

Elektronické podpisy

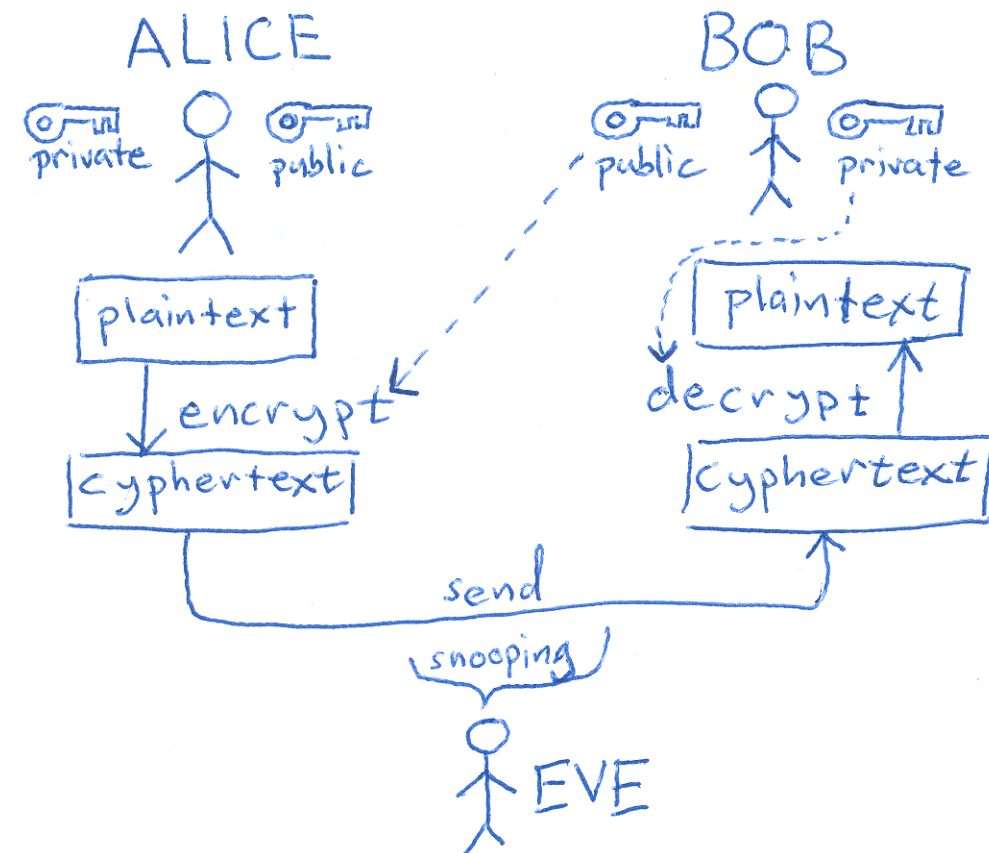
JUDr. Pavel Loutocký, Ph.D., BA (Hons)



Elektronický podpis

Možnosti využití elektronického podpisu byly popsány již v 70. letech 20. století

- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
- Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy
- UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
- Technicky: <https://www.youtube.com/watch?v=Tw5q-SN9ZM8&t=105s>



Co je elektronický podpis?



Email or Phone	Password	Log In
<input type="text"/>	<input type="text"/>	
<input checked="" type="checkbox"/> Keep me logged in	Forgotten your password?	

JUDr. Pavel Loutocký,
Ph.D.,
BA(Hons)

Digitálně podepsal JUDr. Pavel Loutocký,
Ph.D., BA(Hons)
Datum: 2024.03.12 15:26:13 +01'00'

Evolve? Nařízení eIDAS



Co znamená nařízení eIDAS

- eIDAS – **e**lectronic **i**dentification **a**nd **s**ervices
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- Zveřejněno v Úředním věstníku EU dne 28. 8. 2014

Čeho se nařízení týká?

1. Oblast elektronické identifikace (spolupráce, součinnost)

„elektronickou identifikací“ se myslí postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu (čl. 3 odst. 1 nařízení)

Čeho se nařízení týká?

2. Oblast služeb vytvářejících důvěru (sladění úprav)

služby, které slouží k vytváření důvěry:

elektronický podpis, elektronická pečeť, elektronické časové razítko

elektronické doporučené doručování, autentizace internetových stránek

elektronické dokumenty

Čeho se tedy nařízení eIDAS týká?

