EU-Direktive: Elektronische Rechnungen sind jenen in Papierform gleichgestellt

Pfaffhausen, 13. Juli 2010: Heute ist ein Tag der Freude. Wer hätte gedacht, dass wir die Signaturlösungen je wieder aus den europäischen Gesetzen herauskriegen? Und wenn Sie nun eher «Bahnhof» verstehen, dann lesen Sie trotzdem weiter, der nachfolgende Blog soll kurz zusammenfassen, um was es ging und warum der heutige Entscheid des EU-Ministerrates ein weiser Entscheid ist. Wer mehr zum Entscheid selber lesen möchte, findet bei **heise.de eine Zusammenfassung.**

Darum sind Signaturlösungen bei Rechnungen sinn- und zwecklos

Im Zeitalter der Informatik werden zunehmend alle Unternehmensinformationen digital gespeichert. Vorbei die Zeit, als eine jede Firma riesige Papierberge in Archiven führt(e). Hier setzt ein Dokumenten-Management-System (DMS) ein. Ganz egal, ob ein Beleg in Papierform oder als Computerdatei vorliegt, mit einer DMS-Lösung werden sämtliche Informationen elektronisch geführt.

An sich führt ein DMS-System dazu, dass die Informationen sicherer geführt bzw. «gelagert» werden können. Einerseits können die Informationen ohne nennenswerten Aufwand in mehrfacher Ausführung gespeichert werden, auf der anderen Seite können Informationen automatisiert abgelegt werden. Allerdings, **elektronisch gespeicherte Informationen können von «Natur» (d.h. systembedingt) jederzeit geändert werden.** Bei entsprechendem «Vorsatz» können mit einigen Zeilen Programmcode die Bücher elegant «gefälscht» werden.

Die Signaturlösungen waren ursprünglich dazu gedacht, dass die Authentizität (Echtheit) der Informationen zweifelsfrei auch nach langer Zeit festgestellt werden kann. Dazu werden sogenannte Schlüsseldateien erstellt. Meist wird mit einem **privaten Schlüssel (diese Datei darf nicht weitergegeben werden) und einem öffentlichen Pendant (Public Key) gearbeitet.** Der öffentliche Teil wird zusammen mit den zu verifizierenden Informationen (z.B. Rechnungen) weitergegeben. Der

öffentliche Teil des Schlüssels dient dazu, festzustellen, ob eine mit einem privaten Schlüssel erstellte Datei in der Zwischenzeit nicht geändert wurde. Ohne den privaten Schlüssel kann keine Modifikation der Daten erfolgen bzw. der öffentliche Schlüssel würde dann nicht mehr «passen».

Soweit die Theorie. In der Praxis gestaltet sich vieles weit schwieriger. So ist z.B. ein **privater Schlüssel selber beliebig kopierbar.** Wer nicht auf «seinen» privaten Schlüssel aufpasst, sieht sich mit der Problematik konfrontiert, dass ein jeder Dritter, der den privaten Schlüssel «kopieren» konnte, ab diesem Zeitpunkt die gleiche «Identität» einnehmen kann. Eine **weitere Problematik besteht darin, dass der private Schlüssel mit «brute-force» erraten wird.** D.h. es werden systematisch alle möglichen privaten Schlüssel erstellt, wobei nach jedem Versuch getestet wird, ob der öffentliche Schlüssel passt. Ist dies der Fall, wurde der private Schlüssel erraten.

Je nachdem wie lange ein Schlüssel ist, muss ein massiv erhöhter Aufwand an Versuchen abgearbeitet werden, um den privaten Schlüssel zu erraten. Je länger der Schlüssel je höher der Rechenaufwand, um den Schlüssel zu «knacken». Allerdings können nicht beliebig lange Schlüssel festgelegt werden, das Berechnen der Signatur würde sonst zu lange dauern. Und weil gleichzeitig die Rechenkapazität der Computer ein jedes Jahr um Faktoren zunimmt, **gilt ein Schlüssel der heute erstellt wird, nur für eine bestimmte Dauer als sicher.** Meist werden daher entsprechende Schlüssel nur für ca. 1 bis 2 Jahre generiert. Vor Ablauf dieser Zeitspanne wird eine neue Signatur (mit einem neuen Schlüssel) über die Originaldatei(en) sowie die bisherigen (alten) Signaturen erstellt.

Und genau hier liegt das Problem. Dokumente, die während einer Lebensdauer von 10, 20 oder 30 Jahren verfügbar gehalten werden sollen, müssen fast alle Jahre wieder nachsigniert werden. Dadurch entstehen mit der Zeit viele wertlose (alte) Schlüssel, die aber gleichwohl archiviert werden müssen, damit die Authentizität rückverfolgt werden kann. Weiter muss die Identität des Schlüsselinhabers festgestellt werden können. Dies ist aber nur solange möglich, wie kein Dritter Zugang zum privaten Schlüssel erhält. Zudem gilt es beim Erstellen des Schlüssels zweifelsfrei festzustellen, ob der Berechtigte auch jener ist, für den er sich ausgibt.

