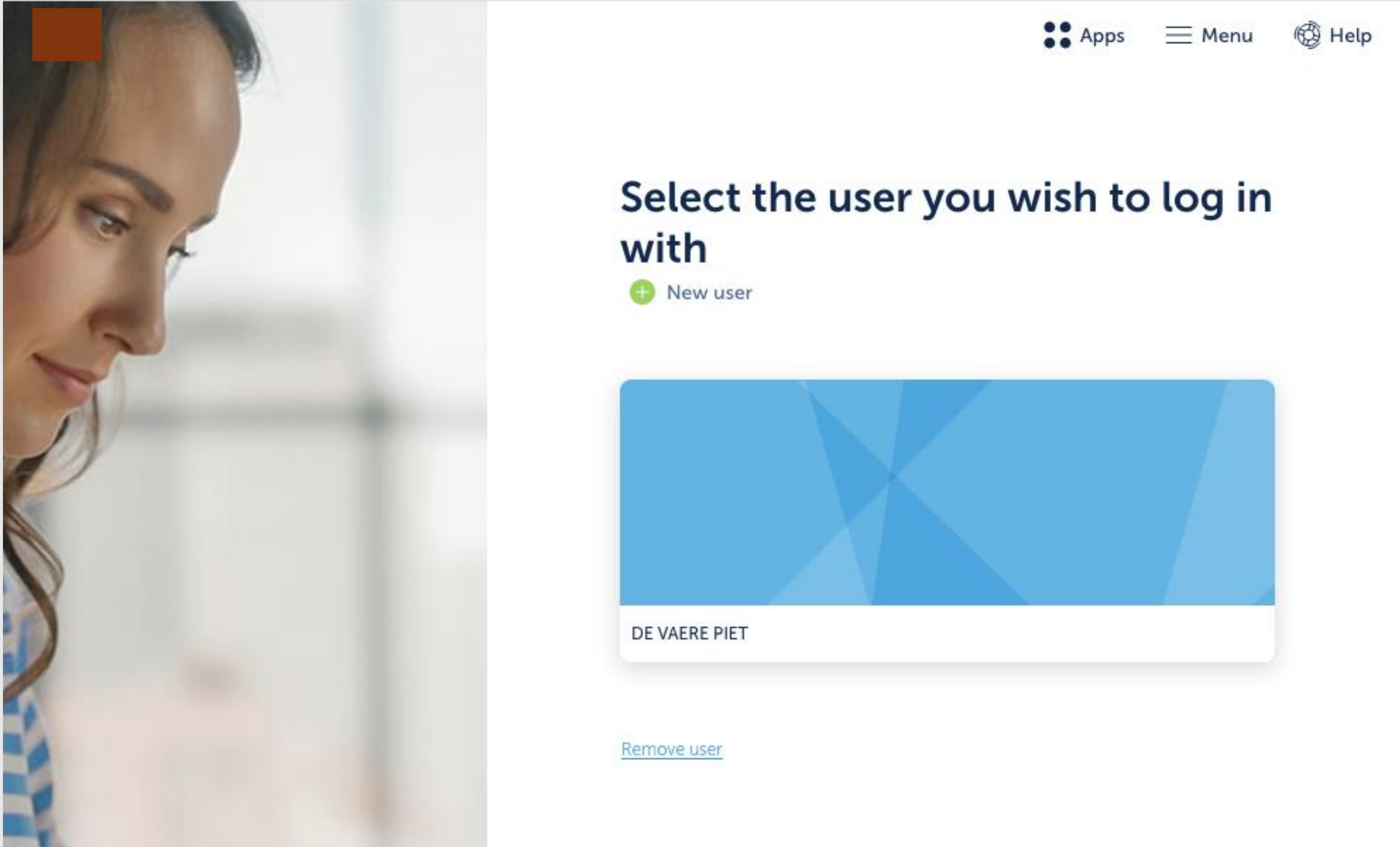
CRA Mondays, 2025-11-24

When Disclosure Fails

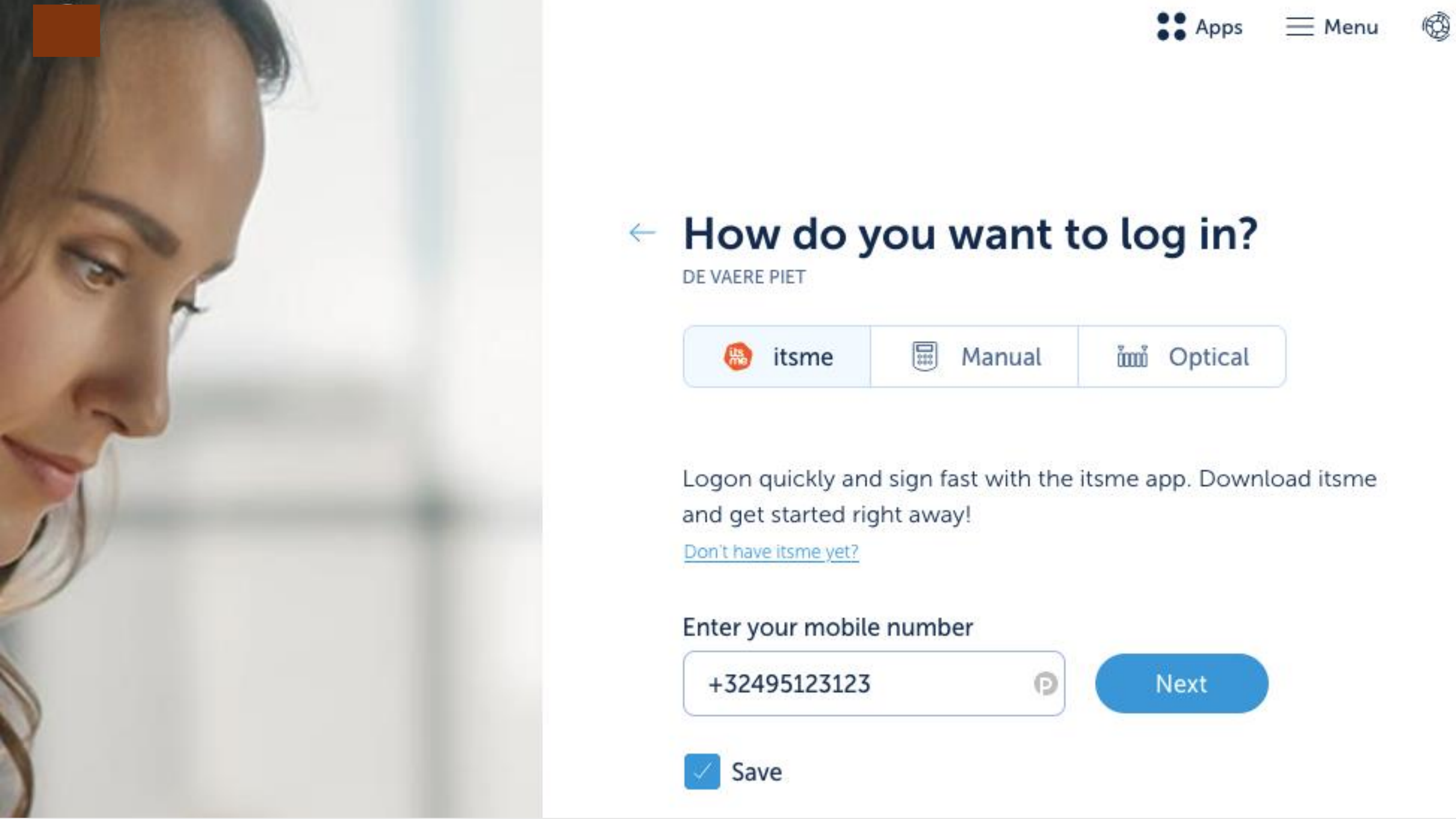
Europe’s Struggle with CVD

Piet De Vaere
Product Security Guru
pdv@productsecurity.ch



Select the user you wish to log in with

DE VAERE PIET



[redacted]

