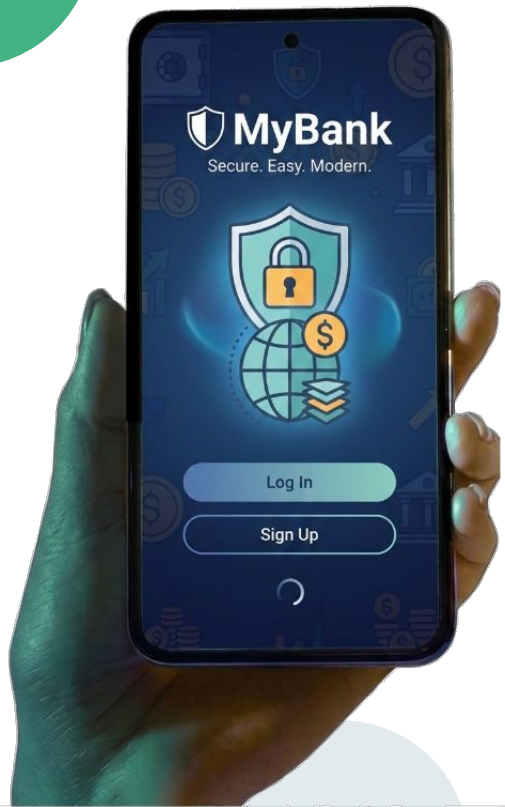
etnetera flow

wultra

LIVE WEBINAR

Building Modern Mobile Banking Apps

April 29, 2026, 3 PM (CEST)



