worldwide network which implements privacy-features. After establishing a connection, both BS and PA require a *Trusted Platform Module* (TPM) to create a trusted environment on the own system. The TPM ensures that the system is in a provable, well defined state that can be shown to external readers. *Direct Anonymous Attestation* (DAA) allows then to proof the validity of another device anonymously. Thus, BS and PA use DAA to verify the other instance and to generate trust between both devices. When having a trusted environment over the network, the gained biometric data as well as the public key information of the Verifier can be submitted to the PA.

## 2.1 Practical Part

This thesis aims to implement the features defined in the previous subsection. Therefore it is assumed that the network discovery delivers a function where the BS gets the corresponding PA using the provided UID.

The *Trusted Environment* for the BS as shown in Figure 2 describes the process that verifies the whole software stack (firmware, boot loader, kernel, driver, executed software, firmware of attached devices, . . . ) by the TPM. Furthermore it should be possible to verify the attached biometric sensors. This depends however on whether the firmware and driver software could be extracted verified and installed on the device.

After having this system implemented, a demonstration platform should illustrate how this system works. The not yet provided, but required interfaces will be simulated in a way that allow to demonstrate the function of the implemented part of this thesis.

## 2.2 Discussion

The implementation and demonstration allows a discussion about benefits and drawbacks of the implementation and a comparison to other possible implementations. This thesis should cover and discuss the following questions:

- How is trust implemented in the BS?
- How is trust generated between PA and BS in both directions?
- What can be done to protect the sensible/biometric data within the system? Which risks are relevant for protection?
- What is necessary to protect sensible data for submission over the network.
- What are the limitations by using a TPM?
- Which systems need a TPM and why?