← How do you want to log in?

DE VAERE PIET

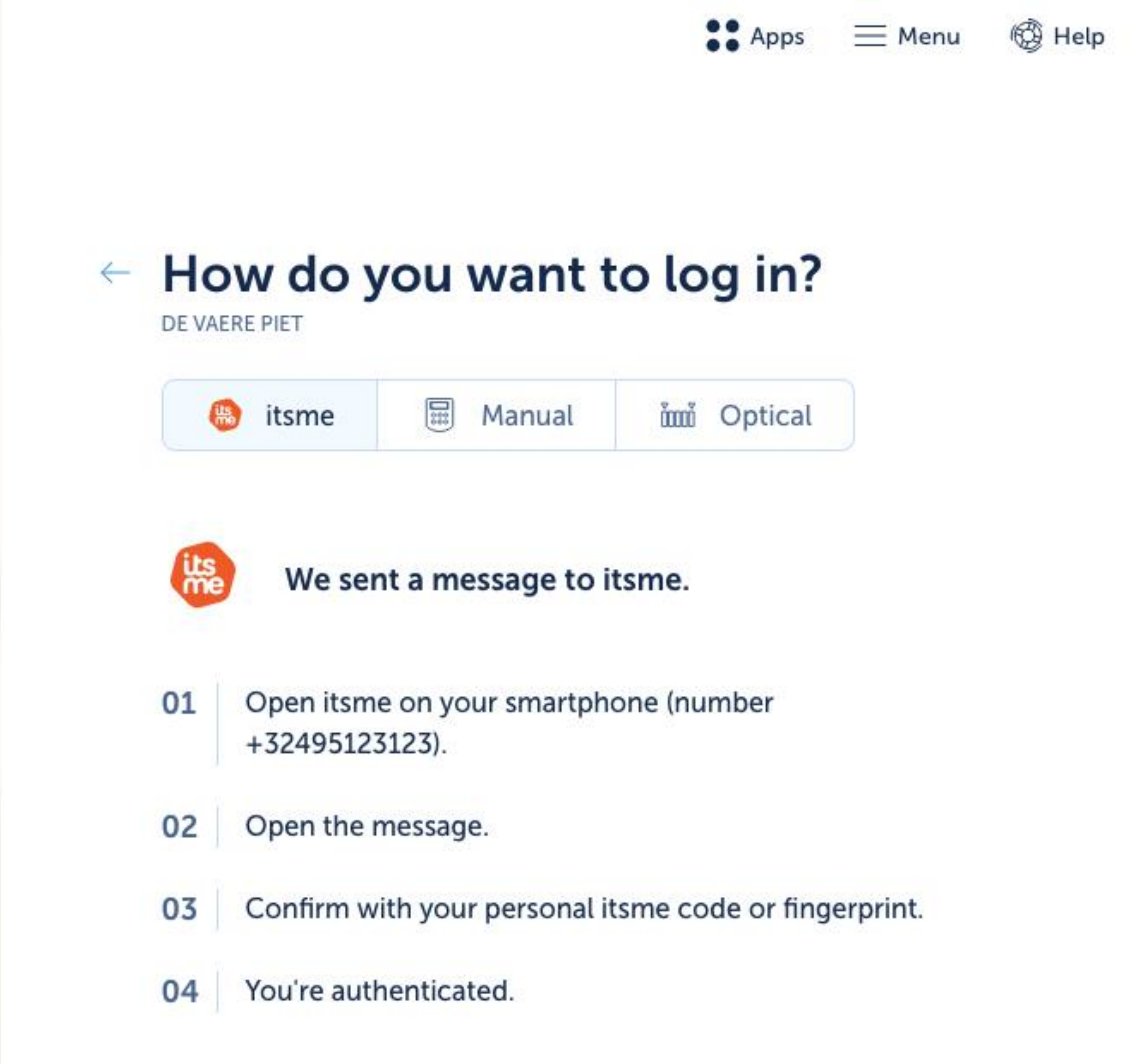
Logon quickly and sign fast with the itsme app. Download itsme and get started right away!

Don't have itsme yet?

Enter your mobile number

+32495123123

☑ Save



How do you want to log in?

