

testen. Von Windows aus ist der Server unter 192.168.0.40 erreichbar. Besonders bei der Entwicklung von Java EE-Anwendungen könnte diese Vorgehensweise von Vorteil sein.

Zwar ist die Abschottung zwischen Wirts- und Gastsystem nicht so radikal wie bei einer Emulatorlösung, doch wirkt sich dies nur im Falle von größeren Instabilitäten aus. Ist eine Testumgebung erst einmal aufgebaut, wird man durch eine nur minimal ausgebremste Linux-Umgebung entschädigt. Laut Angaben der Colinux-Entwickler beträgt der Performanceverlust durch die erforderlichen Taskumschaltungen lediglich drei Prozent. Diese Angaben beziehen sich natürlich nur auf Anwendungen, die keine

grafische Oberfläche besitzen, wie zum Beispiel ein Apache-Webserver oder ein JBoss Application Server. Eine weitere Anwendungsmöglichkeit besteht im Datenaustausch zwischen Windows und Linux, wobei der Anstoß immer von Linux kommen muss. Da Samba ebenfalls bereits vorinstalliert ist, kann der Datenaustausch auch über Freigaben erfolgen. Gegenüber der Möglichkeit über COFS ergeben sich zwar erhebliche Geschwindigkeitseinbußen, doch sollte dieser Weg eingeschlagen werden, wenn höchste Ansprüche an die Datensicherheit gestellt werden. Vorkonfiguriert ist bereits standardmäßig eine Freigabe, die unter dem Namen „samba“ angesprochen werden kann. Eine weitere interessante Anwen-

dungsmöglichkeit ergibt sich aus der Verwendung des VNC Viewer im Eclipse-Plug-in. Auf diese Weise können Bildinhalte serverseitig virtuell ausgewertet werden. Der Assisi-Verlag entwickelt zurzeit einen SWT-Server, der sich zum Teil dieser Technik bedient, um OpenOffice.org und andere „Altlasten“ webfähig zu machen. Ein erster Prototyp lag der Redaktion vor. Als Firefox-Plug-in könnte sich dieser Ansatz zu einer ernsthaften Alternative zu AJAX entwickeln.

Ramin Assisi (Assisi-Verlag)

■ Links & Literatur

- [1] www.colinux.org
- [2] www.opensource.eu.com/colinux
- [3] www.assisipublishing.com

XML Security Plug-In

XML-Sicherheit mit Eclipse verstehen und anwenden

Seit nunmehr gut vier Jahren sind die Empfehlungen des World Wide Web Consortium zu den digitalen Signaturen und der Verschlüsselung mit XML verfügbar. Deren Verbreitung und Verwendung zu fördern hat sich das XML Security-Plug-in zum Ziel gesetzt. Anwender sollen mit dem Plug-in umfassende theoretische Kenntnisse über die Signierung und Verschlüsselung mit XML erlangen. Gleichzeitig stellt das Plug-in ein praktisches und einfach zu bedienendes Tool zum Ausprobieren und Anwenden der umfangreichen W3C-Empfehlungen zur Verfügung.

Das XML Security Plug-In ist ein vollständig frei verfügbares E-Learning-Plug-in für Eclipse 3.1 (für Eclipse 3.0 steht eine ältere und nicht mehr weiterentwickelte Version des Plug-ins zur Verfügung). Im Vordergrund des XML Security Plug-In stehen die praktische Anwendung und das Experimentieren mit den vielfältigen Möglichkeiten der XML-Sicherheit: Beliebige XML-Dokumente können vom Anwender kanonisiert, digital signiert, verifiziert sowie ver- und entschlüsselt werden.

Um möglichst viele von den Benutzern anzusprechen, sind die beim interessierten Anwender erwarteten Voraussetzungen gering: Neben einigen Erfahrungen im Bereich der Kryptographie und natürlich mit XML werden keine weiteren Kenntnisse benötigt. Vorkenntnisse in der XML-Sicherheit sind nicht notwendig.

