



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Verzia 1.1

Podpisové politiky pre ZEP

6. novembra 2005

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Sekcia informačnej bezpečnosti a elektronického podpisu

Budatínska č. 30, 850 07 Bratislava 57

<http://www.nbusr.sk/>

e-mail: sep@nbusr.sk

Obsah

1	Skratky	4
2	Predmet dokumentu	5
3	Spracovanie politiky pre ZEP	6
3.1	Odporúčanie procesu výberu podpisovej politiky v aplikácií pre ZEP	7
3.2	Proces overenia podpisu v aplikácií pre ZEP.....	7
4	Formáty podpisových politík	8
4.1	Prevod ASN.1 podpisových politík do politík pre podpisy vo formáte XAdES ETSI TS 101 903	8
4.2	Textový popis minimálne nutných atribútov podpisovej politiky	9
5	Špecifické podpisové politiky	11
5.1	Podpisová politika pre zaručený elektronický podpis s časovou pečiatkou, pre textové dokumenty v ASCII a v UTF8 kódovaní, pre interný alebo externý typ podpisu	11
Príloha A	Literatúra	12
Príloha B	História	13

1 Skratky

ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
EP	Elektronický podpis
ESS	Enhanced Security Services (enhances CMS)
GMT	Greenwich Mean Time
HTTP	HyperText Transfer Protocol
ISO	International Organization for Standardization
MIME	Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Provider
OID	Object Identifier
PKCS	Public Key Cryptographic Standards, Standards published by RSA, Labs.
RIPMD-160	Race Integrity Primitives Evaluation Message Digest 160
PKIX	internet X.509 Public Key Infrastructure
QC	Qualified Certificate
RSA	Rivest, Shamir and Adleman Algorithm
SHA-1	Secure Hash Algorithm 1
PP	Podpisová politika
SSCD	Secure-Signature-Creation Device
TSA	Time-Stamping Authorities
TSP	Time Stamp Protocol
TST	Time-Stamp Token
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XAdES	XML Advanced Electronic Signature
XER	XML Encoding Rules (for ASN.1)
XML	Extensible Markup Language
ZEP	Zaručený elektronický podpis (Qualified Electronic Signature)

2 Predmet dokumentu

Tento dokument je vydaný v súlade s § 4 vyhlášky NBÚ č. 537/2002 Z. z. o formáte a spôsobe vyhotovenia zaručeného elektronického podpisu, spôsobe zverejňovania verejného kľúča úradu, postupe pri overovaní a podmienkach overovania zaručeného elektronického podpisu, formáte časovej pečiatky a spôsobe jej vyhotovenia, požiadavkách na zdroj časových údajov a požiadavkách na vedenie dokumentácie časových pečiatok (o vyhotovení a overovaní elektronického podpisu a časovej pečiatky). Dokument upravuje používanie podpisových politík pri vytváraní a overovaní zaručeného elektronického podpisu podľa zákona č. 215/2002 Z. z. o elektronickom podpise. Cieľom je sprehľadniť, zjednotiť a najmä zjednodušiť proces vytvárania a overovania zaručených elektronických podpisov (ďalej len „ZEP“) pre subjekty vytvárajúce a overujúce ZEP. Dokument popisuje rámec používania podpisových politík a základnú množinu podpisových politík, ktorá sa v prípade potreby môže rozšíriť o ďalšie podpisové politiky pre zaručený elektronický podpis.

Správne overovanie zaručených elektronických podpisov a certifikačnej cesty, na základe podpisovej politiky, je kľúčovým predpokladom pre zabezpečenie kompatibility a jednotného prostredia elektronického podpisu v oblasti podpisových politík v SR, s ohľadom na prostredie elektronického podpisu najmä v krajinách EÚ.

Cieľom tohto dokumentu nebolo vytvorenie iba samostatného štandardu pre uvedenú oblasť, ale vytvorenie jednoznačného, minimálneho a záväzného profilu podpisových politík pre poskytovateľov certifikačných služieb, tvorcov aplikácií a samozrejme používateľov elektronického podpisu.

Podpisové politiky sú dostupné na webovej stránke

<http://www.nbusr.sk/sk/elektronicky-podpis/podpisove-politiky/index.html>

Použité definície vychádzajú hlavne zo štandardov v Príloha A vyhlášok a zákonov, ktorých definície dokument sumarizuje a upresňuje ich použitie.

