wultra | otpbank

PSD3/PSR Is Raising the Bar:

Fraud, Liability and the Future of Authentication

Ondrej Kupka

Regional Lead - Digital Identity

Oliver Jansta

Customer Relationship Manager

Irina Pohila

Head of Digital Channels & Digital Product Owner - OTP Bank

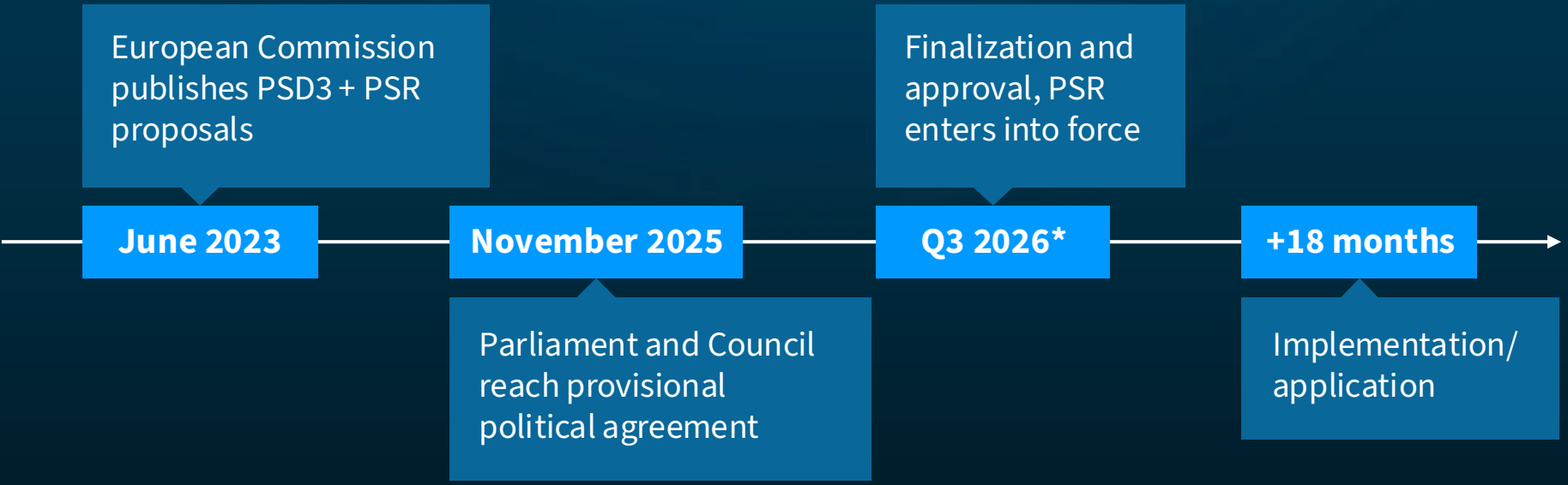
How modern fraud exploits authentication

Typical patterns:

- phishing and fake banking pages
- social engineering and impersonation
- remote-access / screen-sharing abuse
- APP or manipulated payment approval

PSD3/PSR: where are we now?

PSD3/PSR timeline



*Legislative process still ongoing. Direction is now much clearer.

What PSD3/PSR changes for authentication

From:

Do we perform compliant SCA?

To:

Is the authentication journey appropriate for today's fraud risk?

Implications:

1. **Fraud prevention**
2. **Liability and responsibility**
3. **Stronger, more inclusive SCA methods**

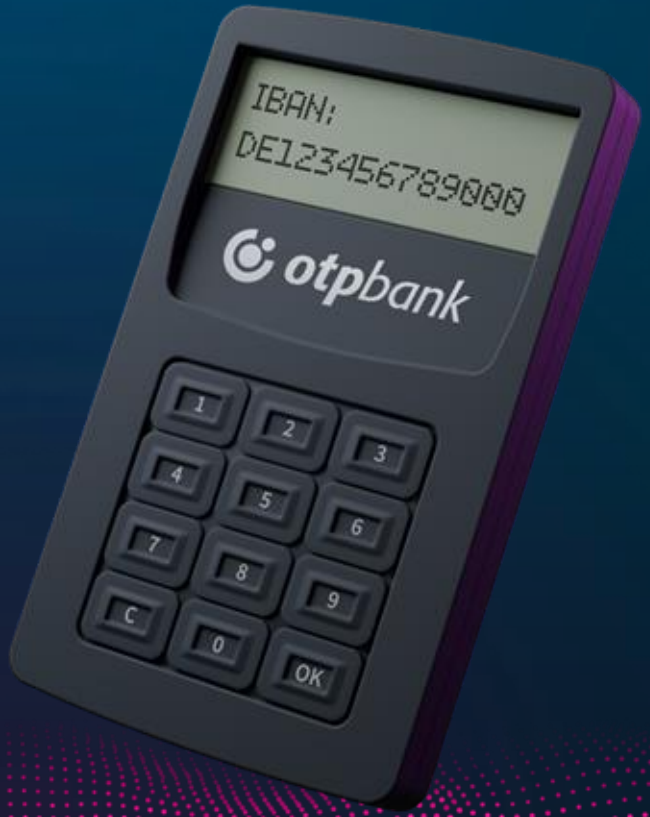
Three authentication questions for PSD3/PSR readiness

1. **Can it be phished or shared?**
   Can the authentication result be copied, dictated or reused?

2. **Does the user see what they approve?**
   Is transaction confirmation clear and independent?

3. **Does one method fit every customer?**
   Does the bank provide a suitable method for different segments?

otpbank



OTP Bank – Starting point

A high-assurance customer segment
with a legacy authentication journey

- **Corporate customers with elevated security requirements**
- **Existing legacy hardware OTP tokens**
- **Manual transaction-data entry and OTP transcription**
- **Need to improve both security and user experience**

Why did OTP Bank Moldova decide it was time to change?

