



#### Overview of elD landscape

Imad Aad C4DT - EPFL

## **EPFL** IDs going digital...

## Why go digital, online?

#### EPFL. Advantages of going digital, online: Money 3 Aad. Oct. 2024 Analog Digital Online Orgato-Owstody Solutions 🗖 111... DUPERCHAIN Gass the c p o C TREEDOM engeri ABMORY 健 Lades PayPal O freedom τωιωτ VIS --- 123H • 1 • 🛃 Alipay`

## **EPFL** Advantages of going digital, online: IDs



## **EPFL** Disadvantages of going online



 Center for Digital Trust Online



TRACES

Image credit: Thinkstock, Getty images

## **EPFL** Going digital + online = success?

#### Among other factors:

• At the right place and at the right time...

In the 80's: "Why do you need to carry a computer if you have cash?" vs. Nowadays: "Why do you need to carry cash if you have a smartphone?"

- Simplicity / usability / better government service delivery
- Economic and development potentials
- <u>Trust</u> (the system, data protection, no / less fraud)

#### Interoperability

## **EPFL** Outline

- Why go digital?
- Trust x eIDs
- Interoperability x eIDs
- The Swiss elD



# IDs, eIDs... what's the trust model behind?



What are their properties and functions?







Overview of eID landscape. I. Aad. Oct. 2024















-----

#### **Electronic identifiers: ID Provider (IDP)**













Certified











# **EPFL** Types of digital identities Who "controls" the identity and its attributes? Centralized Identity Federated Identity

a

User-Centric Identity

Verifier Verifiers

eign Identity

11

Dverview of eID landscape. I. Aad. Oct. 2024

#### **EPFL** OECD Digital Government Studies Digital Government in Chile – Digital Identity



**OECD Digital Government Studies** 

Digital Government in Chile – Digital Identity

GBI Private ITA CAN MOR DI cnrelescut NZL ENK IND AUT Public 151 KOR Optional R1cani National Population Registry Mandatory No Population registry Optional (aga)

Figure 2.1. Digital ID enrolment and National Population Registers



## **EPFL** Self-Sovereign Identities, SSI



#### EPFL Self Sovereign IDs, SSI principles

1. Representation: An SSI ecosystem shall provide the means for any entity—human, legal, natural, physical or digital—to be represented by any number of digital identities.

2. Interoperability: An SSI ecosystem shall enable digital identity data for an entity to be represented, exchanged, secured, protected, and verified interoperably using open, public, and royalty-free standards.

3. Decentralization: An SSI ecosystem shall not require reliance on a centralized system to represent, control, or verify an entity's digital identity data.

4. Control & Agency: An SSI ecosystem shall empower entities who have natural, human, or legal rights in relation to their identity ("Identity Rights Holders") to control usage of their digital identity data and exert this control by employing and/or delegating to agents and guardians of their choice, including individuals, organizations, devices, and software.

5. Participation: An SSI ecosystem shall not require an identity rights holder to participate.

6. Equity and Inclusion: An SSI ecosystem shall not exclude or discriminate against identity rights holders within its governance scope.

7. Usability, Accessibility, and Consistency: An SSI ecosystem shall maximize usability and accessibility of agents and other SSI components for identity rights holders, including consistency of user experience.

8. Portability: An SSI ecosystem shall not restrict the ability of identity rights holders to move or transfer a copy of their digital identity data to the agents or systems of their choice.

9. Security: An SSI ecosystem shall empower identity rights holders to secure their digital identity data at rest and in motion, to control their own identifiers and encryption keys, and to employ end-to-end encryption for all interactions.

10. Verifiability and Authenticity: An SSI ecosystem shall empower identity rights holders to provide verifiable proof of the authenticity of their digital identity data.

#### 11. Privacy and Minimal Disclosure: An SSI ecosystem shall empower identity rights holders to protect the privacy of their digital identity data and to share the minimum digital identity data required for any particular interaction.

12. **Transparency:** An SSI ecosystem shall empower identity rights holders and all other stakeholders to easily access and verify information necessary to understand the incentives, rules, policies, and algorithms under which agents and other components of SSI ecosystems operate.

## Cryptography Basics

## **EPFL** Why do we need encryption?

#### CIA

- Confidentiality
- Integrity
- Availability
- +
- Authentication
- Non-Repudiation

How can we achieve these goals?



