

Durchbruch für Digitale Signatur: Gesetzeskonforme Massensignaturen direkt aus SAP-Anwendungen

- **Utimaco stellt auf der CeBIT eine Produktinnovation vor: Mit dem SignatureServer SmartCard for SAP können gesetzeskonforme Massensignaturen direkt aus mySAP.com-Anwendungen erstellt werden**
- **Damit können zum Beispiel elektronische Rechnungen erstmals in einem durchgängigen digitalen Workflow ohne Medienbrüche gesetzeskonform erstellt und verarbeitet werden**
- **Allein die 1000 größten deutschen Unternehmen können mit dieser Technologie rund 500 Millionen Euro im Jahr einsparen**

Oberursel, 01. März 2005 - In der konsequenten Nutzung elektronischer Kommunikationswege hat die deutsche Wirtschaft noch großen Nachholbedarf – zumindest, wenn es um wichtige Geschäftsdokumente wie Rechnungen geht: 74 Prozent der 1000 größten Unternehmen Deutschlands vertrauen ihre Rechnungen auch im 21. Jahrhundert wie zu Kaiser Wilhelms Zeiten am liebsten der gelben Post an. Dieser Anachronismus kommt der Wirtschaft teuer zu stehen: Alleine die Top-1000-Unternehmen könnten nach Angaben des Frankfurter E-Finance Labs durch den automatisierten elektronischen Rechnungsversand im Geschäftskundenverkehr jährlich bis zu einer halben Milliarde Euro einsparen.

Im Gegensatz zur traditionellen Papierrechnung gelten elektronische Rechnungen, die per Computerfax oder E-Mail zugestellt werden, jedoch nicht ohne weiteres als Urkunde im Sinne des Gesetzgebers. Denn digitale Rechnungen werden von den Finanzbehörden nur dann zum Vorsteuerabzug anerkannt, wenn sie mit einer qualifizierten elektronischen Signatur versehen sind.

Mit dem SignatureServer SmartCard for SAP von Utimaco, der auf der CeBIT in Hannover vom 10.03. bis 16.03.2005 erstmals vorgestellt wird, können Unternehmen elektronische Rechnungen, die direkt aus SAP-Systemen erstellt werden, automatisch mit qualifizierten digitalen Signaturen versehen und verschlüsseln. SAP-R/3-Daten oder -Dokumente werden mit dieser Technologie zusätzlich beim Speichern und Versenden geschützt.

„Zum ersten Mal können elektronische Rechnungen damit in einem durchgängigen digitalen Workflow gesetzeskonform und rationell erstellt und verarbeitet werden. Anwender können so Medienbrüche vermeiden, ihre Geschäftsprozesse weiter optimieren und dadurch erhebliche Kosten einsparen“, erläutert Technologie-Experte Andreas Philipp, Deputy Vice President des Geschäftsbereichs Transaction Security der Utimaco. „Durch den elektronischen Rechnungsprozess erhöhen Unternehmen außerdem die Servicequalität für ihre Geschäftspartner und stärken damit auch die Kundenbindung.“

Der SignaturServer SmartCard wird auf der Pressekonferenz der Utimaco auf der CeBIT am 10.03.2005, 13:00 bis 14:00 Uhr, Convention Center Saal 107, vorgestellt.

Hintergrundinformationen:

Varianten der elektronischen Signatur

Die elektronische Signatur basiert auf einem kryptographischem Verfahren, das es dem Urheber ermöglicht, elektronische Dokumente zu unterzeichnen (zu signieren). Mit einer digitalen Signatur kann verhindert werden, dass Dokumente unbemerkt manipuliert werden. Im deutschen Signaturgesetz wird unterschieden zwischen einfachen elektronischen Signaturen, fortgeschrittenen Signaturen und qualifizierten Signaturen (mit oder ohne Anbieter-Akkreditierung).

Einfache elektronische Signatur

Jegliche Daten (oder Grafiken), die mit anderen Daten (bzw. Dokumenten) logisch verknüpft sind und den Aussteller erkennen lassen (Authentifizierung), gelten als elektronische Signatur. Auch eine eingescannte Unterschrift kann somit bereits als eSignatur betrachtet werden. In der Praxis werden heute jedoch bereits auf dieser Stufe relativ sichere Verfahren angeboten, die aus formalen Gründen als „einfache“ Signatur bezeichnet werden. (→ §2 Nr. 1 SigG)

Fortgeschrittene Signatur (FES)

Die fortgeschrittenen elektronischen Signatur (FES) ist ausschließlich dem Signaturschlüssel-Inhaber zugeordnet und muss seine Identifizierung ermöglichen. Die FES muss mit den Daten, auf die sie sich bezieht, so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann. Um dies zu gewährleisten, wird eine Checksumme (Hash-Wert) über den kompletten Inhalt des signierten Objektes gebildet, verschlüsselt und wie ein Siegel an das Objekt angehängt. (→ §2 Nr. 2 SigG)

Qualifizierte Signatur (QES)

Die qualifizierte elektronische Signatur (QES) erfüllt die erhöhten Anforderungen des deutschen Signaturgesetzes von 1997. Sie berücksichtigt einerseits die fortschreitende technologische Entwicklung, in dem sie den Schlüsselzertifikaten nur eine begrenzte Gültigkeit einräumt und stellt andererseits besondere Anforderungen an die organisatorisch-technischen Gegebenheiten des Zertifikatherausgeber (Trust Center = Certification Authorities). Lediglich die qualifizierte Signatur ist in Deutschland juristisch vollkommen gleichwertig mit der traditionellen (handschriftlichen) Unterschrift – von wenigen, definierten Ausnahmen abgesehen. Europaweit existieren fortgeschrittene elektronische Signaturen. Für den Geschäftsverkehr mit außereuropäischen Ländern gibt es bisher keine verbindlichen Vereinbarungen. (→ §2 Nr. 3 SigG)

Utimaco Safeware AG ist einer der führenden Hersteller von professionellen Lösungen für die IT-Sicherheit. Von Utimaco entwickelte Sicherheitstechnologien und -lösungen schützen die elektronischen Werte von Unternehmen und Behörden vor unberechtigtem Zugriff und gewährleisten die Verbindlichkeit und Vertraulichkeit von Geschäftsprozessen sowie Verwaltungsabläufen in der elektronischen Welt. Der Geschäftsbereich Personal Device Security liefert Technologien und Lösungen zur Gewährleistung von mobiler Sicherheit in den Bereichen starke Authentisierung inkl. biometrischer Verfahren, Verschlüsselung und Integritätskontrolle. Die Produkte und Lösungen sichern Daten in Terminal Server- und Citrix-Umgebungen, auf PCs, Laptops und PDAs am Arbeitsplatz und beim mobilen Einsatz. Der Geschäftsbereich Transaction Security ist spezialisiert auf Sicherheitslösungen für E-Business, E-Government und E-Payment auf Basis eigener Technologien (Telekommunikations-Managementsysteme, Hardware-Sicherheitsmodule, Gateways für E-Mail-Sicherheit, Authentisierung und digitale Signaturen, Public Key Infrastructure und PKI-basierte Anwendungen).