



Българска асоциация  
на разработчиците на софтуер

# Цифрово подписване на документи в Web

Java-базиран framework с отворен код

**Светлин Наков**

Българска асоциация на разработчиците на софтуер

[www.nakov.com](http://www.nakov.com)

[www.devbg.org](http://www.devbg.org)

# Съдържание

- Основни понятия – цифров подпис, цифров сертификат, сертифицираща организация, PKI, защитени хранилища PKCS#12
- Как работи цифровият подпис
- Използване на цифрови подписи и сертификати в Java
- Проблеми при подписването на документи в Web-базирани системи
- Система за подписване на документи в Web-приложения NakovDocumentSigner

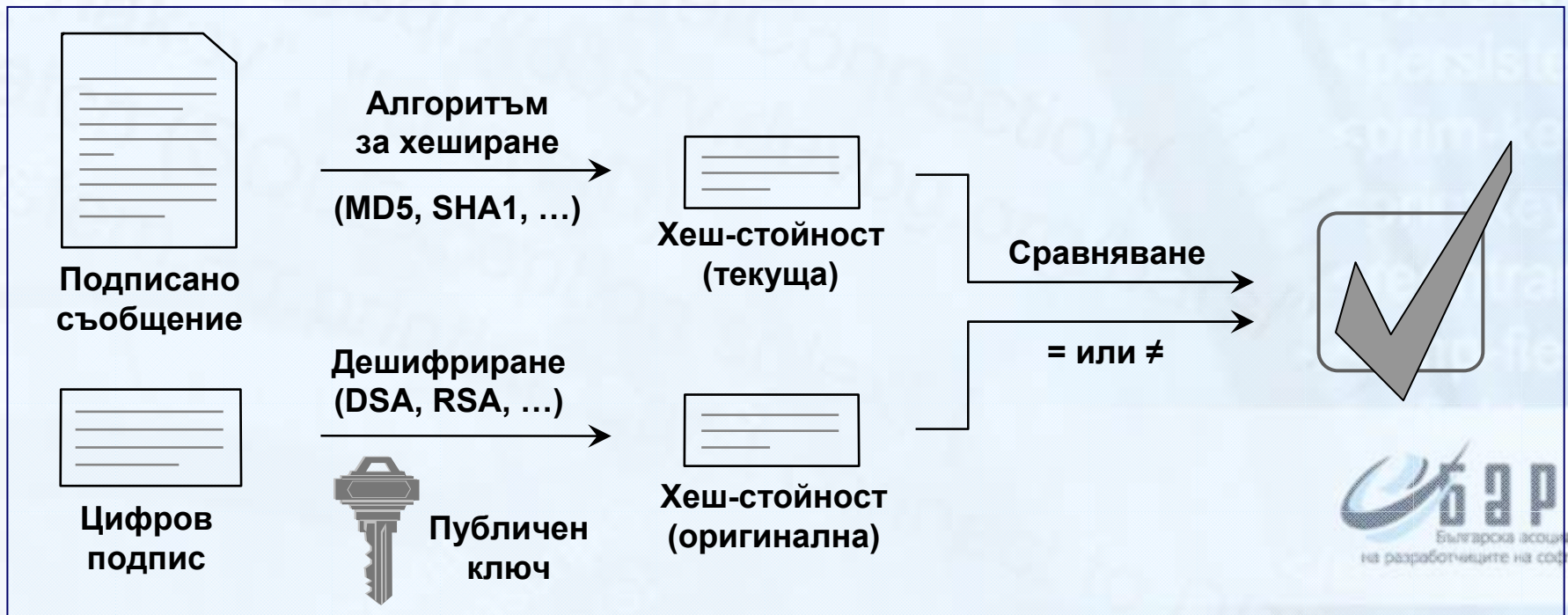
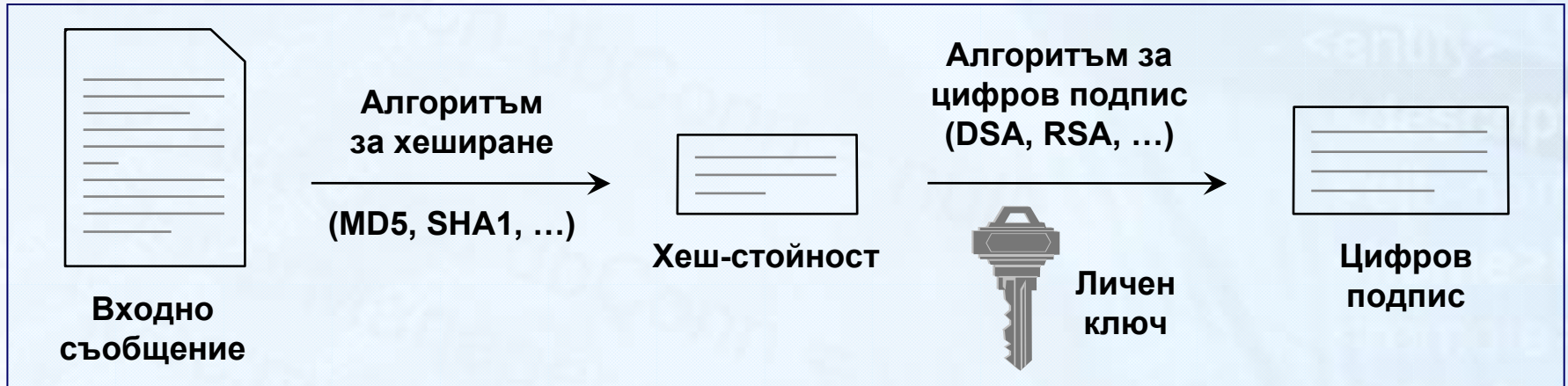
# Основни понятия

