

FAQ eIDAS

1 OBECNĚ

1.1 Co znamená "eIDAS"?

Jedná se o obecně používanou zkratku pro nařízení Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu. Nařízení eIDAS nahrazuje směrnici 1999/93/ES a stanovuje, mimo jiné, právní rámec pro elektronické podpisy, elektronické pečeti, elektronická časová razítka, elektronické dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek. Vzhledem k neutuchajícímu tempu technologického vývoje je Nařízení koncipováno jako technologicky neutrální a otevřené inovacím.

K tomu nařízení eIDAS zavádí dvě základní oblasti elektronických nástrojů:

1. **Systémy elektronické identifikace a autentizace** – přihlašování osob k on-line službám
2. **Služby vytvářející důvěru** – aplikace založené na elektronickém podpisu

Nařízení eIDAS v souvislosti se službami vytvářejícími důvěru zavádí do právního řádu pojmy, jejichž význam volně přibližujeme:

- **Zaručený elektronický podpis/pečeť** – vytvořen na principu asymetrického šifrování, certifikát identifikuje podepisující osobu.
- **Kvalifikovaný elektronický podpis/pečeť** – vytvořen kvalifikovaným prostředkem a je založen na kvalifikovaném certifikátu.
- **Data pro vytváření elektronických podpisů/pečetí** – soukromý klíč ve správě podepisující/pečetící osoby nebo kvalif. poskytovatele služeb.
- **Kvalifikovaný certifikát pro elektronický podpis/pečeť** – vydán kvalifikovaným poskytovatelem a splňuje požadavky dle přílohy I/III eIDAS.
- **Kvalifikovaný prostředek pro vytváření elektronických podpisů/pečetí** – certifikovaný SW nebo HW, certifikační orgán určí členský stát, Komise zveřejní na seznamu.
- **Kvalifikovaný poskytovatel služeb vytvářejících důvěru** – poskytuje alespoň jednu kvalifikovanou službu a orgán dohledu (MV ČR) ji udělil status kvalifikovaný.

Nařízení eIDAS umožňuje kvalifikovaným poskytovatelům zavést a provozovat zcela nové, v praxi dosud neexistující služby. Nově definované služby nařízením eIDAS

- **Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů** – ověřování elektronických podpisů a pečetí na dálku u kvalifikovaného poskytovatele
- **Kvalifikovaná služba uchování elektronických podpisů** – zajistí důvěryhodnost kvalifikovaných elektronických podpisů/pečetí i po uplynutí doby technické platnosti
- **Služba správy dat pro vytváření kvalifikovaných elektronických podpisů a vytváření kvalifikovaných elektronických podpisů jménem podepisující osoby** – správa soukromých klíčů podepisujících osob a vytváření kvalifikovaných elektronických podpisů/pečetí na dálku u kvalifikovaných poskytovatelů

- **Kvalifikovaná služba elektronického doporučeného doručování** – odesílání a přijímání zabezpečeno zaručeným podpisem/pečetí a časovým razítkem

1.2 Jaké novinky podepisování nabízí modul eIDAS?

Mezi hlavní novinky patří:

- rozšířené možnosti ověřování
 - podpora všech požadovaných formátů podpisu – PAdES pro PDF dokumenty, XAdES pro XML dokumenty, CAdES pro binární dokumenty, ASiC pro kontejner datové zprávy
 - podpora všech úrovní – B (podpis), T (B + časové razítko), LT (T + data pro ověření), LTA (LT + archivní časové razítko)
 - rozpoznání nových typů autentizačních prvků - kvalifikovaného el. podpisu, kvalifikované a zaručené el. pečeti
 - možnost ověřování vůči OCSP
 - využívání nových seznamů důvěryhodných certifikátů
 - rozšiřitelnost o integraci s externími nástroji ověřování nebo s kvalifikovanými službami
- rozšířené možnosti podepisování
 - obecná podpora bezpečných prostředků pro vytváření el. podpisů/pečetí
 - rozšiřitelnost o viditelný podpis

1.3 Co je kvalifikovaný podpis?

Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu. Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