DE VAERE PIET

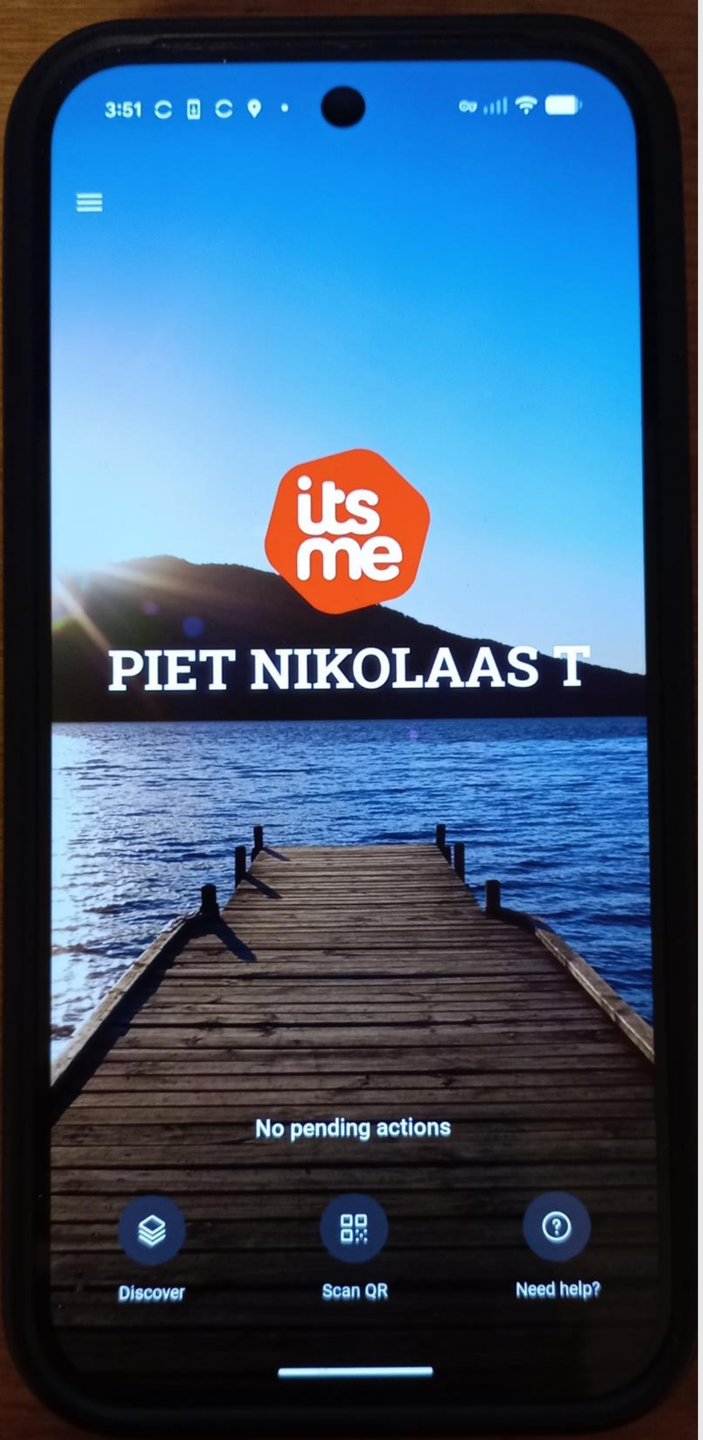
We sent a message to itsme.

01 Open itsme on your smartphone (number +32495123123).

02 Open the message.

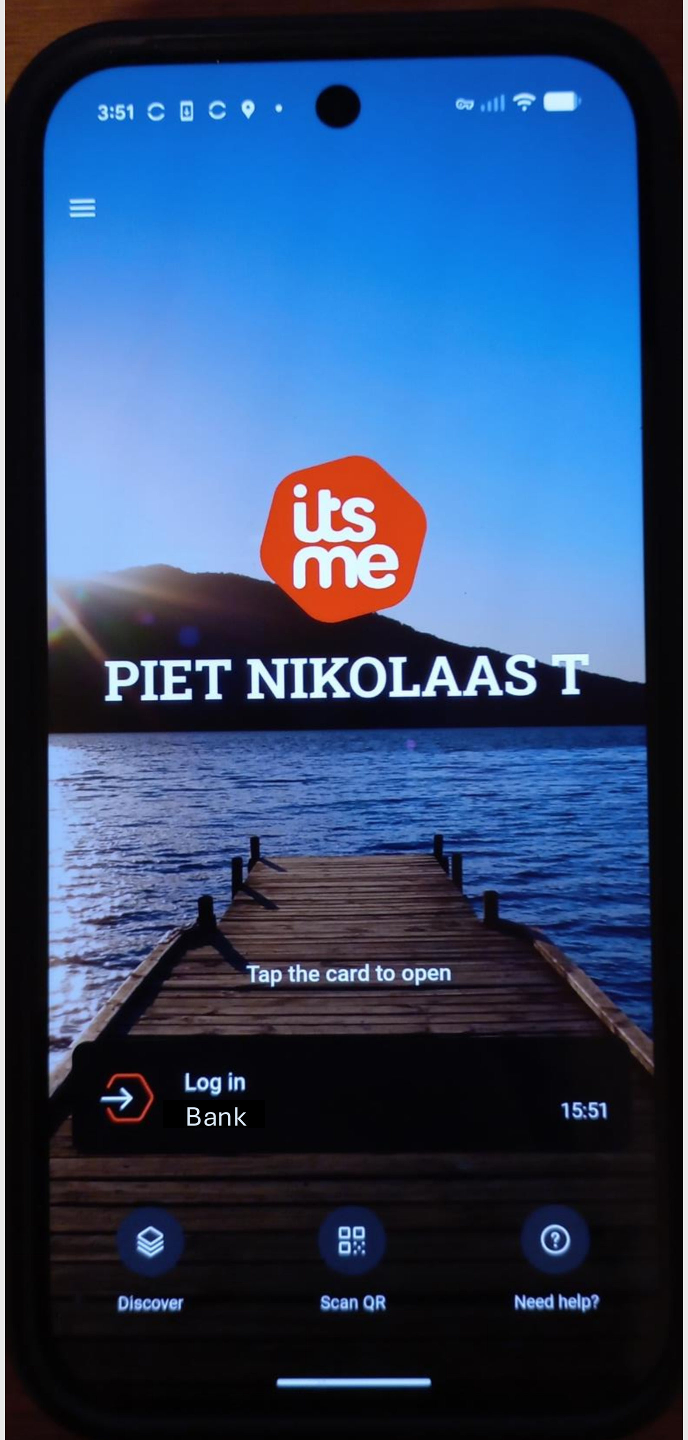
03 Confirm with your personal itsme code or fingerprint.

