

XML nënshkrimet digjitale

Dr. techn. Blerim REXHA
blerim.rexha@cse-ks.com

1 Hyrje

eXtended Markup Language (XML) nënshkrimi digjital është rekomandim nga World Wide Web Consortium (W3C) që definojnë XML sintaksën për nënshkrimet digjitale. XML nënshkrimet digjitale mund të përdoren për të nënshkruar dokumente (resurse) apo pjesë të dokumenteve të çfarëdo lloji e që janë të qasshme përmes shtegut ose ueb adresës. XML nënshkrimi digjital mund të jetë i ndarë nga XML dokumenti i cili nënshkruhet (**detached**), i futur në XML dokumentin (**enveloped**) ose mund të përmbajë dokumentin i cili nënshkruhet (**enveloping**).

2 Çka s'është në rregull me nënshkrimet e zakonshme digjitale?

Dërguesi, i cili dëshiron që një dokument së bashku me nënshkrimin digjital t'ia dërgoj pranuesit vepron si vijon: llogaritë digest-in e dokumentin me anë të ndonjë hash funksioni të njohur siç janë: Secure Hash Algorithm #1 (SHA-1) ose Message Digest #5 (MD-5). Me tutje dërguesi e enkripton digest-in me çelësin e vetë privat. Rezultati i këtij enkriptimi quhet **nënshkrim digjital**. Dërguesi e dërgon dokumentin së bashku me nënshkrimin digjital përmes çfarëdo mjeti (rrjete) transportuese pranuesit, siç është paraqitur në Fig. 1. Dokumenti në këtë rast nuk është i enkriptuar, pra mund të lexohet prej çdo kujt që e pranon këtë informatë.

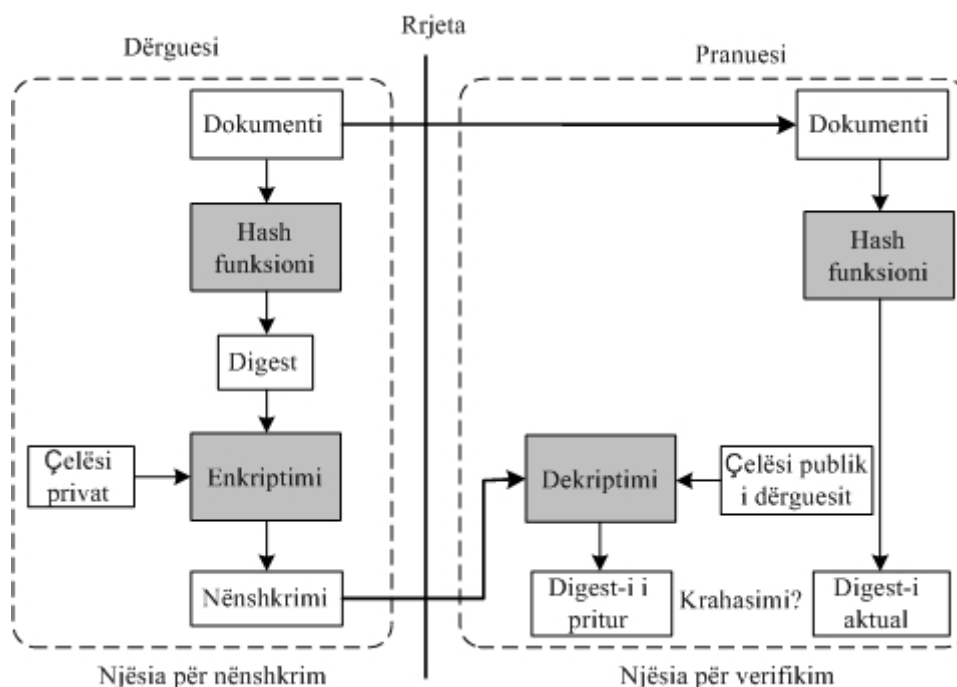


Fig. 1: Nënshkrimi digjital

Pranuesi në anën tjetër e pranon dokumentin (të pa enkriptuar) dhe me anë të të njëjtit hash funksion llogarit digest-in e dokumentin të pranuar. Pranuesi po ashtu e dekripton nënshkrimin digjital të pranuar me çelësin publik të dërguesit, dhe rezultatin e këtij dekriptimi e krahason me digest-in aktual, shih Fig. 1.