Meet the Speakers

Pavel Stambrecht

Head of Technology

etnetera flow

Boris Filčák

Partner Channel Manager

wultra

Ondřej Franek

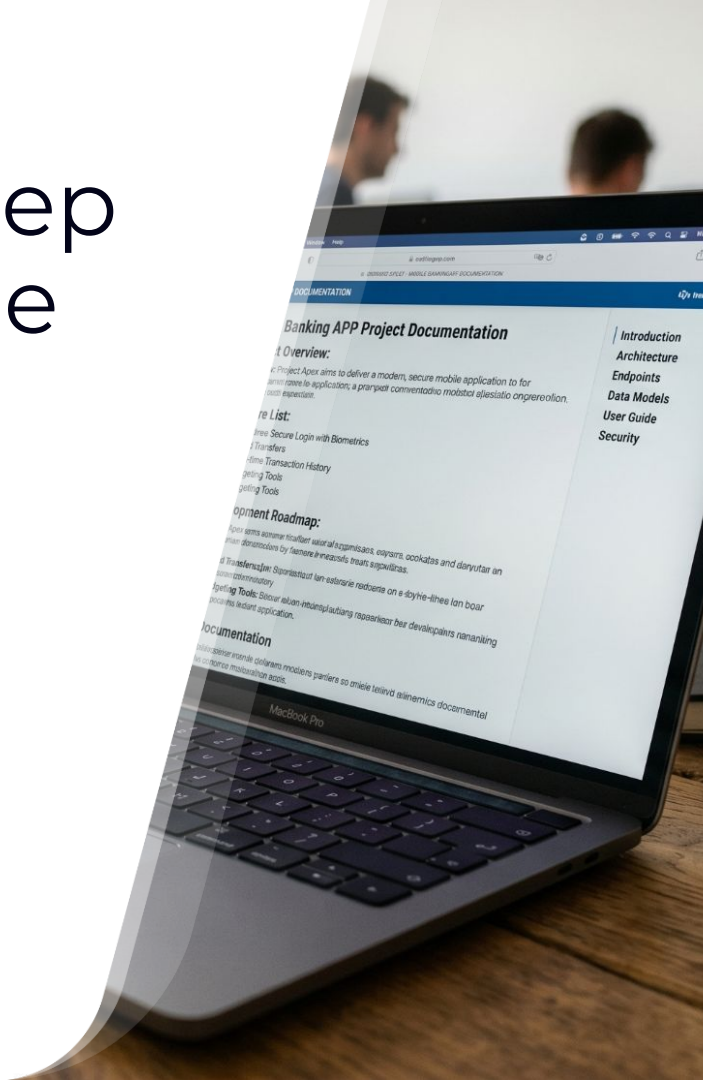
Partner, Solution Delivery – Nordics

etnetera flow

Building high-quality banking mobile applications

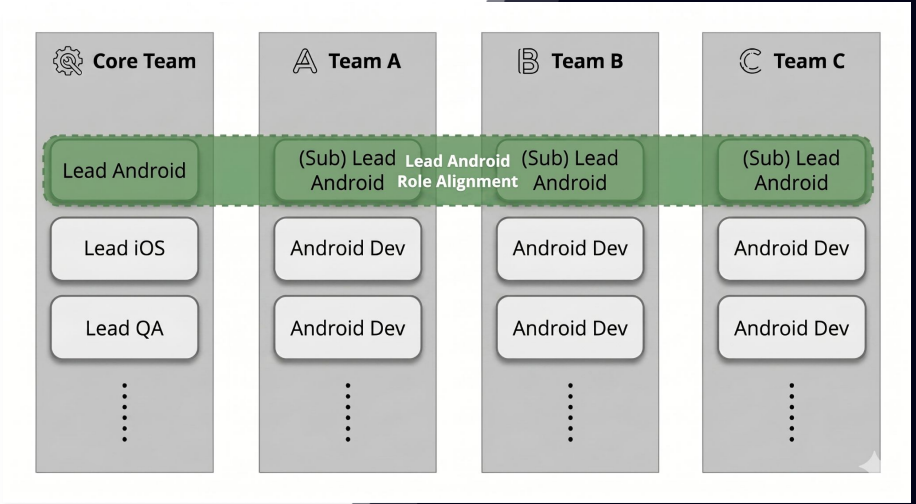
The project itself must keep the know-how. Not people working on it.

- Long-term project
- People join and leave



One team that focuses on project setup, its vision, and architectural decisions.

- The “core” team
- Platform leads and (sub)leads
- Onboarding

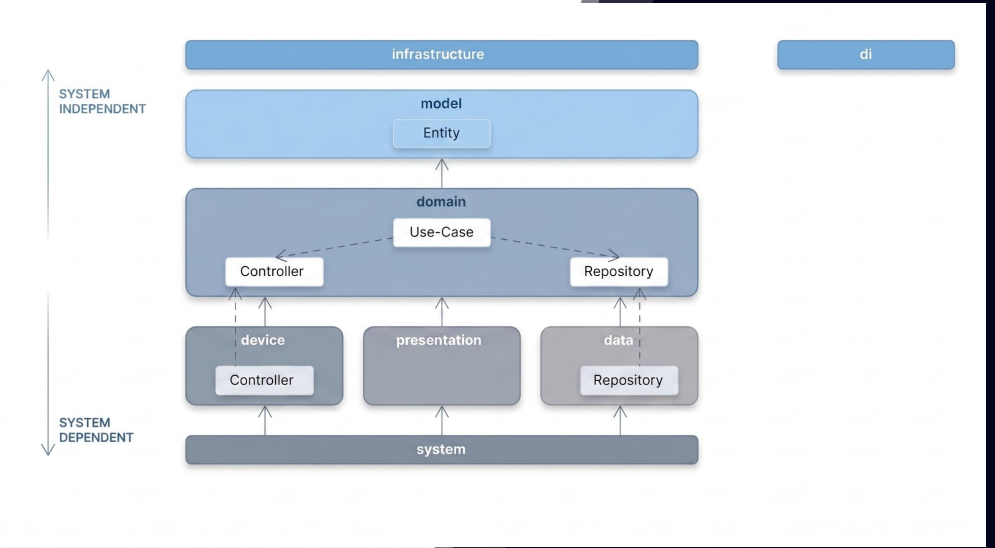


Build a platform for sharing know-how among all developers.

