# Elektronický podpis zpráv

## Legislativní rámec

Požadavky na podepisování zpráv pro informační systém eRecept jsou dány:

* **vyhláškou 54/2008 Sb., předepisování léčivých přípravků**
* **vyhláškou 84/2008 Sb., správná lékárenská praxe**

### Vyhláška č. 54/2008 Sb.

stanoví v § 1 odst. 3 písm. a) následující:

„(3) Pro předepisování léčivých přípravků lze také použít

1. **recept v elektronické podobě** (dále jen „elektronický recept“) zaslaný předepisujícím lékařem centrálnímu úložišti elektronických receptů6) **podepsaný uznávaným elektronickým podpisem** předepisujícího lékaře podle jiného právního předpisu7) (dále jen „elektronický podpis“)

stanoví v § 11 odst. 1 písm. a) následující:

1. **veškerá data odesílaná centrálnímu úložišti elektronických receptů jsou podepsaná elektronickým podpisem,**

a v § 11aodst. 1

1. Lékař pro přístup do registru léčivých přípravků s omezením používá stejné přístupové údaje jako pro komunikaci s centrálním úložištěm elektronických receptů. **Pro komunikaci s registrem pro léčivé přípravky s omezením se § 11 použije přiměřeně.** Registr pro léčivé přípravky s omezením obratem sdělí lékaři, zda jsou splněny podmínky pro předepsání léčivého přípravku s omezením.

### Vyhláška č. 84/2008 Sb.

stanoví v § 12 odst. 1 písm. c) následující:

(1)Recept, výpis z receptu a recept, na který se má opakovat výdej předepsaného léčivého přípravku, se při výdeji opatří

1. podpisem vydávajícího lékárníka; **v případě elektronického receptu se podpis vydávajícího lékárníka nahrazuje jeho zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu** podle zákona o elektronickém podpisu (dále jen „elektronický podpis“),

stanoví v § 17 odst. 1 písm. a) následující:

1. **veškerá data odesílaná centrálnímu úložišti elektronických receptů jsou podepsaná elektronickým podpisem,**

stanoví v §17b, odst. 1:

1. Informační systém lékárny s registrem pro léčivé přípravky s omezením komunikuje prostřednictvím softwarového komunikačního adaptéru. Elektronická komunikace mezi lékárníkem a registrem pro léčivé přípravky s omezením probíhá zabezpečeným způsobem s tím, že
   1. **veškerá data odesílaná registru pro léčivé přípravky s omezením jsou podepsaná elektronickým podpisem,**

## Podepisování zpráv

V souladu s novým nařízením eIDAS je požadavek na prostý elektronický podpis všech zpráv vykládán tak, že musí být zpráva opatřena identifikátorem odesílatele. Tím je identifikátor uživatele obsažený ve zprávě, respektive identifikátor použitý rámci mechanismu HTTP Authorization.

Požadavek na uznávaný nebo zaručený elektronický podpis založený na certifikátu se tak vztahuje pouze pro případy explicitně vyžadované vyhláškou. To jsou aktivní operace založení elektronického receptu a záznamu o výdeji a jejich změny či případně zrušení. Na použití uznávaného nebo zaručeného elektronické podpisu založeného na certifikátu se vztahují tyto požadavky:

* Podpis musí být na produkčním prostředí založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb
  + Postsignum
  + ICA
  + eIdentity
  + slovenský NBÚ
* Podpis na testovacím prostředí musí být založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb anebo na certifikátu od cacerts.org.
* Hashovací funkce pro podpis musí být typu SHA-2
* Úroveň zabezpečení certifikátu je na klientovi – způsob uložení certifikátu a privátních klíčů
  + Soubor
  + Token
  + Úložiště OS
  + Úložiště aplikace

## Výpočet hodnoty DigestValue

**Vstupní předpoklady pro úspěšné podepsání XML dokumentu:**

* XML dokument připravený pro podepsání musí být před podepsáním validní a musí obsahovat definice jmenných prostorů a jejich prefixů
* Dokument musí být v kódování utf-8
* Výpočet **DigestValue** se provádí z XML dokumentu bez Envelope obálky, pouze z XML samotné datové zprávy. XML dokument může být zaslán i JMS rozhraním bez Envelope obálky. Do budoucna by mohl být zaslán i jiným komunikačním kanálem a to beze změny jeho podepisování a na straně IS eRecept validování podpisu.
* **Výpočet** hodnoty elementu **DigestValue** se provádí z root elementu konkrétní zprávy, která obsahuje **pouze** **elementy** **Doklad a Zprava**. Element Signature nesmí být obsažen a to ani prázdný.