Me anë të nënshkrimit digjital arrihet:

- integriteti i shënimeve (dokumentit) - çdo ndërrim i dokumentit, qofte edhe një biti të vetëm rezulton në një digest tjetër me çka ndryshon edhe nënshkrimi digjital i dokumentit, dhe
- jo mohueshmëria e dërguesit – dërguesi nuk mundet me vonë të mohoj se dokumentin e ka nënshkruar dikush tjetër sepse vetëm ai është ne pronësi të çelësit të vetë privat.

Nënshkrimi digjital funksionon vetëm kur kemi një dërgues dhe një pranues. Bizneset bashkëkohore që zhvillohen përmes Internetit kërkojnë që dokumenti apo kontrata për biznes (siç quhet ndryshe) të nënshkruhet nga shumë pjesëmarrës në një transaksion. Secili prej pjesëmarrësve e nënshkruan vetëm një pjesë. Në disa raste kërkohet një renditje strikte e nënshkruarjes së dokumentit (kontratës), p.sh. se pari duhet banka të lejoj shumën e caktuar të parave dhe pastaj klienti të ketë të drejt të blej artikuj ndryshëm. Pjesëmarrësit e ndryshëm në transaksion përdorin poashtu platforma dhe protokolle të ndryshme për enkriptim. **Interoperabiliteti** këtu luan një rol shumë të rëndësishëm sepse të gjithë pjesëmarrësit duhet të jenë në gjendje të kuptojnë njeri-tjetrin.

XML nënshkrimet digjitale përmbushin kërkesat e lartshënuara.

3 Struktura e XML nënshkrimeve digjitale

Struktura dhe sintaksa e XML nënshkrimeve digjitale është përcaktuar me rekomandimin e W3C[1]. XML nënshkrimi digjital mund të aplikohet në çfarëdo lloji të shënimeve. Shënimet në XML dokumentin ruhen si element i veçantë. Po ashtu edhe hash vlera e shënimeve (digest-i) ruhet në XML dokumentin si element i veçantë. Digest-i enkriptohet me çelësin privat dhe ruhet si një XML element. XML nënshkrimi digjital identifikohet me anë të XML elementit **“Signature”** dhe përmban këto XML elemente[2], siç është paraqitur në Fig. 2.

```
<Signature >
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference UR="" ""
      (<Transforms>)?
      <DigestMethod>
      <DigestValue>
    </Reference>)+
  </SignedInfo>
  <SignatureValue>
  (<KeyInfo>)?
  (<Object>)*
</Signature>
```

Fig. 2: XML Nënshkrimi digjital

Disa XML elemente mund të mos paraqiten fare apo vetëm një herë në XML nënshkrimin digjital, kjo është paraqitur me anë të shenjës “?”, shih Fig. 2. Disa elemente duhet të paktën të paraqiten njëherë, shenja “+”, ndërsa disa elemente mund të mungojnë ose të paraqiten disa herë, shenja “*” në Fig. 2.

Përshkrimi i secilit XML element është paraqitur në Tab. 1.

Elementi	Përshkrimi
SignedInfo	Përmban nënshkrimin digjital si dhe informacione shtesë se si është llogaritur ky nënshkrim dhe mbi cilat shënime.
CanonazalizationMethod	Tregon algoritmin që është përdorur për transformuar XML dokumentin në formën e tij kanonike.
SignatureMethod	Tregon algoritmin i cili është përdorur për nënshkrim. Në rekomandimin e W3C janë të specifikuar dy algoritme për nënshkrime digjitale: RSA dhe DSA.
Reference	Identifikon shënimet mbi të cilat është llogaritur nënshkrimi digjital. Ky XML element mund të jetë brenda “signature” XML elementit (enveloping), jashtë tij (enveloped) ose adresë në ndonjë fajll extern (detached).
Transforms	Tregon transformimet siç është kodimi Base64 që janë përdorur para se të llogaritet digest-i i shënimeve, llojin e nënshkrimit (enveloping, enveloped, ose detached) si renditjen e transformimeve.
DigestMethod	Tregon algoritmin që është përdorur për llogarit digest-in (hashin) e shënimeve.
DigestValue	Digest-i i shënimeve, i cili enkriptohet për ta llogaritur nënshkrimin digjital.
KeyInfo	Paraqet informatat e nevojshme për çelësin publik, me anë të cilit mund të verifikohet nënshkrimi digjital (p.sh. X.509 certifikatën digjitale).
Object	Këtu mund të jetë nënshkrimi digjital.