Základné dokumenty legislatívy Slovenskej republiky pre elektronický podpis

<http://www.nbusr.sk/sk/elektronicky-podpis/legislativa/index.html>

Formáty zaručených elektronických podpisov

<http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html>

3 Spracovanie politiky pre ZEP

NBÚ schvaľuje podpisové politiky pre ZEP (ďalej len „schválená PP“). Schválené PP sú zverejnené na webovej stránke NBÚ. Každá podpisová politika pre CMS (ASN.1) podpisy je zverejnená v dvoch formátoch:

- v záväznom DER kódovaní
- v informatívnom XER kódovaní, ako transformácia z DER kódovania, s textovým popisom v slovenskom jazyku.

Schválené PP sú vydané v súlade s dokumentom „Správa podpisových politík“. V uvedenom dokumente je podrobne popísaný aj obsah zaručeného elektronického podpisu schválených PP vo formáte „archivačný podpis“, ktorý pozostáva najmä z postupnosti Hash odtlačkov DER dokumentov schválených PP a časov konca platnosti jednotlivých schválených PP (v položke *notice*, vo formáte *GeneralizedTime*). Formát „archivačného podpisu“ je definovaný v dokumente „Schválené formáty zaručených elektronických podpisov“.

Pri CMS podpisoch musí aplikácia vedieť overiť a aj používateľovi umožniť zobrazit' digitálny odtlačok Hash z časti DER kódovanej podpisovej politiky. Zobrazený odtlačok Hash sa počíta z DER kódovanej podpisovej politiky *SignaturePolicy* bez hlavičky, teda z položiek *signPolicyHashAlg* a *signPolicyInfo*. Vypočítaný Hash je aj súčasťou odkazu na podpisovú politiku, ktorý je uložený priamo v podpisovaných atribútoch CMS podpisu.

Proces kontroly:

- aplikácia pre ZEP, napríklad pri štarte, načíta a overí archivačný podpis „SchvalenePodpisovePolitiky.p7m“, z ktorého po overení získa zoznam mien súborov schválených PP, ich hashov a časov konca platnosti, dokedy sú schválené PP platné,
- podpis zoznamu schválených PP sa overuje s kvalifikovaným certifikátom, ktorý bol podpísaný priamo NBÚ koreňovým certifikátom, a v ktorom je uvedený OID: 1.3.158.36061701.0.0.1.10.5.0.1, (podrobné pravidlá a spôsob overenia podpisu schválených PP sú popísané v dokumente „Správa podpisových politík“),
- získaný zoznam Hash hodnôt schválených PP a časov konca platnosti schválených PP aplikácia neskôr použije pri overovaní, na určenie, či je overovaný podpis zaručeným EP alebo len EP, a či je overovaný elektronický podpis platný,
- pri overovaní ZEP podpisov musí byť za ZEP prehlásený len ten podpis, ktorý v sebe v podpísaných atribútoch obsahuje odkaz na podpisovú politiku (Hash) zhodnú s jednou zo schválených PP zo zoznamu schválených PP, kde zoznam bol získaný v prvom kroku a samotný overovaný podpis bol vytvorený pred časom konca platnosti schválenej PP.

3.1 Odporúčanie procesu výberu podpisovej politiky v aplikácií pre ZEP

Aplikácia pre vytváranie ZEP by mala mať *DropDown* menu, v ktorom bude zoznam podpisových politik (s textom z položky *fieldOfApplication*, z každej podpisovej politiky). Na základe výberu politiky zo zoznamu sa nastaví podpisová politika pre vytváraný podpis.

Podpisovateľ výberom podpisovej politiky určí atribúty podpisu *signerRules*, ktoré musí aplikácia pri podpise vložiť do podpisu. Súčasne výberom politiky definuje atribúty vyžadované od overovateľa *verifierRules*, ktoré overovateľ musí doplniť do podpisu, ak súhlasí s overením podpisu pod politikou, ktorú vybral podpisovateľ. Napríklad pri podpise s časovou pečiatkou nie je podpisovateľ povinný vložiť časovú pečiatku, ale ak overovateľ zistí, že nie je časová pečiatka vložená, musí ju vložiť, lebo to vyžadujú *verifierRules*.

