Bewertung der Einsatzmöglichkeiten von XML Sicherheitslösungen in mobilen Kommunikationsumgebungen

Fabian Pretsch

Ziel

- Implementierung von XML Encryption/Signature in Java
- Testen der Implementierung auf einem PDA
- Bewertung der Ergebnisse
- Theoretische Evaluierung von Alternativen

XML Signature/Encryption

- „Recommendations“ der W3C
- Standards herunterladbar unter www.w3c.org
- Ziel: Definition eines Standards zum sicheren Austausch von XML Dokumenten (insbesondere im wirtschaftlichen Umfeld)
- Grundlage für WSS (Webservice Security)

XML-Encryption

- Komplette Verschlüsselung beliebiger Dateien
- Verschlüsselung einzelner nodes von XML-Dateien

Originaldatei

```
<?xml version="1.0" encoding="ISO-8859-15" standalone="yes" ?>
<booklist>
<!--Kommentar -->
<book>
        <title>Einstieg in XML </title>
        <author>Helmut Vonhoegen</author>
        <publisher>Galileo Computing</publisher>
</book>

...

<book>
        <title>Informationsmanagement</title>
        <author>Stefan Voß</author>
        <publisher>Springer</publisher>
</book>

<book>
        <title>Die Programmiersprache C</title>
        <author>Kernighan, Ritchie</author>
        <publisher>Hanser</publisher>
</book>
</booklist>
```

Verschlüsselt (gesamte Datei)

<?xml version="1.0"?><EncryptedData xmlns=' http://www.w3.org/2001/04/xmlenc#' >
<CipherData>
<n0:KeyInfo xmlns:n0="http://www.w3.org/2000/09/xmldsig#" /
><CipherValue>Hry40ZcWgCYW9gVtcCx9ZN7CZ3P710aTw/x7TVsruLtsqx05UELRQWflAvufeHkbIdHkCLkKiBcRjx7
lhffdePwjPbe6WLHP9eHnBeBLNbEieh13IJT819LIUS5cBj9bhIhlHvMHs9B1wtd3EyHdsHYjQ9fsE4v0vHp4KncNW5Mv
8WNlyaK0NjjWLAcWvvbAz7dG2h3GHviCWRJ5y9phTYaZbrXY0pbGsLdnlMXYoAIi9N5si5aoObhsXZO7pFp1DlAbbj
87sS97Ds4VaFtdUaPFYQJKFSa7LR8AuosiayOk/pVCttAIosz3Rk5cPVeeYgiuq/gbl7QawjeqoCP/MH0E1WgY9xaLiSyK
BRN2rPr1Jv+TfnROrFcdibLQjyFDoSee14B2Y8dnNgMtF1SQNvR6i05HVVEKEB3uE+m2b9HcjokFR9H1ICc16dvGGP
P9fpUOIhWX6cM3iR4pE/EaBhKJxbm9SV6EWOUoB2O6Q2Hponnm7FeiN02UfnfP/qF0iG5qDWJfU8Gk2mhkad8xi506
sqoG8S+b4Srmim5xq51Orb5ZeOAXhntW1CMxjuXfk2vtUFt6jsHlRF9omJarLSwwXEaIvFaS5acd2SjPJo3Fj/b0MqKL8m
XTNZRNsOZ15tm9XbFiETNTI8tUtcXkS8+3Rtodxh74glkSecvaYU0P+yBJDFskeMbeg2soSEExomxzFIiPdYrVNkNVSjJ
GDJZZPyA4rWUp3+ITU7OBKG2K+eX8nlRAdiOh+f4hDPfMlzDbw+0V6BlyDeiA9yCaw1RqDfPBZ9eYWkiwaVNLbrx
FNmSNMPV5ukM77p2TbT6SC4j0j9JO02nJQQGjnShRkID91GmgfR2oCuWyuX4oqE4HFbD08VcUkKoTqzc2I90w847/
0KaIOIUFFsvRAMsnJp/2/PL5CbD9Me6ctVpnEsosKJLusqBxwoN+5Q1Pb923</CipherValue>
</CipherData>
</EncryptedData>