- Криптография с публични (несиметрични) ключове
- Публичен ключ, личен ключ
- Цифров подпис
- Инфраструктура на публичния ключ (PKI)
- Цифрови сертификати – стандарт X.509
- Сертифициращи организации (CA)
  - от първо ниво (VeriSign, GlobalSign, Thawte, Entrust)
  - междинни CA (напр. Бълг. стопанска камара)
  - локални CA (в рамките на организацията)

# ОСНОВНИ ПОНЯТИЯ

- Сертификати
  - Root-сертификати и сертификати на междинни СА
  - Self-signed сертификати
  - Доверени root-сертификати (trusted root CA certificates)
- Вериги от сертификати (certification chains)
- Проверени сертификати – процедура за проверка на сертификат
- Protected keystores – защитени хранилища за ключове и сертификати
  - .PFX и .P12 файлове – стандарт PKCS#12
  - смарт-карти

# Как работи цифровият подпис



# Подписи и сертификати в Java

- **Java Cryptography Architecture (JCA)**
  - Средства за подписване на документи, проверката на цифрови подписи и работа с цифрови сертификати
  - Стандартно API – пакетите `java.security` и `java.security.cert`
  - `java.security.KeyStore`
  - `java.security.PublicKey`
  - `java.security.PrivateKey`
  - `java.security.Signature`
  - `java.security.cert.X509Certificate`
  - `java.security.cert.CertificateFactory`
  - `java.security.GeneralSecurityException`
  - `java.security.cert.CertificateException`
  - Има вградена имплементация в JDK 1.4

# Сертификационни вериги в Java

- Java Certification Path API
  - Стандартни средства за проверка и построяване на сертификационни вериги
  - Основни класове и интерфейси:
    - `java.security.cert.CertPathValidator`
    - `java.security.cert.CertPathBuilder`
    - `java.security.cert.CertPath`
    - `java.security.cert.TrustAnchor`
    - `java.security.cert.PKIXParameters`
    - `java.security.cert.CertPathValidator`
  - Има вградена имплементация в JDK 1.4