3.2 Proces overenia podpisu v aplikácií pre ZEP

Aplikácia musí prekontrolovať podpis na základe podpisovej politiky, pod ktorou bol podpis vytvorený. Identifikátor podpisovej politiky je priamo vložený do podpisu podpisovateľom, do podpisovaných atribútov, a tak je podpisom zabezpečené jednoznačné a nepopierateľné identifikovanie vybranej podpisovej politiky. Overenie s inou politikou, než akú si zvolil podpisovateľ je neprípustné.

Aplikácia pri overení vypíše informáciu o politike, podľa ktorej overuje daný podpis. Táto informácia musí obsahovať OID, Hash a *fieldOfApplication* podpisovej politiky.

Pri overovaní podpisu na základe podpisovej politiky, musia byť splnené všetky požiadavky podpisovej politiky. Napríklad overenie interného podpisu (podpísaný dokument je priamo súčasťou DER podpisu *.p7m) s politikou, ktorá je len pre externý podpis `<externalSignedData> true </externalSignedData>`, sa označí za neplatné.

V prípade, ak nie sú splnené všetky podmienky pre overenie zaručeného elektronického podpisu (napr. formát podpísaného dokumentu, formát podpisu, kvalifikovaný certifikát a ďalšie požiadavky z podpisovej politiky ako: keď podpisová politika obsahuje ROOT certifikát, tak ROOT certifikát certifikačnej cesty sa musí zhodovať s jedným z ROOT certifikátov uvedených v podpisovej politike a pod.), musí byť takto vytvorený zaručený elektronický podpis prehlásený za neplatný. V žiadnom prípade nesmie byť preklasifikovaný na „obyčajný“ elektronický podpis, aj napriek tomu, keby splňal požiadavky, ktoré vyžaduje „obyčajný“ elektronický podpis.

Podpis musí byť prehlásený za neplatný aj v prípade, že aplikácia pri overovaní nedokáže interpretovať celú použitú podpisovú politiku.

Taktiež pri overovaní ZEP, vyhlási nemožnosť overenia podpisu v prípade, ak aplikácia nevie zobrazit' overovateľovi podpísané údaje (napríklad nevie zobrazit' „RTF“ typ dokumentu).

Pri overovaní zaručených elektronických podpisov, musí byť podpis podpisových politik platný ku času kontroly overovaného zaručeného elektronického podpisu overovaného dokumentu.

4 Formáty podpisových politík

Uvedené pravidlá podpisových politík sú hlavne pre podpisy typu CMS (v ASN.1), kde politika je kódovaná v DER. Kvôli prehľadnosti a jednoduchému zobrazeniu politiky v DER je pretransformované DER do XER kódovania.

4.1 Prevod ASN.1 podpisových politík do politík pre podpisy vo formáte XAdES ETSI TS 101 903

Pre XML podpisy ETSI XAdES TS 101 903 môžu platiť rovnaké politiky ako pre CMS podpisy, kedy sa pri spracovaní DER politiky nahradia atribúty ASN.1 za XML elementy podľa tabuľky č.19 z dokumentu „Schválené formáty zaručených elektronických podpisov“.

Ak je požadovaná špeciálna politika pre XML podpisy XAdES ETSI TS 101 903, tak dokument s XML politikou bude spracovávaný binárne a jeho Hash bude uvedený v podpísanom zozname v archivačnom podpise „SchvalenePodpisovePolitiky.p7m“.

Tabuľka 1. Základné algoritmy a atribúty ASN.1 a ich OID

	ASN.1 atribút	OID
1.	id-contentType	1 2 840 113549 1 9 3
2.	id-messageDigest	1 2 840 113549 1 9 4
3.	id-signingTime	1 2 840 113549 1 9 5
4.	Id-aa-ets-otherSigCert	1 2 840 113549 1 9 16 2 19
5.	id-aa-signingCertificate	1 2 840 113549 1 9 16 2 12
6.	id-aa-ets-sigPolicyId	1 2 840 113549 1 9 16 2 15
7.	id-aa-signatureTimeStampToken	1 2 840 113549 1 9 16 2 14
8.	id-aa-ets-certificateRefs	1 2 840 113549 1 9 16 2 21
9.	id-aa-ets-revocationRefs	1 2 840 113549 1 9 16 2 22
10.	id-aa-ets-escTimeStamp	1 2 840 113549 1 9 16 2 25
11.	id-aa-ets-certCRLTimestam	1 2 840 113549 1 9 16 2 26
12.	id-aa-ets-certValues	1 2 840 113549 1 9 16 2 23
13.	id-aa-ets-revocationValues	1 2 840 113549 1 9 16 2 24
14.	id-aa-ets-archiveTimestamp	1 2 840 113549 1 9 16 2 27
15.	id-aa-ets-contentTimestamp	1 2 840 113549 1 9 16 2 20
16.	id-aa-ets-signerLocation	1 2 840 113549 1 9 16 2 17
17.	sha1	1 3 14 3 2 26
18.	ripemd160	1 3 36 3 2 1
19.	shalwithRSAEncryption	1 2 840 113549 1 1 5
20.	rsaSignatureWithripemd160	1 3 36 3 3 1 2
21.	rsaEncryption	1 2 840 113549 1 1 1