- Platform communities
- Regular meetings

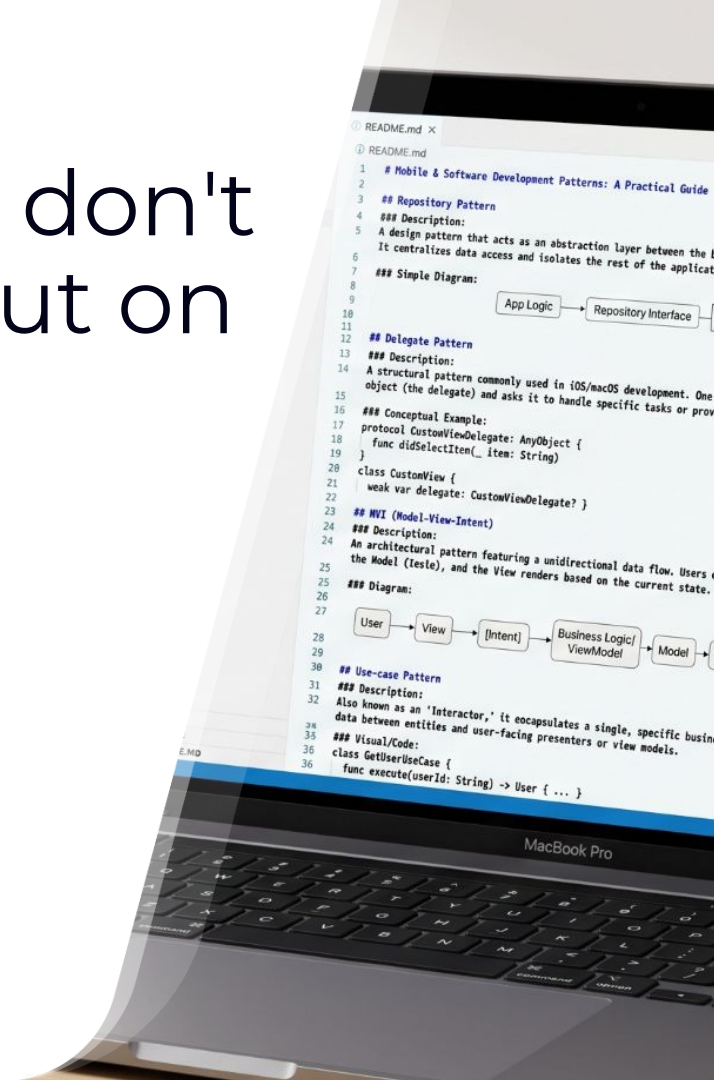
Good architecture keeps a project consistent.

- Clean architecture
- Advanced modularization
- Multi-platform frameworks



During development, we don't want to focus on HOW, but on WHAT.

