FINANCEFORUM

Elektronische Führung und Aufbewahrung von Geschäftsunterlagen

keyon

René G. Eberhard
Dipl. El.-Ing. HTL
CEO

keyon
Schönbodenstrasse 4
8640 Rapperswil
Switzerland

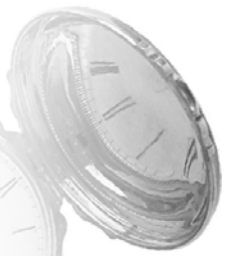
Tel +41 55 220 64 03
Mobile +41 79 456 00 45
Fax +41 55 220 64 01

www.keyon.ch
eberhard@keyon.ch

Agenda

keyon

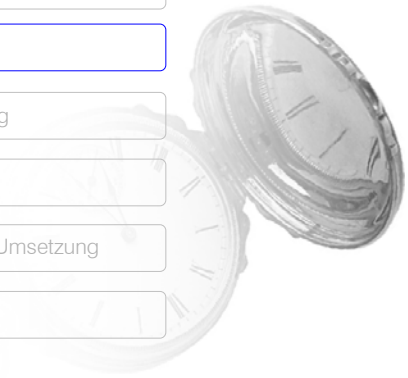
- Über Keyon
- Der Erste Eindruck und die Realität
- Rechtssicherheit bei der Umsetzung
- Technische Umsetzung
- Organisatorische und Betriebliche Umsetzung
- Rückblick auf vier Jahre Erfahrung



Agenda

keyon

- Über Keyon
- Der Erste Eindruck und die Realität
- Rechtssicherheit bei der Umsetzung
- Technische Umsetzung
- Organisatorische und Betriebliche Umsetzung
- Rückblick auf vier Jahre Erfahrung



Der Erste Eindruck und die Realität

keyon

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

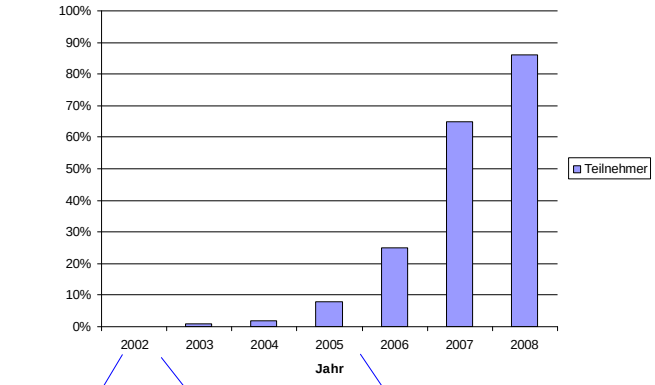
… täuscht. Die Realität:

- Gesetzliche Vorgaben sind seit 2002 in Kraft
- Grosser Nutzen, rasche Amortisation, effizientes 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

keyon

Prognose elektronische Geschäftsprozesse im Handel bis 2008



EIDI-V
GeBüV

EAN PKI

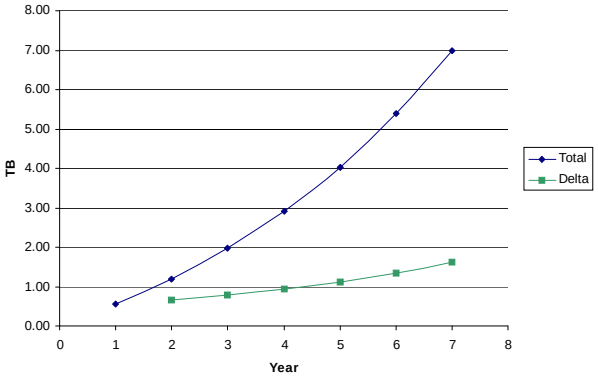
Commodity: Technologie und Prozesse

Der Erste Eindruck und die Realität

keyon

Herausforderungen: Management grosser Datenvolumen

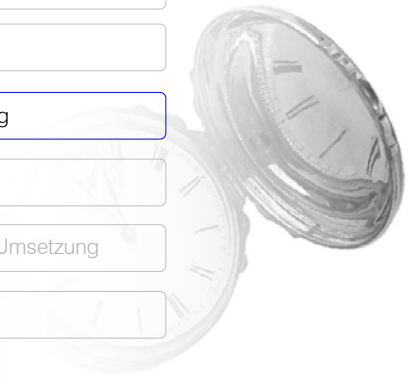
- Exponentielles Wachstum der zu verwaltenden Daten



Agenda

keyon

- Über Keyon
- Der Erste Eindruck und die Realität
- Rechtssicherheit bei der Umsetzung
- Technische Umsetzung
- Organisatorische und Betriebliche Umsetzung
- Rückblick auf vier Jahre Erfahrung



