University of St.Gallen

SCS-ICS

Cybersecurity
& Applied Cryptography
Chair

# Trusted Digital Identity for a Secure Society

**Prof. Katerina Mitrokotsa**
Cybersecurity & Applied Cryptography Chair
School of Computer Science
University of St. Gallen, Switzerland

# Our Team

Katerina Mitrokotsa

*Full Professor in Cyber Security*

Angelina Makri

*Operations & Administration*

Nan Cheng

Post *Doctoral Researcher*

Jenit Tomy

*Doctoral Researcher*

Liujun Yu

*Doctoral Researcher*

Florias Papadopoulos

*Doctoral Researcher*

Wilson Tsuata

*Doctoral Researcher*

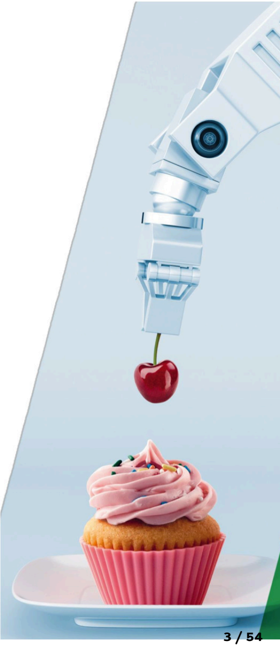
Ioannis Katis

*Doctoral Researcher*

# School of Computer Science, Univ. of St. Gallen

- Established in **Aug. 2020**!
- ~ 140 students across BCS & MCS
- ~ 65 PhDs & postdocs
- 14 faculty members
- 2 Research Institutes (ICS-HSG, ICV-HSG)
- **Research** focusing on:

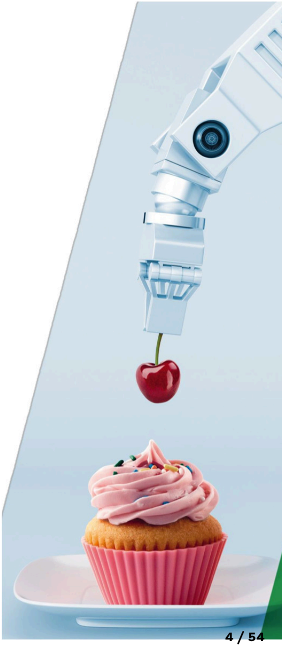
- AI & Machine Learning
- **Cybersecurity & Applied Crypto**
- Data Science & NLP
- Foundations of Computation
- HCI
- Interactions & Communication
- Programming Languages
- Software Systems



# School of Computer Science, Univ. of St. Gallen

- Bachelor of Computer Science
- Master of Computer Science

- Specialisations in:
  - Data Science
  - Software Engineering
  - **New: Cybersecurity**



# Main Research Areas

- Secure & privacy-preserving authentication
- Secure outsourcing of **computations** to untrusted cloud
- Fine-grained **access control** to sensitive data
- **Privacy-preservation** guarantees

## Expertise

- Design **provably secure** protocols/primitives
- **Efficiency** guarantees
- Suitable for **real-world** settings

TReSPASS-ETN

MARIE SKŁODOWSKA-CURIE ACTIONS

INNOVATIVE TRAINING NETWORKS

CYD CYBER DEFENCE CAMPUS

armasuisse

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

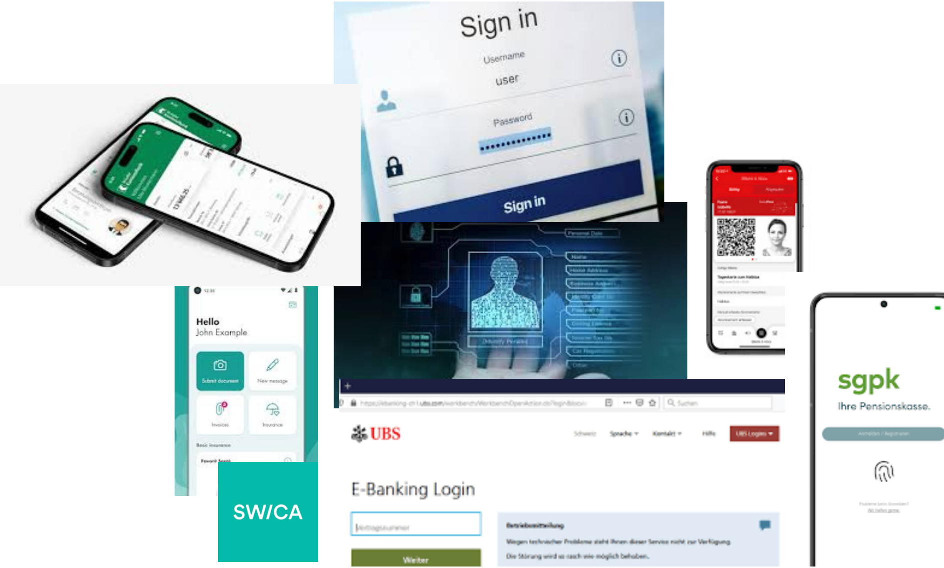
HASLERSTIFTUNG

Universität St.Gallen

# Why the Digital Identity Matters?

# Every day, we generate so much data ...

every piece of it says something **about who you are!**



Betriebsmitteilung

Wegen technischer Probleme steht Ihnen dieser Service nicht zur Verfügung.

Die Störung wird so rasch wie möglich behoben.

| Total Population | Internet Users | Active Social Media Users | Unique Mobile Phone Users |
|---|---|---|---|
| 7.83 BILLION | 4.66 BILLION | 4.20 BILLION | 5.22 BILLION |

Source: HootSuite

# Data Driven World

Healthcare Data

Physical Activity Data

Environmental Data

Financial Transactions

# Identity is no longer just a login

it's a behavioral profile!

# Identity is no longer just a login
it's a behavioral profile!

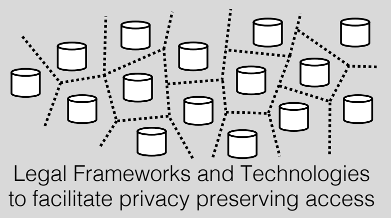
# Digital Identity is becoming a Battlefield!

# Main requirements

Privacy

Robustness

Efficiency



Legal Frameworks and Technologies
to facilitate privacy preserving access

Data Silos
- Privacy Laws
- Competition

- EU General Data Protection Regulation (GDPR) (effective from 2018)
- EU Data Governance ACT (DGA) (effective from 2023)
- Switzerland: New Federal Act on Data Protection (nFADP) (Sept. 2023)

# The influence of Political Factors on Digital Identity

EU Chat Control

UN Cybercrime Convention

Digital Identity Wallet

Cyber War: Ukraine Russia

# EU Chat Control

- The EU dropped its June 20, 2024 vote on "chat control" after failing to secure a majority.
- **Chat control** ⇒ monitor all messaging apps that provide end-to-end encryption (what's up, Signal, ...)
- Main Goal: “Combat child abuse”
- Final vote is expected in **Spring 2026**!

European Commission

# EU Chat Control

- The EU dropped its June 20, 2024 vote on "chat control" after failing to secure a majority.
- **Chat control** ⇒ monitor all messaging apps that provide end-to-end encryption (what's up, Signal, ...)
- Main Goal: “Combat child abuse”
- Final vote is expected in **Spring 2026**!