Die Installation erfolgt – typisch für Eclipse – wahlweise über ein downloadbares Zip-Archiv von der Website [1] oder alternativ über die zugehörige Eclipse-Update-Site [2]. Als Implementierung der XML-Sicherheit verwendet das Plug-in das umfangreiche Open-Source-API Apache XML Security in der jeweils aktuellsten Version [3]. Diese ist im Plug-in enthalten und wird ganz automatisch mitinstalliert. Softwareseitig werden daher nur noch Java 5 und Eclipse 3.1.x benötigt.

Nach der Installation erweitert das Plug-in das Kontextmenü von diversen Eclipse-(XML-)Editoren (z.B. XML-Buddy [4]) sowie den Navigator und Package-Explorer um das Untermenü *XML Security*. In diesem findet der Anwender

zentral an einer Stelle sämtliche Funktionen des Plug-ins zum Kanonisieren, Signieren, Verifizieren sowie Ver- und Entschlüsseln.

Komponenten des Plug-ins

Ganz im Sinne einer Lernsoftware liegt das Ziel des Plug-ins darin, dem Anwender die größtmöglichen Freiheiten zu lassen. Das bedeutet, dass in den Assistenten so viele Einstellungen wie möglich vom Anwender selbst vorgenommen werden müssen. Schritt für Schritt klicken Sie sich so durch die Generierung einer digitalen Signatur oder durch die Verschlüsselung eines XML-Dokuments. Das XML Security Plug-In besteht dazu aus fünf Komponenten, mit denen alle Möglichkeiten der XML-Sicherheit abgebildet werden sollen (Abb. 1).

Die kleinste Komponente dient der Kanonisierung. Die Kanonisierung führt zu einem normalisierten XML-Dokument. Beispielsweise wird das XML-Dokument in UTF-8 kodiert, und Attribute werden alphabetisch sortiert. Normalerweise ist die Kanonisierung ein Vorgang, der bei einer digitalen Signatur automa-

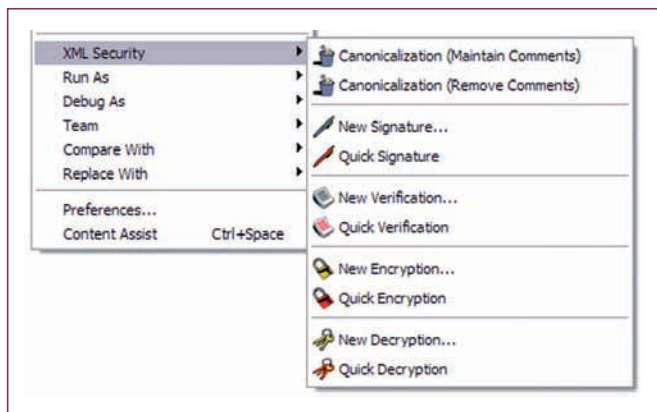


Abb. 1: Das Kontextmenü des XML Security Plug-In

tisch im Hintergrund ausgeführt wird. Die Verfügbarkeit als eigener Menüpunkt soll dem Anwender verdeutlichen, was dabei mit einem XML-Dokument passiert und was sich hinter diesem Begriff verbirgt.

Bei den digitalen Signaturen sowie der Ver- und Entschlüsselung werden die Anwender aufgrund der Komplexität der

ID für die Signatur bzw. Verschlüsselung. Damit wird die Identifikation bei der Verifizierung und bei der Entschlüsselung erleichtert.

Der Assistent zur Entschlüsselung ist einfacher aufgebaut und erfordert lediglich die Angabe der Schlüsseldatei, des verwendeten Algorithmus sowie die Auswahl der Verschlüsselung. Die Verifizierung erfolgt über eine eigene View, die XML Digital Signatures View. In dieser werden alle im XML-Dokument enthaltenen digitalen Signaturen samt Status (gültig oder ungültig) aufgelistet. Ein Doppelklick auf eine Signatur (oder auf das Icon PROPERTIES) öffnet ein Dialogfeld mit weiteren Informationen zur gewählten Signatur.