## **EPFL** (Symmetric) Encryption



This is called <u>symmetric</u> encryption (same secret key for encrypting and decrypting)

Problem: Need a separate channel for sharing the secret key!



## **EPFL** Asymmetric Encryption



#### Example: https://www.second.com/second-secon

### **EPFL** Encryption and Signing



Is that it? No more problems?





## Certificates

#### EPFL. Man in the Middle (MITM) problem





1.6







 Center for Digital Trust Dverview of eID landscape. I. Aad. Oct. 2024 R

#### **EPFL** Certificates

- Certify that a given public key belongs to a given domain (domain verification, DV)
- Issued by Certificate Authorities (CAs)
- CAs have "Root Certificates"
- Browsers have a list of "Root Certificates they trust
- Browsers impose their "rules" for trust





### **EPFL** Take aways

- You (or your browser) cannot trust everyone who's on the path between you and the server (ex. bank)
- You encrypt end-to-end (https)
- The certificate authority (CA) tells you it's the proper "end" (ex. Bank) you're communicating with
- You trust the CA
- CA can potentially cheat (ex. by certifying a Man-in-the-Middle)

#### • You trust more <u>CA + Browsers</u>



## Where's the state in all of this?!

24

Overview of eID landscape. I. Aad. Oct. 2024



## And then came the QWACs

Qualified Website Authentication Certificates

Credit: securityriskahead.eu

### **EPFL** QWACs vs. Traditional (DV) Certificates

	DV Certificates	QWACs
Issued by	Certificate Authorities Certificate Transparency, an IETF technical standard that ensures a CA's issuing history can be examined by the public in order to detect malfeasance; WebTrust for CAs audit; ETSI EN 319 411 audit; section 2.2 of the TLS Baseline Requirements	[Qualified ]Trust Service Providers ([Q]TSPs) duly certified and audited to ensure they meet the stringent standards established by the regulation.
Certifies that	Public key belongs to website	idem + tie to owner org. (EV) "displaying in a user-friendly manner"
Browsers trust	Their list of "Root Certificates"	idem + root certif. of member states
Rules of security / trust	Defined by browser makers	Defined by ETSI

### **EPFL QWACs: Motivation**

- Strengthen the European position against the market power of powerful internet companies
- Reduce the power of large companies behind major browsers (Google, Apple, Microsoft...)
- Sovereignty
- Financial (est. 247M Euros in 2027)
- [No] increased security?

## What's right / wrong?



#SecurityRiskAhead launch July 2022

Credit: securityriskahead.eu



- Critics include: Mozilla foundation, EFF, Int'l group of security experts
- The introduction of this text so late in the **legislative process and behind closed doors** is also deeply concerning for democratic norms in Europe.
- While QWACs deliver verifiable identity information, browser certificates secure and authenticate connections to servers. **Treating them interchangeably undermines established best practices** and security mechanisms,
- It seems inevitable that they will have to create two versions of their software: one for the EU, with security checks removed. We've been down this road before, when export controls on cryptography meant browsers were released in two versions: strong cryptography for US users, and weak cryptography for everyone else.
- The owner of a root certificate can intercept users' web traffic by replacing the website's cryptographic keys with substitutes he controls. Any root certificate trusted by the browser can be used to compromise any website. There are multiple documented cases of abuse, because the security of some certificate authorities has been compromised
- The regulation's technical implementation could serve to expand the ability of governments to surveil both their own citizens and residents across the EU by providing them with the technical means to intercept encrypted web traffic. Countries like Kazakhstan, China and Russia have already tried something like this in the past.

## **EPFL** QWACs vs. Traditional (DV) Certificates

	DV Certificates	QWACs
Issued by	Certificate Authorities	[Qualified ]Trust Service Providers ([Q]TSPs)
	ensures a CA's issuing history can be examined by the public in order to detect malfeasance; WebTrust for CAs audit; ETSI EN 319 411 audit; section 2.2 of the TLS Baseline Requirements	duly certified and audited to ensure they meet the stringent standards established by the regulation.
Certifies that	Public key belongs to website	idem + tie to owner org. (EV) "displaying in a user-friendly manner"
Browsers trust	Their list of "Root Certificates"	idem + root certif. of member states
Rules of security / trust	Defined by browser makers	Defined by ETSI (Note: ETSI has a WG on Legal Interception)