European Commission

## Concerns

- Fundamental Privacy Violation
- **Public distrust:** Surveillance of governments
- **Weakens** Cybersecurity
- **Ineffective** against Cyber Criminals

# United Nations Cybercrime Convention

- On 24 Dec. 2024, the UN General Assembly adopted a treaty to boost **global cooperation against cybercrime**.
- Into force in 2026! (currently in signature phase)

United Nations

HUMAN RIGHTS WATCH

AMNESTY INTERNATIONAL

# United Nations Cybercrime Convention

- On 24 Dec. 2024, the UN General Assembly adopted a treaty to boost **global cooperation against cybercrime**.

- Into force in 2026! (currently in signature phase)

**Main measures-Concerns:**

- **Access** to electronic data (stored/transmitted metadata)
- **Order to disclose** data in the "possession" or "control" of the person/provider

United Nations

HUMAN RIGHTS WATCH

AMNESTY INTERNATIONAL

# European Digital Identity Wallet

- eIDAS 2.0 entered in force in May'24
- All EU member states must provide a European Digital Identity Wallet (EUDI) by **the end of 2026**
- **Fully mobile, secure & user-friendly:** Enabling users to identify themselves to public & private **online services**

EUDI
Wallet
BOARDING PASS
PASSPORT
TESSERA SANITARIA
Bank Name
VISA
AMERICAN EXPRESS

# European Digital Identity Wallet

- eIDAS 2.0 entered in force in May'24
- All EU member states must provide a European Digital Identity Wallet (EUDI) by **the end of 2026**
- **Fully mobile, secure & user-friendly:** Enabling users to identify themselves to public & private **online services**

## Concerns

- Security & Privacy Concerns
- Identity Theft & Fraud
- Profiling/Tracking Individuals

# European Digital Identity Wallet

- eIDAS 2.0 published in December 2023:
  §7: The technical framework of the European Digital Identity
  (a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows for tracking, linking, correlating or otherwise obtain knowledge of transactions or user behaviour unless explicitly authorised by the user.

  (b) **enable privacy preserving techniques** which ensure **unlinkability**, ....
  Annex 11(c) The use of the wallet [..] should not result in the processing of data beyond what is necessary for the provision of wallet services. To ensure privacy, EDIW providers should ensure **unobservability** by not collecting data and not having insight into the transactions of the users of the Wallet.
  §8: [..], relying parties should provide the information necessary to allow for their identification and authentication towards the European Digital Identity Wallets

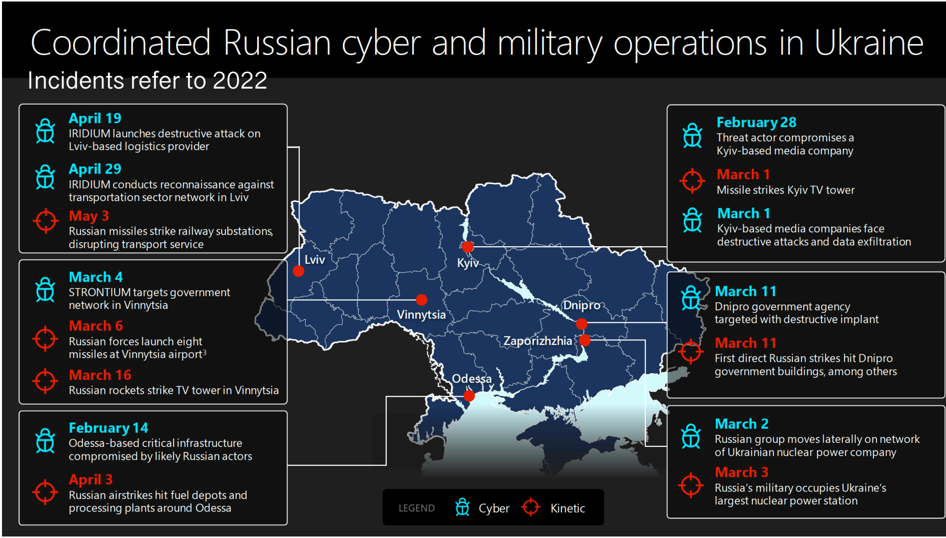
**Not ideal though, privacy is recommended but not required!**

# Electronic Identity & Trust Infrastructure

**Elektronische Identität und Vertrauensinfrastruktur**

Are we ready for this?

# Cyber War - Ukraine Russia



## Coordinated Russian cyber and military operations in Ukraine

Incidents refer to 2022

**April 19**
IRIDIUM launches destructive attack on Lviv-based logistics provider

**April 29**
IRIDIUM conducts reconnaissance against transportation sector network in Lviv

**May 3**
Russian missiles strike railway substations, disrupting transport service

**March 4**
STRONTIUM targets government network in Vinnytsia

**March 6**
Russian forces launch eight missiles at Vinnytsia airport[3]

**March 16**
Russian rockets strike TV tower in Vinnytsia

**February 14**
Odessa-based critical infrastructure compromised by likely Russian actors

**April 3**
Russian airstrikes hit fuel depots and processing plants around Odessa

**February 28**
Threat actor compromises a Kyiv-based media company

**March 1**
Missile strikes Kyiv TV tower

**March 1**
Kyiv-based media companies face destructive attacks and data exfiltration

**March 11**
Dnipro government agency targeted with destructive implant

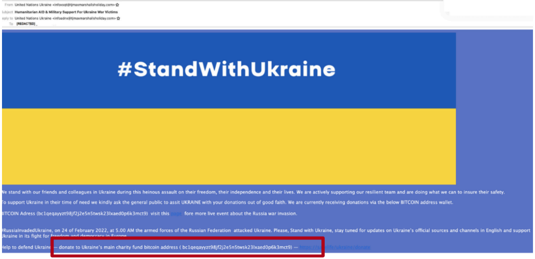
**March 11**
First direct Russian strikes hit Dnipro government buildings, among others

**March 2**
Russian group moves laterally on network of Ukrainian nuclear power company

**March 3**
Russia's military occupies Ukraine's largest nuclear power station

Copyright R. Halbheer, Microsoft Security

# Identity Manipulation in Cyberwarfare: Ukraine



From United Nations Ukraine <infoxsqt@tjmaxmarshallsholiday.com>

Subject **Humanitarian AID & Military Support For Ukraine War Victims**

Reply to United Nations Ukraine <infoadnx@tjmaxmarshallsholiday.com>

To **[REDACTED]**

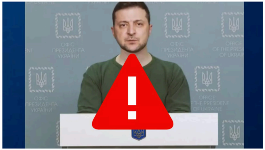
We stand with our friends and colleagues in Ukraine during this heinous assault on their freedom, their independence and their lives. We are actively supporting our resilient team and are doing what we can to insure their safety.

To support Ukraine in their time of need we kindly ask the general public to assit UKRAINE with your donations out of good faith. We are currently receiving donations via the below BITCOIN address wallet.

BITCOIN Adress (bc1qeqayyzt98jf2j2e5n5twsk23lxaed0p6k3mct9) visit this page fore more live event about the Russia war invasion.

#RussiaInvadedUkraine, on 24 of February 2022, at 5.00 AM the armed forces of the Russian Federation attacked Ukraine. Please, Stand with Ukraine, stay tuned for updates on Ukraine's official sources and channels in English and support Ukraine in its fight for freedom and democracy in Europe.

