

keyon

## Aspekte der rechtsgültigen Archivierung basierend auf elektronischen Signaturen

Ein informatives Frühstück mit Praxisbezug zu:

- Rechtlichen Anforderungen
- Management und Compliance
- Praktische Umsetzung

Datum / Ort:

4. November 2008, 08:15 Uhr  
Hotel Park Hyatt Zürich, beim Kongresshaus



# Rechtliche Grundlagen und bisherige Erfahrungen



**René Eberhard**

Dipl. El.-Ing. HTL  
Betriebswirtschafts-Ing. FH NDS  
CEO, Partner

**keyon AG**

Schlüsselstrasse 6  
8645 Jona  
Switzerland

[www.keyon.ch](http://www.keyon.ch)

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

[eberhard@keyon.ch](mailto:eberhard@keyon.ch)

## Agenda

Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

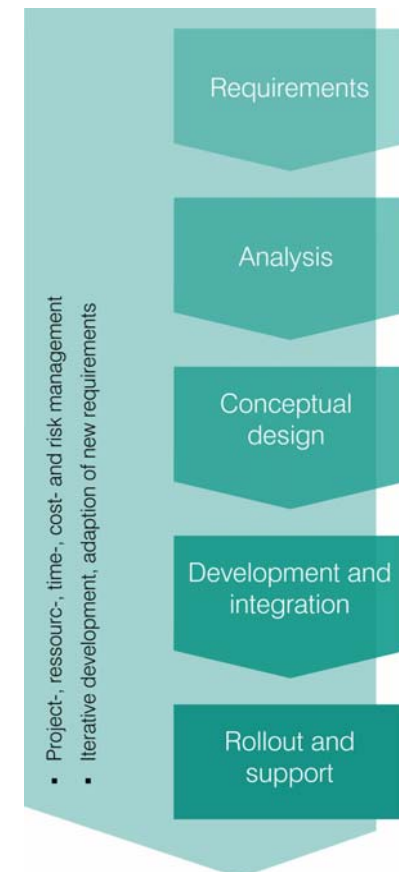
Rückblick auf fünf Jahre Erfahrung

## ■ Keyon in a few seconds

- Schweizerische Aktiengesellschaft seit 1999

Keyon ist ein führender Anbieter von Dienstleistungen und Lösungen in den Bereichen:

- IT-Sicherheit
- Rechtsgültige Verarbeitung und Archivierung von Daten und Rechnungen
- Security- und Risk Management
- Kundenspezifische Softwareentwicklung



### 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 (true-Sign)
- Offizieller Konsultationsteilnehmer des BAKOM im Bereich ZertES.



## Erstklassige Referenzen



### 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



## Agenda

Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

Rückblick auf fünf Jahre Erfahrung

## Der Erste Eindruck und die Realität

### ■ 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

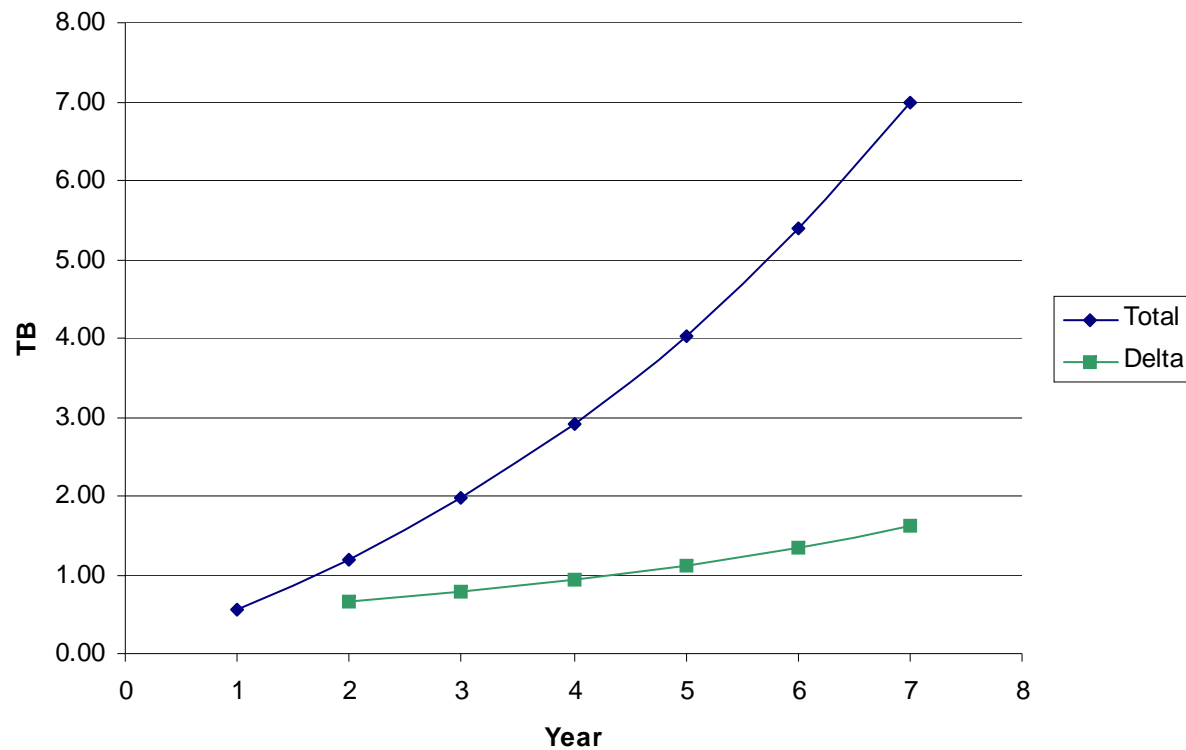
### ■ ... täuscht. Die Realität:

- 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



## Der Erste Eindruck und die Realität

- 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

Rückblick auf fünf Jahre Erfahrung

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 Belegsverwaltung zulässig ist (Art. 957 Abs. 2 OR)

Ordnungsgemässe Aufbewahrung als wesentliches Element der Compliance

## Rechtssicherheit bei der Umsetzung

### ■ 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 (Art. 8)

- Die Informationen sind systematisch zu inventarisieren und vor unbefugtem Zugriff zu schützen.
- Zugriffe und Zutritte sind aufzuzeichnen. Diese Aufzeichnungen unterliegen derselben Aufbewahrungspflicht wie die Datenträger.

Nachvollziehen der Zugriffs: Verhindern der Aktenunterdrückung, gewährleisten des Datenschutzes

## Rechtssicherheit bei der Umsetzung

### ■ Rechtsgrundlagen in der Schweiz - GeBüV

#### Einfluss der GeBüV auf die elektronische Archivierung (Art. 3, Art. 9)

- 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)

Sicherstellen der Integrität: Verhindern der Aktenmanipulation



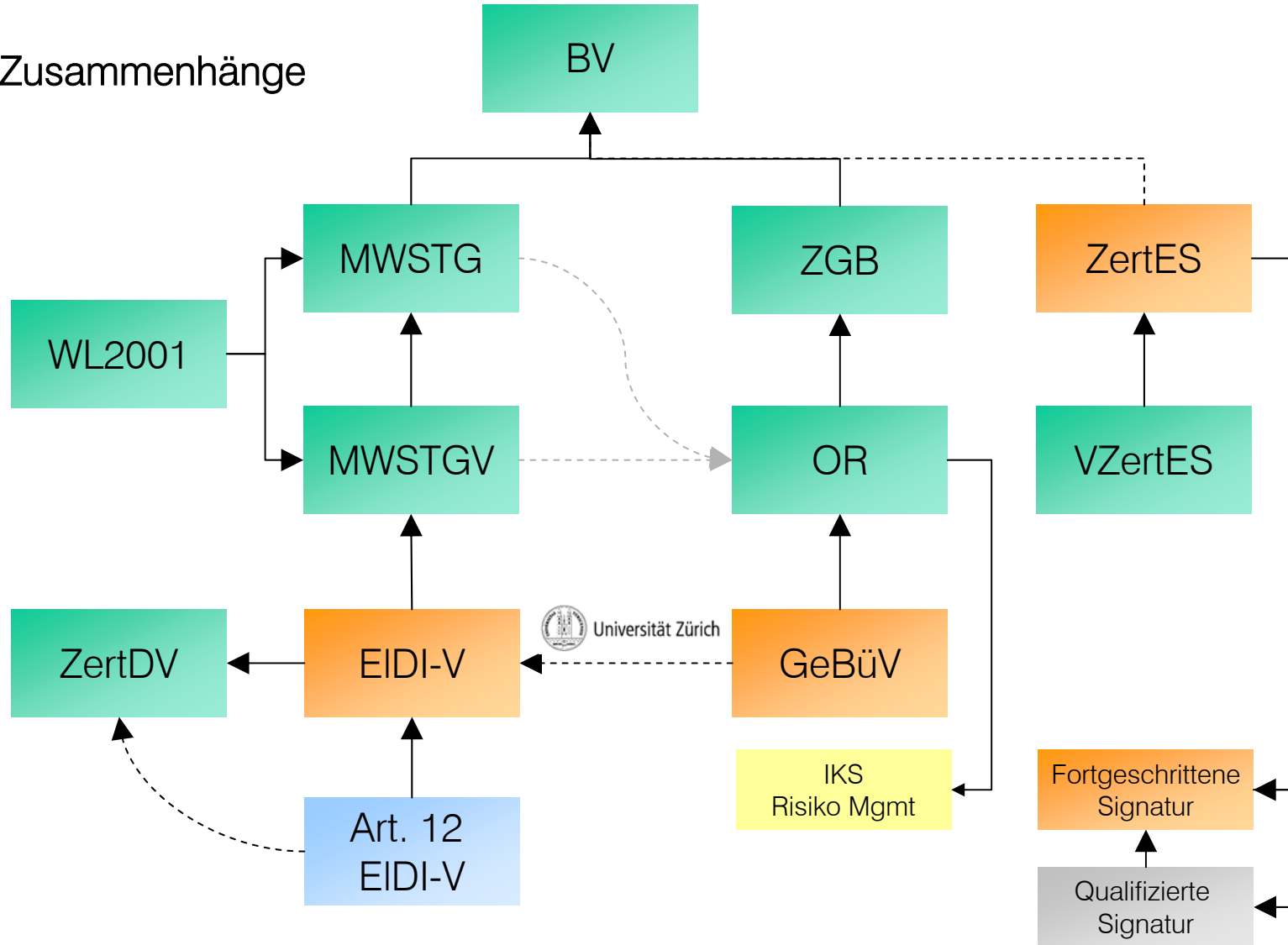
## Rechtssicherheit bei der Umsetzung

### ■ 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 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.

## Agenda

Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

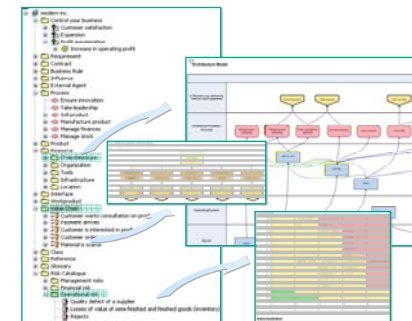
Prozessdokumentation: Grundlage für Compliance