4.2 Textový popis minimálne nutných atribútov podpisovej politiky

```

<SignaturePolicy>
  <signPolicyHashAlg>
    <algorithm>
      OID algoritmu na výpočet hash hodnoty z položiek podpisovej
      politiky signPolicyHashAlg a signPolicyInfo.
    </algorithm>
  </signPolicyHashAlg>
  <signPolicyInfo>
    <signPolicyIdentifier>
      OID podpisovej politiky.
    </signPolicyIdentifier>
    <dateOfIssue>
      Dátum vydania politiky.
    </dateOfIssue>
    <policyIssuerName>
      <GeneralName>
        <directoryName>
          Meno vydavateľa politiky.
        </directoryName>
      </GeneralName>
      <GeneralName>
        <uniformResourceIdentifier>
          Http adresa politiky v DER kódovaní.
        </uniformResourceIdentifier>
      </GeneralName>
    </policyIssuerName>
    <fieldOfApplication>
      Textový popis typu a účelu politiky a pod akým právnym systémom je
      aplikovateľná.
    </fieldOfApplication>
    <signatureValidationPolicy>
      <signingPeriod>
        <notBefore>
          Čas odkedy je politika použiteľná na podpisovanie.
        </notBefore>
        <notAfter>
          Čas dokedy je politika použiteľná na podpisovanie.
        </notAfter>
      </signingPeriod>
      <commonRules>
        <signerAndVerifierRules>
          <signerRules>
            Požiadavky na podpisovateľa.
            <externalSignedData>
              true – externý podpis
              false – interný podpis
              – a ak sa atribút externalSignedData nenachádza, potom je
              politika určená pre obidva typy podpisov
            </externalSignedData>
            <mandatedSignedAttr>
              Zoznam povinných podpísaných CMS atribútov.
            </mandatedSignedAttr>
            <mandatedUnsignedAttr>
              Zoznam povinných nepodpísaných CMS atribútov.
            </mandatedUnsignedAttr>
            <mandatedCertificateRef>
              <signerOnly/>
          </signerRules>
        </signerAndVerifierRules>
      </commonRules>
    </signatureValidationPolicy>
  </signPolicyInfo>
</SignaturePolicy>

```

```

    Do atribútov podpisu Id-aa-ets-otherSigCert, id-aa-signingCertificate alebo XML elementu SigningCertificate je vložený odkaz na certifikát podpisovateľa.
  </mandatedCertificateRef>
  <mandatedCertificateInfo>
    < fullPath/>
    Do položky CMS podpisu certificates v bloku SignedData sú vložené certifikáty celej cesty od certifikátu podpisovateľa, až po dôveryhodný koreňový certifikát.
  </mandatedCertificateInfo>
</signerRules>
<verifierRules>
  <mandatedUnsignedAttr>
    Zoznam povinných nepodpísaných CMS atribútov.
  </mandatedUnsignedAttr>
</verifierRules>
</signerAndVerifierRules>
<signingCertTrustCondition>
  <signerTrustTrees>
    <CertificateTrustPoint>
      Podmienky pre množinu dôveryhodných koreňových certifikátov, na ktorých sa musí končiť certifikačná cesta vytvorená od certifikátu podpisovateľa alebo certifikátu časovej pečiatky.
    <trustpoint>
      Množina dôveryhodných koreňových certifikátov, na ktorých musí končiť certifikačná cesta vytvorená od certifikátu podpisovateľa alebo certifikátu časovej pečiatky.
    </trustpoint>
    <acceptablePolicySet>
      <CertPolicyId>
        Zoznam OID identifikátorov, ktoré musia byť v každom certifikáte certifikačnej cesty od hĺbky určenej nižšie v requireExplicitPolicy. Kontrolný prienik sa robí zo zjednotenia OID z rozšírení certifikátu CertificatePolicies a rozšírení certifikátu QcStatements.
      </CertPolicyId>
    </acceptablePolicySet>
    <policyConstraints>
      <requireExplicitPolicy>
        Určuje, od akej úrovne certifikačnej cesty smerom k certifikátu podpisovateľa sa začne kontrolovať explicitná podpisová politika (napríklad z acceptablePolicySet).
      </requireExplicitPolicy>
    </policyConstraints>
  </CertificateTrustPoint>
</signerTrustTrees>
<signerRevReq>
  <endCertRevReq>
    Spôsob kontroly platnosti certifikátu podpisovateľa alebo časovej pečiatky. Napríklad pomocou CRL, OCSP, ...
  </endCertRevReq>
<caCerts>
  Spôsob kontroly platnosti certifikátov certifikačných autorít pri vytvorenej ceste od certifikátu podpisovateľa alebo časovej pečiatky. Napríklad pomocou CRL, OCSP, ...
</caCerts>
</signerRevReq>
</signingCertTrustCondition>