Help to defend Ukraine — donate to Ukraine's main charity fund bitcoin address ( bc1qeqayyzt98jf2j2e5n5twsk23lxaed0p6k3mct9) — https://s[illegible]elife/ukraine/donate

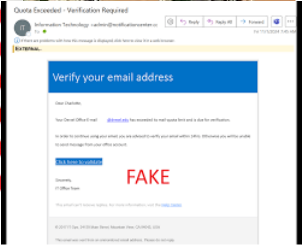


*In the deepfake video, Zelenskyy seemingly told Ukrainian citizens to "lay down arms".* - Euronews via Twitter

## Key Tactics

- **Impersonation** of aid groups (phishing) to donate to Ukraine
- **Fake** government or military emails/videos
- Fake Microsoft/Amazon login pages to **steal** passwords
- Automated **fake accounts** that spread & boost propaganda messages.

# Identity Manipulation in Cyberwarfare: Iran



Quota Exceeded - Verification Required

Information Technology <admin@notificationcenter.cc>

To

Fri 11/15/2024 3:45 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

EXTERNAL...

Verify your email address

Dear Charlotte,

Your Drexel Office E-mail @drexel.edu has exceeded its mail quota limit and is due for verification.

In order to continue using your email you are advised to verify your email within 24hrs. Otherwise you will be unable to send message from your office account.

Click here to validate

Sincerely,
IT Office Team

This email can't receive replies. For more information, visit the help center.

© 2017 IT Ops, [illegible] Mountain View, CA 94043, USA

This email was sent from an unmonitored email address. Please do not reply.

## Key Tactics

- Fake journalist or activist profiles
- Phishing targeting diaspora communities
- **Spoofed government** announcements
- Coordinated fake accounts boosting regime messages

# Connectivity empowers identity, but also endangers ...

- Satellite internet used to bypass **state blackouts**
- Citizens shared information beyond censorship
- Government attempted jamming & **severe penalties**
- Identity Risks: Device use could expose **user identity**

# What about Security in Switzerland?

# Switzerland & IT Security

## Key recent findings (2024-2026)

### Volume of incidents

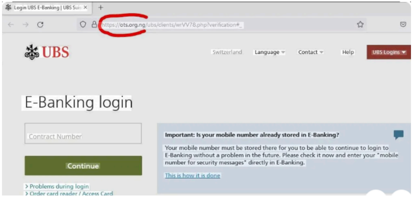
- Switzerland had **65,000 cyber incidents** in 2025, about the same number as before, but more advanced attacks.
- The NCSC logged 63,000 incidents in 2024, almost twice as many as in 2023. [
- In just the first half of 2025, there were already 35,727 reports.

**Semi-Annual Report 2025/1**

https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2025-1.html

# Attack Types Dominating Switzerland

- **Fraud** & **phishing** remain the most reported categories (~ 58% fraud).
- **Phishing attacks** surged from <500k in 2023 to **975,000+** messages in 2024.
- **AI-enhanced phishing** & **scam calls** (e.g., police impersonation scams).
- Ransomware remains a **major threat**, with:
  - **104 ransomware cases** reported in 2025 (up from 92 in 2024).
  - Groups like **Akira** & **LockBit** active in Switzerland.



Login UBS E-Banking | UBS Sui

https://ots.org.ng/ubs/clients/wrVV78.php?verification#_

E-Banking login

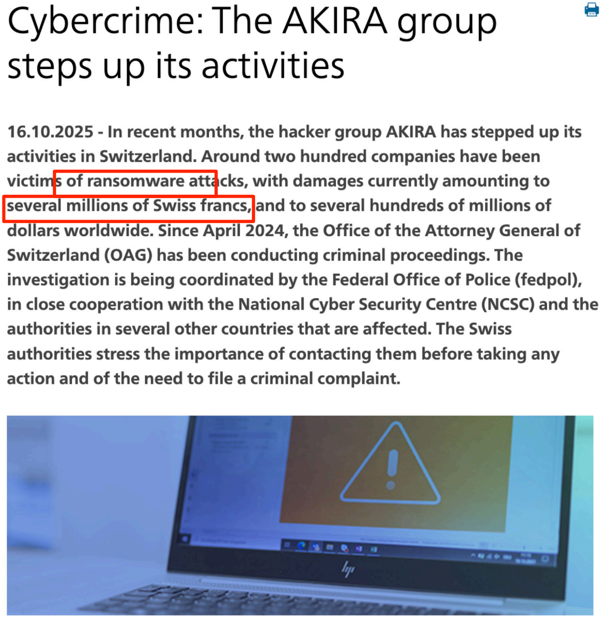
Contract Number

Important: Is your mobile number already stored in E-Banking?

Your mobile number must be stored there for you to be able to continue to login to E-Banking without a problem in the future. Please check it now and enter your "mobile number for security messages" directly in E-Banking.

This is how it is done

# Ransomware: The AKIRA group

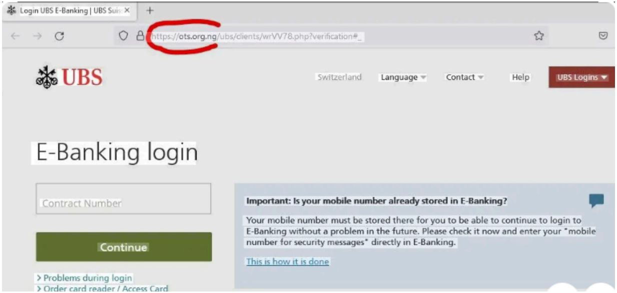


## Cybercrime: The AKIRA group steps up its activities

**16.10.2025 - In recent months, the hacker group AKIRA has stepped up its activities in Switzerland. Around two hundred companies have been victims of ransomware attacks, with damages currently amounting to several millions of Swiss francs, and to several hundreds of millions of dollars worldwide. Since April 2024, the Office of the Attorney General of Switzerland (OAG) has been conducting criminal proceedings. The investigation is being coordinated by the Federal Office of Police (fedpol), in close cooperation with the National Cyber Security Centre (NCSC) and the authorities in several other countries that are affected. The Swiss authorities stress the importance of contacting them before taking any action and of the need to file a criminal complaint.**

# Examples

## Phishing & Smishing

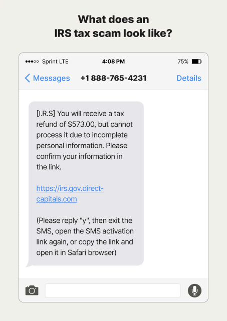

Login UBS E-Banking | UBS Suis
https://ots.org.ng/ubs/clients/wrVV78.php?verification#_
UBS
Switzerland
Language
Contact
Help
UBS Logins
Contract Number
Continue
> Problems during login
> Order card reader / Access Card

E-Banking login

**Important: Is your mobile number already stored in E-Banking?**

Your mobile number must be stored there for you to be able to continue to login to E-Banking without a problem in the future. Please check it now and enter your "mobile number for security messages" directly in E-Banking.

