

# Security of digital banking systems in Poland. Users study 2019.

Wojciech Wodo, Damian Stygar

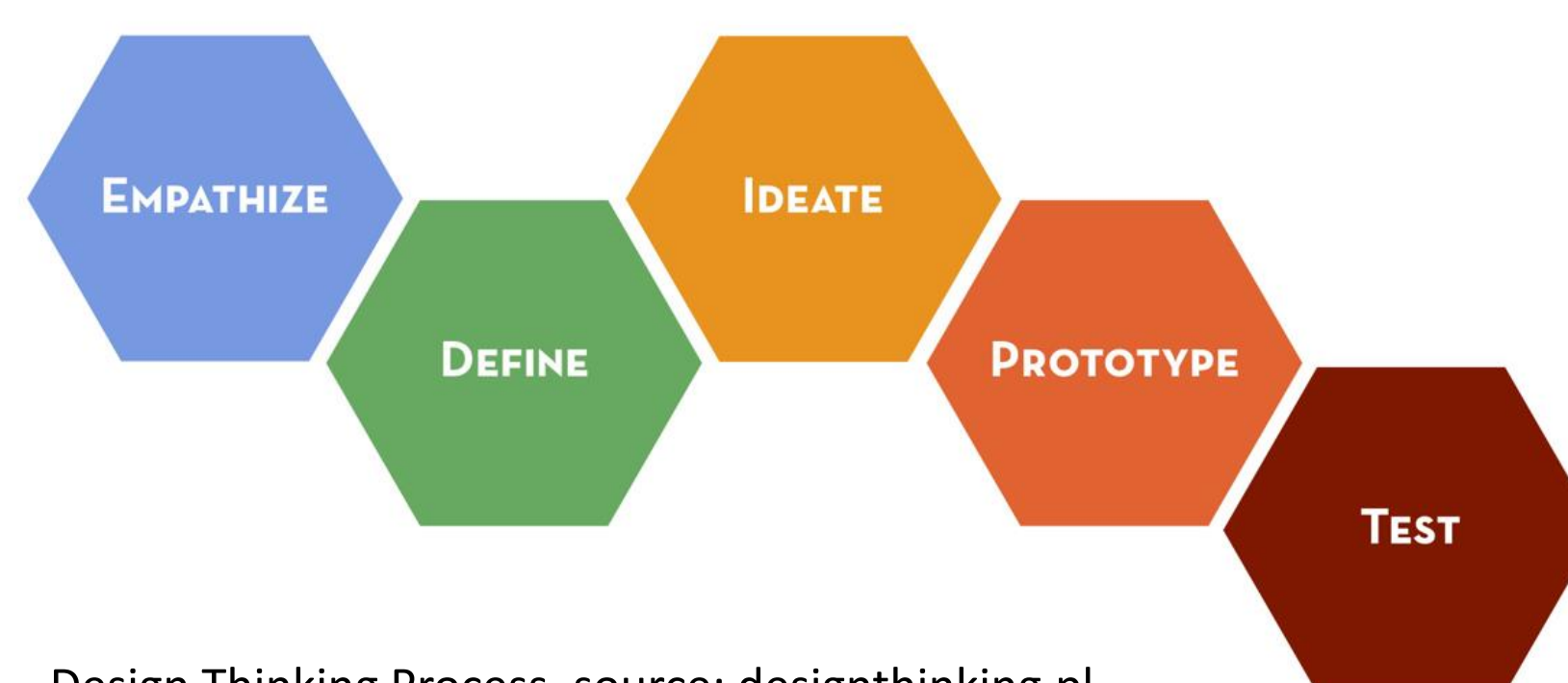
Department of Fundamentals of Computer Science, Wrocław University of Science and Technology, Poland

## Introduction

The year 2019 for the development of digital services and digitization of administration in Poland was very significant. We mean both state administration services, where tax settlement has been fully started for the first time - your e-PIT, new ID cards have been introduced with the electronic layer, the mObywatel application enabling confirmation of identity, but above all preparing the financial sector for the implementation of the PSD2 Directive. This state of affairs is very pleasing from the point of view of economic development and increasing the comfort of implementation of many activities, both private and business. However, behind the rapidly moving digitization comes the risk of cybersecurity threats, lack of user awareness, room for abuse and failure to adapt legal provisions quickly.

## Users' Study

In order to analyze the situation in the area of security technology of electronic and mobile banking services in Poland, exploratory research on the user market was carried out using the Design Thinking methodology. It is a method of creating innovative products and services based on a deep understanding of users' problems and needs, developed at Stanford University in California (Brown, 2009). The main assumption of this method is to focus on the user, because it is he who will bring the answer to the guiding questions related to awareness and approach to electronic banking security systems.