04 You're authenticated.



PIET NIKOLAAS T

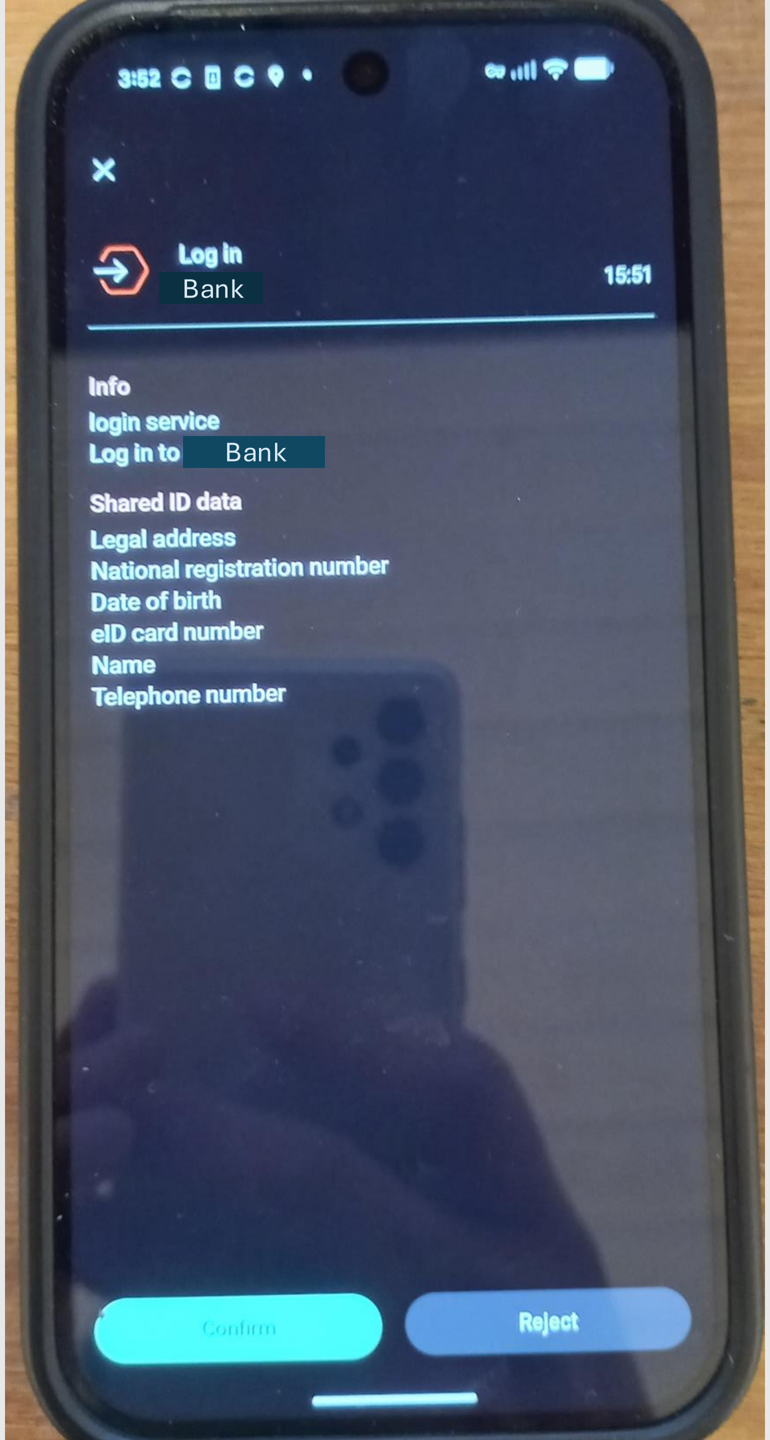
No pending actions



PIET NIKOLAAS T

Tap the card to open

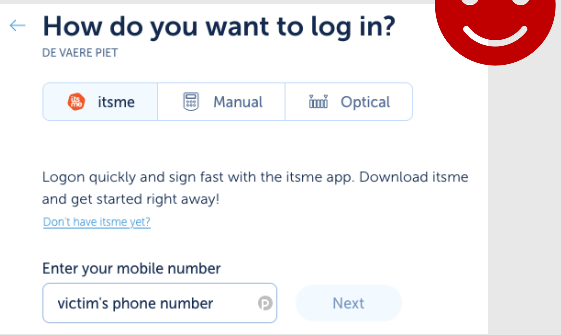
Log in
Bank
15:51



Log in
Bank
15:51

Info
login service
Log in to Bank

Shared ID data
Legal address
National registration number
Date of birth
eID card number
Name
Telephone number



How do you want to log in?

DE VAERE PIET

itme | Manual | Optical

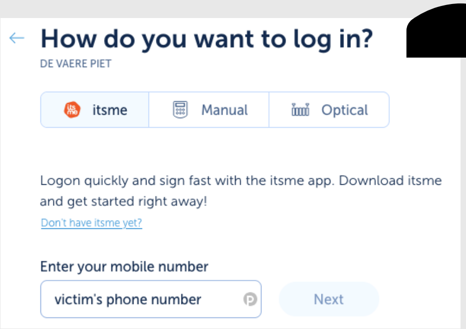
Logon quickly and sign fast with the itsme app. Download itsme and get started right away!

Don't have itsme yet?

Enter your mobile number

victim's phone number

Next



How do you want to log in?

DE VAERE PIET

itsme | Manual | Optical

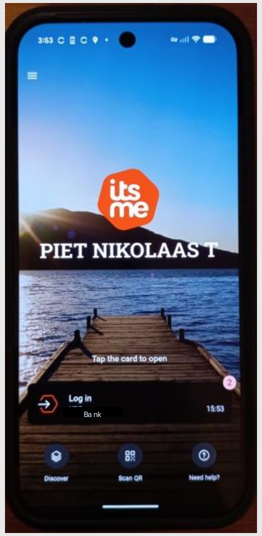
Logon quickly and sign fast with the itsme app. Download itsme and get started right away!

Don't have itsme yet?