- Právní rámec pro důvěryhodné elektronické transakce
- Výměna dokumentů, prokazování totožnosti (atd.) mezi občany, podniky a úřady v členských zemích EU
- Usnadnění přeshraničního obchodování, vyplnění daňového přiznání, účast na veřejných zakázkách, pobírání důchodu, podávání přihlášek ke studiu, atd.

Elektronický podpis dle čl. 3/10 eIDAS

1. data v elektronické podobě,
 2. která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena
 3. a která podepisující osoba používá k podepsání
- Zaručený elektronický podpis umožňuje **jednoznačnou** identifikaci podepisující osoby

Tedy znovu! Co je elektronický podpis?

Loutocký



Email or Phone

Password

Keep me logged in [Forgotten your password?](#)

JUDr. Pavel
Loutocký,
Ph.D.,
BA(Hons)

Digitálně
podepsal JUDr.
Pavel Loutocký,
Ph.D., BA(Hons)
Datum: 2024.03.12
15:26:13 +01'00'

Základní funkce

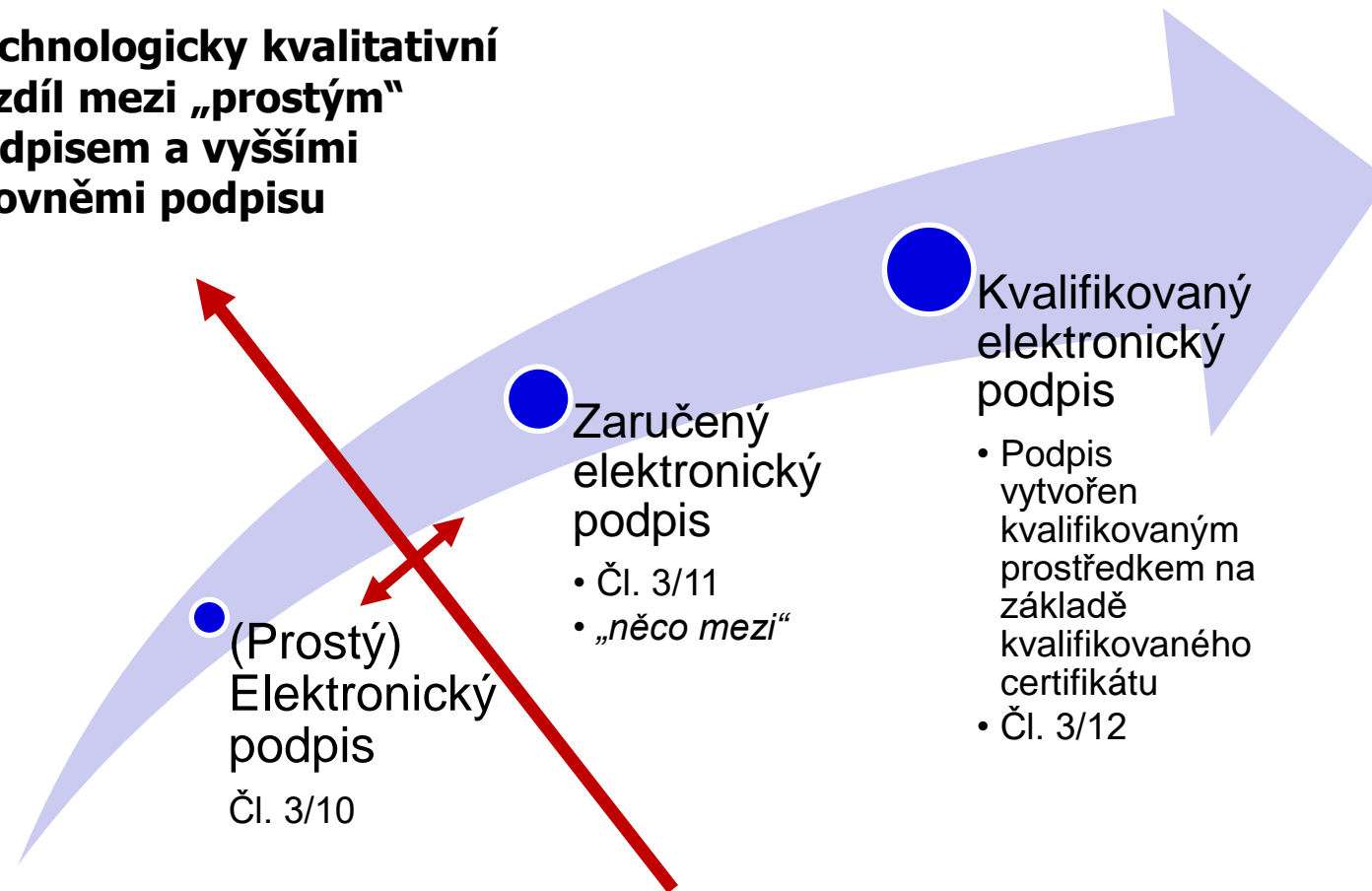
1. Vyjádření souhlasu
 2. Potenciálně identifikace osoby
-
3. Integrita dokumentu v případě technologicky pokročilejších služeb vytvářejících důvěru

