

DIGITALE SIGNATUR IN DER PRAXIS ODER WIE WIRD AUS EINEM ZERTIFIKAT EINE (SICHERE) SIGNATUR?

Der folgende Beitrag befaßt sich besonders mit dem Zusammenspiel von Zertifizierungsdiensteanbieter (ZDA) einerseits und (Web-)Applikationsbetreiber andererseits.

Kein elektronischer Datenverkehr ohne Anwendungen!

Seit 1.1.2000 gibt es in Österreich ein Signaturgesetz und damit verbunden auch bald gesetzeskonforme Zertifikate. Aber wie schaut die Situation bei den Anwendungen aus?

Die Interessenlage der Beteiligten stellt sich wie folgt dar: Das Hauptaugenmerk des Webapplikationsbetreibers ist wohl darauf gerichtet, jene Anwendungen zu entwickeln, die eine gewisse Marktdurchdringung ermöglichen sowie den Sicherheitsaspekt berücksichtigen. Der Benutzer wiederum wird wohl erst dann bereit sein, ein Zertifikat zu erwerben, wenn er dieses auch einsetzen kann. Nichts leichter als das, denn: Durch das Forcieren des Entstehens von Webapplikationen ergibt sich eine klassische „win win“-Situation für alle Beteiligten, d.h. sowohl für den Betreiber von Anwendungen sowie für den ZDA einerseits als auch für den Benutzer andererseits. Je mehr Anwendungen existieren, um so schneller wird sich der zertifikatsbasierte Teil des Elektronischen Geschäfts- bzw. Rechtsverkehrs weiterentwickeln. Wenn man sich beispielsweise mit seinem Zertifikat nicht nur in das Extranet der Wirtschaftskammer einloggen kann, sondern damit auch die Zugangskontrolle im eigenen Unternehmen geregelt wird, wenn einem gleichzeitig ermöglicht wird, Anträge bei den Sozialversicherungsanstalten sowie die Einkommensteuererklärung beim Finanzamt einzubringen und man abends noch „Electronic Banking“ betreiben kann und sich außerdem noch die neueste Software auf sicherem Wege auf seinen Rechner laden kann, dann steht wohl einem Erfolg dieser Technologie nichts mehr im Wege.

Die Basis: Das Zertifikat

Der „kleinste gemeinsame Nenner“ und damit die Ausgangsposition in Zusammenhang mit digitalen Signaturen und in weiterer Folge von Applikationen im E-Commerce bzw. E-Government ist immer ein Zertifikat, das in der sichersten, d.h. signaturgesetzkonformen Variante ein „qualifiziertes“ Zertifikat ist und folgendes sicherstellt:

- Die sichere Überprüfung der Identität des (zukünftigen) Zertifikatsinhabers (Signator),

- die sichere Schlüsselgenerierung und -zuordnung (einer Person wird ein eindeutiger mathematischer Schlüssel, ein public key, nachvollziehbar zugeordnet),
- der zum öffentlichen Schlüssel zugehörige private Schlüssel wird sicher (z.B. auf einer im Besitz des Signators befindlichen Smartcard) verwahrt.

Wie wird nun aus einem Zertifikat eine Signatur?

Schaut man sich eine typische benutzerseitige Public Key Infrastructure (PKI) an, also jene „technische Landschaft“, die notwendig ist, um auf Basis der derzeitigen Technologie (asymmetrische Verschlüsselung) ein Zertifikat in einer Webapplikation einsetzen zu können, so hat diese folgende technische Komponenten:

- (qualifiziertes) Zertifikat,
- Smartcard,
- Smartcardleser,
- Krypto-Library (jene technische Einheit, die beispielsweise die Ver-/Entschlüsselung durchführt),
- SecureViewer (jene technische Einheit, die sicherstellt, daß man nur das signiert, was man auch tatsächlich am Bildschirm sieht).
- Darüber hinaus wird manchmal gefordert, daß auch beispielsweise das Betriebssystem ein sicheres und daher evaluiertes sein muß.

Wenn man nun die sogenannte „sichere elektronische Signatur“ erstellen möchte (und nur sie kann laut Signaturgesetz die eigenhändige Unterschrift ersetzen), so sind neben einem qualifizierten Zertifikat auch die vorhin genannten PKI-Komponenten, und zwar in evaluierter Form, zu verwenden. Haben wir es mit einem Benutzer zu tun, der von seinem PC aus eine sichere Signatur abschicken möchte, so bietet die A-Trust ein Softwarepaket an, nämlich „A-Trust Client“, das die aufgezählten technischen Komponenten enthält. Handelt es sich hingegen um den Hersteller einer Webapplikation, der eine Dienstleistung PKI-fähig machen möchte, so muß sich dieser überlegen, wo genau die Schnittstelle zwischen Zertifikat und Applikation zu sein hat; der „A-Trust Client“ verfügt beispielsweise standardmäßig über ein Application Programming Interface (API). Davon abhängig ist dann auch der Einsatz der PKI-Komponenten. A-Trust bietet mit seinem Expertenteam dem Projektkunden auf alle Fälle die Beratungsleistung an, alle für die Webapplikation notwendigen Bereiche gemeinsam zu erarbeiten und das Projekt in die Realisierungsphase zu führen. Im Idealfall werden in einer

Teststellung erste praktische Erfahrungen der jeweiligen Applikation gesammelt.

