
# Achieving Security from Cryptography AND Biometrics

Tjerand Silde, Norwegian Biometric Forum, 25.05.22

# A Short Bio

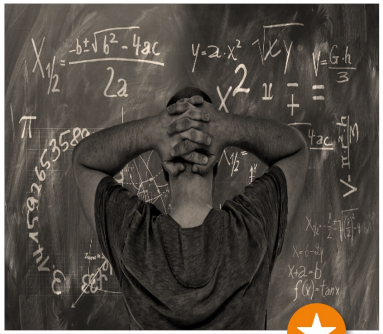
- I am a PhD student in cryptography at NTNU
- Working on designing new, secure protocols
- I submitted my PhD thesis last week

# Pone Biometrics

- I am working part time as a Security and Cryptography Engineer at Pone Biometrics

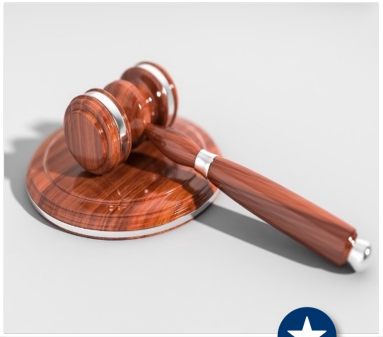
- I will start a Postdoc conducting research on authentication protocols