# Подписване на документи в Web

- Какъв е проблемът?
  - Искаме при изпращане на файлове от Web-приложение тези файлове да се подписват цифрово от изпращача
- Какви са трудностите?
  - Сървърът не трябва да има достъп до личните ключове на потребителите
  - Подписването трябва да става на машината на клиента
  - Стандартните Web-браузъри не поддържат цифрови подписи
  - Готовите решения са доста скъпи



# Подписване на документи в Web

- Как можем да подпишем файл в Web среда на машината на клиента?
  - Отделно приложение при клиента
    - трудности при интеграцията с Web-приложението
    - трудности за потребителите при първоначално инсталиране
    - трудности при поддръжката на много платформи
  - ActiveX контрола
    - работи само под Windows
    - работи само с някои Web-браузъри

# Подписване на документи в Web

- Как можем да подпишем файл в Web среда на машината на клиента?
  - Macromedia Flash
    - не поддържа работа с цифрови подписи
    - не позволява достъп до файловата система
  - .NET Windows Forms контрола
    - поддържа се само от Internet Explorer 6.0
    - изисква инсталиран .NET Framework
    - трудности с достъпа до файловата система
  - **Подписан Java аplet**
    - работи на всички платформи
    - изисква единствено Java Plug-In 1.4

# Подписани Java аплети

- Подписаните Java аплети се изпълняват без ограничения на правата
  - могат да достъпват файловата система
  - могат да използват криптографското API на Java
- Генериране на self-signed сертификат

```
keytool -genkey -alias signFiles -keystore  
SignApplet.jks -keypass !secret -dname  
"CN=My Company" -storepass !secret
```

- Подписване на Java аплет

```
jarsigner -keystore SignApplet.jks  
-storepass !secret -keypass !secret  
Applet.jar signFiles
```

# NakovDocumentSigner

- Система с отворен код за подписване на документи в Web-приложения
- NakovDocumentSigner се състои от:
  - **подписан Java аplet**
    - изпълнява се при клиента
    - подписва файловете преди изпращането им
  - **демонстрационно Web-приложение**, което:
    - посреща подписаните файлове на сървъра
    - проверява валидността на цифровия подпис
    - проверява валидността на сертификата – директно или по сертификационната верига