Technicky to je zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvořený pomocí kvalifikovaného prostředku. Použití kvalifikovaného certifikátů naplňuje požadavky na jednoznačné spojení s podepisující osobou a umožňuje identifikaci podepisující osoby. Při jeho vydání je ověřována totožnost a vydání je vázáno smlouvou. Kvalifikovaný poskytovatel musí vést evidenci dokumentů k vydávání kvalifikovaného certifikátu. Použití kvalifikovaného prostředku je naplněn požadavek na zabezpečení dat pro vytvoření el. podpisu, které má podepisující osoba pod svou výhradní kontrolou. Použití referenčního formátu elektronického podpisu pak naplňuje požadavek vytvoření podpisu takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

1.4 Co potřebuji pro vytvoření kvalifikovaného el. podpisu ?

Pro vytvoření kvalifikovaného elektronického podpisu potřebuji:

- kvalifikovaný certifikát pro elektronické podpisy vydaný kvalifikovaným poskytovatelem
- kvalifikovaný prostředek pro vytváření podpisu, ve kterém je bezpečně umístěn kvalifikovaný certifikát
- nástroj (aplikaci) pro vytvoření elektronického podpisu, který umí využít kvalifikovaný prostředek (vlastní podepisování zpravidla probíhá na kvalifikovaném prostředku)

1.5 Co je kvalifikovaná elektronická pečeť?

Elektronické pečete slouží jako důkaz toho, že elektronický dokument vydala určitá právnická osoba, a poskytují jistotu o původu a integritě dokumentu. Kvalifikovanou elektronickou pečeti rozumíme zaručenou elektronickou pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.

1.6 Co potřebuji pro vytvoření kvalifikované el. pečeti ?

Pro vytvoření kvalifikované elektronické pečeti potřebuji:

- kvalifikovaný certifikát pro elektronické pečeti vydaný kvalifikovaným poskytovatelem
- kvalifikovaný prostředek pro vytváření pečeti, ve kterém je bezpečně umístěn kvalifikovaný certifikát
- nástroj (aplikaci) pro vytvoření elektronického podpisu, který umí využít kvalifikovaný prostředek (vlastní podepisování zpravidla probíhá na kvalifikovaném prostředku)

1.7 Jaký je rozdíl mezi elektronickým podpisem, značkou a pečetí?

Hlavní rozdíl spočívá v právním významu použitého instrumentu a s ním spojeného použití. Pro každý instrument pak potřebuji jiný druh certifikátu. Srovnání jednotlivých instrumentů je uvedeno v následující tabulce:

	Podpis	Značka	Pečeť
Právní dosah	Použitelný ve všech členských státech EU.	Ryze český institut.	Použitelná ve všech členských státech EU.
Použití	Podpisující osobou je fyzická osoba.	Označující osobou může být fyzická i právnická osoba.	Pečetící osobou je pouze právnická osoba.
Právní význam	Projev vůle. Kvalifikovaný podpis má stejné právní účinky jako podpis vlastnoruční.	Označení je projevem vůle. Bez přímého ověření obsahu. Je spojena s označující osobou a umožňuje její jednoznačnou identifikaci a zjistit jakoukoli následnou změnu dat.	Není spojena s vyjádřením vůle pečetící osoby. Platí domněnka integrity a správnosti původu dat spojených s pečetí.
Zaručený/ zaručená	Založen na kvalifikovaném podpisovém certifikátu	Uznávaná značka je založena na kvalifikovaném systémovém certifikátu.	Založena na certifikátu nebo kvalifikovaném certifikátu pro el. pečeť.
Kvalifikovaný/ kvalifikovaná	Založen na kvalifikovaném certifikátu pro el. podpis a vytvořen kvalifikovaným prostředkem.	-	Založena na kvalifikovaném certifikátu pro el. pečeť a vytvořen kvalifikovaným prostředkem.

1.8 Nahrazuje modul eIDAS modul Elektronický podpis?

Nenahrazuje, doplňuje jej o možnost používat kvalifikované prostředky pro vytváření podpisů a pečeti.