- Unified architecture
- Patterns
- Processes
- Do not reinvent the wheel

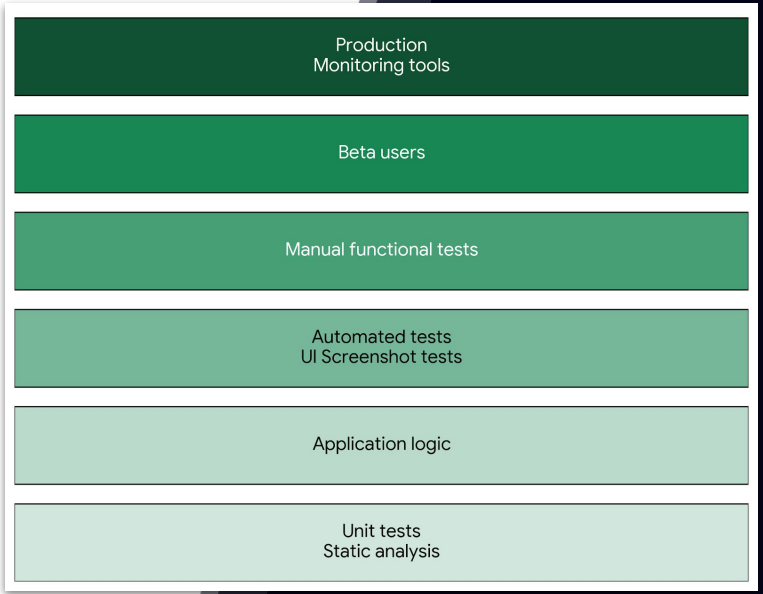


Keep the mindset to never trust anyone, especially not yourself.

- Automated checks
- Self-controlled project
- Self-describing code

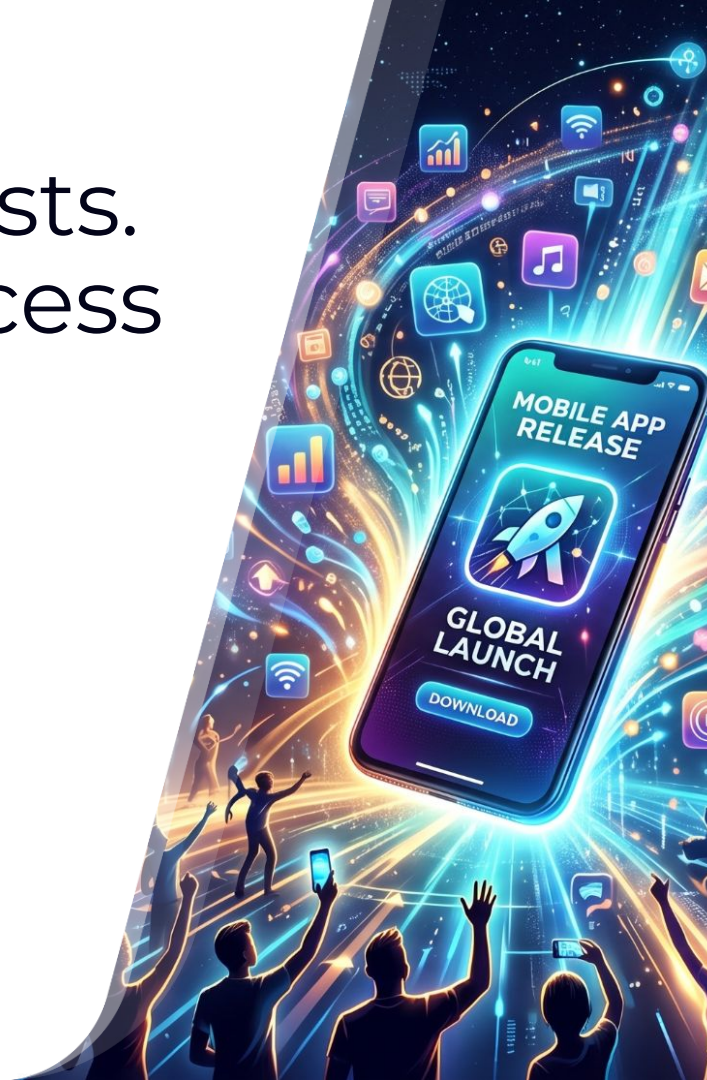
To ensure quality, it's necessary to have several quality control layers.

- Automated tests
- Validation by QA engineers
- Quality gate
- Security tests



It's not only about unit tests. Focus on the release process and monitoring.

- Multi-step release process
- Runtime monitoring
- Advanced error handling



Let third parties review your solution

- Independent view
- Entire solution validation
- Security checks

All teams must act as one

- Internal / Client / Supplier teams → as one team
- Trust
- Mindset to do something extra

Got questions?

