

keyon

Rechtsgültige Archivierung von Daten und Belegen bei der Coop

Informatives Frühstück und Praxisbericht

Referenten
Klaus Eichhorn, Coop
René Eberhard, Keyon AG

Datum / Ort
4. Oktober 2007, 08:15 Uhr
Coop Bildungszentrum, 4132 Muttenz



Rechtsgültige Archivierung bei der Coop

keyon

keyon
Schönbodenstrasse 4
8640 Rapperswil
Switzerland

www.keyon.ch

René G. Eberhard
Dipl. El.-Ing. HTL
Betriebswirtschafts-Ing. FH NDS
CEO

Tel +41 55 220 64 03
Mobile +41 79 456 00 45
Fax +41 55 220 64 01

eberhard@keyon.ch

Agenda



Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

Organisatorische und Betriebliche Umsetzung

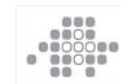
Rückblick auf vier Jahre Erfahrung

Über Keyon



■ Ausgewiesenes Know-How

- Aufbau und Weiterentwicklung der vom EFD anerkannten, EIDI-V konformen CA bei der EAN Schweiz
- Verschiedene, erfolgreich abgeschlossene Projekte im Bereich der elektronischen Rechnungsstellung (EIDI-V) und elektronischen Archivierung (GeBüV)
- Praxiserprobtes Signatur-Framework
- Offizieller Konsultationsteilnehmer des BAKOM im Bereich ZertES.



■ Erstklassige Referenzen

Pass 06

Höchste Sicherheit
mit Lösungen von Keyon



1. Name (Nom)
Cognome (Nom) Surname
Kolliker
2. (Cognome) (Prénoms)
Nom(s) Prénoms(s) Given name(s)
Andrea
3. Nationalité (Nationalité)
Citizen(s) Nationality (Nationality)
Schweiz Suisse Svizzera Switzerland
4. Informations Date de naissance
Date di nascita Data di nascita Data of birth
27. März 1972



Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

Organisatorische und Betriebliche Umsetzung

Rückblick auf vier Jahre Erfahrung

■ **Der Erste Eindruck...**

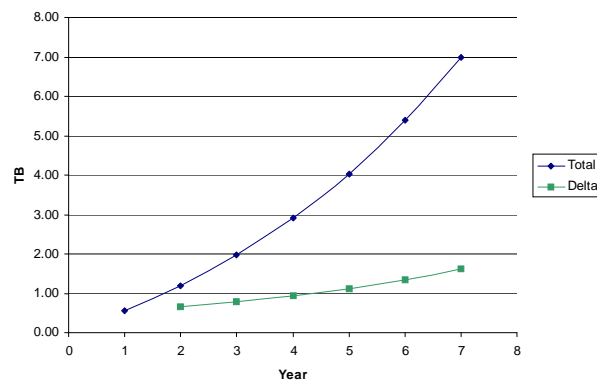
- Neue gesetzlichen Vorgaben die umgesetzt werden müssen
- Hohe Kosten und Aufwände für wenig Nutzen
- Fehlende Richtlinien für die Umsetzung
- Keine Produkte und kein Know-how am Markt erhältlich

■ **... täuscht. Die Realität:**

- Gesetzliche Vorgaben sind seit 2002 in Kraft
- Grosser Nutzen, rasche Amortisation, effiziente Rechnungsverarbeitung, Archivierung und ILM inkl. Umsetzung und Durchsetzung von Revisions- und Compliance Prozessen
- Klaren Richtlinien für die Umsetzung, grosse Rechtssicherheit
- Ausgereifte Produkte und Know-how am Markt erhältlich, kurze Realisierungszeit

■ **Herausforderungen: Management grosser Datenvolumen**

- Exponentielles Wachstum der zu verwaltenden Daten
- Effiziente Bewirtschaftung von Daten (kopieren, löschen, etc.)



Agenda



Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

Organisatorische und Betriebliche Umsetzung

Rückblick auf vier Jahre Erfahrung

Rechtssicherheit bei der Umsetzung



Wie können wir sicher sein, dass die integrierte Lösungen die gesetzlichen Anforderungen erfüllen?