Čl. 25 EIDAS

1. Elektronickému podpisu **nesmějí být upírány právní účinky** a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.
2. **Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.**
3. Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě **se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.**

Druhy elektronických podpisů dle eIDAS

Technologicky kvalitativní
rozdíl mezi „prostým“
podpisem a vyššími
úrovněmi podpisu



Právně má každá úroveň
odlišnou důkazní spolehlivost

Druhy elektronických podpisů dle eIDAS

„Prostý“ elektronický podpis

- cokoli, co nějakým způsobem identifikuje subjekt a je připojeno k jiným datům

Zaručený elektronický podpis

- je založen na certifikátu, ale na ten nejsou kladeny žádné požadavky – může jít i o testovací certifikát (ten může obsahovat jakoukoli informaci)

Kvalifikovaný elektronický podpis

- musí být založen na kvalifikovaném certifikátu pro elektronický podpis a musí být vytvořen pomocí kvalifikovaného prostředku pro vytváření elektronických podpisů (např. čipové karty – eID, tokeny, remote sign)

Uznávaný elektronický podpis jako legislativní zkratka

- Dle § 6 ZSVD: „(i) zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo (ii) kvalifikovaný elektronický podpis“

Příklady druhů elektronického podpisu dle eIDAS

– „prostý“ elektronický podpis

JUDr. Pavel Loutocký, Ph.D., BA (Hons)
Masarykova univerzita / Masaryk University



- Dle OZ navíc úvahy nad „prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby“ – osoba může být určena i jinak než podpisem – úmysl zákonodárce? (IP adresa? hash identifikátor? ...)