Verschlüsseln einzelner nodes

```
<?xml version='  .0' ?><booklist>
<!--Kommentar -->
<book>
        <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"><n0:KeyInfo xmlns:n0="http://www.w3.org/2000/09/xmldsig#" /
><CipherData><CipherValue>EAGXK0GEIEZfRP9kLEoXKlSotqmYFODXB1zhl5TmsqY=</CipherValue></CipherData></EncryptedData>
        <author>Helmut Vonhoegen</author>
        <publisher>Galileo Computing</publisher>
</book>

...

<book>
        <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"><n3:KeyInfo xmlns:n3="http://www.w3.org/2000/09/xmldsig#" /
><CipherData><CipherValue>Sp5JVLdp25L2V1EcIDxMy5eFiuXJD8gPq9dh35EXU7hjFV24cs0UMEs1oAqhIM9r</CipherValue></CipherData>
</EncryptedData>
        <author>Stefan Voß</author>
        <publisher>Springer</publisher>
</book>

<book>
        <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"><n4:KeyInfo xmlns:n4="http://www.w3.org/2000/09/xmldsig#" /
><CipherData><CipherValue>LU19kxS3zSfvq0v4YZ7pl3TuEK8TeDb3hIQgKNRWLofebYJZynUlA8MHqLumm/gF</CipherValue></CipherDat
a></EncryptedData>
        <author>Kernighan, Ritchie</author>
        <publisher>Hanser</publisher>
</book>
</booklist>
```

Unterstützte Verschlüsselungsverfahren

- TripleDES
- AES128
- AES256
- Verschiedene asymmetrische Schlüsseltransportverfahren
- Verschiedene symmetrische Schlüsseltransportverfahren

Formen von XML-Signaturen

- Detached: Die Signatur ist von dem zu signierenden Objekt getrennt. Das Objekt wird durch eine URI identifiziert
- Enveloping: Das Objekt ist ein Teilbaum der Signatur
- Enveloped: Die Signatur ist ein Teilbaum des zu signierenden Objektes, die Signatur wird über den XML-Restbaum des Dokumentes berechnet

Beispiel XML-Signature (detached)

<?xml version="1.0" encoding="ISO-8859-15"?>
<Signature>
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
<Reference URI="file:///home/fab/Diplomarbeit/src/books.xml">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>UuPdzaxg6k94nvlDtWaiGSUHqJQ=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>Pj7s2UzMB9K+0YyE7oVD5irXFbm0fXnzHjFBaG3i3C0CI6o2gOJEBg==</SignatureValue>
<KeyInfo><KeyValue><DSAKeyValue><P>MTA2NzcyMjM4MTkxNzIzNTg4MzMzMDU0MzkwNzkxMDU3MDc4NDMxNTkwMDMyMjgzMzYyNTQ4NDg3NjQxMjYyNDk5MTI0MDQxMjY0MTA2NjE4ODczNDIwNDA2MjE5NDEyODE0MTQ2OTg3NTQ4MjA3NTQzNDg2OTcwMDQwNzg4NjE4NTUxNTUzNjM0MDQ2NzkyMjA0MDI3MDc5MTc=</P>
<Q>MTQwNjQzNzQyMzgzMDE1NDk0NDE0NjU3MjAxNjgwNDUyMzE3NzM0NDY0NTY0MjQxMw==</Q>
<G>Nzc2NDUzNzUwMTMxMTAxMzQwNDU3MjQxODIxMTY3MjUyMzczNjk2Mzc4NDQ3ODY1MzI2NTkwNzc1NTMzNjE5ODM1Mjk1ODExNzI1ODk4NDc2NTU3MjkxNDEzNDU0NTMzNTIwMjUzNDAzODM4ODE2NjYzODM0OTE2NDU2MTc0MzM1ODAwMDA5NTE2OTUxMzU3NTE2NDgyNjc0MA==</G><Y>ODQyMDMyNTYwMzU3MTM2NzYwOTU2NzQxMjM2MzI4MDkyMzU0NTkyMTYxNzU5NDU4MjU0NTM3OTA4MjEyNDgwNTY4MzE5NzY1OTYyOTYzNzg0MDYwNzUyMjYyNTkwNjEyOTgwOTM2Mzg1NzAyMjA0MDQ1NDgxMzU5NDM5ODM5NTI3MjcwNjgwOTExOTE0Mzc1ODA2MTE2NDc2Mg==</Y></DSAKeyValue></KeyValue></KeyInfo>
</Signature>