■ **Rechtsgrundlagen in der Schweiz**

- **ZertES** – Bundesgesetz über die elektronische Signatur, Gleichstellung von elektronischer Signatur und eigenhändiger Unterschrift.
- **EIDI-V** - Verordnung des EFD über elektronisch übermittelte Daten und Informationen. Anforderungen an el. Belege hinsichtlich Vorsteuerabzug, Steuererhebung oder Steuerbezug.
- **GeBüV** – Verordnung über die Führung und Aufbewahrung der Geschäftsbücher

■ **Rechtsgrundlagen in der Schweiz - GeBüV**

- Gestützt auf Artikel 957 Absatz 5 des Obligationenrechts
- Grundsätze der ordnungsgemässer Führung und Aufbewahrung der Bücher.
 - insbesondere die Integrität der Daten und die Dokumentation, sowie die Grundsätze für die ordnungsgemässe Aufbewahrung von Daten (Sorgfaltspflicht, Verfügbarkeit, Organisation, Archiv);
 - im Grundsatz ist gesetzlich geklärt, dass die elektronische Belegsverwahrung zulässig ist (Art. 957 Abs. 2 OR)

Ordnungsgemässe Aufbewahrung als wesentliches Element der Compliance

■ **Rechtsgrundlagen in der Schweiz - GeBüV**

Wesentliche Änderungen

- Nur noch die Bilanz und Erfolgsrechnung sind schriftlich und unterzeichnet aufzubewahren
- Alle übrigen Geschäftsbücher, Buchungsbelege und Geschäftskorrespondenzen können elektronisch geführt und aufbewahrt werden

■ **Rechtsgrundlagen in der Schweiz - GeBüV**

Einfluss der GeBüV auf die elektronische Archivierung

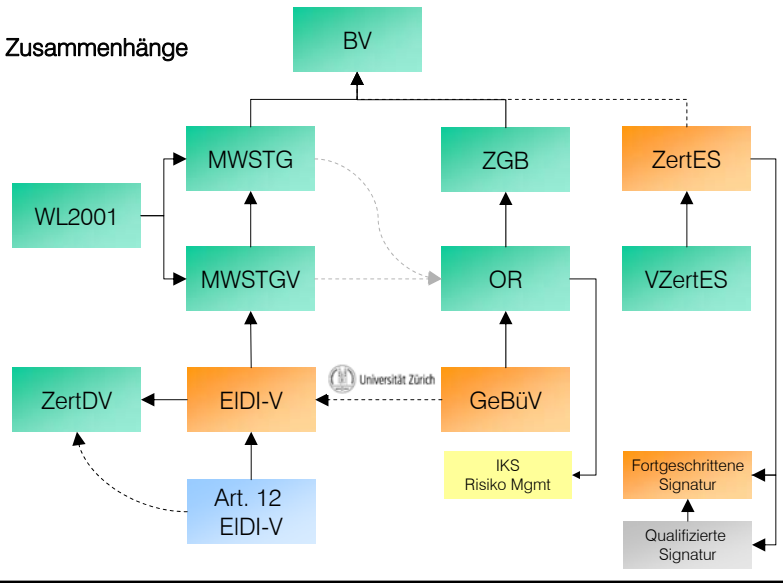
- Unveränderbare Informationsträger
 - Papier, Bildträger, etc
 - CD, DVD, WORM, etc.
- Veränderbare Informationsträger
 - Hard Disk, Band, Flash, CD RW, DVD RW, Floppydisk, etc.
 - Einsatz von elektronischen Signaturen und Zeitstempeln
 - Schutz der Integrität der Daten
 - Prüfbarkeit und Prüfpfad (Protokolle, Log Files)
 - Aufbewahrung und Wiedergabe

■ Grundlage elektronische Signatur

Mathematische Verknüpfung vom Private Key mit den zu signierenden Daten

```
SEQUENCE {
  TO BE SIGNED OBJECT
  ...
  SEQUENCE {
    OBJECT IDENTIFIER
      sha1withRSAEncryption (1 2 840 113549 1 1 5)
    NULL
  }
}
4B 41 98 E7 E6 04 BB DB 20 6B E5 6A F5 82 2A 48
DB 7F 7B D8 51 04 B0 10 74 6D 62 64 18 83 1B F3
72 BA A9 24 B3 02 7C 87 BB DF 84 19 E8 8E B2 D0
3F A9 04 DD C9 7E 2B F6 70 8F 42 E6 40 5E 7C BA
85 A2 9B AD 61 78 DD F6 E4 31 4F 9C 17 C1 38 AF
19 3A 86 2A 89 FA 57 0D A4 68 89 96 AB 35 6F FD
65 6C 5A D1 C0 EF 4F 57 4F 88 C5 F7 74 EA 3F E6
65 0A 22 88 6B 23 2D A3 A8 05 E5 99 FC 89 21 0A
}
```

■ Zusammenhänge



Es ist allgemein anerkannt, dass die Anforderungen an eine elektronische Signatur aus Sicht der der EIDI-V höher sind als aus Sicht der GeBüV. Im Weiteren sind die Anforderungen an eine elektronische Signatur in der EIDI-V klarer definiert als in der GeBüV.

Umsetzung der Lösung nach den Vorgaben der EIDI-V.

Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

Organisatorische und Betriebliche Umsetzung

Rückblick auf vier Jahre Erfahrung

■ Compliance

- Ziel ist es, die Aktivitäten eines Unternehmens nach bestimmten Kriterien messen und beurteilen zu können. Voraussetzung hierfür ist die Beschreibung des Unternehmens oder einzelner Teile davon.
- Es gilt die äusseren und internen Einflussfaktoren, Prozesse, Menschen, Rollen, Systeme und weiteren Aspekte zu erfassen und miteinander in Beziehungen zu bringen.
- Erst dann kann beurteilt werden, welche Risiken, Potentiale und Verbesserungsmöglichkeiten vorhanden sind und ob die entsprechenden Prozesse den Anforderungen bestimmter Gesetze genügen.

Beurteilung der Lösung durch die ESTV



■ E-Business und Archivierung ist Chefsache

- Die Unternehmensführung muss Weisungen und Richtlinien zur elektronischen Führung von Geschäftsbüchern erarbeiten und durchsetzen. Sie ist Verantwortlich für das Einhalten der gesetzlichen Vorschriften. Werden diese nicht eingehalten, droht ein Verlust von Forderungen aufgrund fehlender Beweise oder zivilrechtliche Schadenersatzpflicht.
- Im Streitfall gilt es zu beweisen, dass die Sorgfaltspflichten wahrgenommen wurde. Die Verfahrensdokumentation ist eine Grundlage für die Methodik der Beweisführung.
- Die Einhaltung der definierten technischen und organisatorischen IT Prozesse sind integraler Bestandteil der kaufmännischen Buchführung.



■ Best Practise Standards

- **ISO 27001:** spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.
- **ISO 15489:** regelt die Verwaltung und Aufbewahrung von Unterlagen, die bei privaten und öffentlichen Organisationen für den internen und externen Gebrauch entstehen (ILM)
- **Cobit:** von der ISACA entwickeltes Steuerungsframework für IT-Governance. Umfassender Prüfstandard für IT-Revision, welcher definiert, WAS umzusetzen ist.
- **IT-Grundschutz-Kataloge des BSI:** Bietet eine einfache Methode, dem Stand der Technik entsprechende IT-Sicherheitsmassnahmen zu identifizieren und umzusetzen.

Zertifizierung nicht als primäres Ziel.

■ Erstellen einer Verfahrensdokumentation

- Beschreiben des Unternehmens, der Unternehmensstruktur
- Beschreiben der Organisation und der Verantwortlichkeiten
- Verweisen auf die relevanten Gesetze, Verordnungen und Regulatorien
- Beschreiben der Projektabsicht
- Beschreiben der Geschäftsprozesse



■ **Erstellen einer Verfahrensdokumentation**

- Klassifizierung der Dokumente und Beschreibung des ILM unter Berücksichtigung der Aufbewahrungsfristen
 - Prozess zur Vernichtung der Papierbelege
- Beschreibung der organisatorischen Prozesse, insbesondere interne und externe Revisionsprozesse und Kontrollmechanismen
- Definieren der Prozess- und Systemverantwortlichkeiten
- Festlegen von Arbeitsanweisungen
- Beschreibung der technischen Prozesse, insbesondere
 - Wahrung der Integrität der Daten
 - Systemgrenzen und Datenflüsse
 - Protokollierung
 - Indexierung und Datenzugriffe



■ **Beurteilung der Verfahrensdokumentation**

Eingabe der Verfahrensdokumentation an die Behörden mit dem Ziel einer positiven Beurteilung.

Abbildung wurde entfernt.

Positive, vorbehaltlose Beurteilung durch die Behörden.

■ **Grosser, interner Nutzen der Verfahrensdokumentation**

- Spezifikation der technischen und organisatorischen Prozesse als Grundlage für deren Umsetzung
- Grundlage für Ausbau und Durchsetzung von Richtlinien
- Grundlage für Beweisführung im Schadensfall und Erfüllung der Sorgfaltspflichten
- Grundlage für IKS sowie interne und externe Revisionsprozesse
- Grundlage für Risiko Management

Revidierte Artikel im OR gültig ab 1.1.2008

Art. 663 Bst. b OR: Risiko Management
Art. 728 Bst. a OR: IKS



Agenda

Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

Organisatorische und Betriebliche Umsetzung

Rückblick auf vier Jahre Erfahrung

Welche organisatorischen und betrieblichen Massnahmen müssen umgesetzt werden und warum?

■ **Bausteine**

- Prozessbeschreibung (organisatorisch und technisch)
- Kontinuitäts- und Sicherheitsmanagement
- Organisation und Personal
- Notfallvorsorge-Konzept und Behandlung von Sicherheitsvorfällen
- Datensicherungs- und Migrationskonzept
- Zugriffskonzept
- Change Management
- Mitarbeitersensibilisierung und Schulung
- etc.

