

# Computerworld Dossier PK-Infrastruktur

## An der Infrastruktur führt kein Weg vorbei

**Realisierung** Die Einführung PKI-basierter Technologien ist mit technischen und organisatorischen Aufwänden verbunden und verlangt spezifisches Fachwissen. Erfahrungen zeigen, dass Prozesse sicherer und effizienter umgesetzt werden können.

René Eberhard\*

Eine Public-Key-Infrastruktur (PKI) ist die Grundlage für die elektronische Umsetzung von Strategien und Geschäftsprozessen im Umfeld von Staat, natürlichen oder juristischen Personen. Sie ist die Technologie der Zukunft, auch wenn sie heute nur in bescheidenem Umfang eingesetzt wird. Gefragt sind pragmatische Lösungen, die sich auf die Umsetzung spezifischer Geschäftsprozesse fokussieren. Eines ist jedoch sicher: Unternehmen und öffentliche Verwaltungen können sich den Gesetzen des elektronischen Informationszeitalters nicht entziehen. Sie werden sich in absehbarer Zukunft mit PKI-gestützten Anwendungen und Lösungen befassen müssen.

Lösungen des E-Business und E-Government stellen hohe Anforderungen an die Sicherheit und Verfügbarkeit der Anwendungen und Kommunikationsdienste. Während die Verfügbarkeit über ein Systemdesign mit redundanten Komponenten sichergestellt werden kann, muss die Sicherheit, insbesondere die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit der Daten, über moderne kryptografische Verfahren sichergestellt werden. Hier kommen elektronische Signaturen und entsprechende Zertifikate zum Einsatz.

### Elektronische Identität

Im Internet muss grundsätzlich jede Aussage eines Kommunikationspartners zu seiner Identität als unsicher eingestuft werden. Dieser Umstand ist in der öffentlich zugänglichen Infrastruktur des Internets begründet. Es ist also eine vertrauenswürdige dritte Partei erforderlich, welche die Identität der Kommunikationspartner zuverlässig bescheinigt, ohne selbst an der Kommunikation teilzunehmen. Zertifikate entsprechen einer elektronischen Identität und binden eine Entität an einen kryptografischen Schlüssel. Sie werden von privaten oder öffentlichen Betreibern von Public-Key-Infrastrukturen, sogenannten Zertifizierungsdiensteanbietern, ausgegeben.

Eine PKI besteht grundsätzlich aus einer Zertifizierungsstelle (CA), einer Registrierungsstelle (RA) und einem Verzeichnisdienst. Die Zertifizierungsstelle stellt die elektronischen Zertifikate aus und verwaltet gegebenenfalls die kryptografischen Schlüsselpaare. Die Registrierungsstelle ist verantwortlich für die Identifikation der Teilnehmer gemäss den jeweils geltenden Zertifizierungsrichtlinien. Über den Verzeichnisdienst können die Benutzer die Zertifikate der jeweiligen Kommunikationspartner sowie die Sperlisten der Zertifizierungsstelle abfragen.

Das E-Business in der Schweiz kann sich auf Gesetze und Verordnungen abstützen. Der Fokus liegt dabei auf



den verarbeitungsorientierten Prozessen wie die Aufbewahrung und Archivierung von geschäftlich relevanten Daten oder die Geltendmachung des Vorsteuerabzuges basierend auf elektronischen Rechnungen. Die gesetzlichen Rahmenbedingungen eilen hier der technischen Entwicklung voraus. Ein Grund dafür war das Fehlen eines Zertifizierungsdiensteanbieters in der Schweiz, der Zertifikate ausgeben konnte, welche den gesetzlichen Anforderungen genügen.

### Elektronische Signatur

Seit Dezember 2002 ist es für in der Schweiz ansässige Unternehmen möglich, elektronisch signierte Rechnungen zu verarbeiten, welche von der Eidgenössischen Steuerverwaltung (ESTV) anerkannt werden. Die dazu notwendigen Zertifikate werden von TC Trustcenter ausgegeben, einer in Hamburg domizilierten und in Deutschland akkreditierten Zertifizierungsdiensteanbieterin. Bisher mussten Rechnungen für die Zulassung zum Vorsteuerabzug in Papierform vorliegen. Dadurch waren Unternehmen gezwungen, eine aufwändige Archivierung von Dokumenten sicherzustellen.

Die elektronische Signatur ermöglicht beträchtliche Einsparungen bei den Übermittlungskosten und Archivierungskosten. Mit diesem Schritt setzte die ESTV ein positives Signal im Bereich der elektronischen Geschäftsabwicklung, welches von den Unternehmen umgehend aufgenommen wurde. Verschiedene Lösungen im Umfeld der elektronischen Rechnungsstellung oder in der elektronischen Aufbewahrung von Geschäftsbüchern werden heute bereits angewendet.

### Positiver Impuls

Es ist zu hoffen, dass sich der positive Impuls der ESTV auch auf andere Bereiche der elektronischen Datenverarbeitung überträgt. Durch die zunehmende Vernetzung der Systeme wer-

den Angriffe auf IT-Systeme ortsunabhängig und können durch externe oder interne Personen mit meist geringen technischen Mitteln durchgeführt werden. Viele Unternehmen und Organisationen unterschätzen diese Gefahren. So werden heute beispielsweise immer noch interne oder vertrauliche Informationen über unsichere E-Mails ausgetauscht, was einem Versenden vertraulicher Informationen auf einer Postkarte ohne Umschlag gleichkommt.