Beispiel Enveloping Signature

<Signature>
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
<Reference URI="#books">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>sujHCCxxQyrLhFhNlif7ucGOsNw=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>PGYUqk43ZeF5oQckb0HYCUnWrNeQWqAJszeC17TnPNN/ws7UOpbegA==</SignatureValue>
<KeyInfo><KeyValue><DSAKeyValue><P>MTA2NzcyMjM4MTkxNzIzNTg4MzMzMDU0MzkwNzkxMDU3MDc4NDMxNTkwMDMyMjgzMzYyNTQ4NDg
3NjQxMjYyNDk5MTI0MDQxMjY0MTA2NjE4ODczNDIwNDA2MjE5NDEyODE0MTQ2OTg3NTQ4MjA3NTQzNDg2OTcwMDQwNzg4NjE4NTUxNTUzNj
M0MDQ2NzkyMjA0MDI3MDc5MTc=</P>
<Q>MTQwNjQzNzQyMzgzMDE1NDk0NDE0NjU3MjAxNjgwNDUyMzE3NzM0NDY0NTY0MjQxMw==</Q>
<G>Nzc2NDUzNzUwMTMxMTAxMzQwNDU3MjQxODIxMTY3MjUyMzczNjk2Mzc4NDQ3ODY1MzI2NTkwNzc1NTMzNjE5ODM1Mjk1ODExNzI1ODk4N
Dc2NTU3MjkxNDEzNDU0NTMzNTIwMjUzNDAzODM4ODE2NjYzODM0OTE2NDU2MTc0MzM1ODAwMDA5NTE2OTUxMzU3NTE2NDgyNjc0MA==</
G>
<Y>ODQyMDMyNTYwMzU3MTM2NzYwOTU2NzQxMjM2MzI4MDkyMzU0NTkyMTYxNzU5NDU4MjU0NTM3OTA4MjEyNDgwNTY4MzE5NzY1OTYy
OTYzNzg0MDYwNzUyMjYyNTkwNjEyOTgwOTM2Mzg1NzAyMjA0MDQ1NDgxMzU5NDM5ODM5NTI3MjcwNjgwOTExOTE0Mzc1ODA2MTE2NDc2Mg
==</Y>
</DSAKeyValue></KeyValue></KeyInfo>
<Object
Id="books">PD94bWwgdmVyc2lvbj0nMS4wJyBlbmNvZGluZz0nVVRGLTgnID8+PGJvb2tsaXN0PgoKPGJvb2s+Cgk8dGl0bGU+RWluc3RpZWcgaW4gWE1M
IDwvdGl0bGU+Cgk8YXV0aG9yPkhlbG11dCBWb25ob2VnZW48L2F1dGhvcj4KCTxwdWJsaXNoZXI+R2FsaWxlbyBDb21wdXRpbmc8L3B1Ymxpc2hlcj4KPC
9ib29rPgoKPGJvb2s+Cgo8YXV0aG9yPlfIDtmhlPC9hdXRob3I+Cgk8cHVibGlzaGVyPlZha
GxlbjwvcHVibGlzaGVyPgo8L2Jvb2s+Cgo8Ym9vaz4KCTx0aXRsZT5KYXZhIDEuMTwvdGl0bGU+Cgk8YXV0aG9yPkd1aWRvIEtyw7xnZXI8L2F1dGhvcj4K
CTxwdWJsaXNoZXI+QWRkaXNvbiBXZXNsZXk8L3B1Ymxpc2hlcj4KPC9ib29rPgoKCjxib29rPgoJPHRpdGxlPkM9uc21hbmFnZW1lbnQ8L3Rp
dGxlPgoJPGF1dGhvcj5TdGVmYW4gVm/DnzwvYXV0aG9yPgoJPHB1Ymxpc2hlcj5TcHJpbmdlcjwvcHVibGlzaGVyPgo8L2Jvb2s+CTx0aXRsZ
T5EaWUgUHJvZ3JhbW1pZXJzcHJhY2hlIEM8L3RpdGxlPgoJPGF1dGhvcj5LZXJuaWdoYW4sIFJpdGNoaWU8L2F1dGhvcj4KCTxwdWJsaXNoZXI+SGFuc2V
yPC9wdWJsaXNoZXI+CjwvYm9vaz4KPC9ib29rbGlzdD4=</Object></Signature>