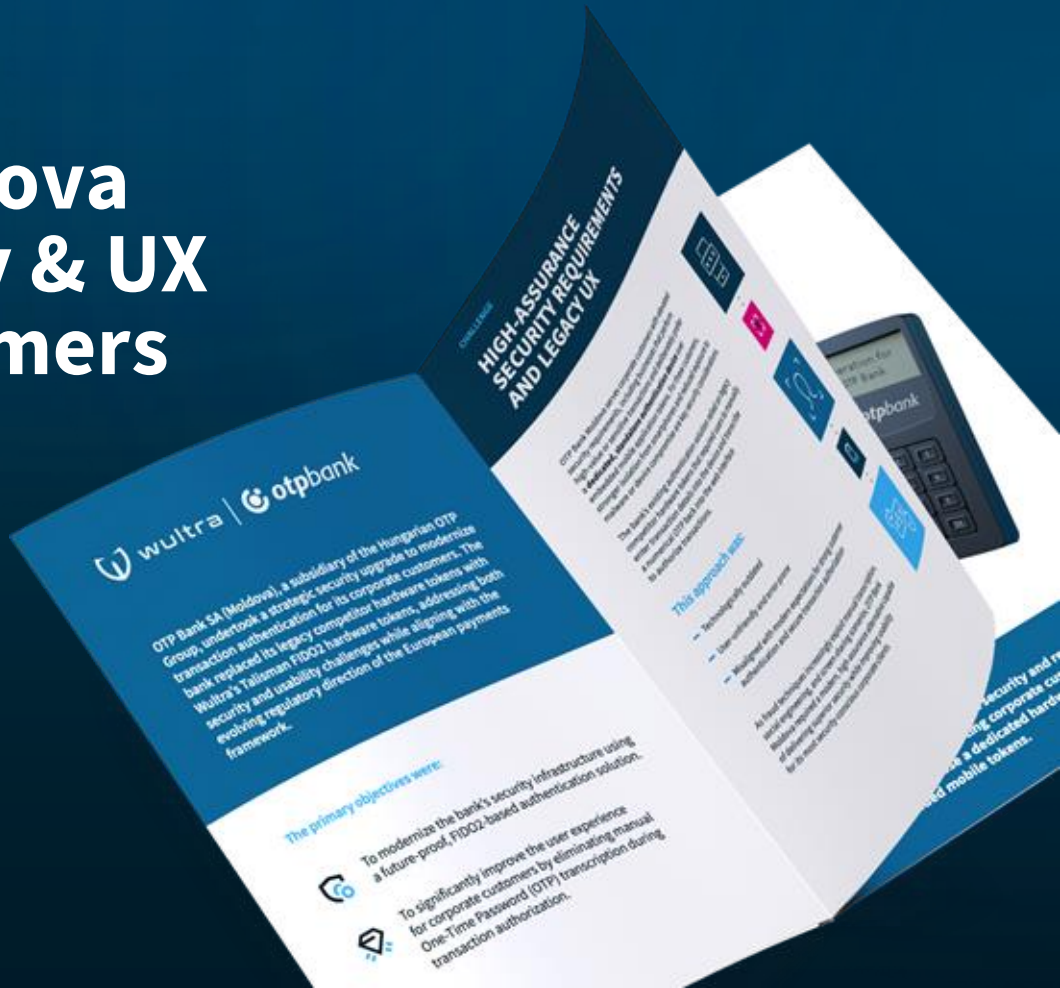
Why not simply move everyone to mobile authentication?

What did you expect from the new authentication solution?

What changed after deployment?

CASE STUDY

How OTP Bank Moldova Modernized Security & UX for Corporate Customers



DOWNLOAD
THE CASE STUDY

OTP vs FIDO2: What changes

How the authentication flow changes when a hardware token replaces manual OTP entry

OTP TOKEN — OLD

Shared Secret
Stored on both the device and the server

Phishable Code
Can be relayed to a fake site in real time

Manual Retyping
Read on one device, typed into another

Code Only
Confirms a number, not the transaction

TALISMAN — FIDO2 / WEBAUTHN

No Shared Secret
Private key never leaves the token

Origin-Bound
Won’t respond on a phishing clone

One Continuous Flow
No switching between devices

WYSIWYS
You sign exactly what you see

Why it matters

Business and compliance impact of moving to phishing-resistant hardware tokens

Phishing-Resistant

Blocks real-time relay attacks

User experience

No rewriting leaves less space for mistakes

Device authenticity

Audit trails and compliance

Smartphone-independent

Aligned with RSR/PSD3

Key takeaways

1. **Fraud-resistant**
   Beyond traditional Strong Customer Authentication
2. **Inclusive**
   Mobile-first, not mobile-only
3. **Frictionless**
   Better security can mean better UX

Get a free sample!

About Wultra

Own digital identity solutions
across software and hardware

2014
FOUNDED

Backed by major financial groups

Gartner
RECOGNIZED BY

★★★★★ 4.8
GARTNER PEER INSIGHTS

CERTIFICATION

What We Do

User Authentication

Single Sign-On

Mobile-First Authentication

Talisman Hardware Token

Passkeys and FIDO2

Identity Beyond Authentication

Digital ID Wallet Gateway

Identity Verification

Electronic Signatures

Mobile App Security

In-App Protection

QUANTUM-SAFE SOLUTIONS

Questions and Answers

wultra

Thank you

www.wultra.com

sales@wultra.com

Ondrej Kupka

Regional Lead - Digital Identity