Ich hätte kaum derart weit ausholen müssen, wenn das System einfach wäre. Und wäre das System einfach(er), so wäre es von den Unternehmen akzeptiert worden. Da dem aber nicht so ist, haben viele Unternehmen bislang einen grossen «Bogen» um Signaturlösungen gemacht und z.B. explizit darauf verzichtet, elektronische bzw. signierte Rechnungen zu erstellen. **Kurz gesagt, solange der Postversand einer Rechnung massiv kostengünstiger ist als die Infrastruktur zum Erstellen von signierten Rechnungen, ist es ganz einfach im Verhältnis nicht stimmig, es zu tun.** Alle entsprechend aufgewendeten Ressourcen sind etwas böse gesagt entweder hinausgeworfenes Geld oder müssen als Trial-and-Error-Versuche abgehandelt werden.

ArchivistaBox hat darauf verzichtet, Signaturlösungen je einzuführen

Als Anbieter eines DMS-Systems stellt sich immer wieder die Frage, ob und wann es sinnvoll ist, Trends und neue Funktionen in ein Produkt aufzunehmen. So stellen wir uns bei unseren Produkten bei jeder Funktion die Frage, wo der Nutzen liegt und zu welchem Preis wir den Mehrwert realisieren können. **Nur wenn wir einen Nutzen zu einem vernünftigen Preis (d.h. in erster Linie ohne Erhöhung der Preise) realisieren können, werden Sie ein neues Feature vorfinden.** Je höher der Mehrwert, je schneller die Realisierung.

Und ja, wir geben es zu, wir sind käuflich, d.h. ein Kunde kann jederzeit eine Funktion bei uns in Auftrag geben. Nicht käuflich sind wir allerdings darin, dass wir ein Feature von allgemeinem Nutzen nur einem bestimmten Kunden zur Verfügung stellen bzw. dass die übrigen Kunden nicht auch «mitprofitieren» können/dürfen. Und ja, ein Kunde, der ein Feature bestellt, darf uns selbstverständlich klar mit auf den Weg geben, wie er es denn gerne haben möchte. Wir denken, dass nur im Zusammenspiel mit dem Kunden überhaupt gute neue Lösungen entstehen können.

Interessanterweise haben wir bei den Signaturlösungen zwar viele Anfragen erhalten, aber kein einziger Kunde war letztlich bereit, eine entsprechende Lösung mitzufinanzieren. Und weil uns das Kosten/Nutzen-Verhältnis ebenfalls nicht erfüllt schien, haben wir darauf verzichtet, Signaturlösungen selber zu implementieren. Damit wir uns richtig verstehen, **selbstverständlich können wir signierte Dokumente seit Urzeiten ablegen, Ebenfalls können wir seit mehr als fünf Jahren die Seiten verschlüsselt ausliefern,** nicht möglich ist einzig das Signieren der von Archivista erstellten Dokumente.

Und wie wir seit heute wissen, wird die Bedeutung der Signaturlösungen durch die Richtlinie des EU-Ministerrates massiv abgewertet. Die Richtlinie ist für alle EU-Staaten bindend, ob die Schweiz diese übernehmen wird, bleibt abzuwarten. Allgemein kann aber gesagt werden, dass Signaturlösungen in der Schweiz weit weniger überhaupt je eine Rolle spielten.

Das können wir für die Authentizität der Daten tun

Kern
punkt bei DMS-Systemen ist es, Informationen verfügbar zu halten. Wurden Sie fälschlicherweise geändert, ist die Authentizität der Daten dahin. Die EU-Richtlinie führt aus, dass jede geeignete Massnahme anzuwenden ist, um die Datenintegrität sicherzustellen. Erlauben Sie mir hier zum Schluss, einige Punkte aufzuzählen, die nach unserer Erfahrung äusserst nützlich sind, die Datum über lange, lange Zeit am Leben zu erhalten:

- Standardisierte und zu 100% offengelegte patentfreie Dateiformate (Tiff, PNG, JPEG)
- OpenSource mit GPL-Lizenz: Programmcode ist vollkommen offengelegt
- Redundante Lösungen auf Stufe Soft- und Hardware (bei der ArchivistaBox ab Titlis vorhanden)
- Umfangreiche Sicherungsmöglichkeiten (Band, Netzwerk, RSYNC, USB-Platten)
- Auslagerungsmöglichkeit der Datenbestände auf nicht wiederbeschreibbare Medien (CD/DVDs)
- Jede Änderung an den Daten wird protokolliert (inkl. Datenextraktion aus Log-Daten)
- Verschlüsselter Zugriff auf Daten sowie ausgefeilte Rechteverwaltung für Benutzer/innen
- Erstellen selbsttragender Archive im laufenden Betrieb (keine zusätzlichen Lizenzen erforderlich)
- Import- und Export-Schnittstellen: Auf- und Abwärtskompatibilität seit mehr als 10 Jahren
- Datenhaltungskonzept seit mehr als 15 Jahren unverändert (Garantie für weitere 30 Jahre)

Das können Sie für Ihre Archive tun

- Unternehmensweite (standortübergreifende) Archive bringen viel Flexibilität
- Applikationsneutrale (zentrales) Management der Dokumente
- (Buchhaltungs-) relevante Belege bereits beim Erstellen archivieren
- Schattenarchive vermeiden — nur jeweils eine Kopie archivieren
- Regelmässige (wiederkehrende) Checks der Daten und Sicherungskopien

Wir hoffen, mit diesen Grundsätzen dazu beizutragen, effiziente Systeme bereitzustellen und ganz allgemein mitzuhelfen, eine jegliche Bürokratie im Keim

ersticken zu können.