Tab. 1: Përshkrimi XML elementeve të nënshkrimit digjital

Gjatë përdorimit të XML elementit **KeyInfo** duhet pasur kujdes të veçantë, sepse përgjuesi i mundshëm i trafikut të shënimeve ka mundësi të vepron si vijon:

- çelësin publik të dërguesit e zëvendëson me çelësin e vet publik,
- e enkripton digest-in me çelësin e vet privat, pra e rillogaritë nënshkrimin digjital dhe nënshkrimin digjital të dërguesit e zëvendëson me nënshkrimin digjital të rillogaritur.

Pranuesi në anën tjetër gjatë vërtetimit të nënshkrimit digjital nuk vëren kurrfarë mangësie sepse nënshkrimin digjital e vërteton me çelësin publik të përgjuesit. Një sulm i tillë njihet si “**man-in-the-middle**”.

Pozita e XML nënshkrimit digjital ndaj XML shënimeve ka nxitur diskutime të gjata në W3C. Duke pasur parasysh kërkesa të ndryshme për platforma të ndryshme W3C rekomandimi për XML nënshkrimet digjitale i përkrah tri format të vendosjes së XML nënshkrimit digjital ndaj XML shënimeve:

- Nënshkrimi i ndarë (detached) – në këtë rast <Signature> elementi ruhet në një fajll të veçantë[2], shih Fig. 3, dhe <Reference> XML elementi shfrytëzon adresën (shtegun) për ti adresuar XML shënimet.

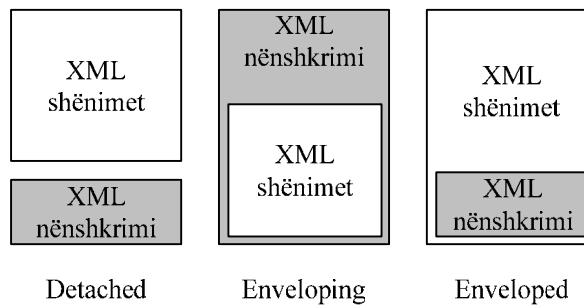


Fig. 3: Pozita e XML nënshkrimit digjital në XML dokumente

- XML nënshkrimi i mbështjellë XML shënimet (enveloping) – në këtë rast <Object> XML elementi i përmban XML shënimet dhe është pjesë e <Signature> XML elementit.
- XML nënshkrimi është i mbështjellur në XML shënimet (enveloped) – në këtë rast <Signature> XML elementi është insertuar në XML shënimet.

4 Për krahasim të XML nënshkrimeve digjitale në .NET

Microsoft .NET (New Enterprise Technology) korniza¹ i përmban të gjitha klasat dhe metodat për për krahasim të XML nënshkrimeve digjitale në hapësirën² *System.Security.Cryptography.Xml*. Klasat dhe metodat për manipulim me XML dokumente gjenden në hapësirën *System.Xml*. Në kornizën .NET klasat dhe metodat për enkriptim/dekriptim gjenden në hapësirën *System.Security.Cryptography*.

Nga [3] mund ta shkarkoni një shembull se si të implementohet nënshkrimi digjital në .NET. Shembulli është i natyrës shkollore dhe ka për qëllim njohjen me format e ndryshme të XML nënshkrimeve digjitale. Fajlli "XML nenshkrimet digjitale.cs" përmban fajllin burimor. Pamja e aplikacionit është paraqitur në Fig. 4. Për qëllime ndihme nga [3] mund të shkarkohet edhe një XML fajll (Porosia.xml) mbi të cilin do të llogaritet nënshkrimi digjital.

Kompajllimi e fajllit burimor "XML nenshkrimet digjitale.cs" prej vijës komanduese (DOS box-it) bëhet me anë të urdhrit:

```
csc "XML nënshkrimet digjitale.cs"
```

dhe pas kompajllimit të suksesshëm gjenerohet aplikacioni i ekzekutueshëm "XML nenshkrimet digjitale.exe".