```

```

<timeStampTrustCondition>
  <cautionPeriod>
    Položku podrobne popisuje dokument „Kontrola certifikačnej cesty“,
    nasledujúci odsek je len čiastočný súhrn zo spomenutého dokumentu.
    Minimálna doba od najstaršej platnej časovej pečiatky podpisu, počas ktorej
    musí overovateľ čakať, aby po nej získal záväzné údaje o platnosti
    certifikátov v certifikačnej ceste podpisovateľa a certifikačnej ceste najstaršej
    platnej časovej pečiatky podpisu. Pri overovaní podpisov s kvalifikovanými
    certifikátmi vydanými podľa slovenskej legislatívy je potrebné čakať iba na
    prvé CRL, po najstaršej platnej časovej pečiatke podpisu.
  </cautionPeriod>
</timeStampTrustCondition>
<algorithmConstraintSet>
  <signerAlgorithmConstraints>
    Množina algoritmov a prípadne minimálna veľkosť ich kľúčov použitých na
    vyhotovenie a overovanie podpisov, certifikátov, časových pečiatok ...
  </signerAlgorithmConstraints>
</algorithmConstraintSet>
</commonRules>
<commitmentRules>
  <CommitmentRule>
    <selCommitmentTypes>
      <CHOICE>
        <empty></empty>
      </CHOICE>
    </selCommitmentTypes>
  </CommitmentRule>
</commitmentRules>
</signatureValidationPolicy>
</signPolicyInfo>
<signPolicyHash>
  Kontrolný Hash integrity podpisovej politiky vypočítaný zo spojených hodnôt zo
  signPolicyHashAlg a signPolicyInfo.
</signPolicyHash>
</SignaturePolicy>

```

5 Špecifické podpisové politiky

5.1 Podpisová politika pre zaručený elektronický podpis s časovou pečiatkou, pre textové dokumenty v ASCII a v UTF8 kódovaní, pre interný alebo externý typ podpisu

Podpisovú politiku je možné použiť pre interné a aj externé typy podpisov, kde pri interných podpisoch je vďaka typu politiky jednoznačné, že sa jedná o podpísaný textový dokument v UTF8 kódovaní. Pri interných CMS podpisoch môže textový dokument začínať MIME hlavičkou, ktorej rozsah typov a kódovaní, kvôli jednoznačnosti pri vytváraní a overovaní ZEP, vymedzuje dokument „Formáty zaručených elektronických podpisov“.

Príloha A Literatúra

- | | | |
|--------------|---|---------------|
| [1] RFC 3280 | X.509 PKI Certificate and Certificate Revocation List | April 2002 |
| [2] RFC 2560 | X.509 PKI Online Certificate Status Protocol | June 1999 |
| [3] NBÚ | Formáty kvalifikovaných certifikátov | November 2005 |

Príloha B História

Verzia:	Dátum vydania:	Poznámka:	Vypracoval:
V 1.0	24.8.2005	Prvé vydanie	Ing. Peter Rybár, NBÚ RNDr. Július Šiška, PhD., KPMG
Verzia 1.1	6.11.2005	Jednotný formát NBÚ dokumentov	Ing. Peter Rybár, NBÚ