Put them in the chat.

wultra

WEBINAR

Security in Mobile Banking

From architecture to the real world

Digital Banking Journey

Three moments where trust is established - and tested

1

Activation

Proving who the user is when entering the digital environment for the first time.

2

Authentication enrollment

Setting up the mechanism that will later verify every action is taken by the legitimate user.

3

Everyday banking

Logins, payments, loan approvals, document signing, open banking - each one a potential entry point.

Sophisticated attackers don’t target just one step, they move across all of them.

CASE STUDY

Investment scam

1 Phone call

60 minutes

€25 000+ lost

Real Scenario

Personal experience

Professional social engineering

Attackers adjust at every stage

You Receive a Phone Call

- Crypto investment
- €10k profit
- Tax implications

You Follow The Instructions

- App download
- Login email
- Withdrawal process

You Lose Money

- SMS notifications
- “Do not interrupt”
- Balance gone
- Loans taken out

What was the turning point?

How many attack vectors could you spot?

What happened and how the attack could have been stopped

Stage	What happened	Mitigation

What happened and how the attack could have been stopped

Stage	What happened	Mitigation
1. **Phone Call**	Social engineering + urgency	Awareness + active voice call detection

What happened and how the attack could have been stopped

Stage	What happened	Mitigation
1. **Phone Call**	Social engineering + urgency	Awareness + active voice call detection
2. **App Install**	-	-

What happened and how the attack could have been stopped

Stage	What happened	Mitigation
1. **Phone Call**	Social engineering + urgency	Awareness + active voice call detection
2. **App Install**	-	-
3. **Login Via Link**	Remote Access Tools downloaded in the background	Anti-Malware Detection

What happened and how the attack could have been stopped

Stage	What happened	Mitigation
1. **Phone Call**	Social engineering + urgency	Awareness + active voice call detection
2. **App Install**	-	-
3. **Login Via Link**	Remote Access Tools downloaded in the background	Anti-Malware Detection
4. **Banking Login**	Credentials captured via active screen monitoring	**Passwordless login,** RASP, Device integrity + session monitoring

What happened and how the attack could have been stopped

Stage	What happened	Mitigation
1. **Phone Call**	Social engineering + urgency	Awareness + active voice call detection
2. **App Install**	-	-
3. **Login Via Link**	Remote Access Tools downloaded in the background	Anti-Malware Detection
4. **Banking Login**	Credentials captured via active screen monitoring	**Passwordless login,** RASP, Device integrity + session monitoring
5. **New Device Registration**	Intercepted SMS OTPs	Phishing proof digital onboarding (ID Verification + Liveness Detection)

What happened and how the attack could have been stopped

Stage	What happened	Mitigation
1. **Phone Call**	Social engineering + urgency	Awareness + active voice call detection
2. **App Install**	-	-
3. **Login Via Link**	Remote Access Tools downloaded in the background	Anti-Malware Detection
4. **Banking Login**	Credentials captured via active screen monitoring	**Passwordless login,** RASP, Device integrity + session monitoring
5. **New Device Registration**	Intercepted SMS OTPs	Phishing proof digital onboarding (ID Verification + Liveness Detection)
6. **Loans & Transfers**	Abuse of trusted session	Behavioral analysis, Fraud detection systems, Step-up Authentication

The bank didn't fail because the attack was invisible.

It failed because the signals were there, and nothing acted on them.

In-App Protection

Strong Customer Authentication

ID Verification

The regulatory ground is shifting

Until Now

- Bank argues gross negligence
- Customer bears the loss if negligence is proven
- Outcomes often favour the bank

Under PSD3/PSR

- Bank must demonstrate measures were active
- Auditable assessment of suspicious behaviour
- Weak or missing controls increase liability exposure

Strong protective measures are no longer just security. They are liability management.

FUTURE CHALLENGES

Being prepared for what comes next

Responding to today's threats is one challenge. Building systems that can adapt when the threat landscape changes - that is another.

wultra

WEBINAR

Thank You

Q & A Session