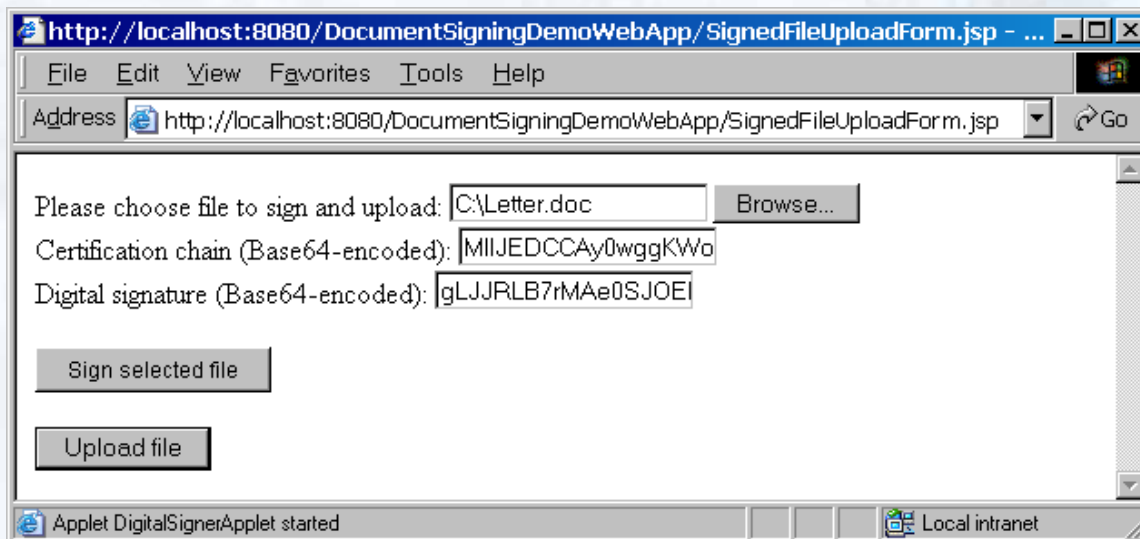
# За подписания аplet

- Вгражда се в HTML формата за изпращане на файл
- Изисква Java Plug-In 1.4 или по-нов
- Изисква потребителят да му разреши да се стартира с повишени права
- При активиране иска от потребителя да избере PKCS#12 хранилище за сертификати (.PFX или .P12 файл) и парола за достъп до него
- Записва цифровия подпис и сертификата заедно с цялата сертификационна верига в скрито поле на HTML формата
- Тестван е и работи с Internet Explorer, Netscape и Mozilla под Windows и Linux