Beispiel Enveloped Signature


```
<?xml version='  1.0?><booklist>
<!--Kommentar -->
<book>
        <title>Einstieg in XML </title>
        <author>Helmut Vonhoegen</author>
        <publisher>Galileo Computing</publisher>
</book>
...
<book>
        <title>Die Programmiersprache C</title>
        <author>Kernighan, Ritchie</author>
        <publisher>Hanser</publisher>
</book>
<Signature>
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
<Reference URI="">
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>sujHCCxxQyrLhFhNlif7ucGOsNw=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>EebsM7/IGWZ1VkS5yCjISYmlaovmNWy2PQsnArTZ3/a7D8Tb8JAnjw==</SignatureValue>
<KeyInfo><KeyValue><DSAKeyValue><P>MTA2NzcyMjM4MTkxNzIzNTg4MzMzMDU0MzkwNzkxMDU3MDc4NDMxNTkwMDMyMjgzMzYyNTQ4NDg3NjQxMjYyNDk5MTI0MDQxMjY0MTA2NjE4ODczNDIwNDA2MjE5NDEyODE0MTQ2OTg3NTQ4MjA3NTQzNDg2OTcwMDQwNzg4NjE4NTUxNTUzNjM0MDQ2NzkyMjA0MDI3MDc5MTc=<
/P>
<Q>MTQwNjQzNzQyMzgzMDE1NDk0NDE0NjU3MjAxNjgwNDUyMzE3NzM0NDY0NTY0MjQxMw==</Q>
<G>Nzc2NDUzNzUwMTMxMTAxMzQwNDU3MjQxODIxMTY3MjUyMzczNjk2Mzc4NDQ3ODY1MzI2NTkwNzc1NTMzNjE5ODM1Mjk1ODExNzI1ODk4NDc2NTU3MjkxND
EzNDU0NTMzNTIwMjUzNDAzODM4ODE2NjYzODM0OTE2NDU2MTc0MzM1ODAwMDA5NTE2OTUxMzU3NTE2NDgyNjc0MA==</G>
<Y>ODQyMDMyNTYwMzU3MTM2NzYwOTU2NzQxMjM2MzI4MDkyMzU0NTkyMTYxNzU5NDU4MjU0NTM3OTA4MjEyNDgwNTY4MzE5NzY1OTYyOTYzNzg0MDYwN
zUyMjYyNTkwNjEyOTgwOTM2Mzg1NzAyMjA0MDQ1NDgxMzU5NDM5ODM5NTI3MjcwNjgwOTExOTE0Mzc1ODA2MTE2NDc2Mg==</Y>
</DSAKeyValue></KeyValue></KeyInfo>
</Signature></booklist>
```

XML Canonicalization

- Die Signatur sollte vom Inhalt des zu signierenden Dokumentes abhängen, nicht von der Darstellung!
- Einheitliche Kodierung (UTF-8)
- Behandlung von Zeilendelimitern (DOS,Unix,Macintosh)
- Behandlung von Kommentaren
- Behandlung von Sonderzeichen
- Eliminierung von nicht relevanten Whitespaces

XML Canonicalization

- Vor der Signierung wird eine kanonische Form des XML-Dokumentes erzeugt
- Die Kanonische Form des Dokumentes wird signiert (die Originaldatei bleibt unverändert)
- Der Empfänger vergleicht die empfangene Signatur mit der Signatur der kanonischen Form des Originaldokumentes

Beispiel

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes" ?>
<booklist  >
<!--Sinnloser Kommentar-->
<book     >

      <title>Einstieg in XML</title>
      <author>Helmut Vonhoegen</author>
      <publisher>Galileo Computing</publisher>

</book    >

</booklist>
```

Kanonische Version

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<booklist>
<book>

    <title>Einstieg in XML</title>
    <author>Helmut Vonhoegen</author>
    <publisher>Galileo Computing</publisher>

</book>

</booklist>
```

Aufbau des Programms

- Initialisierung mittels einer XML-Konfigurationsdatei
- Im wesentlichen nur zwei öffentliche Methoden:
- Sign() bzw. encrypt()
- check(Reader input) bzw. decrypt(...)
- Was wie womit signiert/verschlüsselt wird ist in der Konfigurationsdatei festgelegt

Aufruf

- Aus einem anderen Java-Programm heraus
- Von der Kommandozeile aus

Verwendete Bibliotheken

- Kxml2: Eventauslösender Pullparser (im Gegensatz zum Push-Ansatz von SAX)
- BouncyCastle: Crypto-API mit zahlreichen implementierten Verschlüsselungs-/ Signieralgorithmen
- Beide Bibliotheken sind für den Einsatz mit der Java2 Micro Edition (J2ME) ausgelegt und daher sehr ressourcenschonend

Beispiel Konfigurationsdatei XML-Encryption

<EncConfig>
<Reference>
file:///home/fab/Diplomarbeit/src/books.xml#title
</Reference>

<EncryptionMethod >
http://www.w3.org/2001/04/xmlenc#aes128-cbc
</EncryptionMethod>

<Key>
file:///home/fab/Diplomarbeit/src/aes_key
</Key>
</EncConfig>

Beispiel Konfigurationsdatei XML-Signature

```
<SigConfig>
<Reference Method="detached">
file:///home/fab/Diplomarbeit/src/books.xml
</Reference>

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

<SigMethod>
http://www.w3.org/2000/09/xmldsig#dsa-sha1
</SigMethod>

<Key>
file:///home/fab/Diplomarbeit/src/dsa_opts
</Key>
</SigConfig>
```