**Předpoklady pro úspěšné odeslání podepsaného XML dokumentu:**

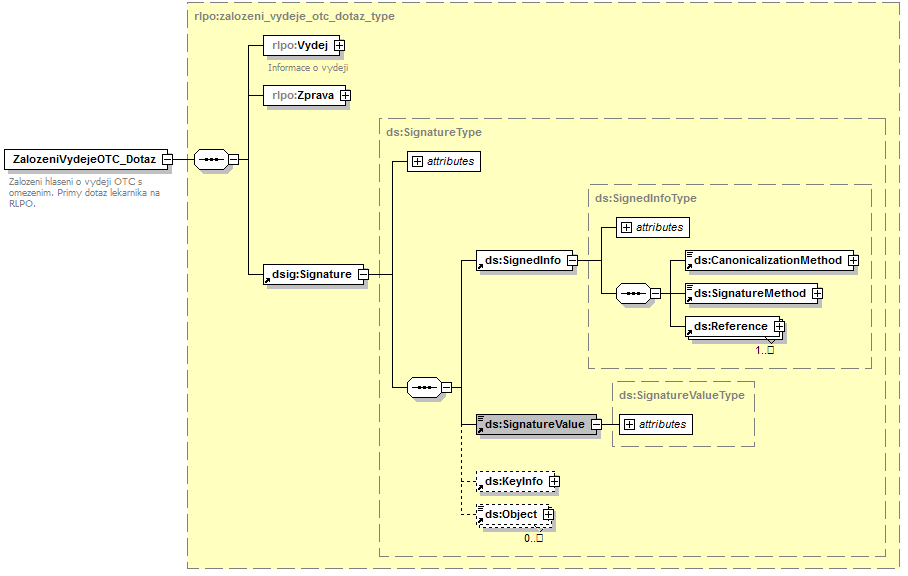
* XML dokument s podpisem nesmí být nijak přeformátován
* Nesmí být přesunuty definice jmenných prostorů např. k Envelope elementu od root elementu původního podepisovaného XML
* Nesmí být provedena žádná změna kódování češtiny
* Nesmí být proveden nic, co změní binární podobu původního podepisovaného XML

## Definice zprávy s podpisem

### Zpráva

Definice zpráv pro komunikaci lékaře a lékárníka s IS eRecept v XSD definičních souborech mají definované tři základní elementy:

* **Doklad** – obsahuje vlastní data pro komunikaci s IS eRecept
* **Zprava** – obsahuje technické informace o zaslané zprávě a času zaslání zprávy
* **Signature** – obsahuje elektronický podpis výše uvedených elementů



Obr. 1 Příklad XSD definice zprávy s podpisem

### Seznam funkcí s vyžadovaným podpisem

Přehled funkcí, které vyžadují elektronický podpis je uveden v Tab. 1.

Tab. 1 Přehled funkcí s vyžadovaným elektronickým podpisem

|  |  |  |
| --- | --- | --- |
| Funkce | Stručný popis | Aktér |
| AppPingZEP | AppPing pro test elektronického podpisu | Lékař, Lékárník |
| ZalozitPredpis | Založení elektronického předpisu | Lékař |
| ZmenitPredpis | Změna elektronického předpisu | Lékař |
| ZalozitVydej | Založení záznamu o výdeji | Lékárník |
| ZmenitVydej | Změna záznamu o výdeji | Lékárník |
| ZalozitVydejOTC | Založení záznamu o výdeji OTC s omezením | Lékárník |
| ZmenitVydejOTC | Změna záznamu o výdeji OTC s omezením | Lékárník |

### Element Signature

je definován v:

* namespace=[http://www.w3.org/2000/09/xmldsig#](http://www.w3.org/2000/09/xmldsig)
* schemaLocation=<http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd>

### Použité algoritmy

Příklady:

<dsig:**CanonicalizationMethod Algorithm**="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>

<dsig:**Transform Algorithm**="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<dsig:**DigestMethod Algorithm**="http://www.w3.org/2001/04/xmlenc#sha256"/>

<dsig:**SignatureMethod Algorithm**="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>

Seznam povolených:

**Transform Algorithm**:

<http://www.w3.org/TR/2001/REC-xml-c14n-20010315>

<http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>

<http://www.w3.org/2006/12/xml-c14n11>

<http://www.w3.org/2006/12/xml-c14n11#WithComments>

[http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n)

<http://www.w3.org/2001/10/xml-exc-c14n#WithComments>

<http://www.w3.org/2000/09/xmldsig#base64>

<http://www.w3.org/2000/09/xmldsig#enveloped-signature>

**CanonicalizationMethod Algorithm**

<http://www.w3.org/TR/2001/REC-xml-c14n-20010315>

<http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>

<http://www.w3.org/2006/12/xml-c14n11>

<http://www.w3.org/2006/12/xml-c14n11#WithComments>

[http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n)

<http://www.w3.org/2001/10/xml-exc-c14n#WithComments>

**DigestMethod Algorithm:**

<http://www.w3.org/2001/04/xmlenc#sha256>  
<http://www.w3.org/2001/04/xmlenc#sha512>

**SignatureMethod:**

<http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>

[http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256](http://tools.ietf.org/html/rfc6931)

[http://www.w3.org/2001/04/xmldsig-more#rsa-sha512](http://tools.ietf.org/html/rfc6931)

[http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512](http://tools.ietf.org/html/rfc6931)

<http://www.w3.org/2009/xmldsig11#dsa-sha256>

### Certifikát

Spolu s podpisem musí být zaslán certifikát uložený v elementu **X509Certificate.**