



AUTOMATICKÝ, AUTOMATIZOVANÝ, DIGITÁLNÍ A ELEKTRONICKÝ – klíčové pojmy a jejich správná interpretace

Standardy **GS1** jsou historicky propojeny s technologickým vývojem. S rostoucí digitalizací se mění nejen jejich využití, ale i jazyk, kterým o nich mluvíme. Tato příručka pomáhá porozumět klíčovým pojmům, které se často zaměňují nebo nesprávně interpretují, což může být v praxi velmi matoucí. Jaký je tedy rozdíl mezi pojmy **automatizovaný**, **automatický**, **elektronický** či **digitální**?



PROČ JE DŮLEŽITÉ ROZLIŠOVAT POJMY

V praxi – a bohužel i v legislativě – se pojmy jako **elektronický**, **digitální** nebo **automatizovaný** či **automatický** velmi často zaměňují. Tyto nepřesnosti mohou vést k nedorozuměním, neefektivní komunikaci mezi systémy a v krajním případě i k právním komplikacím. Správné pochopení těchto termínů je klíčové, pokud chceme například:

- správně implementovat **GS1 standardy**,
- připravit firmu na **digitální pasy výrobků**,
- efektivně využívat **elektronickou výměnu dat (EDI)**,
- zajistit **soulad s právními předpisy**, například s evropským nařízením eIDAS.

AUTOMATIZOVANÝ VS. AUTOMATICKÝ – NENÍ TO TOTÉŽ

V běžné komunikaci se často zaměňují pojmy „automatizovaný“ a „automatický“, přestože označují

rozdílné typy procesů. Tento rozdíl je zásadní – zejména při zavádění technologií, kde může nesprávné pochopení vést k nedorozuměním nebo chybným rozhodnutím.

AUTOMATIZOVANÝ SYSTÉM

Jedná se o proces, který probíhá opakovaně bez nutnosti lidského zásahu a řídí se předem definovanými pravidly. Typickým příkladem je automatizovaný sklad, kde se zboží pohybuje podle nastavené logiky a systém sám rozhoduje o jeho umístění či přesunu.

AUTOMATICKÝ PROCES

Naopak automatický proces je jednorázová činnost, která se spustí bez ručního zásahu, ale nevyužívá složitější logiku nebo integraci.

Příkladem může být například známé automatické otevření dveří. Ty velmi dobře reagují na pohyb, ale následně neprovádějí žádné další rozhodování. Jednoduše se otevrou a posléze opět zavrou.

ELEKTRONICKÝ VS. DIGITÁLNÍ – PODOBNÝ, NIKOLI STEJNÝ VÝZNAM

V digitálním světě se často setkáváme s dalšími dvěma pojmy, které mohou být matoucí či zavádějící. Jsou jimi výrazy elektronický a digitální. Přestože spolu úzce souvisejí, označují odlišné aspekty práce s daty a jejich správné rozlišení je důležité nejen v oblasti technické, ale také právní.

ELEKTRONICKÝ

Pojem elektronický se vztahuje k formě přenosu nebo uchování dat. Typickým příkladem je elektronická faktura, která je zasílána jako e-mail, strukturovaná zpráva nebo doklad podaný prostřednictvím datové schránky.

Elektronický dokument je právně uznávaný, pokud splňuje zákonem stanovené náležitosti.

DIGITÁLNÍ

Pojem digitální označuje obsah a způsob kódování dat – tedy to, jak jsou informace technicky zapsány. Příkladem může být QR kód vytištěný na papíře, který obsahuje digitálně zakódovaná data, i když není elektronicky přenášen.

Digitální dokument nebo faktura není právně ukotvený pojem, i když může být technickým základem elektronického dokumentu.

CO JE DOBRÉ VĚDĚT?

Elektronický dokument je téměř vždy digitální, ale digitální záznam nemusí být elektronický. Správné rozlišení těchto pojmů je klíčové pro právní platnost dokumentů i pro efektivní digitální komunikaci.

ELEKTRONICKÝ PODPIS – ZÁKLADNÍ TYPY A JEJICH VYUŽITÍ

Elektronický podpis je nástroj, který slouží k **ověření identity podepisující osoby** a k zajištění integrity dokumentu – tedy jakési potvrzení, že jeho obsah nebyl po jeho podepsání změněn. V praxi existují tři základní typy elektronických podpisů, které se liší úrovní zabezpečení i právní silou.

PROSTÝ ELEKTRONICKÝ PODPIS

Tento typ podpisu je nejjednodušší, ale také nejméně zabezpečený.

- Může jít o **naskenovaný vlastnoruční podpis**, **kliknutí na tlačítko** typu „Souhlasím“ nebo **podpis na dotykové obrazovce**.
- Vhodný je pro **běžné interní operace**, jako jsou přihlašovací formuláře nebo jednoduché obchodní souhlasy.
- **Neposkytuje žádné technické ověření identity**.

ZARUČENÝ ELEKTRONICKÝ PODPIS

Zaručený podpis již využívá **elektronický certifikát**, který ověřuje identitu podepisující osoby.

