DIAC

Disposable Identity for Access Control

by asvin and OdinS

KEY BENEFITS

- NO NEED OF SMARTCARDS
- NO NEED FOR RFID CHIPS
- NO BIOMETRIC SYSTEMS
- NO NEED FOR PIN CODES
- ✓ EASIER GDPR COMPLIANCE
- ✓ LESS VULNERABLE FOR DATA BREECHES
- ✓ MORE ENDUSER-TRUST IN PERSONAL DATA PROFILING

Currently, Access control systems are mainly based on user identification using Smart cards (with chip) or Contactless cards (RFID).
In other cases are also used biometric systems such as fingerprints or PIN codes.

But these identification systems have privacy and security issues:
user authentication in an access control system, such as loss of the card, data breeches, cloning of cards, disclosure of access PIN to another person, etc. In this context, our solution aims to solve most of the problems that current access control systems have, using innovative solutions and avoiding direct user interaction with access control through de Disposable Identity Framework.

A Disposable Identity is a contextual and temporary identity, limited in terms of scope, time, location allowing endusers to show specific and limited information/credentials in order to validate for a service, in our case, access control of the building.

Our approach overcomes the drawbacks of the current acces control systems in which license to access is granted to individuals and for indeterminate lengths of time.
It also makes sure the issuer limits GDPR compliance by collecting too much irrelevant data, and be less vulnerable in case of data breeches.

The project adds to the debate on identity - digital identity- that has become more mundane since the pandemic. Its approach to privacy preserving access control contributes to more quality of trust of endusers in their profiling of personal data to which recently a large number of citizens have become very aware.

asvin.io

SECURIT

odins.es

This project has received funding from the European Union´s Horizon 2020 research and innovation programme und grant agreement No 958284

Contact:
Rafael Marin-Perez | ODINS
rmarin@odins.es