Brücken schlagen

Vier Schritte, mit denen eine PKI auch über Organisationsgrenzen hinweg nutzbar gemacht wird

Schon zur Jahrtausendwende wurde angekündigt, Public-Key-Systeme seien auf dem Vormarsch. Vor allem große Firmen begannen auf die mit einer Public Key-Infrastruktur (PKI) verbundenen Möglichkeiten der Authentifizierung und Signatur von Nachrichten und Dokumenten zu setzen. Doch ist die zugehörige Technologie heute und in diesem Sinne auch im Alltag der Kommunikation zwischen verschiedenen Organisationen angekommen?

Marieke Petersohn, TeleTrusT – Bundesverband IT-Sicherheit e. V.

Die Antwort auf die eingangs gestellte Frage lautet: Ja und Nein. Dies ist einerseits von der Branche und der möglichen Beeinflussung großer Firmen abhängig: Diese verlangen oftmals von ihren Kommunikationspartnern, dass PKI-Zertifikate für die Kommunikation und Authentifizierung eingesetzt werden. Auch gesetzlich oder im Rahmen elektronischer Ausschreibungsverfahren und bei der Kommunikation mit Behörden werden entsprechende Verfahren verlangt. Der Einsatz von SSL-Zertifikaten im Web ist zum Beispiel aus dem Alltag nicht mehr wegzudenken.

Trotzdem kann man noch nicht davon sprechen, dass die alltägliche geschäftliche Kommunikation zwischen verschiedensten Organisationen – zum Beispiel mittels PKI – ausreichend geschützt würde. Heute hört man sogar, dass die Verbreitung von solchen Schutzmaßnahmen nachgelassen hat.

Hindernisse

Was sind die Gründe dafür? PKI bringt für den Einsatz über Organisationsgrenzen hinweg Hürden mit sich, die offenbar als zu hoch eingeschätzt werden.

Vertrauen herstellen: Die Vertraulichkeit und Integrität der an externe Kommunikationspartner versendeten Daten hängen davon ab, wie sorgfältig dort kryptografische Schlüssel geschützt werden – beide Partner müssen daher die Lösung des Anderen beurteilen und prüfen. Dann kann das Vertrauen auch technisch, durch

zum Beispiel die Installation der Wurzelzertifikate der Partner-PKI, hergestellt werden.

_____ Zertifikate finden und bereitstellen: Für die Prüfung von Signaturen und das Verschlüsseln ist ein Zugriff auf die öffentlichen Schlüssel des Partners notwendig. Dies kann über einen Abruf im Verzeichnisdienst erfolgen oder nach manuellem Austausch der öffentlichen Zertifikate, zum Beispiel über signierte E-Mails.

_____ Einrichtung und Pflege: Diese ersten beiden Schritte sind für alle Partner und auf beiden Seiten notwendig. Das bedeutet für die Einrichtung und Pflege je nach Organisationsaufbau und eingesetzter Technik enormen Aufwand.

_____ Weiterentwicklung: PKI ist noch immer ein Nischenthema. Als Betreiber einer solchen Infrastruktur ist man auf direkten Austausch mit anderen Experten angewiesen, um über Weiterentwicklungen nachdenken und entscheiden zu können.

Lösungsansätze

Bereits seit 2001 beschäftigt sich TeleTrusT gemeinsam mit Experten des vom Verband getragenen Projekts „TeleTrusT European Bridge CA“ (EBCA) mit diesen Hürden. Die folgenden Schritte können nach Erfahrung aus diesem Umfeld die Hürden wesentlich verringern:

Teil eines zentralen Vertrauensnetzwerks sein

Erfüllt eine PKI bestimmte Mindestrichtlinien, kann man es sich zunutze machen, dass es Vertrauensnetzwerke gibt, die dem jeweiligen Partner die Beurteilung der Vertrauenswürdigkeit erleichtern. Ein Beispiel dafür ist das CA-Browser-Forum, welches aufwändig bestimmt, welche Wurzelzertifikate in Browser-Zertifikatsspeichern abgelegt werden. Ein weiterer Ansatz sind Bridge-CAs, die als Vertrauensvermittler fungieren und so die Beurteilung durch die Kommunikationspartner erleichtern. Sie sind herstellerunabhängig und besonders für Betreiber einer unternehmenseigenen PKI, also ein nicht-kommerzielles Trustcenter, geeignet. Die „European Bridge CA“ von TeleTrusT gehört zu diesen Initiativen.

Zertifikate leicht zugänglich machen

Nachdem eine Vertrauensbasis geschaffen wurde, ist eine einfache Methode notwendig, mit der die öffentlichen Schlüssel verfügbar gemacht werden können. Dazu können Organisationen ihren Verzeichnisdienst öffentlich zugänglich machen – dies muss jedoch auch allen Kommunikationspartnern bekannt sein. Dazu lassen sich bekannte Zugriffspunkte wie Proxys oder Gateways nutzen, über die Verzeichnisdienste gleich mehrerer Organisationen erreichbar sind. So kann auch ausgenutzt werden, wenn dieser Zugang bereits vorinstalliert ist.

Dabei ist jedoch zu beachten, dass die Vertrauenswürdigkeit der angeschlossenen Partner auch wirklich sichergestellt ist. Die European Bridge CA stellt dies im Rahmen des EBCA-Verzeichnisdienstes durch die Verknüpfung mit der Vertrauensstellung (s. o.) sicher.

Erleichterung der Pflege durch Zentralisierung

Ist man Teil eines Vertrauensnetzwerks und zum Beispiel über einen externen Verzeichnisdienst erreichbar, muss man Änderungen nur an einer zentralen Stelle durchführen. Damit wird die Einrichtung und Pflege wesentlich erleichtert.

Weiterentwicklung durch Wissensaustausch

In Expertengremien kann ein regelmäßiger und direkter Austausch mit anderen PKI-Experten erfolgen. Als Teil eines Netzwerks wie zum Beispiel der EBCA ist so auch die Diskussion aktueller Herausforderungen möglich.

Fazit

Der Nutzen von Zusammenschlüssen und Netzwerken ist besonders im PKI-Umfeld von der Größe der Initiative und der aktiven Mitarbeit abhängig. Der TeleTrusT möchte dazu aufrufen, sich seinem Vertrauensnetzwerk anzuschließen und so die sichere Kommunikation auch zwischen Organisationen zu fördern. Besuchen Sie im Rahmen der it-sa 2014 am 08. Oktober ab 11 Uhr die TeleTrusT-Veranstaltung im Auditorium und diskutieren Sie mit oder kommen Sie im Nachgang zum TeleTrusT-Stand (Halle 12, Stand 744)! ■

Der TeleTrusT – Bundesverband der IT-Sicherheit e. V. hat zurzeit 236 Mitglieder. Eine aktuelle Liste finden Sie auf www.teletrust.de/ueber-teletrust/mitglieder/