Verwendete Hard-/Software

- Compaq iPAQ
- 206 MHz ARM-Prozessor
- 64 MB Speicher insgesamt
- Betriebssystem: Microsoft PocketPC 3.0
- Java-Runtime: Jeode von Insignia

Benchmark Ver-/Entschlüsselung einer Binärdatei

Sekunde	10kB		100kB		1MB	
	Verschlüsse	Entschlüsse	Verschlüsse	Entschlüsse	Verschlüsse	Entschlüsse
TripleDE	0,2	0,3	1,8	1,9	19,0	17,6
AES128	0,18	0,2	2,0	1,0	15,1	14,0
AES256	0,18	0,2	2,0	1,0	15,7	14,0

Benchmark Ver-/Entschlüsselung einzelner nodes (1 node = 1 kB)

Sekunde	10kB/nodes		100kB/nodes		1MB/nodes	
	Verschlüsse	Entschlüsse	Verschlüsse	Entschlüsse	Verschlüsse	Entschlüsse
TripleDE	0,4	0,2	3,2	2,0	32,7	20,0
AES128	0,31	0,17	2,8	1,6	31,0	17,0
AES256	0,31	0,18	3,0	1,9	33,0	17,2

Benchmark Signieren/Überprüfen einer Binärdatei

Sekunden	10kB		100kB		1MB	
	Signiere	Überprüfe	Signiere	Überprüfe	Signiere	Überprüfen
DSA/SHA-	0,6	0,8	1,0	1,0	6,2	6,2

Benchmark Signieren/Überprüfen einzelner nodes (1 node = 1 kB)

Sekunden	10kB/nodes		100kB/nodes		1MB/nodes	
	Signieren	Überprüfe	Signieren	Überprüfe	Signieren	Überprüfen
DSA/SHA-	0,7	0,8	1,4	0,9	11,7	10,4

Alternativen

- IPSec (IP Security)
- SSL/TLS (Secure Socket Layer / Transport Level Security)
- PGP (Pretty Good Privacy)

IPSec

- Verschlüsselung auf Verbindungsebene
- Bestandteil von IPv6
- Für IPv4 verfügbar
- Integration in bestehende Systeme relativ aufwendig

SSL/TLS

- Verschlüsselung auf Transportschichtebene
- Erstmals in Netscape Navigator V3.0
- Integration in bestehende Systeme relativ leicht (per Webbrowser)
- Kann keine Streaming-Inhalte verschlüsseln (nur mit TCP anwendbar)

PGP

- Verschlüsselung auf Anwendungsschichtebene
- Ursprünglich von Phil Zimmermann entwickelt
- Für Privatpersonen kostenlos
- Quellcode war zeitweise frei verfügbar
- OpenPGP: Standard für PGP-Implementierungen
- Bekannteste alternative Implementierung: GPG

Datenorientierte Verschlüsselung <-> verbindungsorientierte Verschlüsselung

- Verbindungsorientierte Verfahren
  - IPSec, SSL/TLS
  - Es wird die Verbindung verschlüsselt
  - Für den Benutzer transparent
- Datenorientierte Verfahren
  - PGP, XML-Encryption/-Signature
  - Es werden Dateien verschlüsselt
  - Für den Benutzer nicht transparent (expliziter Programmaufruf notwendig)

Sicherheitsaspekte der Verfahrensgruppen

- Verbindungsorientierte Verfahren
  - Schlüsselaustausch erfolgt automatisch
  - Identifizierung des Verbindungspartners durch X509v3-Zertifikate
- Datenorientierte Verfahren
  - Schlüsselaustausch erfolgt i.d.R. manuell
  - Identität des Verbindungspartners bekannt

Sicherheitsaspekte in Ad-hoc Netzwerken

- Funkverbindungen
  - Leichter Zutritt für Unbefugte -->Man-in-the-middle Angriffe
- Zertifikate-Server i.d.R. nicht vorhanden
  - Zertifikate fallen für die Identifizierung des Verbindungspartners aus
- Deutlich erhöhte Angriffsgefahr im Vergleich zu konventionellen/kabelbasierten Netzwerken

Fazit

- Die vorhandenen Resourcen der PDA-Hardware reichen aus, um fortschrittliche Verschlüsselungsverfahren sinnvoll zu nutzen
- Aufgrund der Verschlüsselung auf Anwendungsschichtebene ist XML-Encryption/-Signature in Ad-hoc Netzwerken sicherer als verbindungsorientierte Verfahren

Ende der Präsentation

- Fragen?