PKI-Technologien bieten ein hohes Mass an Sicherheit und können in vielen Bereichen der elektronischen Datenverarbeitung eingesetzt werden. Neben der Sicherung der elektronischen Kommunikation werden Zertifikate auch eingesetzt, um Daten sicher zu archivieren oder moderne Zugriffskonzepte in heterogenen IT-Infrastrukturen umzusetzen. Immer mehr Anwendungen im Desktop-, Infrastruktur- und Applikationsbereich unterstützen standardmässig Zertifikate. Andere Applikationen können mit Hilfe moderner PKI-Frameworks mit geringem Aufwand angepasst oder erweitert werden.

### Zertifikate erhältlich

Jedes Unternehmen und jede öffentliche Verwaltung kann eine eigene Public-Key-Infrastruktur aufbauen und Zertifikate ausgeben. Die Investitionen sind abhängig von einer Vielzahl technischer, organisatorischer und rechtlicher Parameter und werden meist unterschätzt. Grundsätzlich lohnt sich der Aufbau einer eigenen PKI nur für grössere Firmen. Daneben besteht die Möglichkeit, Zertifikate von öffentlichen Zertifizierungsdiensteanbietern, wie etwa TC Trustcenter, zu beziehen. Die Anforderungen an einen solchen Anbieter bezüglich Registrierungsprozess, Verwaltung und Publikation von Zertifikaten und Sperlisten sind abhängig vom jeweiligen Einsatzzweck.

Ein öffentlicher Anbieter von Zertifikaten muss aber nachweisen können,

dass die technischen und organisatorischen Prozesse gemäss den jeweiligen Zertifizierungsrichtlinien ablaufen. Im weiteren muss er garantieren, dass die PKI hochverfügbar in einem IT-Hochsicherheitszentrum steht und nur von speziell geschultem Personal mit entsprechenden Zugriffsrechten bedient wird. Ausserdem sollte der Anbieter nachweisen können, dass er über einen nachhaltigen Businessplan und ausreichende Finanzmittel verfügt, um langfristig die Geschäftstätigkeit weiterzuführen.

### Noch fehlen Anbieter

Um den Rollout der Zertifikate oder die Kommunikation mit Partnern ausserhalb des eigenen Unternehmens zu vereinfachen, sollten die Root-Zertifikate des Anbieters bereits in den gängigen Browsern und Applikationen vorinstalliert sein. Kein Anbieter von öffentlichen Zertifikaten in der Schweiz erfüllt derzeit alle oben genannten Anforderungen. Unternehmen und andere interessierte Kreise haben aber die Möglichkeit, Zertifikate bei ausländischen Zertifizierungsdiensteanbietern zu beantragen. Die Registrierung von Personen oder sogenannten Corporate PKI-Administratoren kann oft sehr einfach über Schweizer Partner erfolgen. Corporate PKI-Administratoren können Personen innerhalb des Unternehmens eigenständig registrieren. Die Verwaltung von Corporate Zertifikaten kann den jeweiligen Anforderungen des Unternehmens angepasst werden.

Eine Public-Key-Infrastruktur ist einer der wichtigsten Mosaiksteine in einem umfassenden elektronischen Geschäftsprozess. Mit der Verfügbarkeit von Zertifikaten können sich die Unternehmen nun den wirklichen Herausforderungen des E-Business stellen. Denn eine optimale Steigerung der Wertschöpfung kann nur durch möglichst voll elektronische und damit automatisierbare Geschäftsprozesse erreicht werden.

### Dossier: PK-Infrastruktur

## Anwendungen entwickeln sich

Fredy Haag

Als die Telekurs der Schweizer Zertifizierungsstelle Swisskey im Mai 2001 den Geldhahn zudrehte, hatte sie bis dahin rund 25 Millionen Franken in den Aufbau einer Public Key Infrastructure (PKI) investiert. Ökonomische Gründe waren für die Einstellung verantwortlich, liessen die Banken als Träger der Telekurs verlauten. Anschliessend herrschte während knapp vier Monaten Funkstille. Schliesslich schickten sich drei Firmen an, Swisskey zu beerben: Wisekey, Swissign und Swisscert.

Weil der Betrieb einer Zertifizierungsstelle als autonomes Profitcenter, wie der Fall Swisskey zeigte, kein lukratives Geschäft ist, wurde auch die Forderung nach einem Engagement des Bundes laut. Der Bund als Herausgeber von Zertifikaten ist naheliegend, da er die natürliche und oberste Autorität ist, Identitäten festzustellen. Und dank den Einwohnerkontrollämtern in den Gemeinden, den kantonalen Passbüros sowie den flächendeckenden Poststellen ist er bereits im Besitz einer idealen Infrastruktur für die landesweite Verteilung von digitalen Identitäten.

Der Bund hat ohnehin ein grosses Interesse an einer gesamtschweizerischen Infrastruktur. Denn die laufenden E-Government-Projekte wie Gütecheck und E-Voting benötigen in späteren Phasen allesamt eine Public-Key-Infrastruktur.

Artikel in dieser Ausgabe:

- An der Infrastruktur führt kein Weg vorbei, Seite 8,
- Die digitale Identität setzt zum Sprung an, Seite 10,
- PKI leistet Schützenhilfe für Webservices, Seite 10.

\*René Eberhard, Geschäftsführer von Keyon. Keyon ist spezialisiert auf E-Business- und IT-Security-Lösungen, Partner von TC Trustcenter.