#### EPFL Result...

- "The EU wants to force browsers to accept certain certification bodies. In doing so, it intervenes in a system of technical requirements and market economic forces in which there is a lot of need for improvement - but in which a lot can also be broken" [CT magazine]
- Outcry by foundations and scientists
- "Trust the private sector more or less than the authorities?" That is the question



## More on whom to trust...

32

Overview of eID landscape. I. Aad. Oct. 2024

### **EPFL** Trust registries

- Who's allowed to verify?
  - Ex: Discotheque claiming to be a cantonal authority
- Who's allowed to ask for what?
  - Ex: Discotheque asking for diplomas
- Who's allowed to issue what?
  - Ex: Ministry of health issuing driving licenses



34

### All that was about whom to trust

### How about what to share / disclose?

## **EPFL** Privacy issues: Data Minimization

- Selective disclosure
  - how about signature validity?

Zero-Knowledge Proofs

- Why data minimization?
  - Privacy principles + GDPR; Swiss DPA; eID law...



35

## **EPFL** Privacy issues: [un]linkability

- Holder linkability
- Issuer linkability
- Verifier linkability
- Which signature algo. support this?BBS / BBS+
- Revocation issues?



## **EPFL** Challenges and open questions

#### (Some) **User-related** questions:

- Awareness raising against risks / scams.
- User literacy for being in control.
- Would e-ID custodians help (for "distributed" SSI)?
- Put all the "intelligence" in the wallet?

### Short break?

# Interoperability

### **EPFL** Interoperability issues

#### Technical

- Solve it in the wallet?
- More on C4DT's Factory webpage: <u>https://c4dt.epfl.ch/article/?cat=10</u>
- Trust Registries
  - Who provides them? Wallet provider? Government?
- Legal

Distitut Trust

• ex. Signature qualifications

2624/16	<b>Destination</b>	Gryptingstephy .	Demonistrike	(Baraga	
Willing artenetises, and doll-illines.					
Dependentianed Monetty Parameteristics		009+(04)	biblionen (Rail)		
RTF and RTF have enfrances	so-JWT (sa)	908+154			
Clerk 12 Foundation		Neti Grantian Identify Damlinck (K)	DENCIN		
P <sub>NR</sub> ; even IP atao imperante nto	w30.010 190		Freet Spanning Profoedi Prete Prete Profoedi Profoedi Prete Prete	Hey Greet Heorige Inheatracture ISE/10(29)(N)	
Nic	was des [Rei] Cremente Cremente [Rei] Mik] 2007-10 [Rei]	065+ (Joli DOPA (DA) DDDSA (DA) DDDSA (Da) Test subm: 33e(		States Cas (Cas)	
voitit	PERMIT				
	into erafice	and molenvental	ion		
A state of a limit of and a state of a	100 C 100	C. mailing zero-	PDC-mm	A THE DRIVE AN	
1.5	[94]	Provincingo prostra (75-2)	Pai)	are delations	
OpenWalter Feurdalten	SC-IWTIDN		OD/VC INE		
	Footalete and	define least therea	works		
DJ GDAG ACY RAFTIEL	KOLJWITIKA DA DALIDIA MIC VODM DALIDIA MIC VODM	tiajoğilicoda. Gel	DE-WC (SM)	Oktivatilet rementioni Tursi Register	
Shins e-ritiSosherik A - REOPOSAL 3140	SC-JWT(Bel	%A(20.0006A 26)	OID-FWC (SHE	Personalitati Matandina Fuat Ropicter	
laisteit - Ionasia I - HOPOSAL (11)	1909-10 (Gel	162+ (34)	оючно вне рессым рат;	Recording Accountation Statistical Trust Registry	
Swim e-10 - Taon Roadinap (200306-18)- randronal (2003	M3C DID (Ga) EU: SO-JWE DHC Phil ADON- LC (SH)	PL: PC:054(71); 9DD:7(34) PR: 005+(50)	oitrive (sv)	Rescuellen Antonistatus Standular (191) Tunt Register	

40



-----

#### Standards, norms, guidelines...

World Bank's ID4D Practitioner's Guide



#### EXAMPLE 1: ID-KAART IN ESTONIA-SMART CARD AND MOBILE ID

Estonia has the most highly developed national ID card system in the world (Williams-Grut 2016). It has issued 1.3 million of its smart ID-Kaarts, each with a unique identifier that allows citizens to access over 1,000 public services, such as health care, online tax filing, and online voting. Estonia is now one of the most digitally advanced nations in the world with regard to public services. It wants to become a "country as a service," where secure digital identity plays a central role. Key identifying data such as name, date of birth , unique ID number and digital certificates are stored in the smart card chip for authentication and digital signing of documents. The access to each of these digital certificates keys is protected by a secret PIN which only the user knows.