Rechtssicherheit bei der Umsetzung

keyon

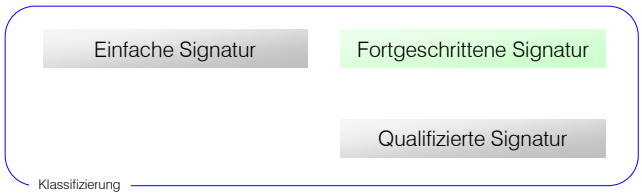
Wie können wir sicher sein, dass die integrierte Lösungen den gesetzlichen Anforderungen genügen?

Rechtssicherheit bei der Umsetzung

keyon

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



Rechtssicherheit bei der Umsetzung

keyon

EIDI-V (SR 641.201.1)

Verordnung des EFD über elektronisch übermittelte Daten und Informationen

- Gestützt auf Art. 45 MWSTG
- Regelt die technischen, organisatorischen sowie verfahrenstechnischen Anforderungen an die Beweiskraft und Kontrolle von elektronisch oder in vergleichbarer Weise übermittelten und aufbewahrten Daten und Informationen
  - Zwingender Einsatz von elektronischen Signaturen und Zeitstempeln für Schutz der Integrität der Daten und Authentifizierung der Parteien
  - Prüfbarkeit und Prüfpfad (Protokolle, Log Files)
  - Aufbewahrung und Wiedergabe
- Als digitale Signatur im Sinne dieser Verordnung gelten nur Signaturen, die: Mit Mitteln erzeugt werden, die der Inhaber unter seiner alleinigen Kontrolle halten kann.

Rechtssicherheit bei der Umsetzung

keyon

GeBüV (SR 221.431)

Verordnung über die Führung und Aufbewahrung der Geschäftsbücher

- 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)
- … technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten (z.B. digitale Signaturverfahren) und die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten werden

Rechtssicherheit bei der Umsetzung

keyon

ZertES (SR 943.03)

Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur

- Gestützt auf die Artikel 95 Absatz 1 und 122 Absatz 1 der Bundesverfassung
- Regelt die Voraussetzungen, unter denen sich Anbieterinnen von Zertifizierungsdiensten im Bereich der elektronischen Signatur anerkennen lassen können
- … eine elektronische Signatur, die folgende Anforderungen erfüllt: Sie wird mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann.

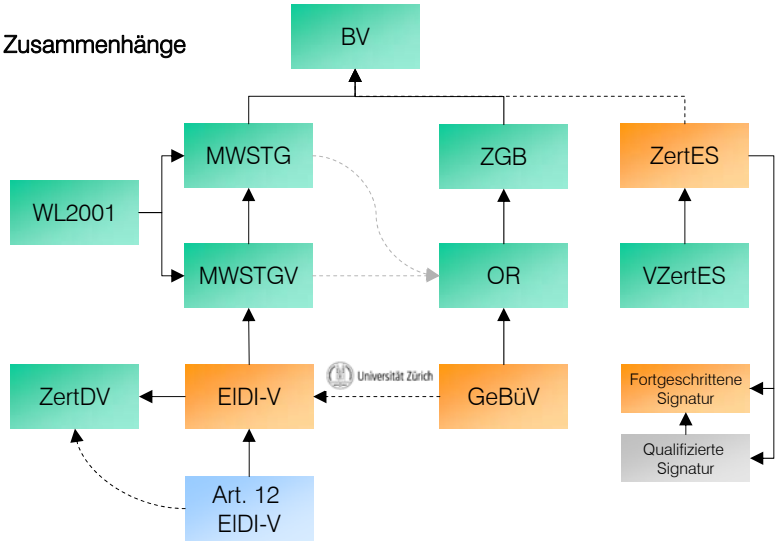
Der eigenhändigen Unterschrift gleichgestellt ist die qualifizierte elektronische Signatur, die auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten beruht.