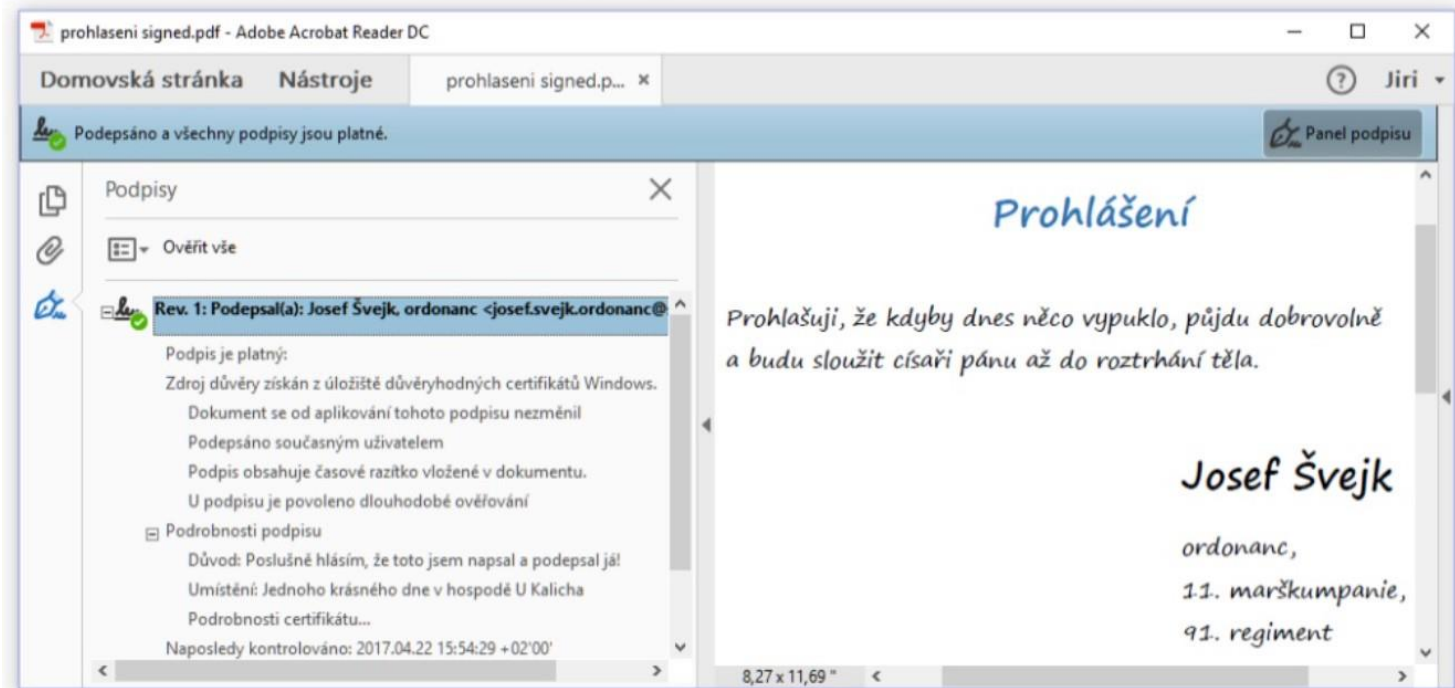
Zaručený elektronický podpis – čl. 26

- Zaručený elektronický podpis musí splňovat tyto požadavky:
 - a) je jednoznačně spojen s podepisující osobou;
 - b) umožňuje identifikaci podepisující osoby;
 - c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a
 - d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Příklady druhů elektronického podpisu dle eIDAS

– zaručený
elektronický
podpis

příklad zaručeného el. podpisu



- **pozor: zaručený el. podpis nezaručuje identitu podepsané osoby !!!**
 - formou zaručeného elektronického podpisu se lze (velmi snadno) podepsat za kohokoli jiného
 - zaručený podpis může „patřit“ i někomu, kdo vůbec neexistuje (jako fyzická osoba)
- zaručuje pouze neměnnost (integritu) toho, co je podepsáno

Kvalifikovaný elektronický podpis

- Kvalifikovaný (eIDAS) = uznávaný (starý zákon o el. podpisu)
- Čl. 28 a násl. nařízení eIDAS
 - Kvalifikované certifikáty
 - Požadavky kladené na certifikáty
 - Certifikace a postupy
 - Zveřejnění seznamu certifikačních prostředků
 - Požadavky na ověřování certifikátu
 - kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů
 - kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů

Kvalifikovaný elektronický podpis (dle čl. 3 eIDAS)

- „**kvalifikovaným elektronickým podpisem**“ zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy;
- „**kvalifikovaným certifikátem pro elektronický podpis**“ certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v **příloze I**
- „**kvalifikovaným prostředkem pro vytváření elektronických podpisů**“ prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v **příloze II**

Kvalifikovaný elektronický podpis – Příloha I

Kvalifikované certifikáty pro elektronické podpisy obsahují:

- a) označení, ..., že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis;**
- b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru...;**
- c) alespoň jméno podepisující osoby nebo pseudonym. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;**
- d) data pro ověřování platnosti elektronických podpisů...;**
- e) označení začátku a konce doby platnosti certifikátu;**
- f) identifikační číslo certifikátu;**
- g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;**
- h) údaj o místě, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g)**
- i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu;**
- j) ...**

Kvalifikovaný elektronický podpis – Příloha II

1. Kvalifikované prostředky pro vytváření elektronických podpisů vhodnými technickými prostředky a postupy přinejmenším zajistí, aby:

- a) **byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů**, která byla použita při vytváření elektronického podpisu;
- b) data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu se mohla **prakticky vyskytnout pouze jednou**;
- c) bylo přiměřeně zajištěno, že data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu **nelze odvodit a že elektronický podpis je v současnosti dostupnými technickými prostředky spolehlivě chráněn proti padělání**;
- d) oprávněná podepisující osoba měla možnost data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu **spolehlivě chránit před jejich zneužitím třetí osobou**.

2. Kvalifikované prostředky pro vytváření elektronických podpisů **nesmějí měnit podepisovaná data** ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním.

