VALMIDO

Secure Digital Life

UNIFIED AUTHENTICATION UX ON SMARTPHONE & COMPUTER
THE DEVICE-BASED AUTHENTICATION FOR ALL BUSINESSES AND USERS
VALMIDO MAKES AUTHENTICATION EASY, SECURE AND COST EFFECTIVE

THE FUTURE IS PASSWORD-LESS !

Every organization wants increased security while maintaining user friendliness when authenticating the digital credentials of their legitimate users.

There are multiple drivers behind the need:
- cost optimization of IT
- protection against ransomware and phishing
- more flexible remote working policies,
- simplified employee workflows

LONGER AND MORE COMPLEX PASSWORDS ARE NOT THE ANSWER !

A VERSATILE FUTUREPROOF INTEROPERABLE CERTIFIED FIDO2 IDENTIFICATION OFFER

1. THE FIDO2 CARD, a multi-application token in a zero-trust environment, becomes the security extension of your smartphone + your laptop by establishing wireless communication with both.

2. SDK + PHONE APP An open platform made to enhance user interaction when needed. An SDK and an App store allow you to be in control of your phone Apps

3. WEB SERVICES, allowing the user to self-manage services such as initialization, data back-up for theft/ loss declaration with smart restore

FINANCIAL BENEFITS

$72 SAVINGS PER EMPLOYEE PER YEAR
MICROSOFT CASE STUDY

Microsoft affirmed a monthly cost of $12M on password management services for its 163k employees, translating into a $72 cost for each password unblocking procedure!

Microsoft states that the likelihood of an account being compromised drops more than 99.9% if multi-factor authentication is used… and "Fido2 is the next generation MFA technology"   Source

ZERO ACCOUNT TAKE OVER
GOOGLE CASE STUDY

When Google upgraded from one-time mobile pass-words (OTPs) to Fido tokens: source

late '17	migration kick-off
by Jan '21	140 000 employees migrated
by Dec '21	Result: Zero account takeovers
	-92% fewer IT support calls

PERSONALISATION

Graphical personalisation is possible on both sides:
- On the sensor/screen side: adding a small logo or photo
- On the back: plenty of space to add large photo(s) & logo(s) using all traditional printing technologies

VALMIDO

S e c u r e   D i g i t a l   L i f e

Wireless charge

SIMPLE TO USE YET PACKED WITH TECHNOLOGY

Far from another "single usage piece of hardware", our Fido2 card is engineered around 6 key values:

Secure updates: on-card apps and firmware can be updated post issuance through secure protocols, making the card futureproof

Measurable security: onboard apps can be certified with the highest security certification such as Common Criteria and FIPS

Multi-application: benefits from state-of-the-art firewalling technology leveraged form 20+ years of smart card know-how. On board app examples include physical access control, Fido authentication, e-mail security, payment, access to classified files & documents, Block-chain asset management and more

Wireless connectivity: supports both NFC and BLE standard & open industry protocols supported by iOS, Android, MacOS, Windows, Linux and other operating systems

Biometrics: operated with fingerprints hence ensures personal traceability & non-repudiation If the card is lent or stolen, it cannot be used by a third party. Biometrics never leave the card!

Wireless charge with generic Qi charger typically runs for 1 week+

A USER-CENTRIC SOLUTION

- Digital credentials never leave the card
- Biometrics means nothing to remember
- Users control their personal & professional identities and when, how, and by whom these can be accessed
- GDPR compliant by design

WHAT'S NEXT: BOOK YOUR PILOT

We believe in a customized offer for each organization. To achieve the optimized solution, your pilot will comprise of:

DIAGNOSIS PHASE: you define your organizational workflow and processes

DESIGN PHASE: Illustrating how the Fido card will fit into your work environment during critical steps (employees and/or customers)

PILOT PHASE: A time-limited test loop with selected employees and applications where our technical support closely monitors for improvement opportunities

FINAL RECOMMENDATION: Valmido provides a report with lessons learned and recommendations on how scaling up should be envisaged

---

Simple & Secure Ensuring access is only granted to legitimate users

> INCREASE SECURITY & USER FRIENDLINESS WHILE REDUCING COST

> IMPROVE PRODUCTIVITY BY ALLOWING WORKFORCE TO FOCUS ON THEIR WORK