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.

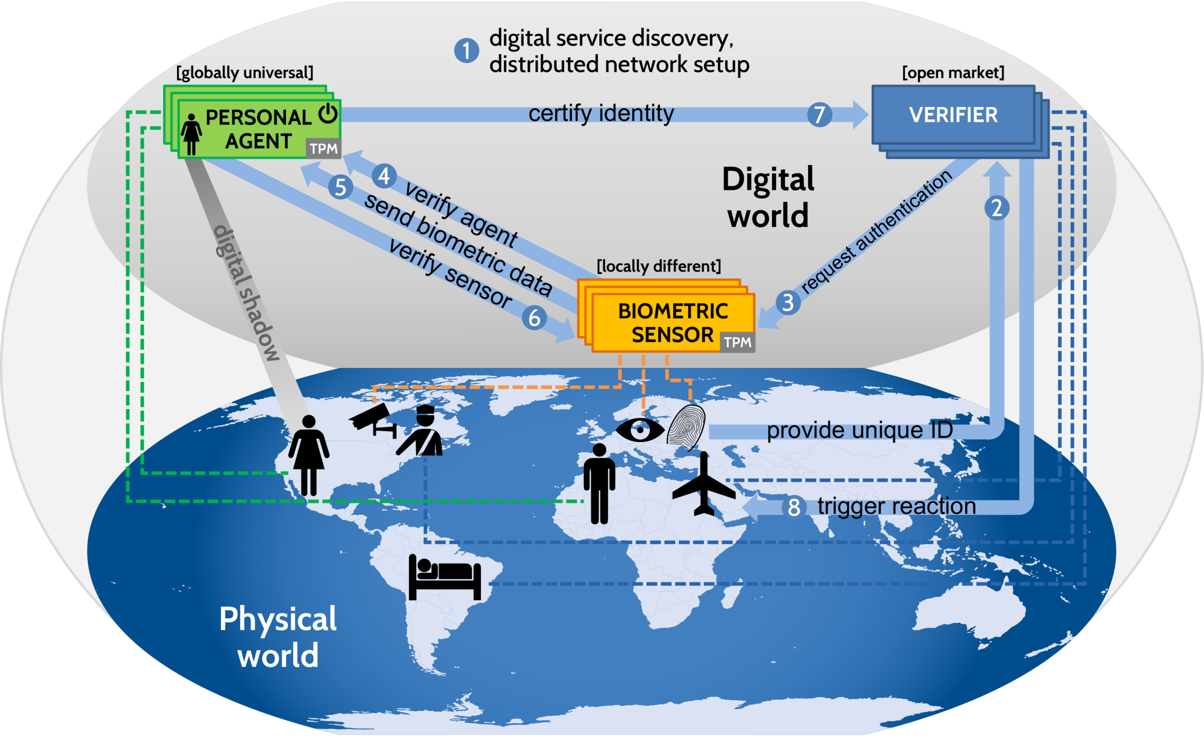

Figure 1: Overview of the Digidow Project

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 ID (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 to identify 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. Since the

PA holds all required data to identify its corresponding user, it 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

This master thesis will cover a major part of Digidow's BS. 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 thesis will assume, that a personal agent is available for the corresponding user. Second and more important for this thesis is the question, how the BS and the PA trusts each other. A *Trusted Platform Module* (TPM) is able to address this problem by generating trust by cryptography. 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 the whole software stack (firmware, boot loader, kernel, driver, executed software, firmware of attached devices, . . .).

The next step is to find a way to trust the yet unknown PA instance. Again the system's TPM may help with a function called *Direct Anonymous Attestation* (DAA). Both, BS and PA have to trust each other to submit the biometric data payload to the PA for further processing. During this phase, privacy features should be implemented to prevent misuse with sensitive data from the user.

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 can a BS find the corresponding PA?
- 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 are the limitations by using a TPM?
- Which systems need a TPM?