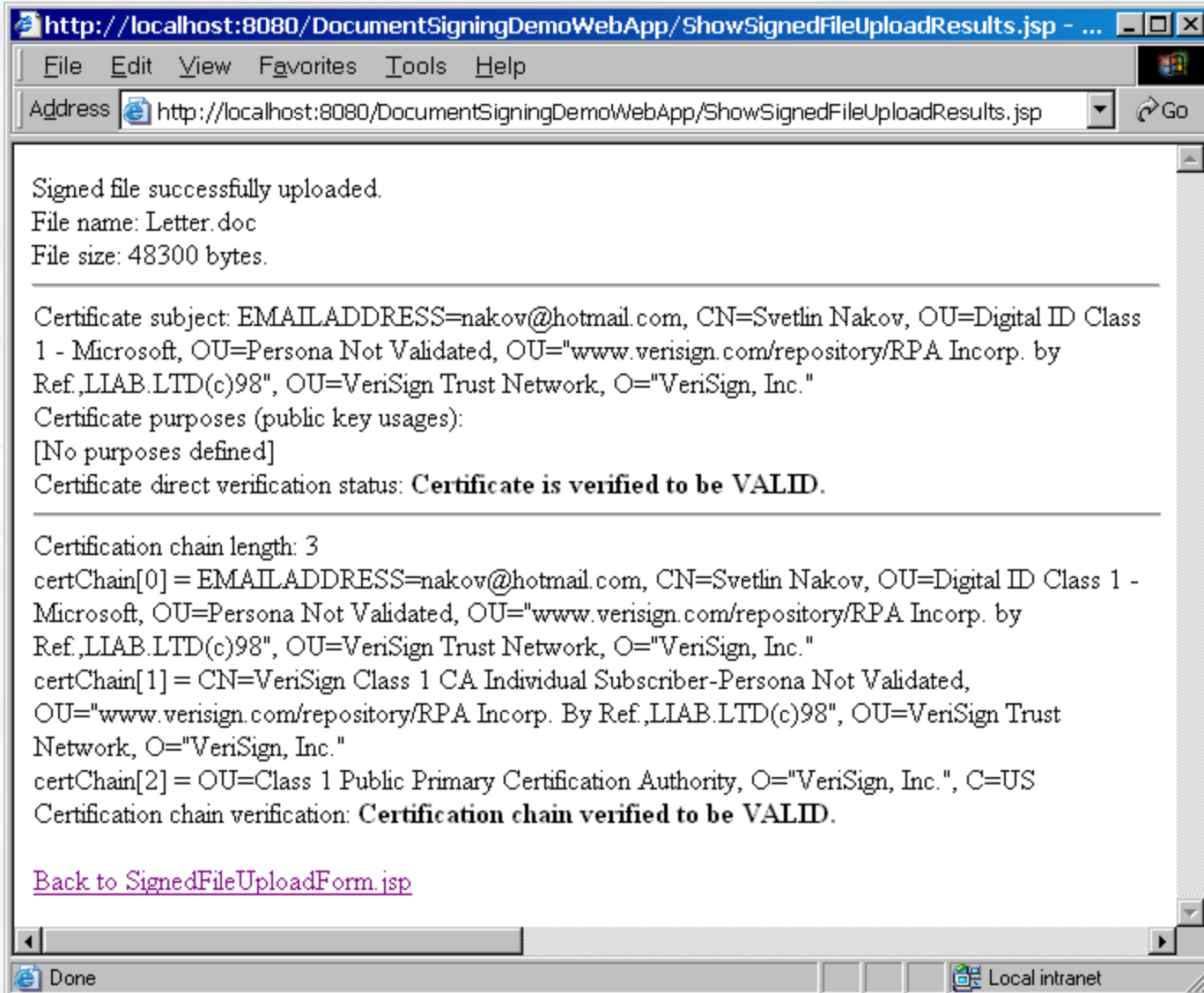
# За Web-приложението на сървъра

- Базирано на J2EE и Struts framework
- Проверява цифровия подпис на получения файл чрез Java Cryptography Architecture
- Проверява сертификата на изпращача за валидност по два начина:
  - Директно – чрез проверка дали използваният сертификат е директно подписан от някои от trusted Root-сертификатите
  - Чрез сертификационната верига – проверява цялата сертификационна верига на сертификата чрез Java Certification Path API
- Тествано с Apache Tomcat 4.0 и JDK 1.4

# НаковDocumentSigner в действие



# NakovDocumentSigner в действие



http://localhost:8080/DocumentSigningDemoWebApp/ShowSignedFileUploadResults.jsp - ...

File Edit View Favorites Tools Help

Address http://localhost:8080/DocumentSigningDemoWebApp/ShowSignedFileUploadResults.jsp Go

Signed file successfully uploaded.  
File name: Letter.doc  
File size: 48300 bytes.

---

Certificate subject: EMAILADDRESS=nakov@hotmail.com, CN=Svetlin Nakov, OU=Digital ID Class 1 - Microsoft, OU=Persona Not Validated, OU="www.verisign.com/repository/RPA Incorp. by Ref.,LLAB.LTD(c)98", OU=VeriSign Trust Network, O="VeriSign, Inc."  
Certificate purposes (public key usages):  
[No purposes defined]  
Certificate direct verification status: **Certificate is verified to be VALID.**

---

Certification chain length: 3  
certChain[0] = EMAILADDRESS=nakov@hotmail.com, CN=Svetlin Nakov, OU=Digital ID Class 1 - Microsoft, OU=Persona Not Validated, OU="www.verisign.com/repository/RPA Incorp. by Ref.,LLAB.LTD(c)98", OU=VeriSign Trust Network, O="VeriSign, Inc."  
certChain[1] = CN=VeriSign Class 1 CA Individual Subscriber-Persona Not Validated, OU="www.verisign.com/repository/RPA Incorp. By Ref.,LLAB.LTD(c)98", OU=VeriSign Trust Network, O="VeriSign, Inc."  
certChain[2] = OU=Class 1 Public Primary Certification Authority, O="VeriSign, Inc.", C=US  
Certification chain verification: **Certification chain verified to be VALID.**

[Back to SignedFileUploadForm.jsp](#)

Done Local intranet



# Демонстрация



# Ресурси

- Серия от статии “Цифрово подписване на документи в Java-базирани Web-приложения”:
  - Част 1 – Основни понятия –  
<http://www.developer.com/security/article.php/3083161>
  - Част 2 – Как работят цифровите подписи –  
<http://www.developer.com/security/article.php/3092771>
  - Част 3 – Цифрови подписи и сертификати в Java –  
<http://www.developer.com/security/article.php/3105261>
  - Част 4 – Проблеми с цифровите подписи в Web –  
<http://www.developer.com/security/article.php/3288571>
  - Част 5 – NakovDocumentSigner: система с отворен код за подписване на документи в Web-приложения –  
<http://www.developer.com/security/article.php/3298051>
- Официален сайт на NakovDocumentSigner –  
<http://www.nakov.com/documents-signing/>

# Цифрово подписване на документи в Web

Java-базиран framework с отворен код

# Въпроси?