Rückblick auf fünf Jahre Erfahrung

## Compliance

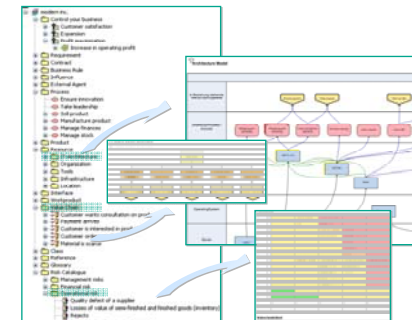
- Ziel ist es, die Aktivitäten eines Unternehmens nach bestimmten Kriterien messen und beurteilen zu können. Voraussetzung hierfür ist die Beschreibung des Unternehmens oder einzelner Teile davon.
- Es gilt die äusseren und internen Einflussfaktoren, Prozesse, Menschen, Rollen, Systeme und weiteren Aspekte 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



## 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

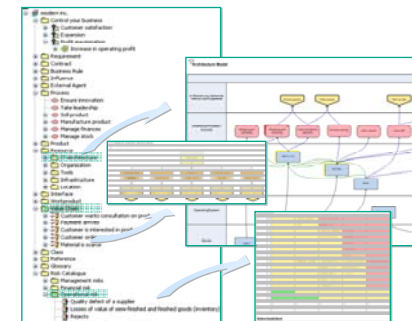
- **ISO 27001:** spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.
- **ISO 15489:** regelt die Verwaltung und 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-Grundschatz-Kataloge des BSI:** Bietet eine einfache Methode, dem Stand der Technik entsprechende IT-Sicherheitsmassnahmen zu identifizieren und umzusetzen.

Zertifizierung nicht als primäres Ziel.

## Prozessdokumentation: Grundlage für Compliance

### 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

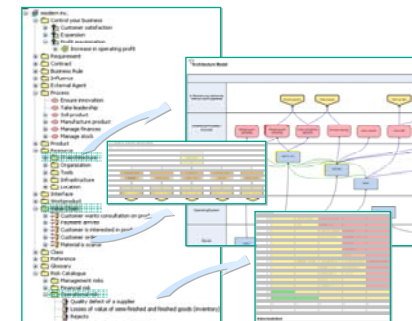




## Prozessdokumentation: Grundlage für Compliance

### 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.

Bild wurde entfernt

#### Schlussfolgerung

Wir stellen fest, dass die beschriebenen Abläufe zur Verarbeitung und Aufbewahrung den Vorgaben der Mehrwertsteuer entsprechen. Eine Überprüfung Beleg/Archiv wie auch in umgekehrter Richtung durch Einsichtsberechtigte wird gewährleistet.