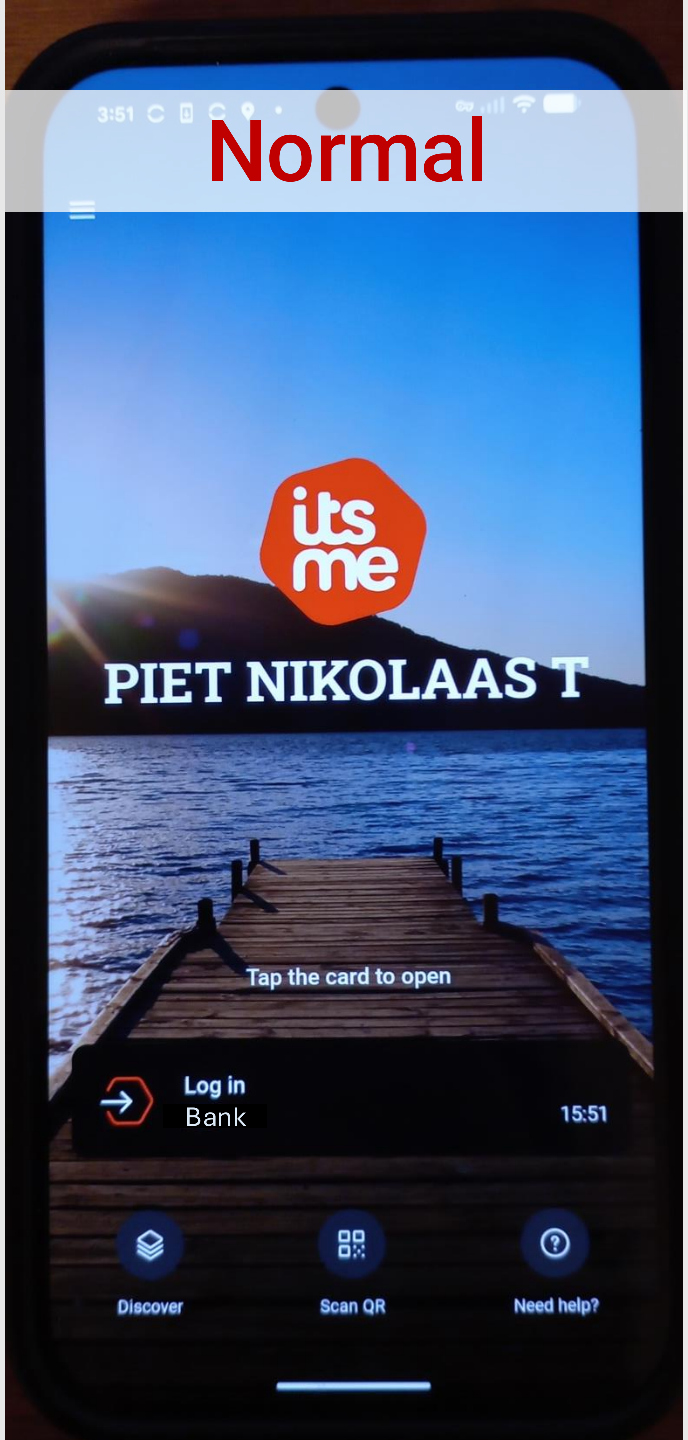
Enter your mobile number

victim's phone number

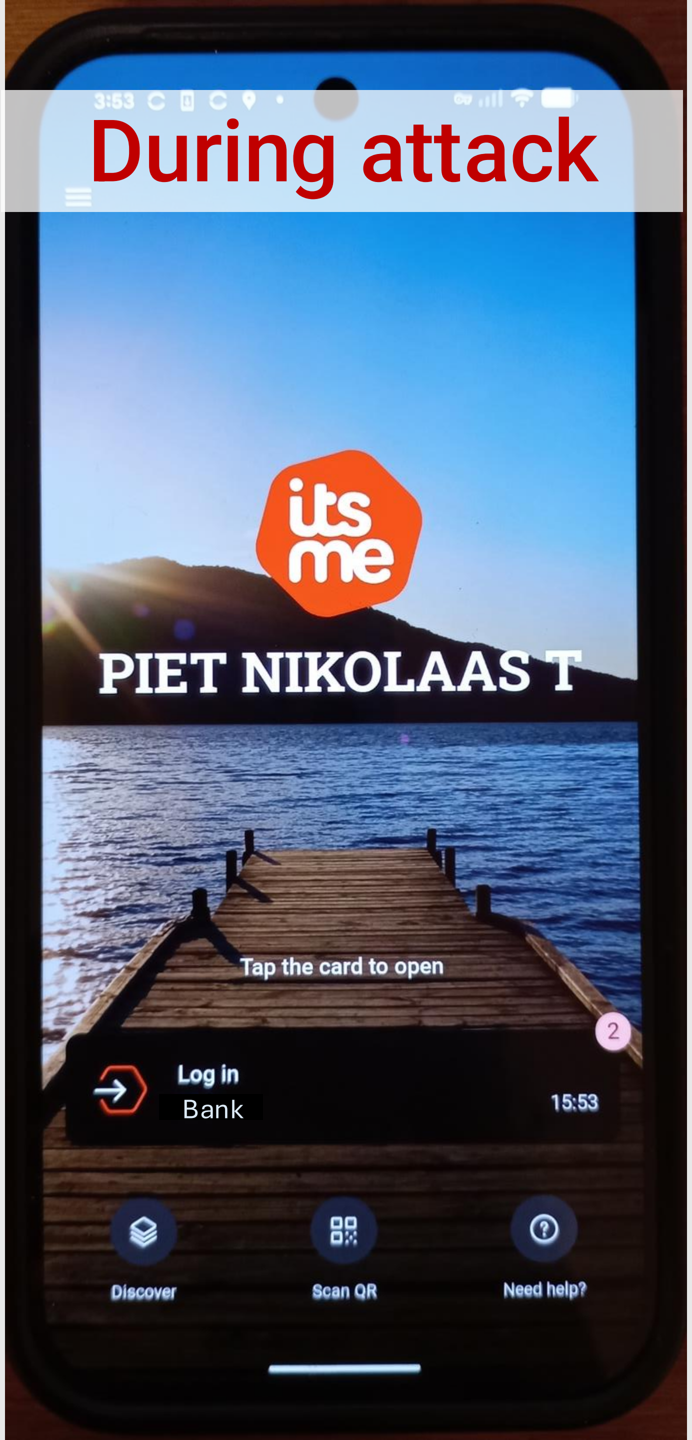
Next



?