3. Data pro vytváření elektronických podpisů **může jménem podepisující osoby vytvářet nebo spravovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru**.

Kvalifikovaný elektronický podpis – Příloha II

Seznam vydávaných kvalifikovaných poskytovatelů, prostředků (apod.) v České republice:

<https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/>



Kvalifikovaný elektronický podpis

Remote sign? – serverová řešení, mobilní řešení

eIDAS:

Bod odůvodnění 51) *Podepisující osoba by měla mít možnost svěřit kvalifikované prostředky pro vytváření elektronických podpisů do péče třetí straně, pokud jsou zavedeny odpovídající mechanismy a postupy, které zajišťují, že podepisující osoba má výhradní kontrolu nad používáním svých dat pro vytváření elektronických podpisů, a použitím tohoto prostředku jsou splněny požadavky na kvalifikovaný elektronický podpis.*

Bod odůvodnění 52) *Vytváření elektronického podpisu na dálku, jehož prostředí spravuje poskytovatel služeb vytvářejících důvěru jménem podepisující osoby, přináší mnohé ekonomické výhody, a bude tedy pravděpodobně stále častější. Aby však bylo zajištěno, že tyto elektronické podpisy budou z právního hlediska uznávány stejně jako elektronické podpisy, které jsou vytvářeny v prostředí spravovaném výlučně uživatelem, měli by poskytovatelé nabízející služby elektronického podpisu na dálku uplatňovat zvláštní postupy pro zajištění bezpečnosti v oblasti řízení a správy a používat důvěryhodné systémy a produkty zahrnující zabezpečené kanály pro elektronickou komunikaci, a zajistit tak spolehlivost prostředí, v němž jsou elektronické podpisy vytvářeny, a zaručit, že je toto prostředí používáno pod výlučnou kontrolou podepisující osoby. V případě kvalifikovaného elektronického podpisu vytvořeného pomocí prostředku pro vytváření elektronických podpisů na dálku by se měly použít požadavky stanovené v tomto nařízení, které jsou použitelné na kvalifikované poskytovatele služeb vytvářejících důvěru.*

Kvalifikovaný elektronický podpis

eIDAS 2.0:

Čl. 3/23a: ‚kvalifikovaným prostředkem pro vytváření elektronických podpisů na dálku‘ kvalifikovaný prostředek pro vytváření elektronických podpisů, který jménem podepisující osoby v souladu s článkem 29a spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru

+

„Článek 29a

Požadavky na kvalifikovanou službu správy kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku

1. Správu kvalifikovaných prostředků pro vytváření elektronických podpisů na dálku jako kvalifikované služby provádí pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který:
 - a) vytváří nebo spravuje data pro vytváření elektronických podpisů jménem podepisující osoby;
 - b) bez ohledu na přílohu II bod 1 písm. d) kopíruje data pro vytváření elektronických podpisů pouze pro účely zálohování, jsou-li splněny tyto požadavky:
 - i) bezpečnost zkopírovaných souborů dat je na stejné úrovni jako u původních souborů dat;
 - ii) počet zkopírovaných souborů dat nesmí přesáhnout minimum potřebné pro zajištění kontinuity služby;
 - c) splňuje všechny požadavky uvedené v certifikační zprávě konkrétního kvalifikovaného prostředku pro vytváření elektronických podpisů na dálku vydané podle článku 30.
2. Do 21. května 2025 stanoví Komise prostřednictvím prováděcích aktů seznam referenčních norem a v případě potřeby stanoví specifikace a postupy pro účely odstavce 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.“

Authority pro kvalifikované podpisy v ČR

- První certifikační autorita, a. s.
- Česká pošta, s. p.
- eIdentity a. s.

Nově:

- Komerční banka, a.s. (6/2023)
- Správa státních služeb vytvářejících důvěru (11/2023) - příspěvková organizace DIA
- Informace o certifikovaných subjektech a nástrojích: <https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/>

MUNI
LAW

Děkuji za pozornost.

Nějaké otázky?

loutocky@muni.cz

Další zajímavé odkazy ohledně certifikátu

- rozcestník DIA: <https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/>
- eIDAS Dashboard: <https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home>
- seznam prostředků elektronické identifikace: <https://info.identitaobcana.cz/KvalifikovaniSpravci.aspx>