# The SwissPass FIDO2 Protocol: Simple and Easy Authentication

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Dr. Annett Laube
Expert: Prof. Dr.Andreas Spichiger (Bundeskanzlei, Digitale Transformation und IKT-Lenkung)
Industrial partner: Michael Gerber - SBB CFF FFS, Bern

An authentication protocol for the new SwissPass version was developed that extends the FIDO2 protocol with an Attribute Provider. After authentication, the attributes of the SwissPass holder are available to Relying Parties. This relieves them of attribute management responsibilities and eliminates the tedious onboarding process. The result is a simplified authentication process that improves user privacy and friendliness while retaining the security features of FIDO2.

## Introduction

To explore new applications for the FIDO2 authenticator on the latest SwissPass card, a study was conducted on behalf of SBB. The study revealed a unique combination of features: Notably, a significant majority of the Swiss population already owns a SwissPass, thereby possessing a built-in FIDO2 authenticator. Furthermore, the card is linked to a SwissPass account. Based on these findings, an authentication protocol was developed. It complements the FIDO2 protocol with an Attribute Provider managing the SwissPass accounts.

## The SwissPass FIDO2 Protocol

The developed protocol is very simple to use: the SwissPass holders simply tap their SwissPass card once at an NFC reader of a Relying Party. The FIDO2 key registration and authentication processes are automatically conducted. In a second step after authentication, the SwissPass holder's identity is verified through a second channel such as email or SMS. Two protocol variants were developed: the first allows the Relying Party to request attributes for creating the second channel, while the second variant involves the Attribute Provider offering a communication service without sharing attributes.

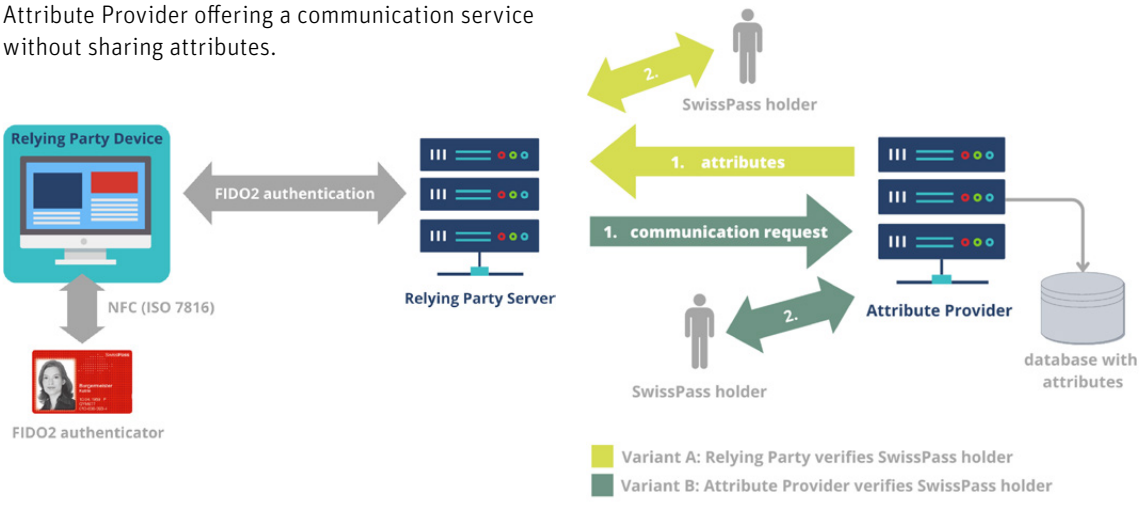
## Protocol Features

The developed protocol provides many benefits for both users and Relying Parties. For users, the protocol is simple to use since there is no onboarding process and most of the protocol is automated. Data is protected as much as possible, even concealing attributes from Relying Parties depending on the protocol variant.

Since the SwissPass card and account are managed by the central Attribute Provider, Relying Parties are no longer burdened with those tasks, reducing operational cost while increasing security through strong multifactor authentication.

## Outlook

The SwissPass FIDO2 Protocol will be further developed by BFH on behalf of SBB. One application of the protocol is an SBB internal project to provide charging stations for their electric vehicle fleet. More applications could be envisioned such as a secure and flexible door access protocol.




Actors involved in the SwissPass FIDO2 Protocol

Dominic Beat Martin Baumann
d.baumann36@gmail.com

Coralie Rohrer
coralie.rohrer@gmail.com