Normal



During attack

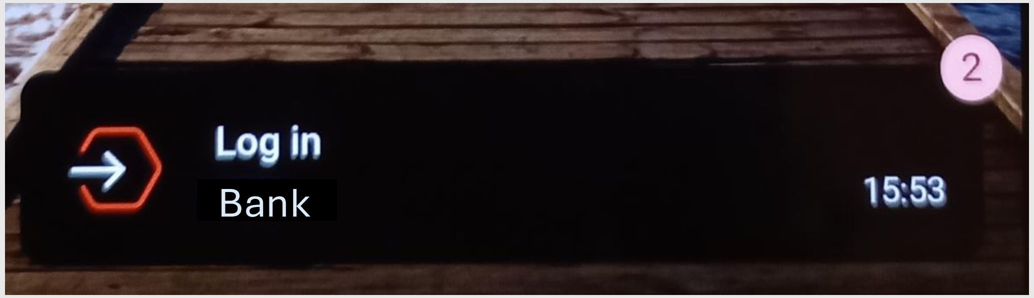
The login flow has 3 major flaws

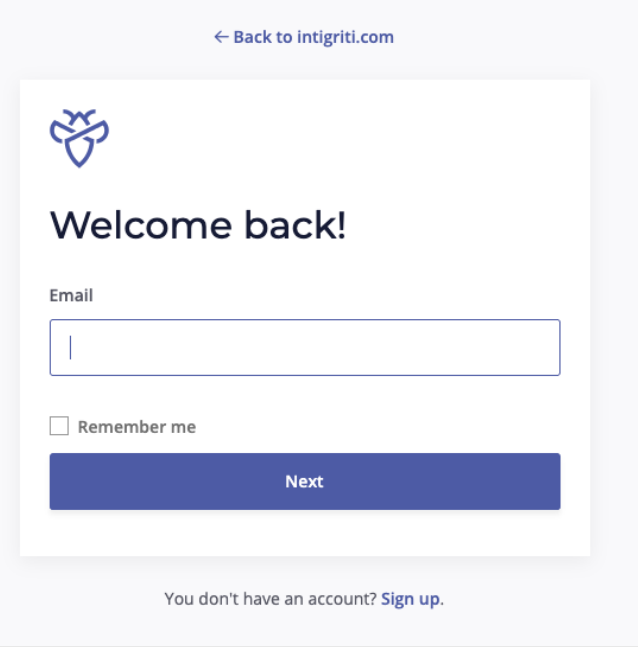
No binding between browser session & authentication request

No authentication of the user in the browser

You need at least one of these

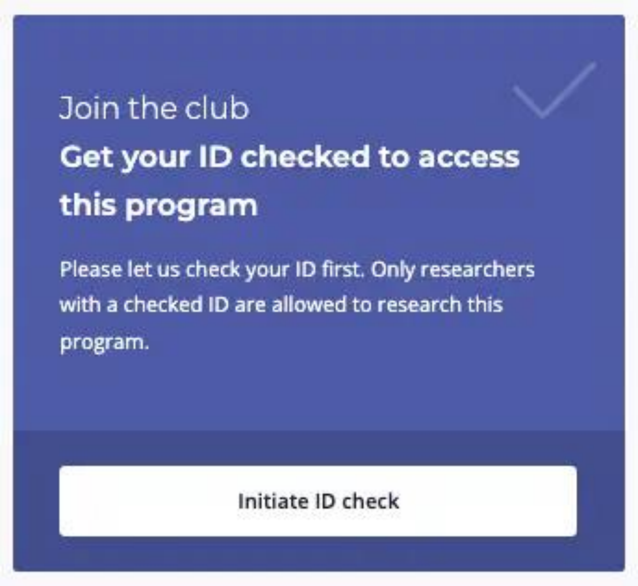
UI doesn’t inform user about concurrent requests





Welcome back!

You don't have an account? Sign up.



Join the club

Get your ID checked to access this program

Please let us check your ID first. Only researchers with a checked ID are allowed to research this program.

> “In no circumstance can you make anything related to the investigation public unless to the extent required by law;

> “This is a responsible disclosure program without bounties.

From: Piet
To: Bank CERT, Belgian national CSIRT

Beste Bank CERT,

I would like to report the following critical vulnerability in your online banking system.
You can reach me on piet@devae.re or +41 123 123 123

Identification of the concerned system:

- Bank Live online banking
- Itsme
- Potentially many other web services that use the Itsme login service

Simplified description of the potential vulnerability:
When logging in to KBC online banking, there is nothing that binds the login request shown by the itsme app to the brower session that is being logged in. This means that it is trivial for an adversary to trick a victim to authenticate the adversaries session.

Outcome: **Attacker gains full access to victims online banking environment**.

No technical skills are required to perform this attack

See this youtube video for a demo of the attack: https://www.youtube.com/watch?v=xxxxxxx

Met vriendelijke groeten
Piet De Vaere

From: Belgian national CSIRT
To: Piet

Dear Pieter,

Thank you for your report and for your interest in contributing to cybersecurity improvements.

After reviewing your submission, we would like to inform you that the organization involved—BANK—has its own dedicated vulnerability disclosure policy in place. According to the CVDP law, if an organization has such a policy publicly available, researchers are required to follow the procedure outlined there rather than reporting the issue via the CVDP.

You can find the official disclosure guidelines for KBC here:

https://www.kbcbrussels.be/retail/en/information/secure4u/responsible-disclosure-policy.html

Additionally, we noticed that the proof-of-concept video associated with your submission currently has over 30 views. Please be aware that KBC’s responsible disclosure policy explicitly states:

You do not make any information about the investigation you performed public without prior approval of KBC Brussels, unless required by law.

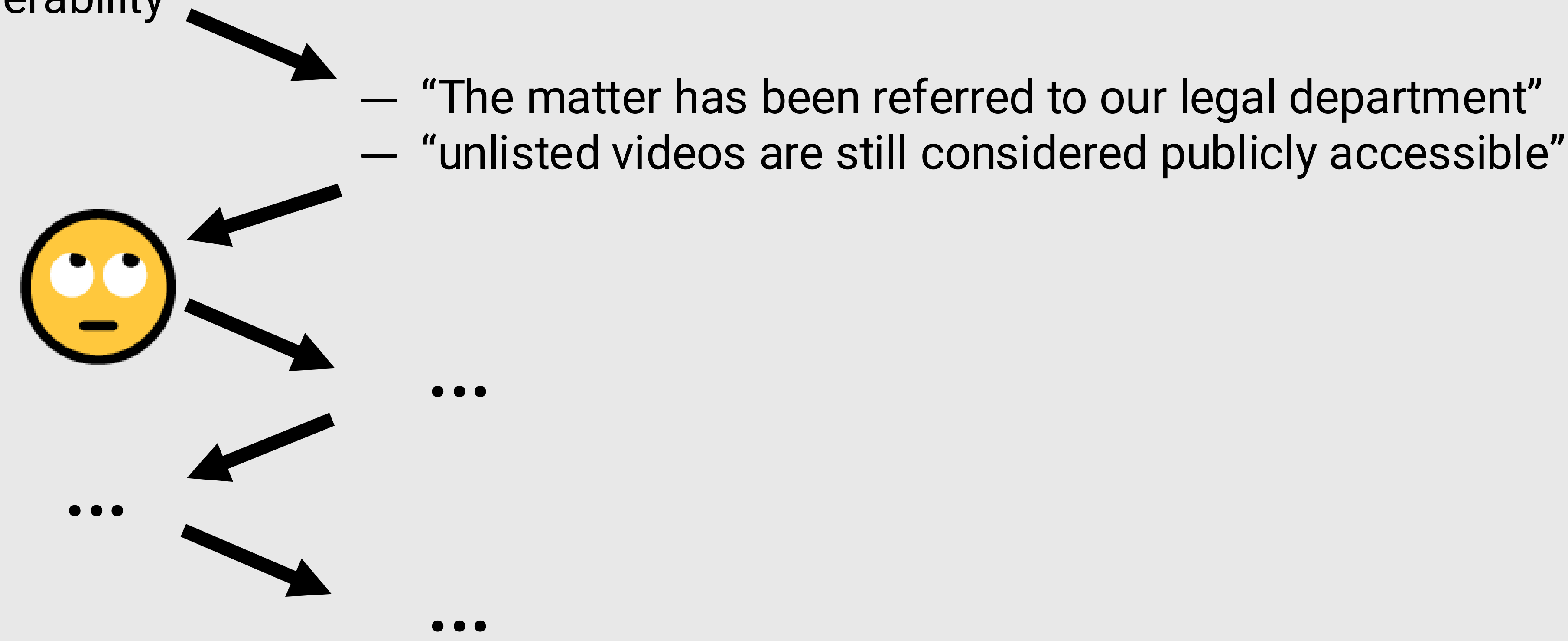
In light of this, we highly recommend you remove the video until you’ve coordinated directly with KBC and received their explicit consent.