Design Thinking Process, source: designthinking.pl

## Personas

**Naive Nadia** - This person has little knowledge of current banking systems. She is usually familiar with the very basic principles of using electronic or mobile payments, and her knowledge of attacks on electronic banking is often low or negligible. This results in Nadia's conviction that she cannot be the target of a hacker attack, because she is an unattractive target because she does not have a large amount of financial resources and is not an important person.

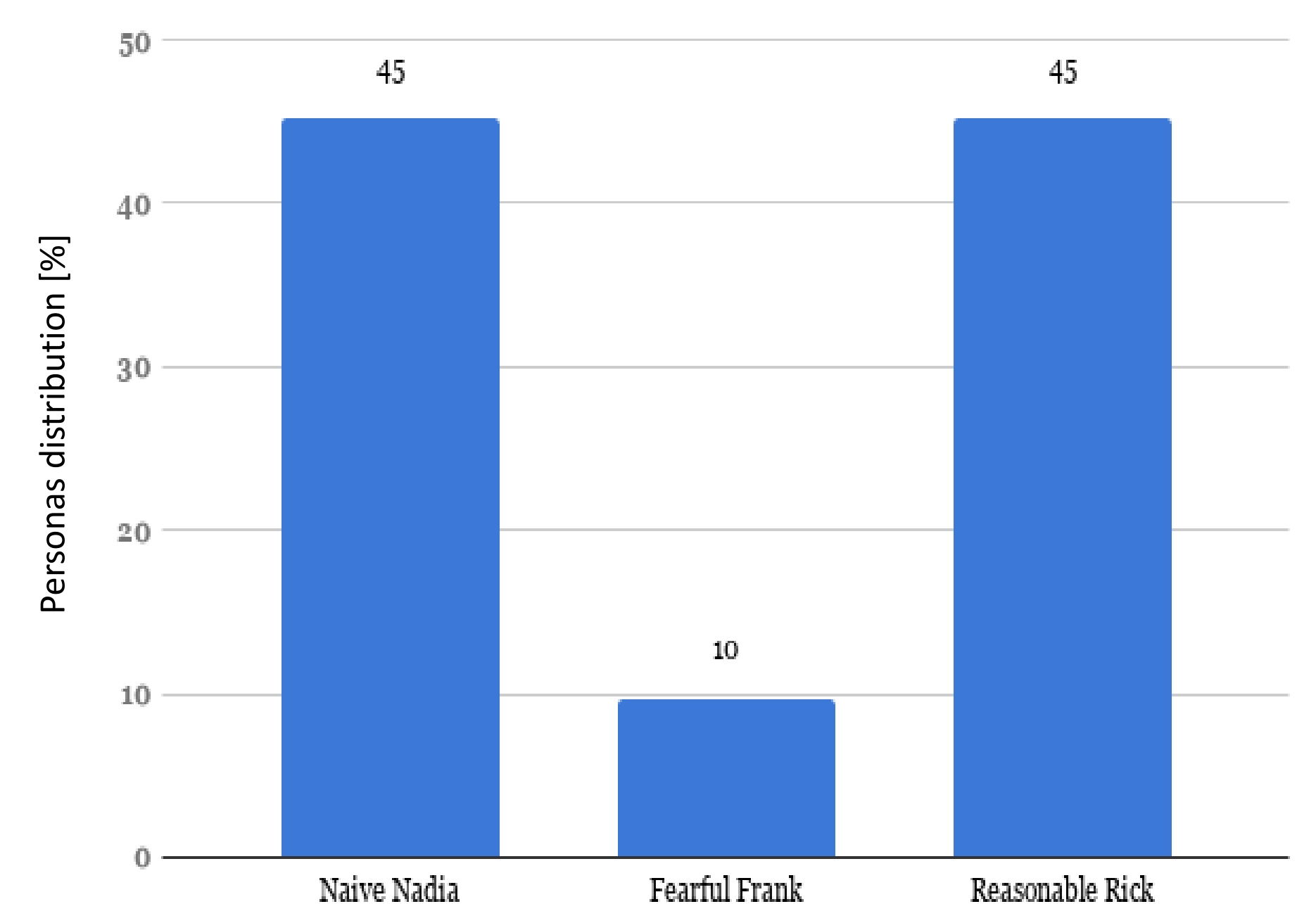
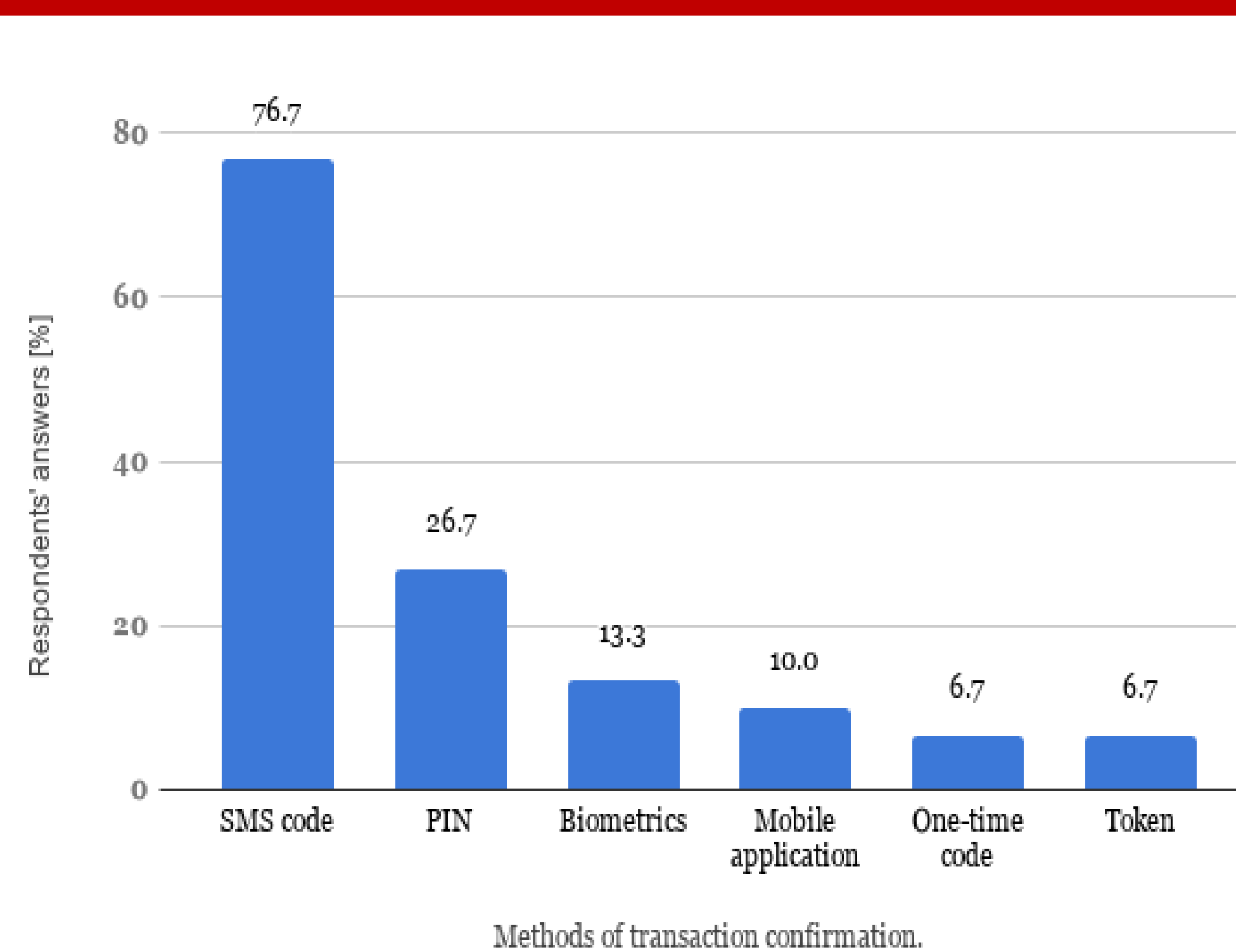
**Fearful Frank** - A person who has some concerns about electronic and mobile banking. Despite his fears, he uses modern solutions but with great uncertainty. Frank has some knowledge related to banking, but it is usually not complete, which can lead to various inaccuracies.

**Reasonable Rick** - A person well-versed in banking and new technologies, aware of the risks associated with cyberattacks on electronic finance. Rick knows and applies various security mechanisms and generally adheres to security principles. This person draws knowledge from various sources, they are often reliable and proven.

## How do you imagine an ideal electronic / mobile payment security system?

The most frequent indications are the greater use of biometrics, e.g. fingerprint, iris scan. Such solutions inspire the trust of respondents, regardless of their age or experience in electronic banking. This was indicated by both younger and older people. Based on some interviews, an image of a person is also created for whom comfort is definitely more important than safety. Such a person would gladly give up, for example, confirming activities by using SMS codes. This opens the way to the popularization of biometric solutions. In addition, attention was paid to the problem of the multitude of data for logging in to various websites. The respondents believe in the security of banking solutions and would be more willing to use the possibility of authentication through a banking service, as it is the case with the ePUAP website. This creates a chance to introduce solutions such as myID.

## What methods of transaction confirmation do you use?



## Persona's result