- Zajišťuje také **integritu dokumentu**, tedy záruku, že dokument nebyl po podpisu změněn.
- Tento druh podpisu se běžně používá v **obchodní komunikaci**, například při vystavování elektronických faktur.
- Je vhodný pro dokumenty, které vyžadují **vyšší důvěryhodnost**, ale ne nutně právní rovnocennost s vlastnoručním podpisem.

KVALIFIKOVANÝ ELEKTRONICKÝ PODPIS

Nejsilnější forma elektronického podpisu, která splňuje **nejpřísnější právní požadavky**.

- Vyžaduje **kvalifikovaný certifikát** a **bezpečné zařízení** (např. čipovou kartu nebo USB token).
- Je **právně rovnocenný vlastnoručnímu podpisu** a uznávaný ve všech členských státech EU.
- Používá se při **podepisování smluv, komunikaci se státní správou** nebo **úředních podáních**.

ELEKTRONICKÁ PEČEŤ – DIGITÁLNÍ RAZÍTKO ORGANIZACE

Elektronická pečeť je nástroj, který slouží k ověření původu a integrity elektronického dokumentu, podobně jako elektronický podpis. Na rozdíl od podpisu však není spojena s konkrétní osobou, ale s organizací – například firmou, bankou nebo úřadem.

Můžeme si ji představit jako digitální razítko, které potvrzuje, že dokument skutečně pochází od dané instituce a nebyl po jeho vytvoření změněn.

Stejně jako elektronický podpis se i elektronická pečeť dělí podle úrovně zabezpečení:

- **Prostá pečeť** – základní úroveň bez technického ověření.
- **Zaručená pečeť** – využívá certifikát a ověřuje původ dokumentu.

- **Kvalifikovaná pečeť** – nejvyšší úroveň, uznávaná napříč EU, vhodná pro důvěryhodnou komunikaci mezi organizacemi.

Elektronické pečeti se běžně používají při automatizovaném podepisování velkého množství dokumentů, jako jsou faktury, certifikáty nebo potvrzení. Jsou důležitým prvkem v digitální komunikaci, zejména tam, kde je potřeba garantovat důvěryhodnost bez přímého zapojení jednotlivce.

ELEKTRONICKÉ ČASOVÉ RAZÍTKO – PROČ A KDY HO POUŽÍT?

Elektronické časové razítko je důvěryhodný údaj o tom, **kdy byl dokument vytvořen nebo podepsán**. Slouží jako důkaz, že dokument existoval v určitém čase a od té doby nebyl změněn. V kombinaci s elektronickým podpisem nebo pečetí výrazně zvyšuje **právní jistotu** a **důvěryhodnost elektronických dokumentů**.

PŘÍKLADY POUŽITÍ ČASOVÉHO RAZÍTKA:

- **Podepisování smluv** – časové razítko potvrzuje, kdy byla smlouva elektronicky podepsána, což je důležité například při dodržení lhůt nebo při právních sporech.
- **Archivace elektronických faktur** – razítko zajišťuje, že faktura byla vystavena v daném čase a nebyla zpětně upravena.
- **Úřední podání** – při komunikaci se státní správou (např. daňové přiznání, žádosti) je časové razítko důkazem o včasném doručení dokumentu.
- **Certifikáty a osvědčení** – razítko potvrzuje platnost dokumentu v konkrétním okamžiku, což je důležité například u technických nebo bezpečnostních certifikátů.
- **Digitální pasy výrobků** – časové razítko může být součástí historie produktu, například při změně vlastností, aktualizaci dat nebo při reklamaci.

V některých případech je použití **kvalifikovaného elektronického časového razítka** vyžadováno zákonem – zejména u dokumentů, které mají být dlouhodobě uchovány nebo mají právní účinky.

CERTIFIKAČNÍ AUTORITY

Certifikační autorita (CA) je důvěryhodná instituce,

kteří hraje zásadní roli v oblasti elektronické bezpečnosti a asymetrické kryptografie. Jejím hlavním úkolem je ověřovat identitu subjektů (například osob, organizací nebo serverů) a na základě tohoto ověření vydávat **certifikáty pro elektronické podpisy, pečeti nebo časová razítka**. Tyto certifikáty slouží k zajištění bezpečné elektronické komunikace, k elektronickému podepisování dokumentů a k ověřování pravosti a integrity dat.

Podle evropského nařízení **eIDAS** a českého zákona č. 297/2016 Sb. rozlišujeme:

KVALIFIKOVANOU CERTIFIKAČNÍ AUTORITU

- Tato autorita musí být **akreditovaná** a **registrovaná**.
- Vydává **kvalifikované certifikáty** pro elektronický podpis, pečeť nebo časové razítko.
- Její certifikáty mají **právní účinky** jako vlastnoruční podpis.

NEKVALIFIKOVANOU CERTIFIKAČNÍ AUTORITU

- Může vydávat komerční certifikáty.
 - Nemá právní váhu kvalifikovaného podpisu, ale může být užitečná pro běžnou komunikaci.
- Důvěra v certifikát je založena na důvěře v certifikační autoritu. Pokud CA dodržuje bezpečnostní standardy a má dobré jméno, její certifikáty jsou považovány za důvěryhodné. Proto je vždy nezbytné vybírat akreditovanou certifikační autoritu.

