Digidow's Biometric Sensor

Proposal for Master Thesis

Michael Preisach, BSc

December 2018

1 Motivation

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 planned identification process in this project.

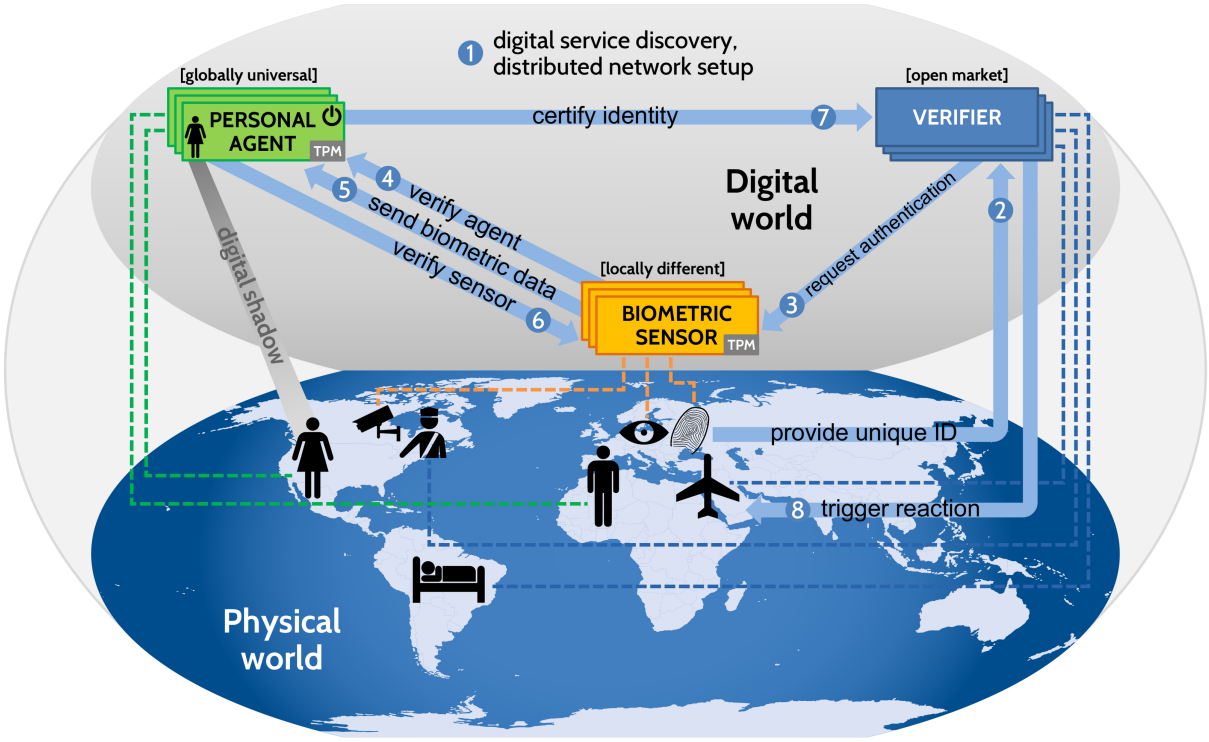

Figure 1: Overview of the Digidow Project

After service discovery (1) over a distributed network, a user should be able to be identified by that system. When a person intends to get access by this system, she initially should provide a unique ID (2). Given this information, the *Verifier* asks the *Biometric Sensor* to gain biometric data of this person(3). In fact, one can use any form of data which uniquely identifies a single person. Once, this data is retrieved, the Biometric Sensor finds the user's *Personal Agent*, builds trust (4, 6) in between and submits the data subsequently(5). Since the Personal Agent holds all required data to identify its corresponding user, it is able to

decide whether the claim is correct or not (7). Based on that decision, 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

This master thesis will cover a major part of the *Biometric Sensor*. When a request of the *verifier* appears, the system captures data from the biometric interface, wraps and submits it to the *personal agent*, where further processing is done. Two essential questions arise while doing so. First, the system has to identify the corresponding personal agent. This problem should be solved with the service discovery part. Second and more important for this thesis is the question, how the sensor system and the personal agent trusts each other. Therefore one is able to generate trust via a *Trusted Platform Module* (TPM). Another question is how the system interacts with attached sensors that get the sensible data.

2.1 Practical Part

One goal of this thesis is to set up a system which is *trustworthy*. This means that the system's TPM can verify every major part of the executed software (firmware, boot loader, kernel, driver, executed software, firmware of attached devices, ...).

Furthermore a program should read data from attached sensors. This data should then be sent to the personal agent for further processing. Before this can be done, both, Personal Agent and the Biometric Sensor have to trust each other. The TPM provides a function called *Direct Anonymous Attestation* to tackle this problem. Since the TPM is a passive part in the system, these features have to be accessed with a custom program.

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.

3 Discussion

The implementation and demonstration allows then 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:

- What is trust?
- How does the TPM benefit to the system's trust?
- What are the limitations by using a TPM?
- What is necessary to trust a system with a TPM?
- How can trust be generated between Personal Agent and Biometric Sensor?