This is how it is done



**What does an IRS tax scam look like?**

[I.R.S] You will receive a tax refund of $573.00, but cannot process it due to incomplete personal information. Please confirm your information in the link.

https://irs.gov.direct-capitals.com

(Please reply "y", then exit the SMS, open the SMS activation link again, or copy the link and open it in Safari browser)

Quiz!! Lets see phishing examples!

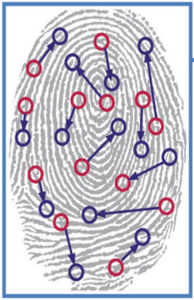
`https://www.propharma.ch/de/phishing-test-formular/`

# How does the Digital Identity really work?

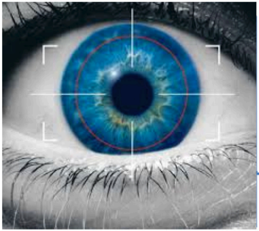
# Biometric authentication

- Quick, accurate & user friendly authentication
- Used widely in various access control systems

# Common Biometric Traits

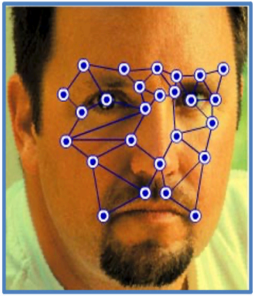


fingerprint



iris

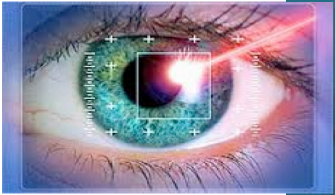
face



voice

# Biometric authentication for Access Control

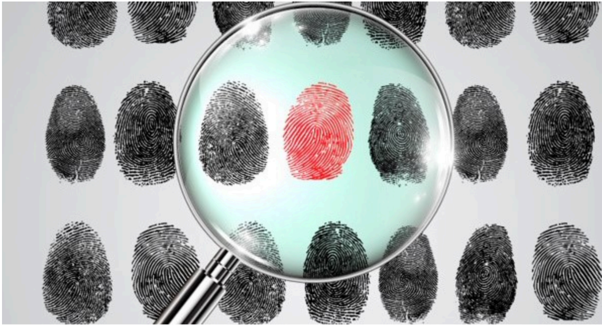
- Passport control via Iris recognition
- For frequent travellers



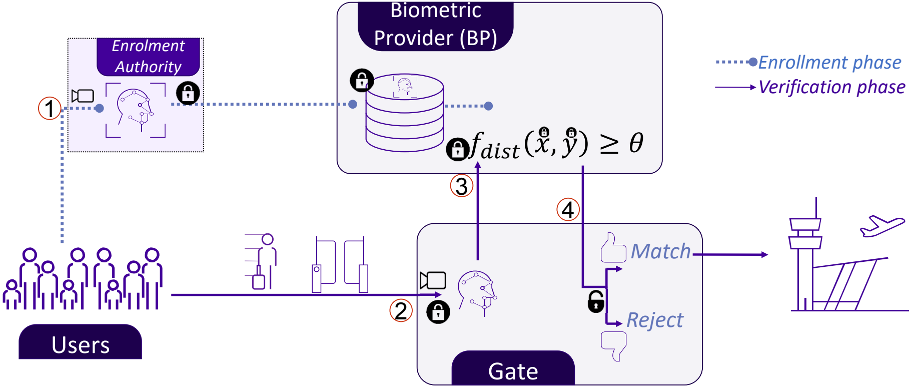
Stand exactly on the feet

# Need for Privacy-preserving Biometric Authentication

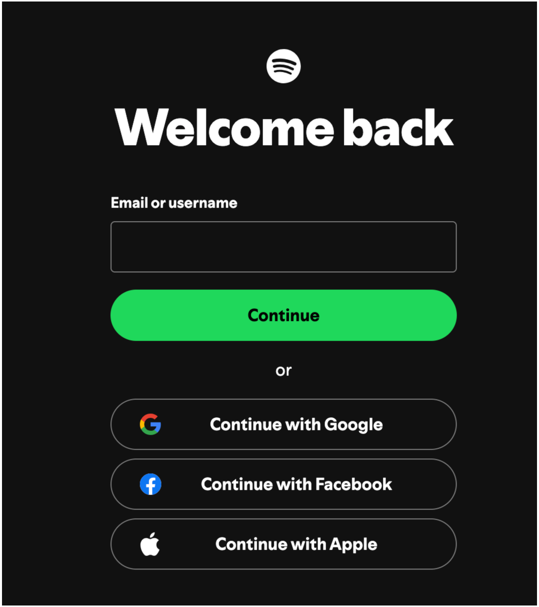
- Biometric cannot be revoked
- Stolen Biometrics may lead to:
  - Identity theft
  - Tracking individuals
  - Profiling
  - Reveal sensitive information (race, diseases)



# A Use Case: Flight Boarding Control



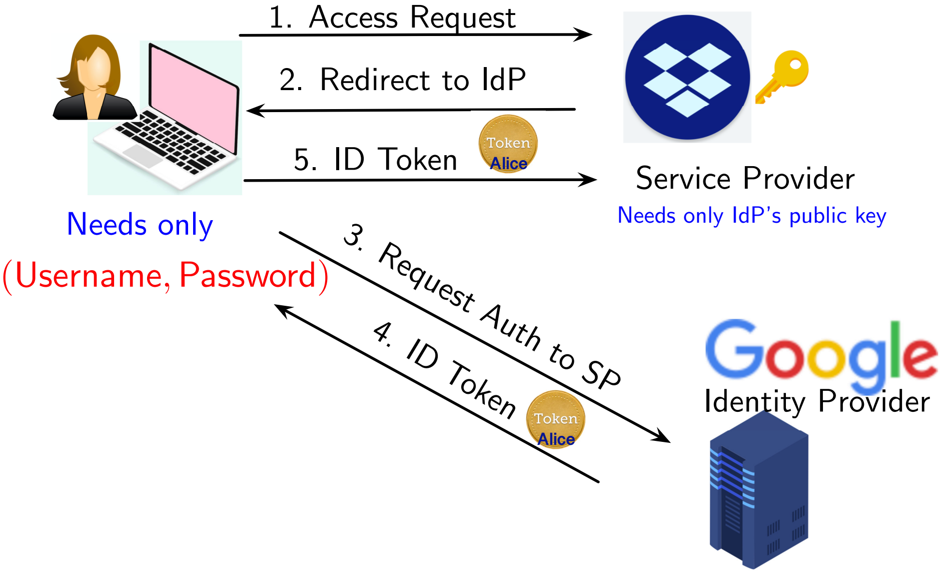
# Simpler Authentication? Single Sign On



Welcome back

Email or username

# OAuth what is it?



1. Access Request

2. Redirect to IdP

3. Request Auth to SP

4. ID Token

5. ID Token

Service Provider

Needs only IdP's public key

Identity Provider

Needs only

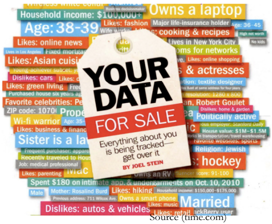
(Username, Password)

Major Risks: Tracking/Profiling Identity Theft

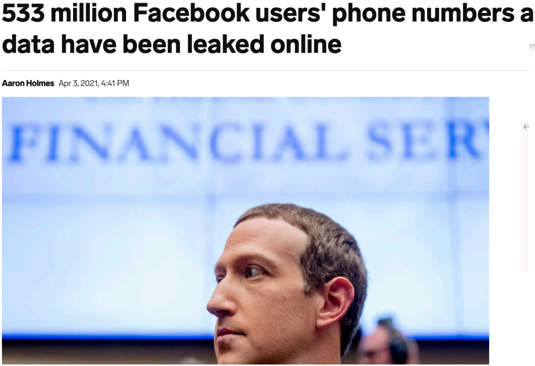
# Why the Digital Identity fails?