Source: Catalog of Technical Standards for Digital Identification Systems. ID-ID initiative, The World Bank.



#### Standards, norms, guidelines...

NIST Digital Identity Guidelines





SP 800-63-3 Digital Identity Guidelines

SP 800-63A Enrolment & Identity Proofing







SP 800-63C Federation & Assertions

### **EPFL** elDs around the world



#### (EU ID wallet, ARF)





## China ?



# EPFL How does the future look like?

Different regional eIDs

Non-interoperable

Sovereignty issues

Economical issues

Will some dominate the international market, while others remain "regional"?





### **Dive into the Swiss elD**

45

Overview of eID landscape. I. Aad. Oct. 2024

## **EPFL** Swiss eID: law



▲ The government has called for joint efforts to pash alwed with digitalization despise opters' rejection of the efform fundament of KeyroperOtherse Deuter



#### **EPFL** Swiss eID: Ambition level



### **EPFL** Swiss eID: legal signing?

#### No (legal) signing, it's only eID

Unlike EU's elDAS

0	Conflotencion prices Conflotencion prices Conflotencion prices Conflotencion prices		Fechez La plateforme de publication du droit fédéral				
A	nuel	Procédures de vorseduction	Feuille förlerske	Ansuel officiel	Receivation	Tekh	
			-	-		-	

Accuell > Receil systematique > 9 Economie - Ceeperation technique > 94 Commerce 3 943.89 Loi Noder de la signature discincriges (Loi sur la signature ellectronique, 5031)

#### Informations générales

A	- T		have seen	and and	
	ALC: 1	0.2	10 C T	I VILL	12.41

Aproviation	3538
Dickion 13	cidoambre 2003
Entrée en vigueur	1 Jenvier 2005
300100	8028045085
Decision abr.	18 // ars 2016
Date diabrogation	1 janvier 2017
Source also.	8020164051
Longerets) de la put	dication
	DE FR IT

#### [ RS 943.03 ]

Loi fédérale du 19 décembre 2003 su domaine de la signature électroniqu

	Tourses les ver
Loi fédérale	+ 01.01.3030
de la signature électroi	+ 01.01.2017
Loi sur la signature électre	
	Révisions

#### Informations ganerales

ce texts-est en vigueur			
Abriviation	3424		
<b>P</b> -bision	18 mars 2016		
Entrégen vigweur	1 janvier 2017		
Source	PO 2016 4631		
Languest) de la publication DE FRIT			
Languees) de la pui	DEFRIT		
Chromelogie	DEFRIT Chronologie		
Chronologie Mocifications	DEFRIT Chronologie Modifications		

Comparateur de lanques

outl

	Toutes les versions			
le conti	+ 01.01.2020	HTML PDF DOC		
le certi lectroi	• 01.01.2017	POF		
* WACTE	Révisions			

#### 943.03

CD Développer tout | Weiger article | Fermer tout )@

#### Loi fédérale

sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques<sup>1</sup>\*

#### (Loi sur la signature électronique, SCSE)

du 18 mart 2016 (Etat le 111 janvier 2020)

11 Les termes désignant des persennes d'appliquent également aux l'emmes et aux hommes.

L'Assemblée fédérale de la Confédération suisse,

```
vules art 95 al. 1, et 122 al. 1, de la Constitution<sup>2</sup>,
vu le message du Conseil fédéral du 15 janvier 2014<sup>3</sup>.
```

arrête:

#### FRE 101

<sup>10</sup> FE 2014 95 3

#### 

- (# Art. 1 Objet et but

<sup>1</sup> La présente loi règle:

- les expenses daigualite auxquelles doivent répondra certains certricats numériques et leur utilisations
- les conditions auxquailes les fournisseurs de services de certification dans le domaine de la signature electromique et das autres applications das certificats numériques (services de certification) peavent être Needominute:
- Les deales et les des aix des técnetes privat se partempters de part des destificant an