Bei den bereits durchgeführten Projektgesprächen haben sich dabei insbesondere folgende zwei Bereiche herauskristallisiert, auf die seitens des Projektkunden das Hauptaugenmerk zu legen ist:

- 1) Was sind eigentlich meine genauen Anforderungen an die Applikation, d.h. wer ist mein Benutzerkreis? Sind diese User mit bestimmten „Rechten“ ausgestattet wie z.B. Beruf? Wenn ja, wer vergibt bzw. widerruft diese? Gibt es auch abgestufte Berechtigungen?
Die Beantwortung dieses Fragenkomplexes ist relevant für den Zertifikatsinhalt, denn nur auf diesen stützt man sich in der Applikation.
- 2) In welcher Form, Intensität und an welcher Stelle im Datenfluß meiner Webapplikation werden die folgenden kryptographischen Komponenten eingesetzt?
 - **Authentifizierung**
In welchem Stadium benötige ich sie und wie sicher sollte es sein? Wie und woran erkenne ich den Zugriffsberechtigten? Welches Zertifikatsfeld ist dabei relevant?
 - **Vertraulichkeit**
Welche Bereiche möchte ich wann im Datenfluß ver-/entschlüsseln und welche Sicherheitsstufe/Schlüssellänge/Technologie verwende ich dabei? Wo sind gegebenenfalls sensible Daten in meiner Applikation?
 - **Signatur**
Benötige ich die sichere elektronische Signatur in meiner Applikation tatsächlich? Aufgrund welcher Anforderungen ergibt sie sich (technisch, organisatorisch oder rechtlich)? Auf welchen Zertifikatsinhalt stützt sich die Signatur?

Es sei darauf hingewiesen, daß der **Zahlungsverkehr** mit **keiner** dieser 3 Komponenten elektronisch abgewickelt werden kann. Dafür stehen Anwendungen wie beispielsweise Secure Electronic Transaction (SET) zur Verfügung, die zwar auch Zertifikate verwenden, allerdings anders aufgebaut sind. Weiters ist darauf aufmerksam zu machen, daß die Komponente der **Anonymität** ebenfalls grundsätzlich **kein** Bestandteil von Zertifikaten ist; schließlich geht es ja um elektronische Identitäten!

Faktor Zeit - ab wann sind sichere Webapplikationen möglich?

Die A-Trust stellt dazu fest, daß die für ein qualifiziertes Zertifikat notwendigen technischen Anforderungen derzeit gerade in europäischen Arbeitsgruppen ausgearbeitet werden, wobei eine Beschlußfassung Ende 2000 erfolgt sein wird. Erst dann wird die Industrie gewillt sein, die genannten Komponenten produzieren und evaluieren zu lassen. Ein qualifiziertes Zertifikat wird dann voraussichtlich im ersten Quartal 2001 verfügbar sein.

Webapplikationsseitig darf man den zeitlichen Aufwand keinesfalls unterschätzen. Eine Anwendung läßt sich nicht innerhalb von zwei oder drei Wochen realisieren, sondern nimmt eher - vom Konzept bis zur Realisierung und Systemintegration - einige Monate in Anspruch. Daher kann man mit den diesbezüglichen Projektgesprächen nicht früh genug beginnen. Wenn jeder der Beteiligten seine „Hausaufgaben“ macht, dann wird es die ersten sicheren Applikationen im zweiten Quartal 2001 geben.

Welche weiteren Maßnahmen wären hilfreich?

- **Öffentliche Einrichtungen**, also Behörden nach Signaturgesetz oder Initiativen wie „E-Business-Austria“ könnten folgenden wertvollen Beitrag leisten:
Für ein rasches Entstehen von Applikationen wäre eine **Liste** mit jenen **evaluierten PKI-Komponenten**, die eine sichere elektronische Signatur ermöglichen, hilfreich. Der Applikationsbetreiber bzw. -entwickler sollte diese Liste konsultieren können und im Idealfall auch die Information bekommen, welche PKI-Komponente in welcher Version mit welcher kompatibel ist. Da hinter einer solchen Liste ein gewisses Maß an Qualitätsmanagement und Administration steht - es wären unterschiedliche Softwarepakete mit allen Integrationen und Produktabnahmen laufend zu überwachen - kann diese Aufgabe unmöglich ein Privater übernehmen. Von einer derartigen Liste könnte nicht nur der Applikationsbetreiber und der ZDA einen Vorteil ziehen, sondern es wäre auch ein wichtiger Schritt für eine positive Weiterentwicklung des E-Commerce und E-Government gesetzt. Letztendlich könnte vor allem die breite Öffentlichkeit profitieren, zumal ein solche Liste das Durchdringen der elektronischen Welt mit Anwendungen beschleunigen würde.
- **Applikationsbetreiber** und **ZDA's** wie z.B. die A-Trust müssen darüber hinaus neben den oben beschriebenen Aufgaben intensive Bewußtseinsbildung betreiben.

Ausblick

Trendmäßig geht man aus heutiger Sicht davon aus, daß die ersten Anwendungen im Behörden- und Bankenbereich starten werden, sich in weiterer Folge auf die Unternehmen ausbreiten werden und in einem dritten Schritt auch die Privaten einbinden werden.

Wer eine einschlägige Applikation entwickeln und betreiben möchte, kontaktiert am besten die Experten der A-Trust unter office@a-trust.at. Auf jeden Fall sollten Sie die Website der A-Trust besuchen: www.a-trust.at.

Christoph Reissner, A-Trust GmbH, Wien, Jänner 2001