НАРОДНА БАНКА СРБИЈЕ

У П У Т С Т В О

О БЛИЖИМ ТЕХНИЧКИМ УСЛОВИМА И НАЧИНУ ЕЛЕКТРОНСКОГ ПОТПИСА XML ДОКУМЕНАТА КОЈИ СЕ ДОСТАВЉАЈУ НБС

ВЕРЗИЈА 1.6

23. Мај 2023. године

Упутство је израђено на основу Одлуке о електронском потписивању докумената с подацима које банке достављају Народној банци Србије, ''Службени гласник РС'', бр. 28/2009 (на страни 77 под редним бројем 1090), објављеном на дан 24.април 2009.године, и на основу Упутства о допуни Упутства о формату и намени електронских порука којима друштва за осигурање достављају НБС статистичке и друге податке од 16.04.2009.године , и на основу Упутства о допуни Упутства о подацима које кастоди банке електронски достављају НБС од 16.04.2009.године, и на основу Упутства о допуни Упутства о електронском достављању НБС месечних извештаја друштава за управљање добровољним пензијским фондовима од 16.04.2009.године 2009.године.

1 ЕЛЕКТРОНСКИ ПОТПИС

1.1 Увод

Електронски потпис за XML документ је дефинисан у препоруци XML Dsig (у даљем тексту препорука) W3 конзорцијума (http://www.w3.org/)
Препорука дефинише XML синтаксу и правила за креирање електронског потписа.
У оквиру препоруке су дефинисани:

- који алгоритам за креирање електронског потписа се користи
- који алгоритам се користи за израчунавање hash вредности ili message digest-a
- који алгоритам се користи за трансформацију документа у канонички облик
- структура електронског потписа
- врсте електронског потписа
- обавезни и опциони елементи структуре електронског потписа

Детаљна спецификација електронског потписа за XML документе може се погледати на адреси http://www.w3.org/TR/xmldsig-core/

1.2 Општа структура

Општи изглед ове структуре са свим обавезним и опционим елементима је приказан испод:

```
<Signature>
  <SignedInfo>
    <SignatureMethod />
    <CanonicalizationMethod />
    <Reference>
      <Transforms>
      <DigestMethod>
      <DigestValue>
    </Reference>
    <Reference /> etc.
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```


Препорука XML Dsig дозвољава употребу у три врсте електронског потписа:

- Enveloping signature
- Enveloped signature
- Detached signature

Од ове три врсте користи се ***Enveloped signature***.

Употребом ове врсте потписа обезбедили смо да структура постојећих XML докумената који постоје у досадашњој размени података између Народне банке Србије и пословних субјеката остане непромењена. Структура електронског потписа се додаје на крају документа и садржана је у самом XML документу.

1.3 Структура електронског потписа (*Enveloped signature*)

Структура електронског потписа XML документа у електронској размени података је приказан испод:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
   <SignedInfo>
     <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-
xml-c14n-20010315" />
     <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">
      <Transforms>
      <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </Transforms>
      <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

      <DigestValue>ClhQZ8H0lh1chKd22zQas6eCW9Y=</DigestValue>
      </Reference>
   </SignedInfo>


<SignatureValue>IaF1Dy77OiJJa0VOOxCamp4g8YRd4x2Ei...</SignatureValue>
   <KeyInfo>
   <X509Data>
       <X509Certificate>MIIG1jCCBb6gAwIBAgIESK....</X509Certificate>
    </X509Data>
  </KeyInfo>
</Signature>
```

1.4 Услови валидности XML документа са електронским потписом

Електронски сертификат потписника **мора бити квалификовани сертификат** издат од регистрованог сертификационог тела (CA) у Србији.

Субјекат у електронској размени података у XML формату мора доставити списак серијских бројева електронских сертификата чији ће приватни криптографски кључеви бити употребљивани за потписивање XML докумената који се шаљу Народној банци Србије

Списак серијских бројева сертификата ће се достављати путем посебно креираног XML документа.

Електронски потписан XML документ са становишта електронског потписа ће бити потпуно валидан и прихваћен уколико су испуњени следећи услови:

- XML документ је синтаксно валидан и исправан
- XML документ је електронски потписан и садржи припадајући квалификовани електронски сертификат са јавним кључем (у оквиру *X509Certificate* елемената)
- серијски број сертификата је пријављен код НБС као валидан за коришћење у размени података
- синтакса XML електронског потписа је креирана према датој спецификацији
- електронски потпис је валидан
- електронски сертификат је валидан (ово укључује проверу повучености сертификата временске валидности, провера сертификационог ланца, проверу издаваоца сертификата, …)

1.5 Апликација за израду квалификованог електронског потписа

Апликација за израду квалификованог електронског потписа треба да омогући креирање квалификованог електронског потписа само кориснику који поседује квалификовани електронски сертификат. Ово укључује проверу самог сертификата потписника у сврху утврђивања да ли је сертификат квалификован сертификат издат од регистрованог сертификационог тела у Србији.