Gegen die beschriebene Lösung haben wir keine Vorbehalte anzubringen.

## Prozessdokumentation: Grundlage für Compliance

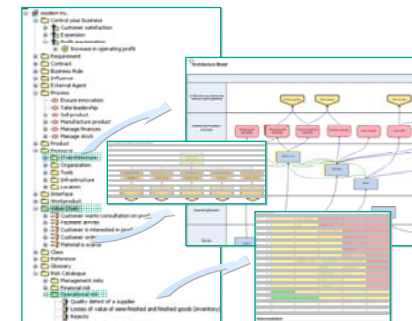
### ■ Grosser, interner Nutzen der Verfahrensdokumentation

- 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



- **Wesentliche Punkte der Umsetzung**
  - 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!

## Agenda

Über Keyon

Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Prozessdokumentation: Grundlage für Compliance

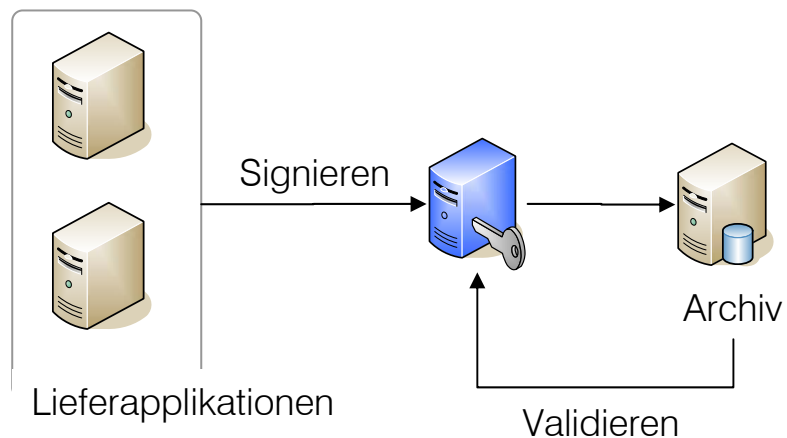
Rückblick auf fünf Jahre Erfahrung

## Rückblick auf fünf Jahre Erfahrung

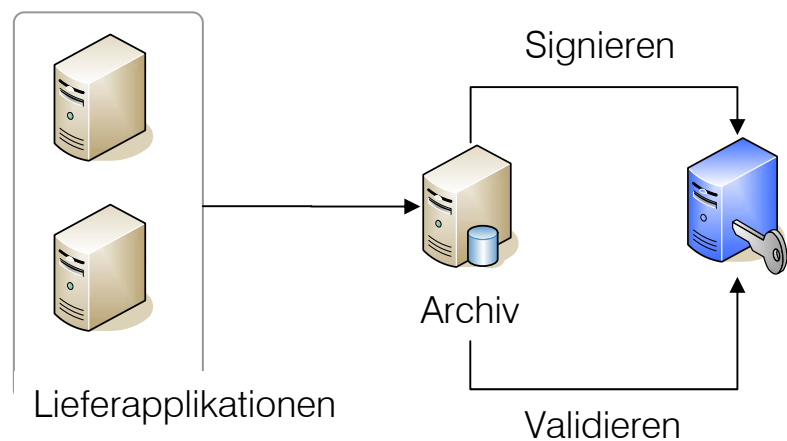
- Auszug aus Referenzen im Bereich GeBüV / EIDI-V
  - Credit Suisse
  - Coop
  - IBM
  - Unilever
  - Herbert OSPELT Anstalt
  - Walo Bertschinger
  - Swisscom
  - Syntrade
  - Manor
  - CompuDATA EDI Dienstleister (OEM Lizenznehmer)
  - SwissTainer (OEM Lizenznehmer)



Einfache technische Integration von true-Sign



Pre-Processing



Post-Processing

## Rückblick auf fünf Jahre Erfahrung

- Geringe Projektrisiken, effiziente Umsetzung
  - Organisatorisches, technisches und rechtliches Know-how ist vorhanden
  - Technologie und Dienstleister sind verfügbar (commodity)
  - Einfache Integration von true-Sign in Archivsysteme
  - 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

keyon

Bei Fragen stehe ich Ihnen gerne zur Verfügung.

keyon

Aus Gründen Ihrer Sicherheit