# Data Breaches!! Need for Robust Solutions!

PHONE
INFRASTRUCTURE REMOTE BUSINESS
SECURITY SERVER TABLET
DATA
DATA BREACH
LAPTOP
PC TECHNOLOGY
REMOTE
EMAIL TECHNOLOGY NETWORK
NETWORKING INFRASTRUCTURE NETWORKING
BUSINESS COMPUTER MOBILE SYSTEM
GEO

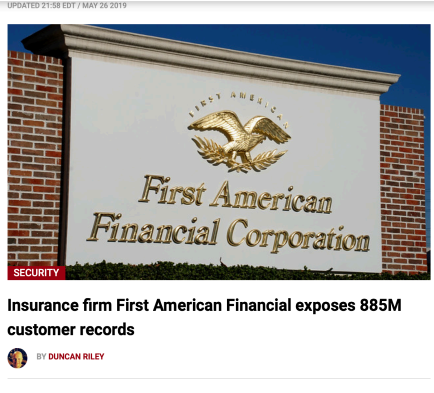


Source (time.com)



# 533 million Facebook users' phone numbers and personal data have been leaked online

Aaron Holmes Apr 3, 2021, 4:41 PM



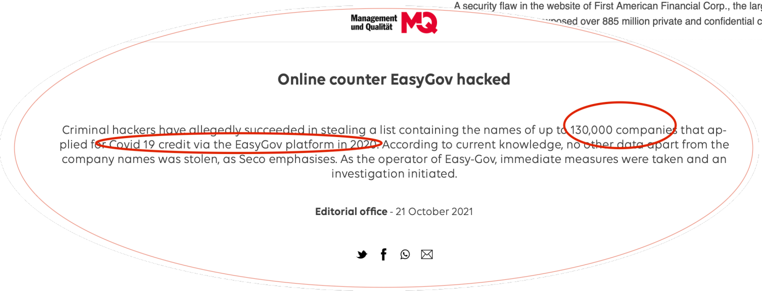
UPDATED 21:58 EDT / MAY 26 2019

## Insurance firm First American Financial exposes 885M customer records

BY DUNCAN RILEY

A security flaw in the website of First American Financial Corp., the large real estate title

xposed over 885 million private and confidential customer records dating



Management und Qualität MQ

## Online counter EasyGov hacked

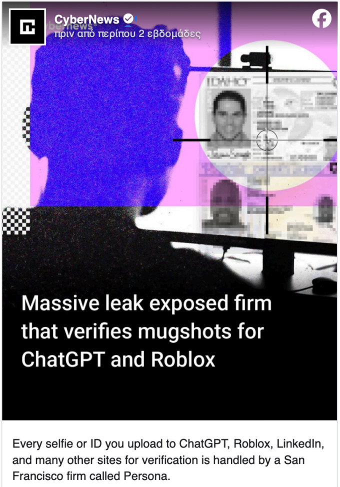
Criminal hackers have allegedly succeeded in stealing a list containing the names of up to 130,000 companies that applied for Covid 19 credit via the EasyGov platform in 2020. According to current knowledge, no other data apart from the company names was stolen, as Seco emphasises. As the operator of Easy-Gov, immediate measures were taken and an investigation initiated.

**Editorial office** - 21 October 2021

# When Identity Checks Become Surveillance

## The Persona Leak

- An ID-checking company **accidentally exposed** its internal code.
- It revealed **hundreds of hidden automated** checks.
- These included watchlists, face-matching, and risk scores.
- Data from simple ID checks was fed into **larger surveillance** systems.



CyberNews
πριν από περίπου 2 εβδομάδες

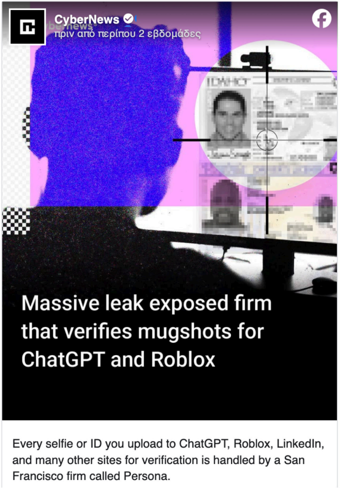
Massive leak exposed firm that verifies mugshots for ChatGPT and Roblox

Every selfie or ID you upload to ChatGPT, Roblox, LinkedIn, and many other sites for verification is handled by a San Francisco firm called Persona.

# When Identity Checks Become Surveillance

## The Persona Leak

- An ID-checking company **accidentally exposed** its internal code.
- It revealed **hundreds of hidden automated** checks.
- These included watchlists, face-matching, and risk scores.
- Data from simple ID checks was fed into **larger surveillance** systems.



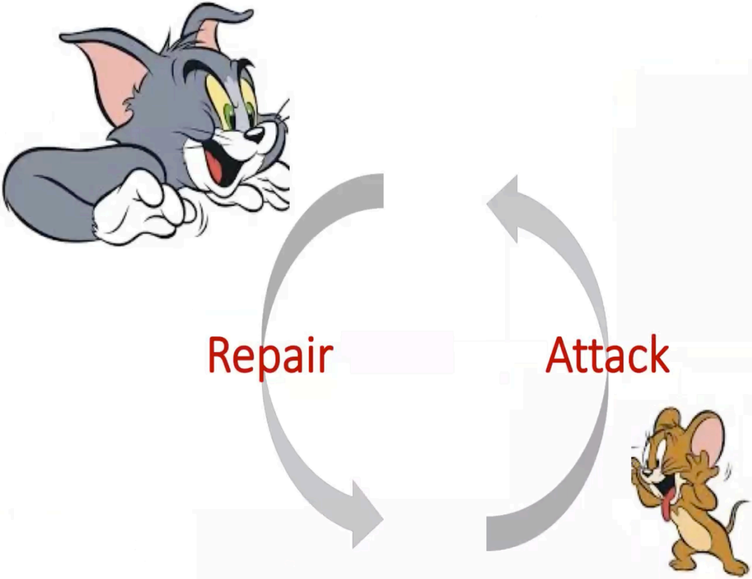
CyberNews

πριν από περίπου 2 εβδομάδες

Massive leak exposed firm that verifies mugshots for ChatGPT and Roblox

Every selfie or ID you upload to ChatGPT, Roblox, LinkedIn, and many other sites for verification is handled by a San Francisco firm called Persona.