# Pone Biometrics



**University and R&D**

**Norwegian Company**



**Patents granted**

**Expert Team**

**Pilot Partners Market**

# OFFPAD

Discreet, 2,5 mm thick

Slips into mobile cases and wallets

Separate ARM-Cortex M4 processor

Infineon secure element

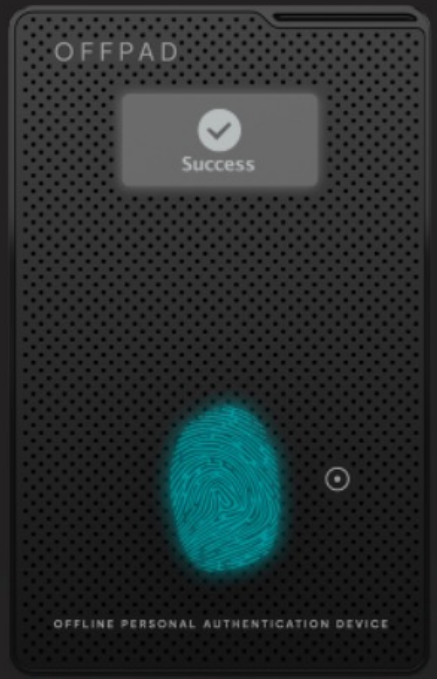
IDX3200 fingerprint sensor

Trusted e-ink display

1 Mb Flash

NPC 102A2EV

Complies with highest security standards




Simple log in, no password required, no need for updated passwords

Faster log in, immediately with one touch

Always with you, store it together with your phone

Enables single sign on (SSO) with your fingerprint

Works with all FIDO2 certified apps and services, including IAM platforms

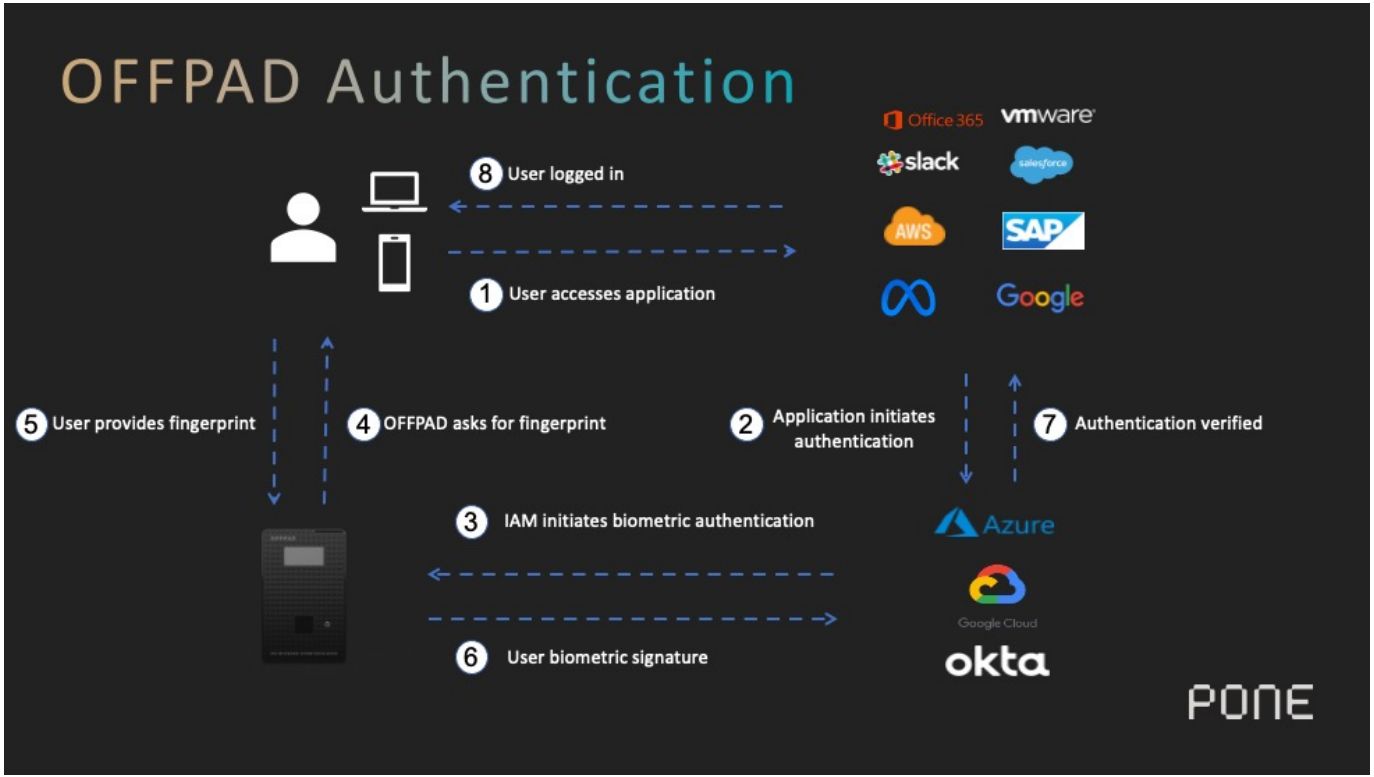
User-friendly and decentralized

Open API to work with all endpoint devices

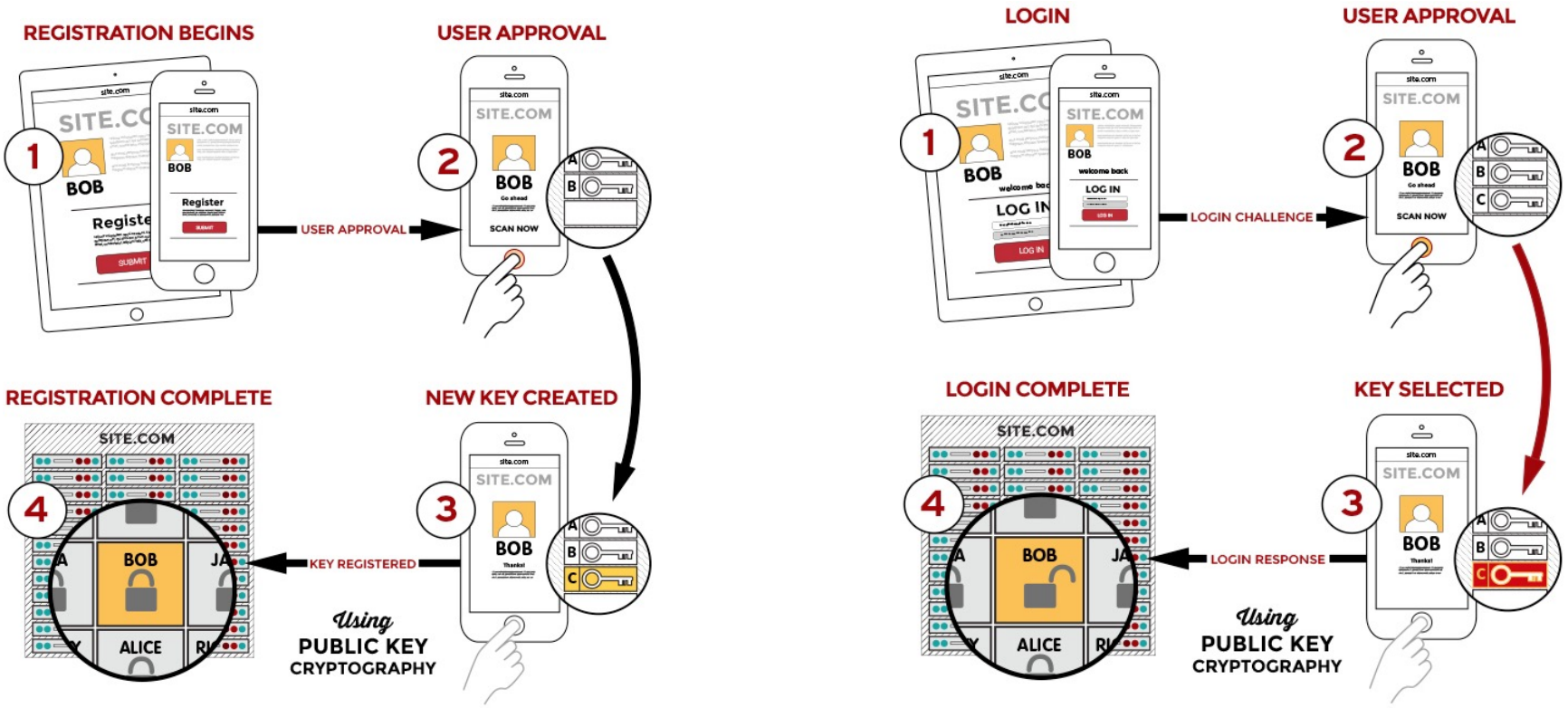
Seamless integration with IT structure

One user per card

# OFFPAD


OFFPAD Authentication
8 User logged in
1 User accesses application
5 User provides fingerprint