SignedXML është klasa, e cila përdoret për krijimin e XML nënshkrimeve digjitale. Me anë të metodës *ComputeSignature()* llogaritet nënshkrimi digjital ndërsa me anë të metodës *CheckSignature()* bëhet verifikimi i nënshkrimit digjital.

¹ Framework
² Namespace

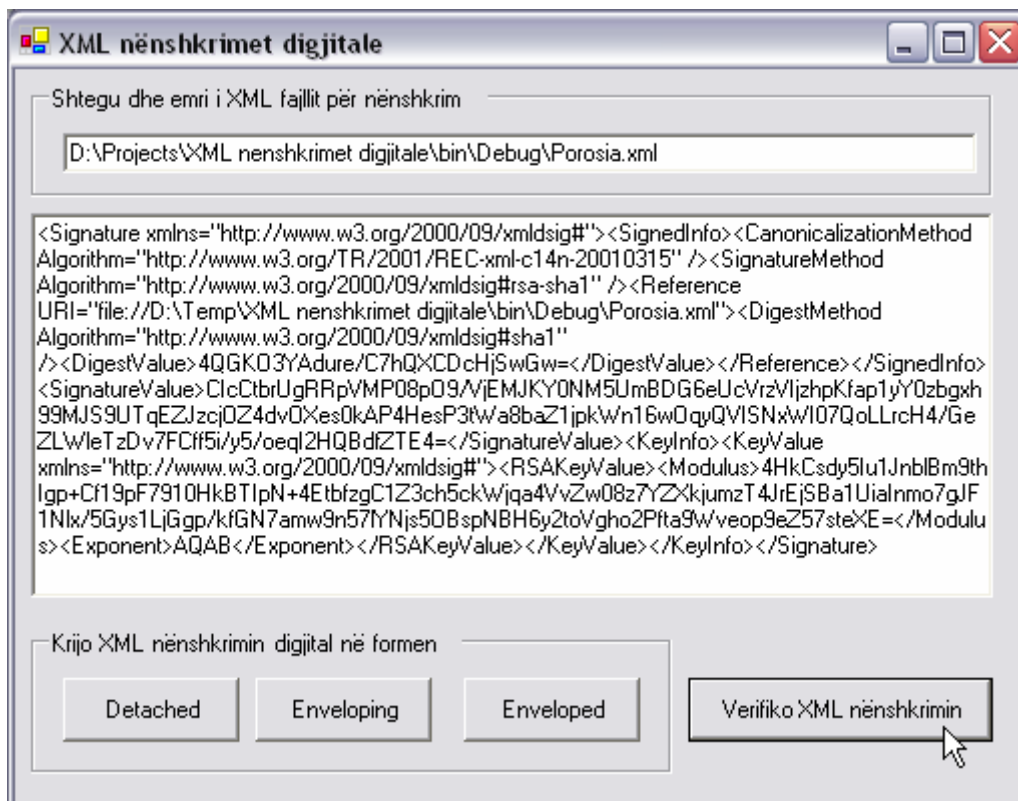


Fig. 4: Pamja e aplikacionit për testimin e XML nënshkrimeve digjitale

5 Përmbledhje

Me anë të nënshkrimeve të zakonshme digjitale nuk është e mundur që dokumenti të nënshkruhet në formë të pjesshme dhe prej shumë njësive. Me anë të XML nënshkrimeve digjitale është e mundur që një dokument të nënshkruhet në formë të pjesshme dhe prej njësive të ndryshme. Kërkesë kjo e pashmangshme për bizneset bashkëkohore përmes Internetit. Se cila formë e nënshkrimit: detached, enveloping ose enveloped do të përdoret varet prej kërkesave konkrete të aplikacionit.

Referencat

- [1] W3C, XML-Signature Syntax and Processing, W3C Recommendation 12 February 2002, <http://www.w3.org/TR/xmldsig-core/>
- [2] Mathew MacDonald& Erik Johansson, C# Data Security , Worx Press, January 2003
- [3] Blerim Rexha, XML nënshkrimet në .NET, "http://www.cse-ks.com/downloads/XML_nenshkrimet_digjitale.cs", 29.09.2005