1.9 Bude po vydání modulu eIDAS i nadále podporován Modul Elektronický podpis?

Ano, bude. Avšak doporučujeme pořízení modulu eIDAS popř. jiné řešení pokrývající potřeby ověřování a podepisování kvalifikovaným elektronickým podpisem nebo pečeti.

1.10 Bude podepisování pomocí modulu El. podpis splňovat nadále legislativní normy?

Stávající modul El. podpisu podporuje uznávané podpisy a značky definované podle zákona č. 227/2000 Sb. Po dobu přechodného období dvou let bude možné tyto podpisy a značky používat. Modul však nerozezná zaručený podpis založený na kvalifikovaném certifikátu od kvalifikovaného podpisu. Taktéž není schopen rozeznat pečeť. Pro ověřování kvalifikovaného podpisu, pečeti nebo kvalifikované pečeti a vytváření kvalifikovaného podpisu/pečeti doporučujeme pořízení modulu eIDAS.

1.11 Budu moci podepsat novým el.podpisem dle eIDAS i bez modulu?

Ano, pokud použijete jiný nástroj pro vytvoření elektronického podpisu. Podepsaný soubor pak můžete připojit k dokumentu ve spisové službě.

1.12 Co se stane, když nenaimplementuji modul eIDAS?

Pokud nenaimplementujete modul eIDAS neověříte, zda:

- byl použit kvalifikovaný podpis
- byla použita pečeť nebo kvalifikovaná pečeť
- dokument je podepsán správným formátem el. podpisu

Podpora seznamu důvěryhodných certifikátů - dočasně stávající způsob správy v ICZ; je nutné přejít na získávání údajů přímo z nových důvěryhodných seznamů.

Bez rozšíření o modul eIDAS nezískáte podporu kvalifikovaných prostředků pro vytváření elektronických podpisů/pečetí na kterých je uložen soukromý klíč (smart card, HSM nebo jiným).

2 TECHNICKY

2.1 Jaké jsou HW / SW požadavky na nový modul?

Podmínkou je splnění HW/SW nároků pro verzi 2.30 a součinnosti, které jsou zveřejněny na supportních stránkách e-spis.

2.2 Kam mám nahrát elektronickou pečeť?

Vlodek – Pečeť se vytváří na základě certifikátu nebo kvalifikovaného certifikátu pro elektronickou pečeť vydaným kvalifikovaným poskytovatelem služeb. Po přechodnou dobu bude certifikát uložen místo kvalifikovaného systémového certifikátu pro značku. V budoucnu by měl být uložen v kvalifikovaném prostředí.

3 DŮVODY K ZAKOUPENÍ

3.1 Co jako zákazník získám, pokud si pořídím modul eIDAS?

Získáte možnost vytvářet kvalifikovaný el podpis a pečeť a ověřovat je v souladu s nařízením eIDAS.

3.2 Proč bych jako zákazník měl chtít modul eIDAS?

Abyste úkony spojené s vytvářením kvalifikovaných el. podpisů, razítek, pečeti a jejich validaci prováděli automatizovaně v prostředí spisové služby ICZ e-spis.

3.3 Proč bychom si měli objednat / zakoupit nový modul eIDAS, pokud je to víceméně jen upgrade Modulu El. podpisu a platíme si to v maintenance?

Není součástí maintenance.

4 POROVNÁNÍ MODULŮ

4.1 Co „umí“ moduly Elektronický podpis a eIDAS? Srovnávací tabulka!

V souvislosti se zavedením eIDAS se vás změny dotknou pouze v případě, že ve správě spisovny používáte službu přerazítkování dokumentů časovým razítkem.

Pokud využíváte přerazítkování časovým razítkem:

- Do doby vypršení platnosti časového razítka není nutné nic měnit
 - o Ověřování platnosti časového razítka bude probíhat vůči vydávající autoritě,
 - o Podepisování bude probíhat stávajícím časovým razítkem a elektronickou značkou/podpisem podle původních nastavení.
- Současně s instalací nové verze ICZ e-spis a komponenty pro ověřování bude instalována nová verze správy spisovny, která umožní pro ověřování/podepisování využít nových prostředků dle nařízení eIDAS.