### **EPFL** Swiss elD: other

Not mandatory to have; Mandatory to accept

- Linked to a person or to a device?
  - -> device + secure enclave
    - Social Inclusion?
- No (legal) signing, it's only eID
   Unlike EU's eIDAS
- EU compatible?
  - How about BBS/BBS+ / ZKP etc.?
- + digital wallet
- Note: Don't confuse eID with online logins

### **EPFL** Swiss elD: other

#### FOITT's sandbox(es)

Expected to be launched in 2026

	ape. I. Aad. Oct. 2024
Contraction to the second description of the	
isone Participation Ecosystem Serbodings Electronic penalsional delang licence	
Parregage - Fartispation -	

hublished on 22 November 2023

#### Why do we need participation?

The e-ID and the rust infrastructure are beingoet up primarily for people living in Switterland. To ensure that they will understand, trust and use thee-Project Organisation offers nations energy of embarraing information and participating in the project. This also means chatche knowledge and experience outside the federal Administration (an be brought into the project. The idea is to creaty opportunities to participate in addition to the formal mechanism optional referendum, etc.). Or you have any ideas for further porticipation opportunities? We look forward to learing from you.

Follow the news / join participation meetings: https://www.eid.admin.ch/en/why-do-we-needparticipation

#### takenike to early HI neoralities

unce or twise a momen we send ou, the 4-au nowsletter, in which we report on inportant developments in the e-ID project and draw your attention to forthcoming events, especially the sarbcpation meetings.



50

Constant of





#### **EU** Regulations, eIDAS

- The elDAS Regulation evolved from Directive 1999/93/EC, which set a goal that EU member states were expected to achieve in regards to electronic signing.
- The directive also **allowed each member state to interpret the law** and impose restrictions, thus preventing real interoperability, and leading toward **a fragmented scenario**.
- In contrast with this directive, eIDAS ensures mutual recognition of the eID for authentication among member states, thus achieving the goal of the Digital Single Market.
- elDAS is primarily **designed to tackle identification** challenges experienced by **digital <u>public</u> services**.
- Yet, Member States are also encouraged to support the voluntary reuse of eIDAS-based eIDs by the private sector.

#### **EU** Regulations, eIDAS

The Regulation provides the regulatory environment for the following important aspects related to electronic transactions:

- Digital identity: a European-wide framework for digital authentication of citizens, with legal validity. Nine principles of EU digital identity have been defined: user choice, privacy, Interoperability and security, trust, convenience, user consent and control proportionality, counterpart knowledge and global scalability.
- Advanced electronic signature: An electronic signature is considered advanced if it meets certain requirements:
  - Olt provides unique identifying information that links it to its signatory.
  - The signatory has sole control of the data used to create the electronic signature.
  - It must be capable of identifying if the data accompanying the message has been tampered with after being signed. If the signed data has changed, the signature is marked invalid.
  - There is a certificate for electronic signature, electronic proof that confirms the identity of the signatory and links the electronic signature validation data to that person.
  - Advanced electronic signatures can be technically implemented, following the XAdES, PAdES, CAdES or ASiC Baseline Profile (Associated Signature Containers) standard for digital signatures, specified by the ETSI.
- Qualified electronic signature, an advanced electronic signature that is created by a qualified electronic signature creation device based on a qualified certificate for electronic signatures.
- Qualified digital certificate for electronic signature, a certificate that attests to a qualified electronic signature's authenticity that has been issued by a qualified trust service provider.
- Qualified website authentication certificate, a qualified digital certificate under the trust services defined in the eIDAS Regulation.
- Trust service, an electronic service that creates, validates, and verifies electronic signatures, time stamps, seals, and certificates. Also, a trust service may provide website authentication and preservation of created electronic signatures, certificates, and seals. It is handled by a trust service provider.

#### **EU** Regulations, eIDAS

- The regulatory obligations and security needs to which they are subject in terms of identity verification have placed **banks and financial institutions in a strategic position**.
- More and more institutions are exploring how they could leverage the procedures that they have put in place to verify customers' identity for other parties by **acting as identity providers**.
- eIDAS-based eIDs offer the possibility to provide a strong authentication of users (natural and legal persons), based on ID information endorsed by governmental authorities across Europe.

List of