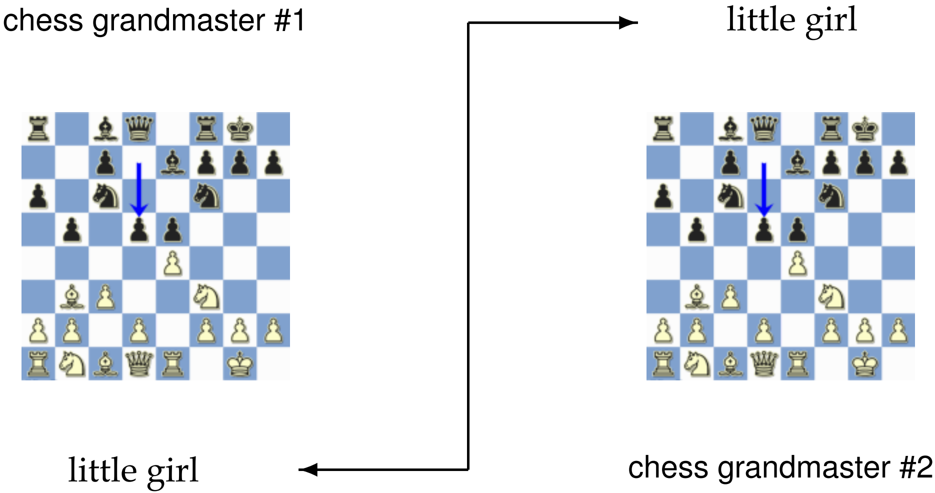
**Lesson:** Convenience ID checks can turn into **monitoring** when transparency is missing.



Repair

Attack

## Relay Attacks - Playing against two Chess Grandmasters



chess grandmaster #1

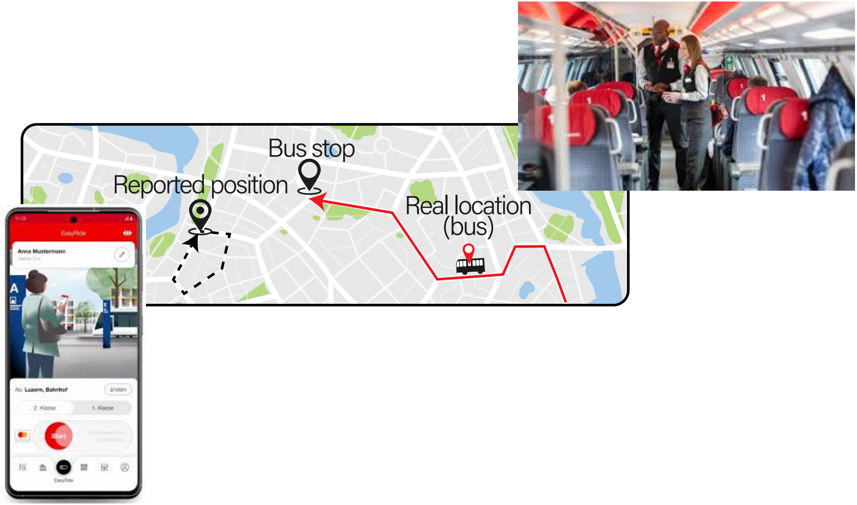
little girl

little girl

chess grandmaster #2

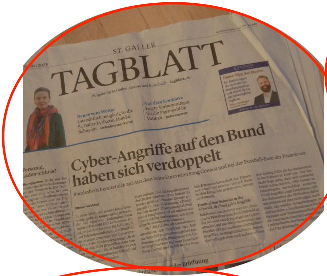
T. Beth and Y. Desmedt. Identification tokens - or: Solving the chess grandmaster problem. In CRYPTO, pages 169–177, 1990.

# SBB FreeRide Attack



- **FreeRide** exploits **fake GPS data**
- Tricks SBB easy ride into thinking a user is “walking”, enables **free rides**
- Trust unverified **device-reported proximity**
- PayRide fixes this by linking user location to **train’s actual position**.

# Cyberattacks - Locally



ST. GALLER TAGBLATT

6. Mai 2025

Ausgabe für St. Gallen, Gossau und Rorschach tagblatt.ch

**Neues vom Wetter** Unersättlich neugierig ist die St. Galler Lyrikerin Monika Schnyder. Ostschweizer Kultur

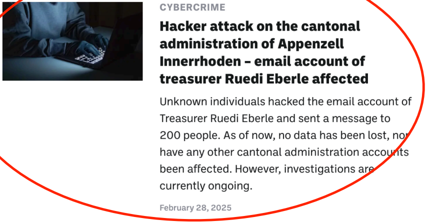
**Vor dem Konklave** Letzte Vorbereitungen für die Papstwahl im Vatikan. Schwerpunkt

**Cyber-Angriffe auf den Bund haben sich verdoppelt**

Bundesbern bereitet sich auf Attacken beim Eurovision Song Contest und bei der Fussball-Euro der Frauen vor.

Othmar von Matt

**Dreimal war Selenski in der Schweiz, dreimal gab's Angriffe**

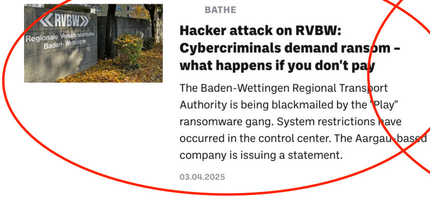


CYBERCRIME

**Hacker attack on the cantonal administration of Appenzell Innerrhoden – email account of treasurer Ruedi Eberle affected**

Unknown individuals hacked the email account of Treasurer Ruedi Eberle and sent a message to 200 people. As of now, no data has been lost, nor have any other cantonal administration accounts been affected. However, investigations are currently ongoing.

February 28, 2025

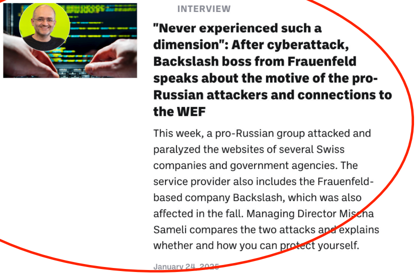


BATHE

**Hacker attack on RVBW: Cybercriminals demand ransom – what happens if you don't pay**

The Baden-Wettingen Regional Transport Authority is being blackmailed by the "Play" ransomware gang. System restrictions have occurred in the control center. The Aargau-based company is issuing a statement.

03.04.2025



INTERVIEW

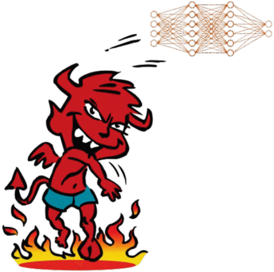
**"Never experienced such a dimension": After cyberattack, Backslash boss from Frauenfeld speaks about the motive of the pro-Russian attackers and connections to the WEF**

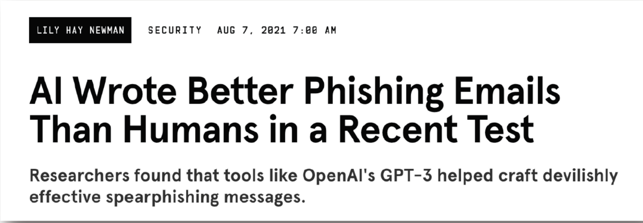
This week, a pro-Russian group attacked and paralyzed the websites of several Swiss companies and government agencies. The service provider also includes the Frauenfeld-based company Backslash, which was also affected in the fall. Managing Director Mischa Sameli compares the two attacks and explains whether and how you can protect yourself.

January 24, 2025

# AI makes things harder?

Phishing is done **easier**!