Kind regards,
Cybersecurity Centre for Belgium (CCB)
CVDP Team

Piet

- Reported to Bank CERT
- Bank policy requires verified ID, I don’t want to do that
- Vulnerability potentially affects many more entities
- The youtube video is unlisted.
- I read the law differently
- Let’s address the vulnerability

National CSIRT



- “The matter has been referred to our legal department”
- “unlisted videos are still considered publicly accessible”

🙄

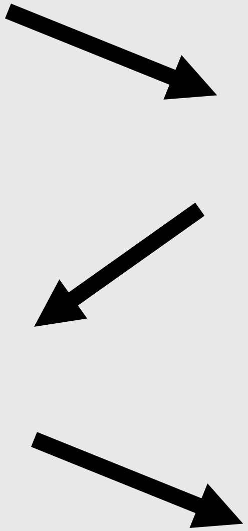
...

...

...

Piet

It’s been two weeks since the last message from CSIRT. I assume I can make this information public now.



…

Bank

“The information provided was already known to us and assessed with due care.”

You can legally not make this public.

There is no vulnerability.

“you are not legally permitted, nor do you have a legitimate interest, to disclose these findings (again) which could be considered incitement to commit IT crimes.”

Belgian NIS2 law

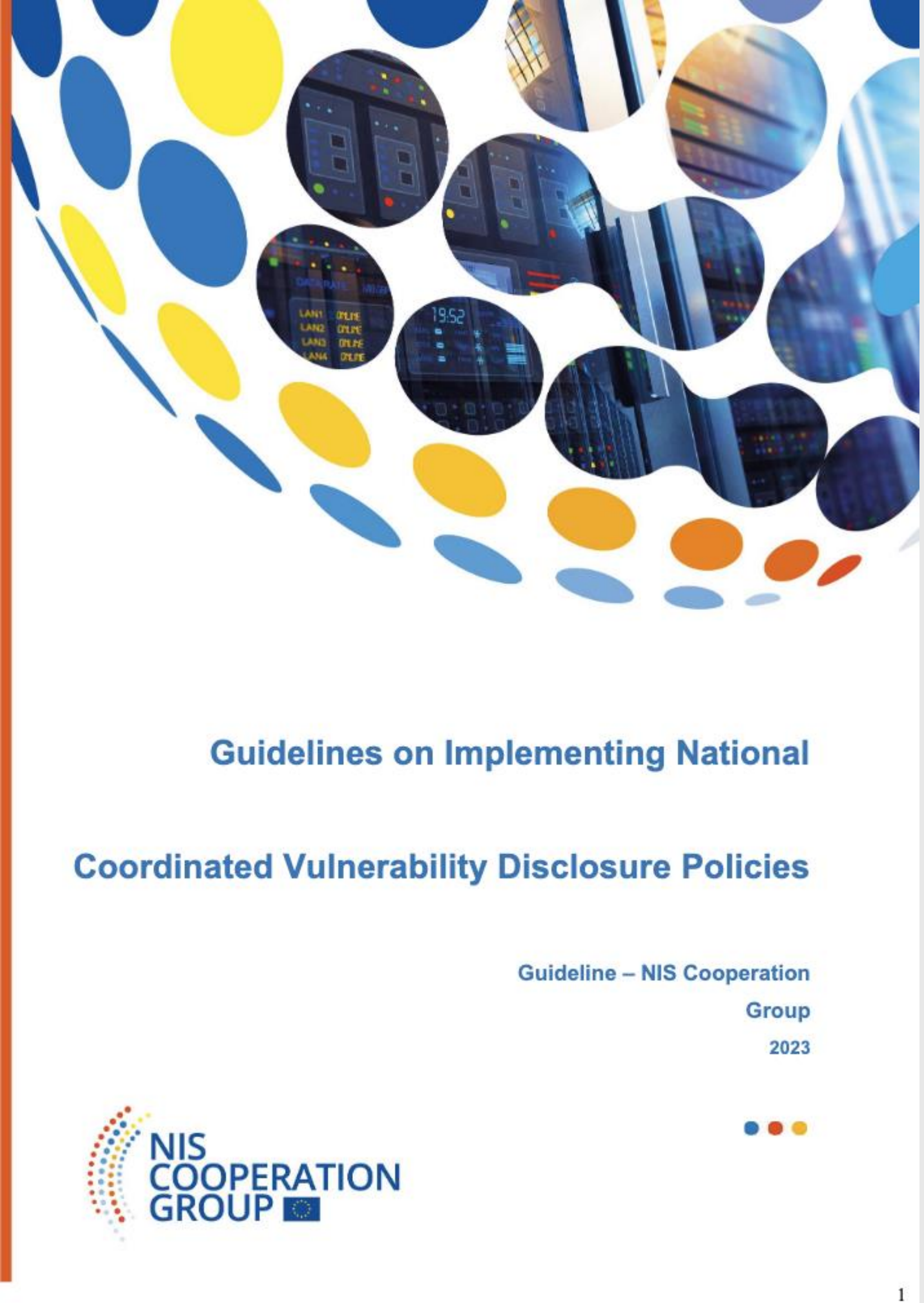
Article 22: CSIRT should act as a CVD coordinator

- Any person may report a potential vulnerability to CSIRT
- CSIRT ensures that the vulnerability is properly followed up on

Article 23 creates a safe harbor; legal immunity if:

1. Acted in good faith
2. No disclosure without consent from CSIRT
3. Inform affected org & CSIRT within 24h of discovery
4. Follow the procedure outlined by affected org