4 OFFPAD asks for fingerprint
2 Application initiates authentication
7 Authentication verified
3 IAM initiates biometric authentication
6 User biometric signature
Office 365
vmware
slack
salesforce
AWS
SAP
Google
Azure
Google Cloud
okta
PONE

# The FIDO Protocol



# White House Memo

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

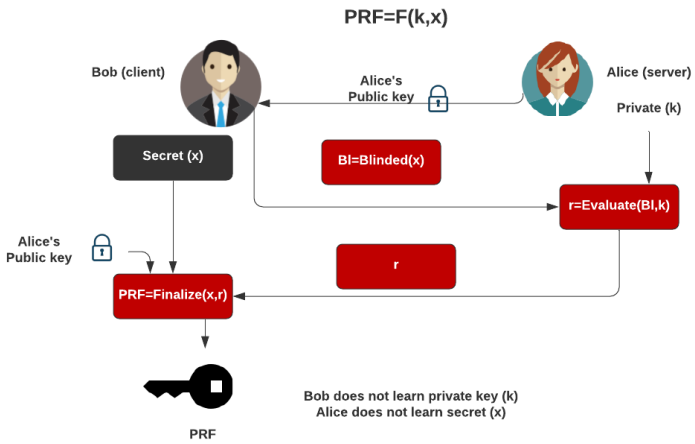
# PONE Research and Engineering

- Upgrade to post-quantum security
- Secure implementation
- Quality and efficiency of biometric sensors

- Key-management
- Robust backup
- Upgrading firmware
- Secure delivery
- Self-hosted services

# Research on Biometrics AND Cryptography

- Design protocols where we can boost security by combining biometrics AND cryptography?
- Oblivious-PRFs, private set-intersection, private information retrieval, zero-knowledge proofs, multi-party computation, homomorphic encryption, …
- Design protocols that are secure against quantum adversaries



# Thank you! Questions?

Contact: tjerand.silde@ntnu.no
Website: tjerandsilde.no