4.1.1 Rozdíly v ověřování

	modul Elektronický podpis	modul eIDAS (nový)
Zaručený podpis na QC	✓	✓
Značka	✓	✓ (dočasně)
Kvalifikovaný podpis	✘	✓
Kvalifikovaná pečeť	✘	✓
Časové razítko	✓	✓
Úroveň podpisu	B, T	B, T, LT, LTA
Podporovaný formát	SMIME (email), PAdES, CAdES (Datová zpráva)	PAdES, CAdES, XAdES, ASiC; SMIME (email)
Podpora důvěryhodných seznamů	✘ (nyní dočasně udržováno)	✓
Využívání OCSP	✘	připravujeme

4.1.2 Rozdíly v podepisování

	Modul Elektronický podpis	Modul eIDAS (nový)
Zaručený podpis na QC	✓	✓
Uznávaná značka	✓	✓ (dočasně)
Kvalifikovaný podpis	✗ (MSCAPI)	✓ (MSPCAPI, PKCS#11*)
Vizuální podpis	✗	✓ (modul)
Kvalifikovaná pečeť	✗ (MSCAPI)	✓ (MSPCAPI, PKCS#11*)
Časové razítko	✓	✓
Úroveň podpisu	B, T	B, T
Podporovaný formát	PADES, SMIME (email)	SMIME, PADES, XAdES (spisovna)
Podpora důvěryhodnosti dle eIDAS	✗	Podpora LT, LTA pro PADES, XAdES

4.2 Umožní mi současný modul El. podpis ověřovat podpisy vydané zahraničními poskytovateli?

Podpora seznamu důvěryhodných certifikátů - dočasně stávající způsob správy v ICZ; je nutné přejít na získávání údajů přímo z nových důvěryhodných seznamů.

4.3 Umožní mi nový modul větší zastupitelnost v rámci organizace?

Ne. Naopak zpřísňují se podmínky podepisování o používání bezpečných prostředků, které by se neměly dostat z rukou držitele certifikátu, hlavně soukromého klíče.

5 UŽIVATELSKY

5.1 Musím mít nastavenou revalidaci (tedy přerazítkování před vypršením certifikátu)?

V současné době to povinností není. Na druhou stranu pro zajištění digitální kontinuity a tím udržení věrohodnosti dokumentu je vhodné provádět přerazítkování. Zde doporučujeme nasazení modulu eIDAS, který je schopen prodlužovat elektronické podpisy dokumentů, dle současných standardů.

5.2 Musím razítkovat všechny PDF už při podpisu?

Vždy je vhodné spojit podpis přímo s věrohodným údajem o čase a předejít případnému sporu o čase podpisu a též nebezpečí uplynutí platnosti podpisového certifikátu před tím než bude opatřen podepsaný dokument časovým razítkem.

5.3 Jak se espis bude stavět k emailum podepsaným již dle nového nařízení, pokud nebudu mít modul?

Ačkoli se nejedná o podporovaný formát podpisu, budou emailové zprávy ověřovány i nadále.

5.4 Postačuje mi pro stávající činnosti modul Elektronický podpis?

Po přechodnou dobu dvou let bude možné nadále používat zaručený elektronický podpis a zaručenou elektronickou značku založené na kvalifikovaném certifikátu (uznávaný el. podpis/značka). Nicméně v průběhu tohoto přechodného období bude nutné zavést kvalifikované prostředky pro vytváření kvalifikovaného elektronického podpisu, pečeti a časového razítka tak, jak je upravuje eIDAS.

V současné době spisová služba umožňuje vytvářet uznávaný elektronický podpis a uznávanou elektronickou značku dle zákona č. 227/2000 Sb. Na klientské straně se vytváří na základě soukromého klíče certifikátu uloženého buď v úložišti certifikátů OS Windows, nebo v souborovém systému.

Modul eIDAS je rozšířen o podporu nástrojů pro vytváření elektronických podpisů, jejichž soukromý klíč je uložen na kvalifikovaném prostředku (smart card, HSM nebo jiným).