Erfolgsfaktor Mensch!

■ **Revisionsprozesse**

- Nachweis der Einhaltung der in der Verfahrensdokumentation beschriebenen technischen und organisatorischen Prozesse
- Periodische Überprüfung der Integrität der archivierten Dokumente

■ **Beleg**

- MWST konformer Rechnungsinhalt (Art. 37 MWSTG, etc.)
- Integrität der Daten (elektronische Signatur, EIDI-V, GeBüV)
- Authentizität der Daten (elektronische Signatur, EIDI-V)
- Maschinelle Auswertbarkeit (EIDI-V)
- Papieräquivalent zum elektronischen Beleg

■ **ERP**

- Validierung der elektronischen Rechnung vor der Verbuchung
- Korrekte Verbuchung des Geschäftsvorfalles
- Verknüpfung vom ERP (Buchungssatz) ins Archiv (Beleg), retrograde Prüfspur
- Indexerstellung für die Auswertung und sicherstellen der Lesbarkeit der Buchungssätze
- Revisionszugriff

Der Fokus liegt auf der Revision des Geschäftsprozesses.
Neu sind elektronische Dokumente als Grundlage für die Informationsbeschaffung.

■ **Archiv**

- Verknüpfung vom Archiv (Beleg) ins ERP (Buchungssatz, progressive Prüfspur)
- Indexerstellung für die Auswertung und sicherstellen der Lesbarkeit der archivierten Daten
- Integritätsnachweis im Rahmen der Langzeitarchivierung (Validierung der elektronischen Signatur)
- Langzeitarchivierung (Archivierung grosser Datenmengen innerhalb der gesetzlichen Aufbewahrungsfrist, Backup / Restore, Business Continuity Planning, etc.)
- Migrationskonzept (Datenformat, el. Signatur, Archivsoftware)

■ **Weitere technische Prozesse**

- Protokollierung der Prozessschritte
- Archivierung der Inhouse-Formate und der Validierungsprotokolle
- Dedizierter Validierungsservice für Einsichtsberechtigte

Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

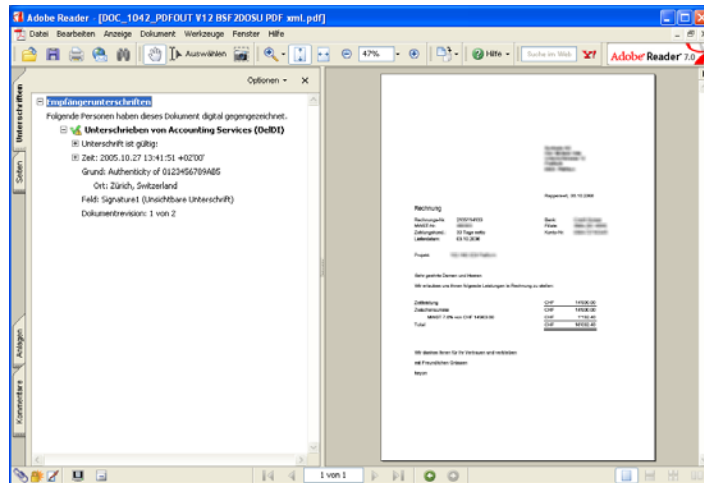
Organisatorische und Betriebliche Umsetzung

Rückblick auf vier Jahre Erfahrung

■ **Umsetzung unterschiedlicher elektronischer Geschäftsprozesse**

- Projekte im Bereich Finance, Handel, Industrie und Dienstleistungen
- Rechnungsverarbeitung, Steuer relevante Prozesse
 - Rechnungsstellung und Self-Billing
 - Inhouse oder ausgelagerte Verarbeitung im In- und Ausland
 - Nationale und Internationale Rechnungsverarbeitung
- Rechtsgültige Archivierung elektronischer Daten
 - Migration grosser Datenmengen vom WORM auf HD
 - Kostengünstige Archivierungskonzepte unter Verwendung von elektronischen Signaturen

■ Bank- und Rechnungsbelege für Partner und Kunden



■ Geringe Projektrisiken, effiziente Umsetzung

- Organisatorisches, technisches und rechtliches Know-how ist vorhanden
- Technologie und Dienstleister sind verfügbar (commodity)
- Projektumsetzung in time und in budget

■ Gesetzgebung

- Abstimmung der gesetzlichen Bestimmungen mit der technischen Entwicklung
 - EIDI-V II
 - TAV Zert-ES

Vielen Dank für Ihre Aufmerksamkeit



Bei Fragen stehe ich Ihnen gerne zur Verfügung.



Aus Gründen Ihrer Sicherheit