☹



Guidelines on Implementing National

Coordinated Vulnerability Disclosure Policies

Guideline – NIS Cooperation Group

2023

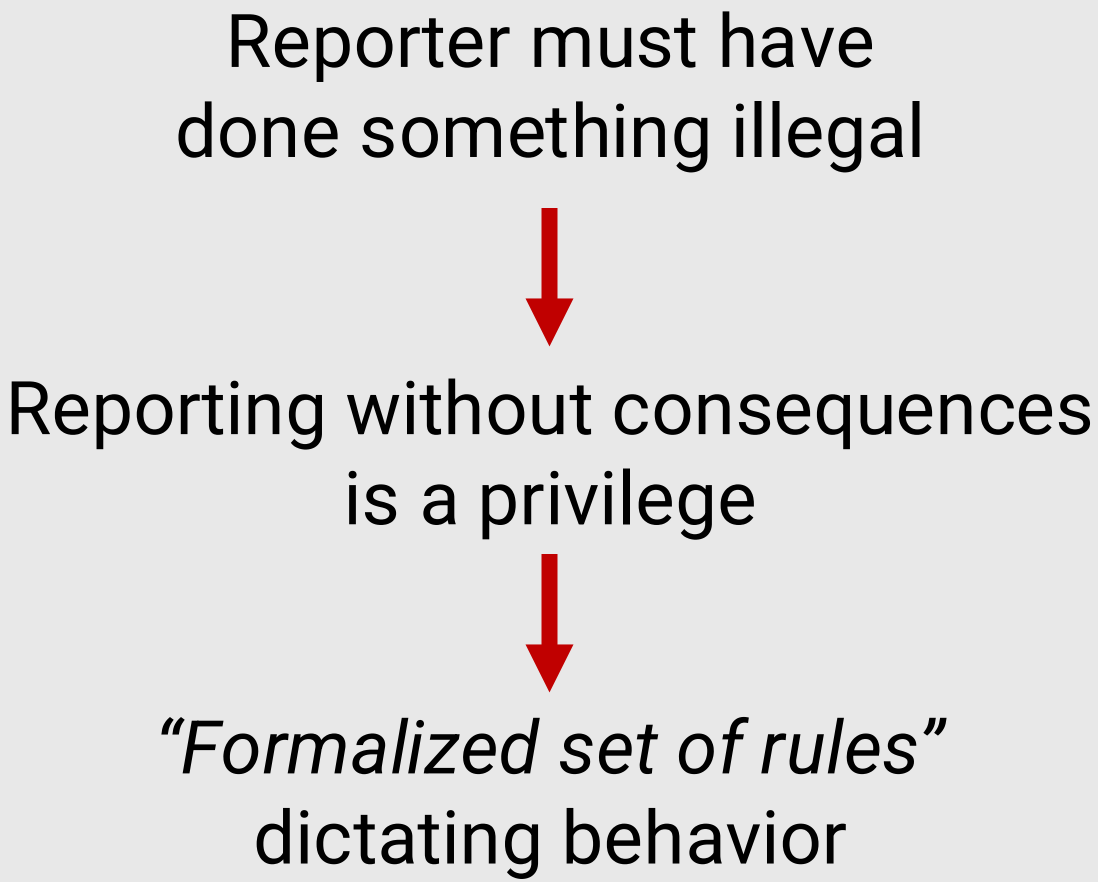
NIS COOPERATION GROUP

1

CVD policy:

A formalized set of rules for searching for and reporting vulnerabilities, with an emphasis on coordinated handling of information about these vulnerabilities, in order to limit the damage caused by unintentional or untimely disclosure or by non-responsive counterparties. These rules should (…) provide a guarantee that the entities involved in the process will not disclose vulnerability information without due coordination.

The Cooperation Group’s definition of CVD is flawed



Reporter must have done something illegal

Reporting without consequences is a privilege

“Formalized set of rules” dictating behavior

NIS2 Art 12.
“The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party.”

CRA Art 13.
“Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies”

Belgian law & NIS CG definition come from good intentions.

Main idea: CVD policy is a de-facto contract between
that protects researchers and reporters

Problems:

Coercion (i) is disrespectful towards reporters
(ii) doesn't work when there's no (theoretical) crime

Power imbalance towards affected organizations
→ We know that pressure is needed to force action

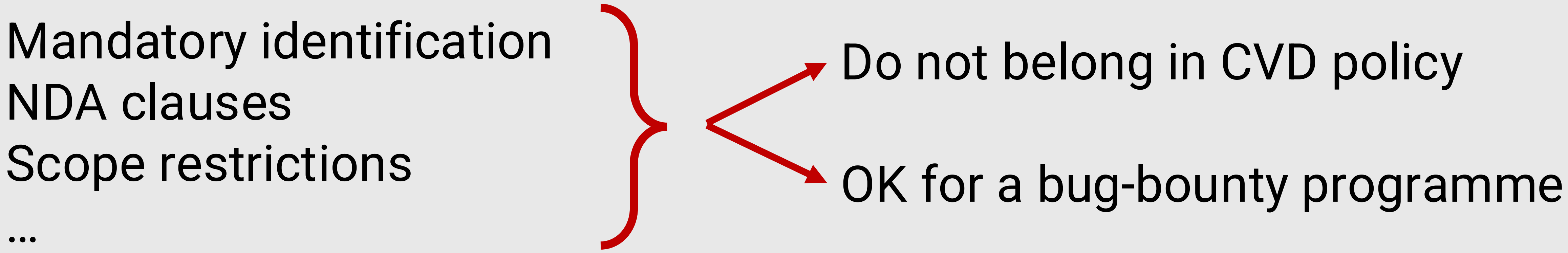
Undermines the history & spirit of CVD

CVD is not a bug bounty

NIS Cooperation Group conflates CVD and bug bounty

If someone found a vulnerability they should always be able to report

Orgs can set rules for reward-based research



Mandatory identification
NDA clauses
Scope restrictions
…

Do not belong in CVD policy

OK for a bug-bounty programme

CVD policy:

A public commitment by an organisation to receive and handle vulnerability reports in good faith, offering assurances that reporters acting responsibly will not face legal threats, while committing to investigate reports, communicate transparently, and coordinate disclosure timelines in order to reduce risk and protect users.

Reward Programme:

A reward programme (such as a bug bounty or recognition scheme) is an optional incentive mechanism that may exist alongside, but never substitute for, a CVD policy. It sets out the scope and conditions under which researchers may look for and report vulnerabilities in a system or product, in exchange for monetary or non-monetary rewards.

CVD and FOSS

How can the FOSS community support CVD?

How do we interact with national CSIRTs?

How do we support manufacturers, governments, and operators to turn disclosures into (upstreamed) patches?