DOPORUČENÍ PRO PRAXI

Aby digitální komunikace ve firmě fungovala spolehlivě a v souladu s právními požadavky, je důležité dodržovat několik zásad:

- **Vždy si ověřte, jaký typ podpisu nebo dokumentu je požadován legislativou.** Například elektronická faktura nebo smlouva může vyžadovat kvalifikovaný elektronický podpis, zatímco běžný souhlas v aplikaci odpovídá prostému podpisu.
- **Používejte přesné pojmy, zejména v odborných textech.** Zaměňování výrazů jako „digitální“ a „elektronický“ může vést k nedorozuměním – a v některých případech i k právní neplatnosti dokumentu.
- **Spolupracujte s akreditovanou certifikační autoritou.**
- **Využívejte GS1 standardy jako nástroj pro efektivní digitalizaci a automatizaci.** Pomáhají zajistit jednotnost, srozumitelnost a důvěryhodnost dat napříč celým dodavatelským řetězcem.

LEGISLATIVA K DANÉ PROBLEMATICE ČR/EU

EVROPSKÁ LEGISLATIVA

Nařízení eIDAS (EU) č. 910/2014

- Plný název: Nařízení o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.
- Platí **přímo ve všech členských státech EU**.
- Zavádí:
 - jednotná pravidla pro elektronické podpisy, pečeti, časová razítka, doručování a certifikáty,
 - tři úrovně elektronického podpisu: **jednoduchý, zaručený a kvalifikovaný**,
 - právní rovnost **kvalifikovaného elektronického podpisu** s vlastnoručním podpisem.

LEGISLATIVA ČESKÉ REPUBLIKY

Zákon č. 297/2016 Sb.

- Název: **Zákon o službách vytvářejících důvěru pro elektronické transakce** (nahrazuje zákon 227/2000 Sb. a nahrazen novelou zákona 297/2016 Sb.)
- Tento zákon přizpůsobuje české právo požadavkům nařízení eIDAS.
- Upravuje:
 - podmínky pro poskytování služeb důvěry (např. certifikační autority),
 - pravidla pro používání kvalifikovaných prostředků pro elektronický podpis a pečeť,
 - povinnosti subjektů veřejné správy při používání elektronických podpisů a pečeti.

Zákon č. 89/2012 Sb.

- Název: **Občanský zákoník**
- Stanovuje, že k **platnosti právního jednání** učiněného v písemné formě je třeba podpis.
- Umožňuje, aby podpis měl **elektronickou podobu**, pokud splňuje zákonné požadavky.

Zákon č. 563/1991 Sb.

- Název: **Zákon o účetnictví**
- Problematikou elektronické komunikace se zabývají **§ 31 a § 33**

§ 31 – Úschova účetních záznamů

- Elektronické záznamy lze uchovávat v **digitální formě**, pokud splňují požadavky na bezpečnost a dostupnost.
- Umožňuje **předávání účetních záznamů elektro-**

nicky státním orgánům (např. finančnímu úřadu).

§ 33 – Společná ustanovení

- Stanovuje, že elektronická komunikace je **rovnocenná** papírové formě, pokud splňuje zákonné požadavky.
- Umožňuje využití **elektronických podpisů a pečeti** pro ověřování dokumentů.

Zákon č. 235/2004 Sb.

- Název: **Zákon o dani z přidané hodnoty (DPH)**
- Problematikou o elektronické komunikaci se zabývají **§ 34 a § 35a**

§ 34 – Zajištění věrohodnosti původu, neporušenosti obsahu a čitelnosti daňových dokladů

- Stanovuje požadavky na **elektronické daňové doklady**.
- Musí být zajištěna:
 - **věrohodnost původu** (např. elektronický podpis),
 - **neporušenost obsahu**,
 - **čitelnost** po celou dobu uchování.

§ 35a – Elektronické uchovávání daňových dokladů

- Umožňuje **uchovávat daňové doklady elektronicky**, pokud jsou splněny podmínky uvedené v § 34.

Zákon č. 499/2004 Sb.

- Název: **Zákon o archivnictví a spisové službě**
- Problematikou elektronické komunikace se zabývají **§ 2, § 63 a § 65**

§ 2 – Vymezení pojmů

- **Dokumentem** se rozumí každá zaznamenaná informace, **v analogové i digitální podobě**.
- Zákon tedy výslovně uznává **elektronické dokumenty** jako rovnocenné analogovým.

§ 63 – Výkon spisové služby

- Spisová služba může být vedena **v listinné nebo elektronické podobě**.
- Elektronická podoba musí splňovat požadavky na:
 - **věrohodnost původu**,
 - **neporušenost obsahu**,
 - **čitelnost** po celou dobu uchování.

§ 65 – Uchovávání dokumentů

- Dokumenty v elektronické podobě musí být uchovávány tak, aby byla zajištěna jejich **čitelnost a autenticita**.
- Umožňuje **předávání dokumentů elektronicky** do archivů, pokud jsou splněny technické a právní podmínky.