LILY HAY NEWMAN SECURITY AUG 7, 2021 7:00 AM

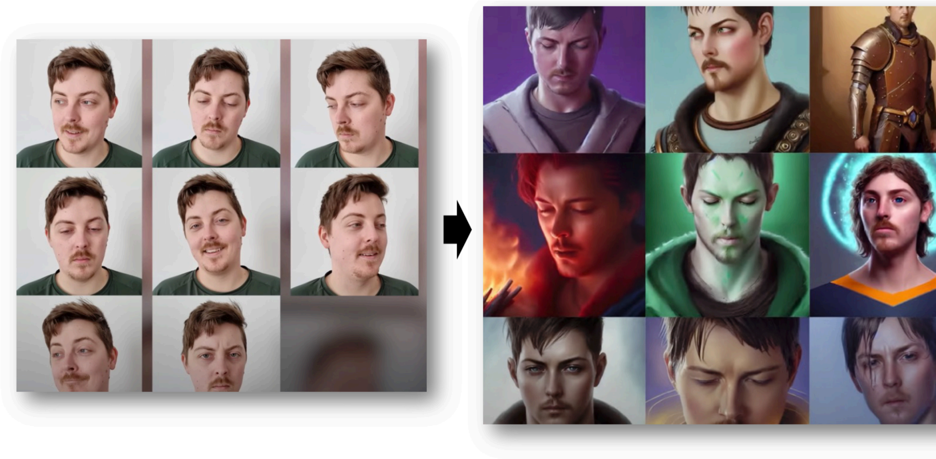
AI Wrote Better Phishing Emails Than Humans in a Recent Test

Researchers found that tools like OpenAI's GPT-3 helped craft devilishly effective spearphishing messages.

Copyright F. Tramer

# AI makes things harder?

Deep fakes for **everyone**!



*https://www.youtube.com/watch?v=FaLTztGGueQ, James Cunliffe*

# When AI Assistants Become a Threat

### Risk Pattern

- Installed as apps, extensions, or system helpers.
- Operate continuously & invisibly once trusted.
- Accesses sensitive data (tokens, cookies, identity info).
- Sends data externally **without visibility**.

# When AI Assistants Become a Threat

**Risk Pattern**

- Installed as apps, extensions, or system helpers.
- Operate continuously & invisibly once trusted.
- Accesses sensitive data (tokens, cookies, identity info).
- Sends data externally **without visibility**.

## Identity Consequences

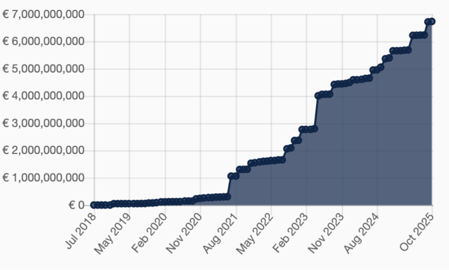
- **Loss of control** over personal or organizational accounts.
- Unauthorized actions performed under the user's identity.

# Do Regulations Help?

# Do Regulations Help?

## Total GDPR Fines (2018–2025)

- **Cumulative fines:** Over €6.22 billion as of May 2025.
- **Number of fines:** More than 2,500 fines issued across Europe.
- **Average fine:** Approximately €2.36 million

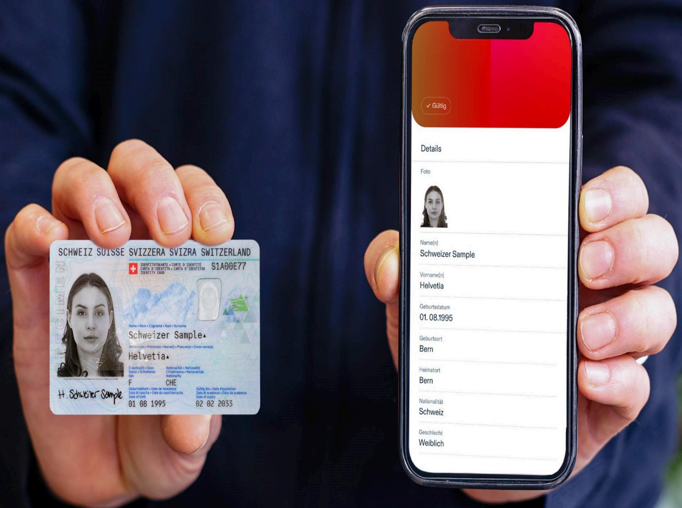


| Company | Fine Amount (€) | Year |
|---|---:|---|
| Meta (Facebook) | 1.2 billion | 2023 |
| Amazon | 746 million | 2021 |
| TikTok | 530 million | 2025 |
| LinkedIn | 310 million | 2024 |
| Uber | 290 million | 2024 |
| WhatsApp (Meta) | 225 million | 2021 |

Table: Top Companies Fined Under GDPR

# What about the Swiss e-ID?

# The e-ID is a Digital Identity Card


SCHWEIZ SUISSE SVIZZERA SVIZRA SWITZERLAND
IDENTITÄTSKARTE • CARTE D'IDENTITÉ
CARTA D'IDENTITÀ • CARTA D'IDENTITAD
IDENTITY CARD
S1A00E77
SPECIMEN
Name • Nom • Cognome • Num • Surname
Schweizer Sample
Vorname(n) • Prénom(s) • Nome(i) • Prenum(s) • Given name(s)
Helvetia
Geschlecht • Sexe • Sesso • Schlattaina • Sex
F
Nationalität • Nationalité • Cittadinanza • Naziunalitad • Nationality
CHE
Geburtsdatum • Date de naissance • Data di nascita • Data da naschientscha • Date of birth
01 08 1995
Gültig bis • Date d'expiration • Data di scadenza • Data da scadenza • Date of expiry
02 02 2033
H. Schweizer Sample

✓ Gültig

Details

Foto

Name(n)
Schweizer Sample

Vorname(n)
Helvetia

Geburtsdatum
01.08.1995

Geburtsort
Bern

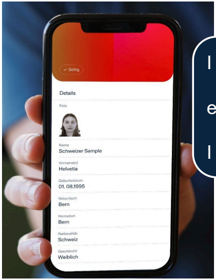
Heimatort
Bern

Nationalität
Schweiz

Geschlecht
Weiblich

# The Swiss e-ID

- **Stored** on smart phone
- Bound on device (keys stored in secure enclave)
- **Holder binding** (device + picture)
- Privacy: unlinkability of presentations (using batch issuance)
- Open Source Software
- **External tests:** pentests, bug bounties
- Use static ECDSA signature & hash functions



Name
Schweizer Sample

Vorname(n)
Helvetia

Geburtsdatum
01. 08.1995

Geburtsort
Bern

Heimatort
Bern

Nationalität
Schweiz

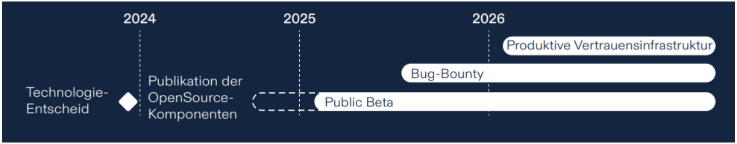
Geschlecht
Weiblich

I own an e-ID, it’s valid today.

e-ID is not revoked.

I am of legal age.

# Swiss e-ID Roadmap



2024
2025
2026
Produktive Vertrauensinfrastruktur
Bug-Bounty
Technologie-Entscheid
Publikation der OpenSource-Komponenten
Public Beta

## 2024

- Technology decision
- Electronic driving learner’s permit (eLFA) built using the future E-ID technology stack

## 2025

- Public beta of tech stack, incl. SWIYU Wallet
- **Vote on referendum (Sept. 28)**

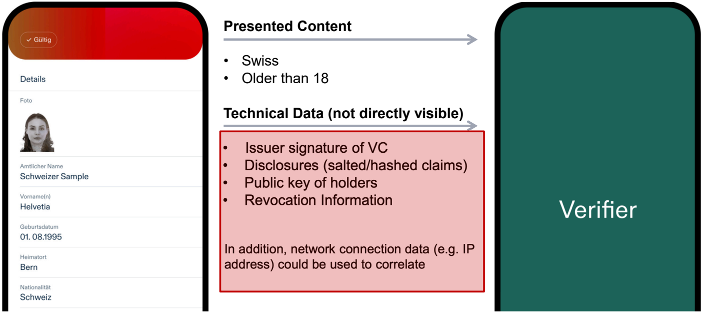
## 2026 Q3/Q4

- Earliest possible launch date for E-ID

## 2027+

- Improved unlinkability (issuer and verifier collusion)
- PQC
- Accountability?

# Goal Unlinkability of Presentations



✓ Gültig

Details

Foto

Amtlicher Name
Schweizer Sample

Vorname(n)
Helvetia

Geburtsdatum
01. 08.1995

Heimatort
Bern

Nationalität
Schweiz

**Presented Content**

- Swiss
- Older than 18

**Technical Data (not directly visible)**

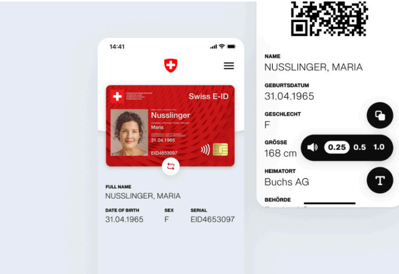
- Issuer signature of VC
- Disclosures (salted/hashed claims)
- Public key of holders
- Revocation Information

In addition, network connection data (e.g. IP address) could be used to correlate

# Issuance: How the e-ID Is Created

## What the issuer does

- Turns each piece of information into a **salted hash**
- Puts all these digital fingerprints into a **digital signature**



Nusslinger
Maria
31.04.1965
EID4653097

FULL NAME
NUSSLINGER, MARIA

DATE OF BIRTH 31.04.1965
SEX F
SERIAL EID4653097

NAME
NUSSLINGER, MARIA

GEBURTSDATUM
31.04.1965

GESCHLECHT
F

GRÖSSE
168 cm

HEIMATORT
Buchs AG

BEHÖRDE

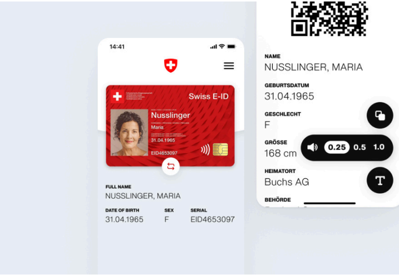
# Issuance: How the e-ID Is Created

### What the issuer does

- Turns each piece of information into a **salted hash**
- Puts all these digital fingerprints into a **digital signature**

### What the user receives

- **Digital signature** (contains only hashes, not the real data)
- **Disclosure objects** (the real information + the random noise, kept private until needed)



FULL NAME
NUSSLINGER, MARIA

DATE OF BIRTH
31.04.1965

SEX
F

SERIAL
EID4653097

NAME
NUSSLINGER, MARIA

GEBURTSDATUM
31.04.1965

GESCHLECHT
F

GRÖSSE
168 cm

HEIMATORT
Buchs AG

BEHÖRDE

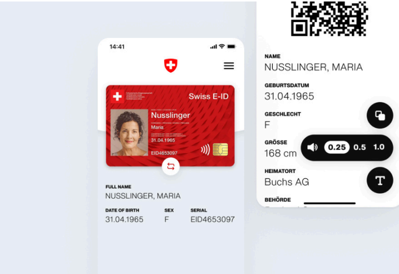
# Issuance: How the e-ID Is Created

### What the issuer does

- Turns each piece of information into a **salted hash**
- Puts all these digital fingerprints into a **digital signature**

### What the user receives

- **Digital signature** (contains only hashes, not the real data)
- **Disclosure objects** (the real information + the random noise, kept private until needed)



FULL NAME
NUSSLINGER, MARIA

| DATE OF BIRTH | SEX | SERIAL |
|---|---|---|
| 31.04.1965 | F | EID4653097 |

NAME
NUSSLINGER, MARIA

GEBURTSDATUM
31.04.1965

GESCHLECHT
F

GRÖSSE
168 cm

HEIMATORT
Buchs AG

BEHÖRDE

### Key idea

- The issuer signs the hashes; the user controls the real data

# Why Secure and Private Identity Matters

## Identity is now everywhere

- We use it to log in, travel, pay, vote, communicate.
- Attacks are rising: phishing, deepfakes, stolen biometrics.
- Companies & governments **collect more data** than people realize.

## Real-world risks

- **Persona scandal:** selfies sent into hidden surveillance systems.
- Internet shutdowns (e.g., Iran) show how identity can be controlled.
- Biometric leaks cannot be undone, you cannot change your face.

# Our Work: Building Trustworthy Digital Identity

## What we aim for

- Identity that **protects** people, not exposes them.
- Systems where **users choose** what they reveal.

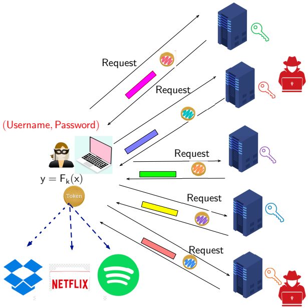
# Our Work: Building Trustworthy Digital Identity

## What we aim for

- Identity that **protects** people, not exposes them.
- Systems where **users choose** what they reveal.

## What we build

- **Privacy-preserving** identity primitives.
- Cryptographic tools that prevent tracking & profiling.
- Foundations used in systems like the **Swiss e-ID**.



Decentralised, Private & Secure Authentication

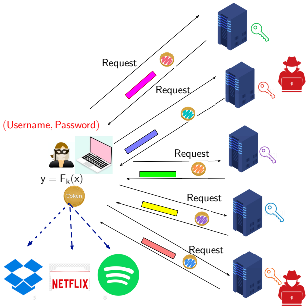
# Our Work: Building Trustworthy Digital Identity

## What we aim for

- Identity that **protects** people, not exposes them.
- Systems where **users choose** what they reveal.

## What we build

- **Privacy-preserving** identity primitives.
- Cryptographic tools that prevent tracking & profiling.
- Foundations used in systems like the **Swiss e-ID**.



Decentralised, Private & Secure Authentication

## Our goal:

Give people digital identity **they can trust**, even when the world around them is not trustworthy.

# Closing Remarks

- **Cybersecurity:** a challenging & multidimensional
- **Privacy:** A right for every individual!
- **New Technologies:** High Capacity for Abuse &**Attacks**!
- We can provide practical solutions to **overcome** many existing problems!

Thank you for your Attention!

Contact: https://cybersecurity.unisg.ch