Empfehlungen und den daraus folgenden zahlreichen Kombinationsmöglichkeiten von jeweils eigenen Assistenten unterstützt. Bei den digitalen Signaturen und der Verschlüsselung bestehen die Assistenten aus mehreren Seiten. Hier gilt es u.a. auszuwählen, was gesichert werden soll (das gesamte XML-Dokument, eine Textmarkierung oder ein durch XPath spezifiziertes Dokumentfragment), welche Algorithmen dabei verwendet werden sollen und welche speziellen weiteren Einstellungen, wie beispielsweise die zu verwendende Signaturvariante, aktiviert werden müssen. Kurze Hinweise in allen Assistenten unterstützen den Anwender dabei beim Ausfüllen. Nach der Eingabe aller erforderlichen Informationen werden die gewählte Aktion durchgeführt und das XML-Dokument signiert oder verschlüsselt. Empfehlenswert ist stets die Angabe einer optionalen

Neben den assistentengestützten Varianten zum Sichern von XML-Dokumenten können erfahrene Anwender nahezu alle Funktionen des Plug-ins auch mit (fast) nur einem Klick mit den so genannten Quick Functions durchführen. Quick Functions stehen für die Operationen Signieren, Verifizieren sowie Ver- und Entschlüsseln zur Verfügung. Dabei legt der Anwender zunächst in den Preferences fest, welche Einstellungen beim Signieren oder Verschlüsseln verwendet werden sollen. Fast alle Informationen können hier vorab eingegeben werden, lediglich sicherheitskritische Angaben wie Passwörter müssen bei jedem Aufruf angegeben werden. Ein Klick auf QUICK ENCRYPTION verschlüsselt so z.B. ein XML-Dokument mit einem Klick, die Schritt-für-Schritt-Eingabe über einen der Assistenten entfällt.

Um dem Anwender auch die theoretischen Kenntnisse zu vermitteln, enthält

das XML Security Plug-In eine umfangreiche deutschsprachige Online-Hilfe, den XML Security Guide. Dieser ist in zwei Bereiche aufgeteilt: Der erste Teil, XML-Sicherheit, enthält umfassende Erläuterungen zu den W3C-Empfehlungen zur XML-Sicherheit. Der Anwender erfährt hier beispielsweise, wie eine digitale Signatur mit XML aufgebaut ist, welche Elemente sie enthält und was die Funktion der verschiedenen Elemente und Attribute ist. Enthalten sind außerdem kurze Beschreibungen verwandter Empfehlungen wie die Canonicalization oder das Basic Security Profile. Der zweite Teil der Hilfe, Plug-in genannt, beschreibt die Funktionsweise und Verwendung des XML Security Plug-In. Schritt für Schritt wird der Anwender hier durch die Erstellung einer digitalen Signatur und anderen Funktionen des XML Security Plug-In geleitet.

Als Ergänzung zur Online-Hilfe stehen mit der aktuellen Version 1.5 des XML Security Plug-In verschiedene mehrsprachige Cheat Sheets zur Verfügung, die Einsteigern beim ersten Sichern von XML-Dokumenten und den ersten Versuchen mit dem Plug-in hilfreich zur Seite stehen.

Fazit

Das XML Security Plug-In stellt einen praktisch orientierten Einstieg in die XML-Sicherheit dar. Neben Entwicklern können auch Lernende und Lehrende die Grundlagen der XML-Sicherheit erlernen und in ihrer Eclipse-Plattform gleichzeitig praktisch ausprobieren. Das Plug-in wird ständig weiterentwickelt und gepflegt und steht allen Nutzern kostenlos zur Verfügung. Auf der Webseite zum Plug-in [1] finden sich neben der aktuellsten Version des Plug-ins umfangreiche Informationen zur XML-Sicherheit und zum Plug-in, ein Forum und vieles weitere mehr.

Domimik Shadow (Trivadis)

Links & Literatur

- [1] www.xml-sicherheit.de
- [2] www.xml-sicherheit.de/update
- [3] xml.apache.org/security
- [4] www.xmlbuddy.com