



PUSHPASS



»secure easy convenient«

KEYLABS UG

App based hardware-authentication
and password management

Our idea

Pushpass is the first password manager to unite the simplicity of an app with the security of a hardware two-factor solution in a single easy to use solution. Today users are faced with managing multiple logins for all their services. As a result, users and their information are vulnerable. Users end up using identical and/or weak passwords across multiple services or store their passwords insecurely in the cloud. Pushpass generates strong unique passwords and stores them securely on the users smartphone. When a user wishes to access a particular login from another paired device, a push notification is sent to his smartphone allowing the user to confirm or deny the access. Pushpass works just as seamlessly on the users smartphone as well. Because all the users sensitive information is stored locally, it never is at risk in the cloud. Furthermore, storing credentials and sensitive information locally ensures that the data remains accessible for offline use.

Team

Dmitry Nedospasov (Dr.-Ing.)
Bernhard Klammer (B.A.)
Roman Roibu (B.Sc.)

Sector

Security, Internet of Things

Mentor

Prof. Dr. Jean-Pierre Seifert,
Faculty IV – Electrical
Engineering and Computer
Science

Support

EXIST start-up grant (2015)

Year founded

2016

www.pushpass.io

Gefördert durch:

