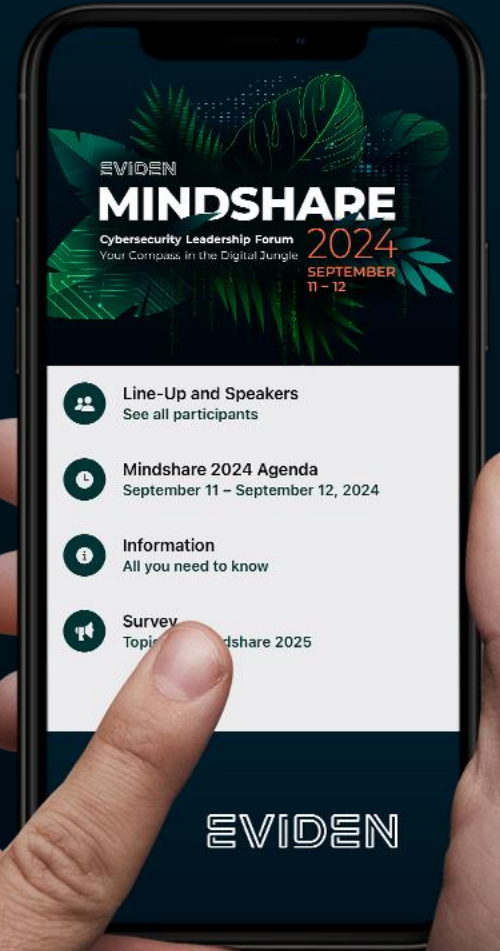


MINDSHARE 2024 AGENDA



SCAN NOW !





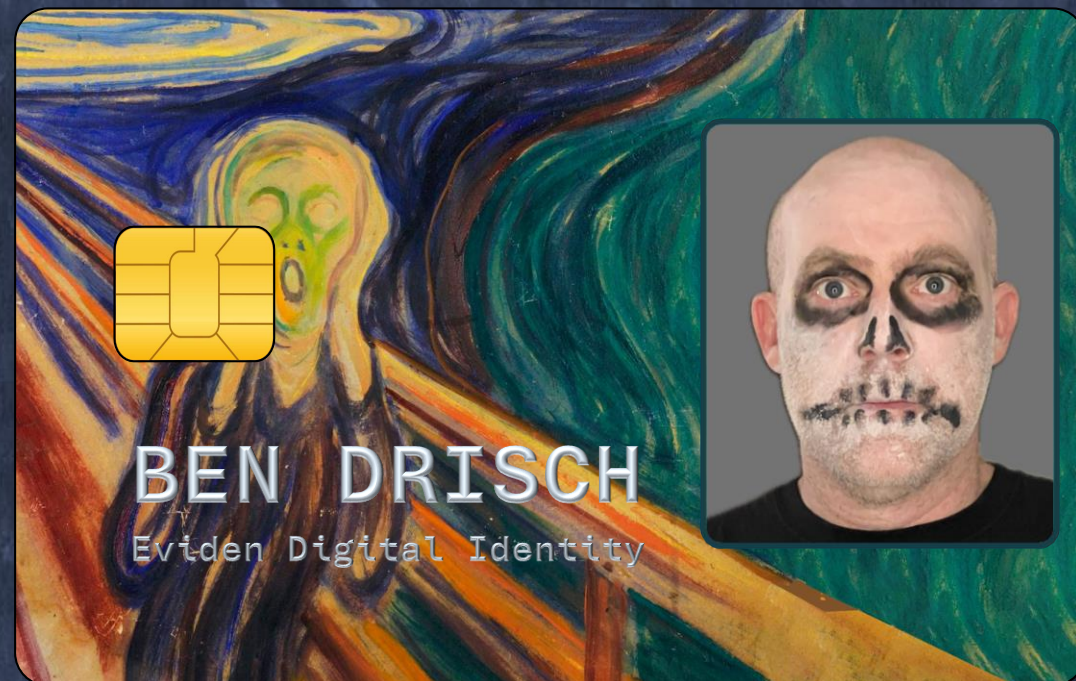
eID Blunders

Ben Drisch

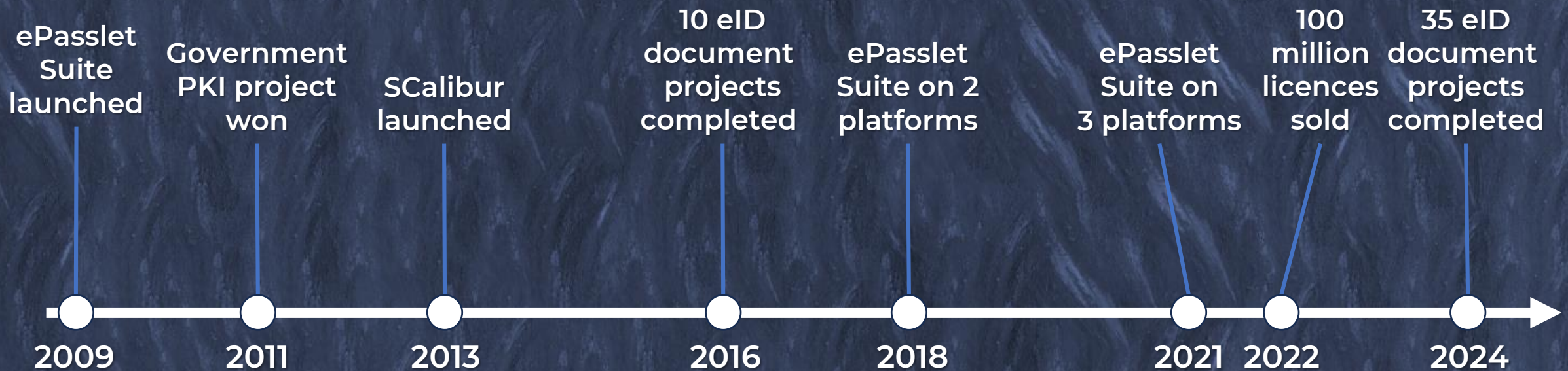
Marco Smeja

Eviden Digital Identity

Mindshare 2024



Our official Citizen ID history



Our unofficial Citizen ID History



Open
Source
Disaster

2012



Vendor Lock
to Citizen
Data

2015



cryptovision
became a
Country

2019



Proprietary
Security
Mechanisms

2023



**This is a talk about
the dark side of the
eID business**

**Be prepared to see
the worst**



Open Source Disaster



Open
Source
Disaster



Vendor
Lock to
Citizen Data



cryptovision
became a
Country



Proprietary
Security
Mechanisms



Smaller country



eID with digital signature



**A middleware shall
enable various signature
use cases**



Open source eID middleware
was aimed to be deployed



**Card Support insufficient
No upgrades available
(security and functionality)**



After pilot phase open
source middleware turned out to be
unusable



**Use commercial software with
maintenance included**

**This is also mandated by the EU
Cyber Resilience Act**



**Be aware of open source
software limitations**



Vendor Lock (Citizen Data)



Open
Source
Disaster



Vendor
Lock to
Citizen Data



crypto
vision
became a
Country



Proprietary
Security
Mechanisms



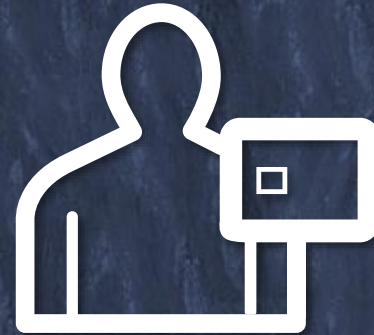
Mid-sized country



Multi-application eID



**A well-working multi-
application eID project**



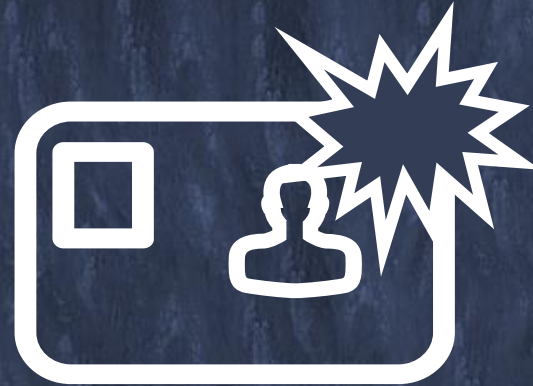
Personalisation service provider had limited access to citizen data required for personalization



Customer had to buy "operator cards" for personalization at astronomical costs



Changes to eID
infrastructure were
locked



Personalization solution was replaced

**Initial costs for change,
but paid off in the long run**



cryptovision became a Country



Open
Source
Disaster



Vendor
Lock to
Citizen Data



cryptovision
became a
Country



Proprietary
Security
Mechanisms



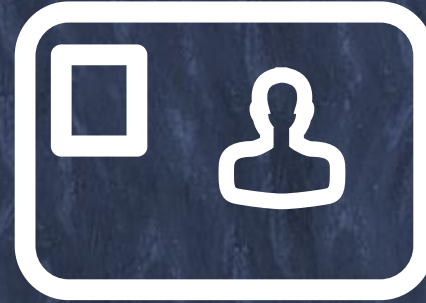
**Country with eventful history
in Europe**



Electronic driving licence



I got a call from the German Federal Police about official documents that were issued by the country "cryptovision"



We provided tools for personalization to the customer that contained test certificates with "cn = cryptovision"



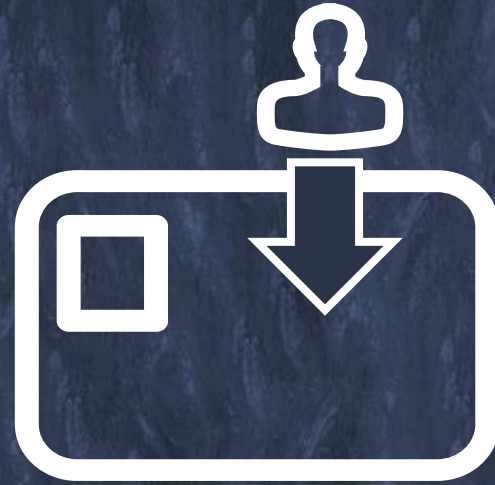
When verified the Driving License would return "cryptovision" as issuer



Test tools and data were
used for productive eID
cards



Temporary acceptance of
“cryptovision” eID cards



We make it too easy
for you ...?



Vendor Lock (Infrastructure)



Open
Source
Disaster



Vendor
Lock to
Citizen Data



cryptovision
became a
Country



Proprietary
Security
Mechanisms



Mediterranean country

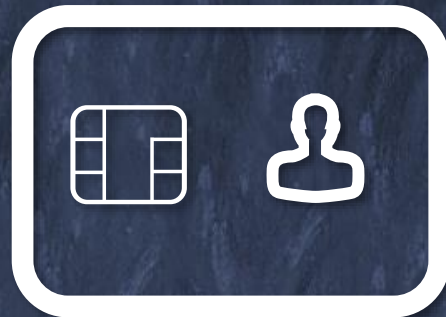


National eID card

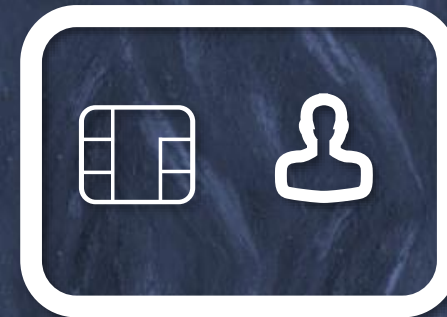


Old card of an eID system
was to be replaced

Old chip, EOL



New chip





Infrastructure
included
proprietary security
mechanisms



Infrastructure and terminals could not be easily updated



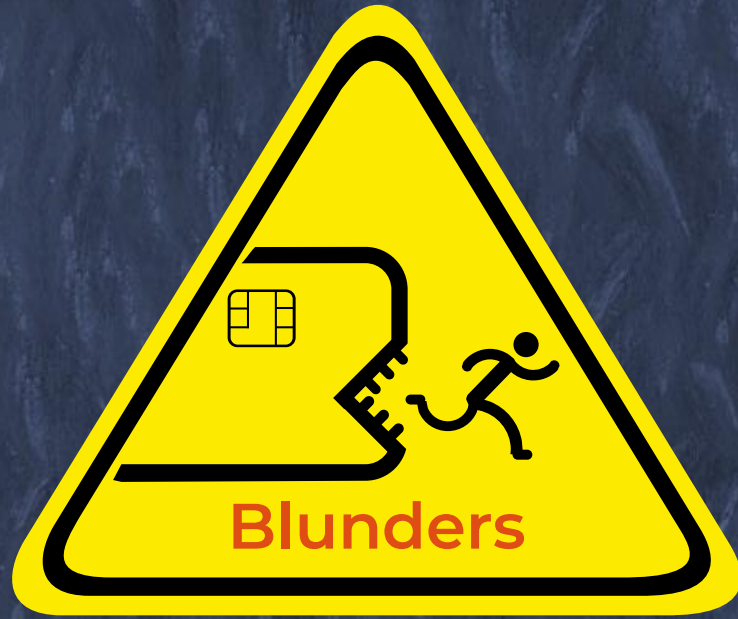
Issuer almost ran
out of eID
documents



Solution: adapt eID card to infrastructure, not the other way around
ePasslet Suite architecture allowed for comprehensive customization



Use open standards



Conclusion



- In the eID business a lot is not as it seems
- Accidents happen





- Use open standards
- Avoid vendor locks
- Be careful with open source software
- Testing is essential

EVIDEN



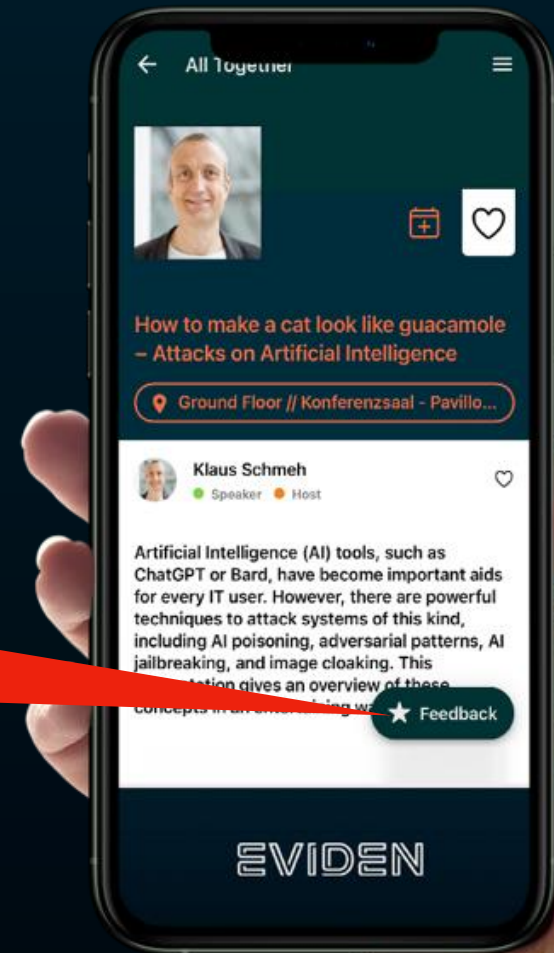
END

Questions?

TAKE A MINUTE AND GIVE US FEEDBACK ...



**RATE
NOW!**





Security Policy Blunder



Small and rich country



Luxury ePass



**A country, somewhere in
the world**



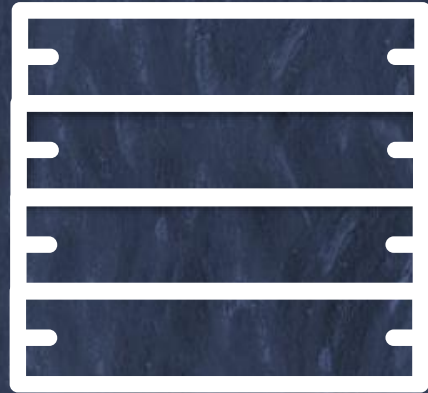
**A well-working eID
document project**



Generally high security standards and certified solutions



Storage and shipping of empty passports not covered by security policy



**Boxes with passport
blanks vanished**



Forgeries possible



**Security policy
was extended**



**Take a holistic
approach**



Double Key Incident



Western country



Multi-application eID



**A country, during
the Covid time**



**Multi-application eID
launched with successful
key ceremony**



Country in code* in CSCA
certificate consisted of two letters

* All country codes consist of three letters, except Germany (D)



Certificates not standard-compliant



**Consultant was already
on his way home**



Consultant ...

... did a U-turn before the airport

... took a new Covid test

... performed key ceremony again



Testing is
essential