1.6 Пример потписаног XML документа DR310109_01_99999999.xml

```
<?xml version="1.0" encoding="WINDOWS-1250"?>
<ZaSlanje>
        <Dokument>
                <DatumStanja>31.01.2009</DatumStanja>
                <Obrazac>DR</Obrazac>
                <MaticniBroj>99999999</MaticniBroj>
                <RedniBroj>1</RedniBroj>
                <PodatkeObradio>Petar Petrovic</PodatkeObradio>
                <Kontakt>011 1234567,email:petar.petrovic@nbs.yu</Kontakt>
                <SlogDR>
                     <SifraPodatka>1.1.</SifraPodatka>
                     <Iznos1>1288</Iznos1>
                     <Iznos2>1389</Iznos2>
                     <Iznos3>1588</Iznos3>
                     <Iznos4>1689</Iznos4>
                     <Iznos5>1788</Iznos5>
                     <Iznos6>1889</Iznos6>
                     <Iznos7>1988</Iznos7>
                     <Iznos8>1089</Iznos8>
                    <Iznos9>1089</Iznos9>
                    <Iznos10>1089</Iznos10>
                </SlogDR>
        </Dokument>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
     <Reference URI="">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>bOnJtjT8ttu+OLJQq1MSLTcfzN4=</DigestValue>
     </Reference>
 </SignedInfo>
 <SignatureValue>I4CUqGULFhXSwSFN...</SignatureValue>
 <KeyInfo>
  <X509Data>
       <X509Certificate>MIIG1jCCBb6j...X509Certificate>
  </X509Data>
 </KeyInfo>
</Signature>
</ZaSlanje>
```

1.7 Спецификација

- **CanonicalizationMethod** – **Canonical XML -** детаљна спецификација алгоритма се може наћи на адреси **http://www.w3.org/TR/2001/REC-xml-c14n-20010315**
- **SignatureMethod** – асиметрични алгоритам за креирање потписа RSA-SHA1
- **Reference** – пошто се потписује читав XML документ, референца је празна - URI="" (тзв. null URI)
- **Transform** елементе описује алгоритам трансформације **http://www.w3.org/2000/09/xmldsig#enveloped-signature**
- **DigestMethod** – алгоритам за рачунање hash-a SHA1 - **http://www.w3.org/2000/09/xmldsig#sha1**
- **DigestValue** – елеменат садржи израчунату hash вредност, приказује се у *base64* формату
- **SignatureValue** – вредност електронског потписа у *base64* формату
- **X509Certificate** у оквиру **KeyInfo** структуре садржи објекат електронског сертификата (**X509 V3**) у *base64* формату

2 CR – Пријављивање потписника електронских извештаја код НБС

Да би субјекат у електронској размени података могао да шаље податке, електронски сертификат потписника мора бити пријављен код НБС. Сертификати који могу да се користе у ове сврхе морају бити квалификовани и пријављени код НБС. НБС не прави разлику између личних и корпоративних (сертификат који је издат на име запосленог у некој институцији) сертификата.

Структура обрасца CR који служи за пријављивање сертификата код НБС је приказан испод. Овај образац мора да буде електронски потписан приватним кључем везаним за сертификат који је иницијално пријављен код НБС.

Касније се могу користити сви сертификати који су регистровани код НБС.

НАЗИВ ТАГА	САДРЖАЈ	ТИП	НАПОМЕНА
<Dokument>			
<DatumVazenja>	Датум за који достављате податке, сматра се за датум важења података, односно промене података	Date DD.MM.YYYY	Датум важења одговара датуму у називу фајла
<Obrazac>	Шифра податка	Text CC	Иста као у називу податка, дужине 2
<MaticniBroj>	Матични број банке, друштва за осигурање , друштва за управљање пензијским фондовима	Number 8N	Нумеричка вредност дужине 8
<RedniBroj>	Редни број слања података за задати датум стања	Integer NN	Редни број мора бити исти као у називу фајла
<PodatkeObradio>	Име и презиме особе која је податке обрадила	Text 240C	Текст податак дужине 240
<OdgovornoLice>	Име и презиме одговорног лица	Text 240C	Текст податак дужине 240
<Kontakt>	Телефон, факс, или и-мејл адреса одговорног лица	Text 240C	Текст податак дужине 240
Сви елементи заглавља су обавезни и стандардни су за све поруке			
SlogCR			
<SerijskiBroj>	Серијски број електронског серфитиката који се пријављује код НБС као потписник електронског извештаја за НБС	Text	Алфанумерички податак Обавезно попуњено
<Izdavalac>	Издавалац сертификата, сертификационо тело које издаје квалификовани сертификат по евиденцији у НБС;	Number N	Нумерички податак Обавезно попуњено
<Status>	Статус сертификата 1-активација (пријављивање у бази података) 0- деактивација сертификата Ако се доставља први пут, уписује се у регистар у НБС, ако већ постоји мења се само статус	Number N	Нумерички податак Обавезно попуњено
<Signature>	Синтакса XML електронског потписа мора бити креирана према датој спецификацији		Дигиталан потпис мора бити валидан Обавезно попуњено
Динамика достављања –ДНЕВНА по насталим променама			

