PONE
BIOMETRICS

Black paper
20210901

WHY A STRONG AUTHENTICATION STRATEGY IS A MUST

Pone Biometrics A/S

Hard facts

THE PASSWORD IS DEAD; LONG LIVE THE HUMAN TOUCH

A single password reset request costs companies on average $70 every time. 30% to 50% of all IT help desk calls are regarding password resets. 57% of employees prefer passwordless authentication, and 56% would recommend a hardware device to manage their authentication.

THE HARSH CYBERSECURITY BUSINESS REALITY

Most successful cyberattacks are result from human errors, and 70% of all breaches originate from end-point devices. Deploying a solid security strategy makes sense. Besides analyzing your overall digital systems and working systematically to counteract weaknesses, you can take an effective first vital measure by:

→ Adding hardware-based authentication devices to perform strong authentication by leveraging fingerprint biometric

→ Optimizing the cybersecurity education of the individuals to increase the digital protection of your most sensitive information

51%	55%	69%	67%
Employees use the same password	Companies do not use 2-factor authentication	Employees share their password with colleagues	People do not use 2-factor authentication in their everyday life

The change has
only just begun

ZERO TRUST IS NOT A SECURITY SOLUTION. IT IS A STRATEGY.

The Covid 19 pandemic has forced many organizations to embrace remote work. It creates the necessity to protect sensitive information as data breaches exposed 36 billion records in the first half of 2020.

The Covid 19 pandemic forced many organizations to embrace remote work. This also accelerated the need to protect sensitive information as home networks often offer a poor security level. During the first six months of 2020 data breaches exposed 36 billion records. In May 2021 alone, another 8.4 billion passwords were published online. Recently one user posted billion password entries onto a popular hacker forum, exposing credentials such as private login information for Gmail, Facebook, Apple and PayPal. In other words, everybody's security is at risk.

A ZERO-TRUST SECURITY MODEL IMPROVES THE CYBER-SECURITY STRATEGY BY CREATING:

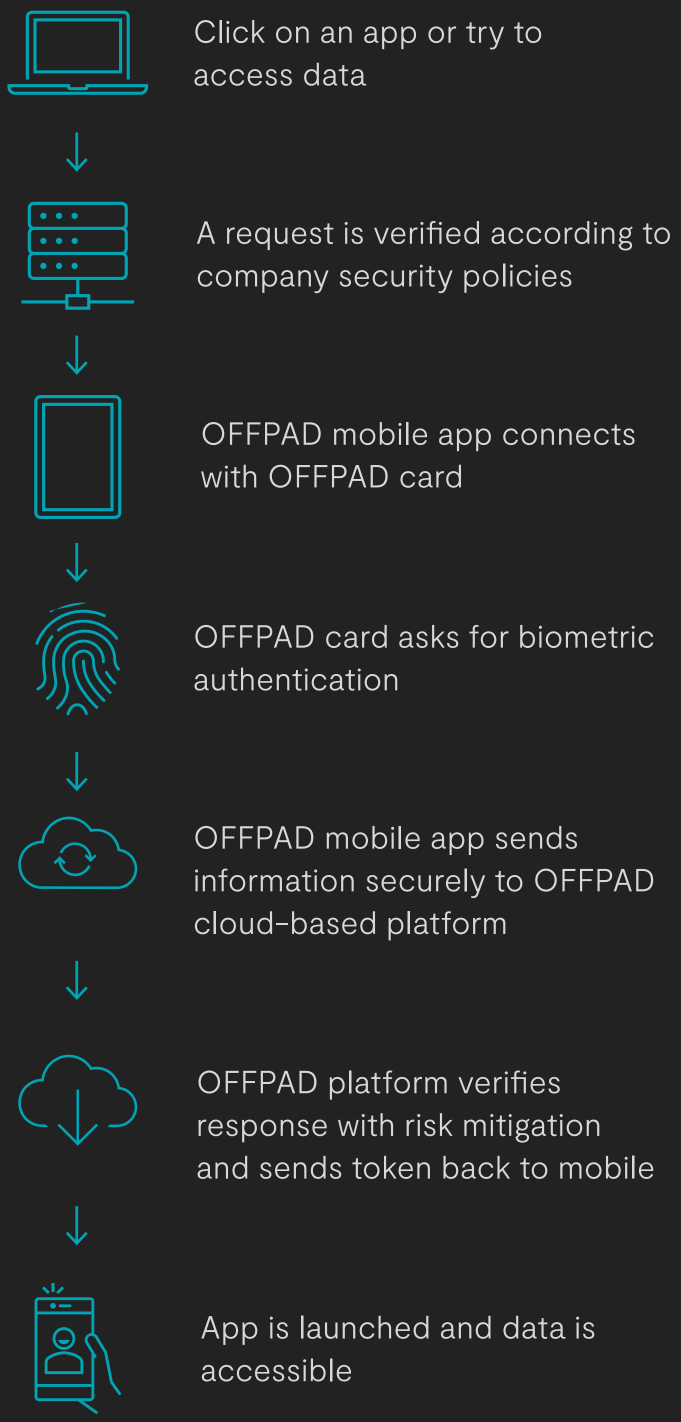
→ Network segmentation to bit by bit control traffic flow and reduce attack vectors

→ Trust zones that minimize the number of authorized users, protocols and transactions to access sensitive data

→ Zero trust segmentation that centralizes unknown threats detections, monitor network, data traffic and reports

Security	SE EAL5+Infineon SLJ52GDT111CS	Height	54 mm
	Global Platform™ 2.1	Width	85,6 mm
	Java Card™ 3.0.5	Thickness	2,25 mm
	RSA 1024/2048 bits	Communication	BLE (Bluetooth 5.0) NFC
	DES/3DES		ISO/IEC 14443-B
	AES 128/192/256 bits		
	SHA-1, SHA-2, SHA-256		
Algorithms	OATH TOTP		
	FIDO2		
Display	e-ink 2.5		
Biometric	IDX3200 fingerprint sensor		
Battery	Wireless charging		

A simple solution
is at hand



Click on an app or try to access data

A request is verified according to company security policies

OFFPAD mobile app connects with OFFPAD card

OFFPAD card asks for biometric authentication

OFFPAD mobile app sends information securely to OFFPAD cloud-based platform

OFFPAD platform verifies response with risk mitigation and sends token back to mobile

App is launched and data is accessible

CONSTANT HIGH-LEVEL R&D PREPARES THE WORLD FOR THE FUTURE

Most existing cybersecurity solutions and sensitive transactions are based on traditional cryptographic algorithms. The emergence of embedded systems and the rise of quantum computing have forced companies to rethink their product strategy quickly. Today, it is necessary to optimize the memory size and energy consumption of the cryptographic algorithms and to design innovative and new post-quantum algorithms.

Pone Biometrics has top research laboratories and researchers and continuously invests in research and development to deliver top-of-the-range solutions that combine convenience and high security. Our latest projects focus on:

→ Developing and embedding state of the art cryptographic mechanisms to include lightweight cryptographic, incremental cryptographic and post-quantum cryptographic

→ Testing, selecting and embedding the best biometric sensor and associated enrolment and matching algorithms to protect the hardware against attacks on biometric capture devices (PAD) and to ensure that the match on the card complies to current security legislation and trends

→ Strengthening traditional firmware update by integrating recent trusted computing-based firmware update

Top research laboratories and researchers

NTNU
Norwegian University of
Science and Technology

simula

Fraunhofer