2.1 Пример XML формата CR310109_01_99999999.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
<ZaSlanje>
  <Dokument>
  <DatumVazenja>31.01.2009</DatumVazenja>
  <Obrazac>CR</Obrazac>
  <MaticniBroj>99999999</MaticniBroj>
  <RedniBroj>01</RedniBroj>
  <PodatkeObradio>Petar Petrovic</PodatkeObradio>
  <OdgovornoLice>Petar Petrovic</OdgovornoLice>
  <Kontakt>011 44444444</Kontakt>
   <SlogCR>
     <SerijskiBroj>48AAAE98</SerijskiBroj>
     <Izdavalac>1</Izdavalac >
     <Status>1</Status>
   </SlogCR>
   <SlogCR>
     <SerijskiBroj>52BFGE98</SerijskiBroj>
     <Izdavalac>1</Izdavalac>
     <Status>0</Status>
  </SlogCR>
   <SlogCR>
     <SerijskiBroj>52ABC98</SerijskiBroj>
     <Izdavalac >1</Izdavalac>
     <Status>0</Status>
    </SlogCR>
    </Dokument>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
     <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
     20010315" />
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
   <Reference URI="">
   <Transforms>
     <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
   </Transforms>
   <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
   <DigestValue>uZyYODqrbmjhp0oI93o2ohkGByI=</DigestValue>
   </Reference>
   </SignedInfo>
 <SignatureValue>rQzJQlUga6jvaSHQytwRG8b...</SignatureValue>
 <KeyInfo>
    <X509Data>
    <X509Certificate>MIIHGDCCBgCgAwIBAgIESPyh8zA...</X509Certificate>
    </X509Data>
  </KeyInfo>
  </Signature>
  </ZaSlanje>
```

2.1 Списак издавалаца

Издавалац	Назив CA	Назив правног лица
1	Posta CA 1	Javno preduzeće "Pošta Srbije"
2	-	-
3	PKS CAClass1-Kvalifikovani sertifikati	Privredna komora Srbije
4	Halcom BG CA PL	Halcom a.d. Beograd RS
5	MUPCA Gradjani	Sertifikaciono telo MUP Republike Srbije
6	ESS IQCA1	E-Smart Systems d.o.o
7	Halcom BG CA PL 3	Halcom a.d. Beograd RS
8	Halcom BG CA PL e-signature	Halcom a.d. Beograd RS
9	Halcom BG CA FL e-signature	Halcom a.d. Beograd RS
10	Pošta Srbije CA 1	Javno preduzeće "Pošta Srbije"
11	PKS CA Class1	Privredna komora Srbije
12	MUPCA Gradjani 3	Sertifikaciono telo MUP Republike Srbije
13	MUP Gradjani CA 4	Sertifikaciono telo MUP Republike Srbije
14	MUPStranciCA4	Sertifikaciono telo MUP Republike Srbije

2.2 Поруке о грешкама које се односе на верификацију електронског потписа и сертификата

800 Greska utvrdjena parsiranjem - kontaktirajte vaseg programera
801 Digitalni potpis nije validan
802 XML dokument ne sadrzi digitalni potpis
803 XML dokument sadrzi vise od jednog digitalnog potpisa
804 Status digitalnog sertifikata je nepoznat (problemi u proveri sertifikata) - kontaktirajte NBS
805 Digitalni sertifikat je povucen
806 Digitalni sertifikat je vremenski nevalidan
807 Root sertifikat nije medju trusted sertifikatima
808 Kriptografska greska u proveri digitalnog sertifikata - kontaktirajte NBS
809 Izdavalac digitalnog sertifikata nije registrovani CA u R. Srbiji
810 Nije pronadjen digitalni sertifikat u sklopu digitalnog potpisa
811 Digitalni sertifikat nije registrovan kod NBS
812 Digitalni sertifikat je nevalidan
813 Ne postoji čitav lanac poverenja
814 Lanac poverenja nije kreiran
820 Digitalni sertifikat nije kvalifikovani sertifikat
830 Status sertifikata nije proveren
839 Dokument nije validan
840 Nedefinisana greska - pozovite NBS

* дешава се у случају кад апликација не може да провери статус сертификата у листи повучених сертификата (CRL) из различитих разлога (листа је временски невалидна, итд.)

** грешка која иницијално није детаљно обрађена

*** НБС ће интерно имати информацију о званично регистрованим сертификационим телима у Србији

Грешке које нису иницијално детаљно обрађене биће накнадно описане у поступку тестирања и продукционог окружења уколико буде долазило до таквих грешака. У интерном тестирању нисмо били у могућности да испитамо сва могућа сценарија која би доводила до свих могућих грешака. Уколико буде било потребе поруке о грешкама ће бити накнадно допуњене.