Willenserklärung

Rechtssicherheit bei der Umsetzung

keyon

Zusammenhänge



Rechtssicherheit bei der Umsetzung

keyon

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.

keyon

Erstellen einer Verfahrensdokumentation

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

Rechtssicherheit bei der Umsetzung

keyon

Beurteilung der Verfahrensdokumentation

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

Bild wurde entfernt

Rechtssicherheit bei der Umsetzung

keyon

Grosser, interner Nutzen der Verfahrensdokumentation

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

Agenda

keyon

Über Keyon

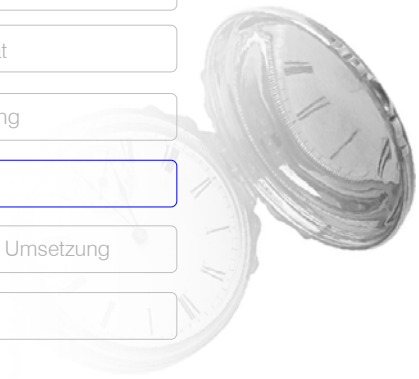
Der Erste Eindruck und die Realität

Rechtssicherheit bei der Umsetzung

Technische Umsetzung

Organisatorische und Betriebliche Umsetzung

Rückblick auf vier Jahre Erfahrung



Technische Umsetzung

keyon

Welche Varianten und Komponenten gibt es bei der technischen Umsetzung der Lösung?

Technische Umsetzung

keyon

Unterscheidung der Datenträger

- 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

Technische Umsetzung

keyon

Im folgenden fokussieren wir uns auf die rechtsgültige Archivierung auf veränderbaren Datenträgern unter Verwendung von elektronischen Signaturen.

Elektronischen Signaturen

keyon

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
}
```

keyon

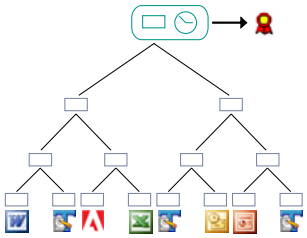
Unterscheidung der Signaturverfahren

- Einzelsignatur

  Jedes Dokument wird einzeln signiert.

- Hash-tree

  Der Hashwert einzelner Dokumente wird über definierte Verfahren kombiniert und signiert.



Welches sind die Vor- resp. Nachteile der Verfahren?

keyon

Unterscheidung der Signaturverfahren

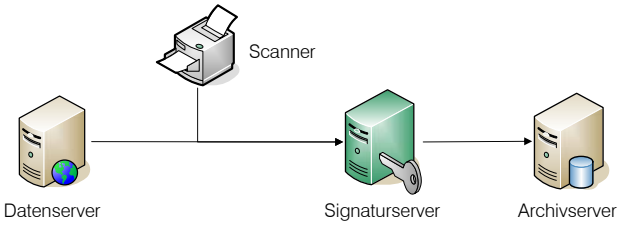
- Embedded oder detached Signatur
  - Die elektronische Signatur in das zu signierende Dokument eingebettet
  - Die elektronische Signatur wird getrennt mit einer logischen Verknüpfung zum Dokument verwaltet.
- Generische oder formatabhängige Signatur
  - Die elektronische Signatur wird gemäss dem zugrunde liegenden Dokumentenstandard signiert (z.B. XML-DSig, PDF, EDIFACT, etc.)
  - Die elektronische Signatur wird unabhängig vom zugrunde liegenden Standard signiert

Was sind die Entscheidungskriterien für ein spezifisches Verfahren?

Technische Umsetzung

keyon

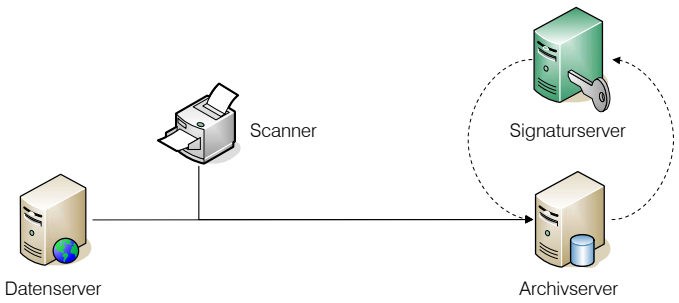
- **Integrationskonzepte**
  - Signieren vor dem Ablegen der Daten ins Archiv
    - Z.B. Embedded Signatur



Technische Umsetzung

keyon

- **Integrationskonzepte**
  - Signieren nach dem Ablegen der Daten ins Archiv
    - Z.B. Detached Signatur

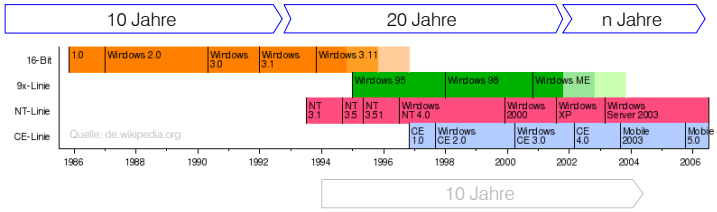


Technische Umsetzung

keyon

Integrierte Signaturlösung vs. anbieterneutrale Signaturlösung

- Nahtlose Integration der Signaturlösung in die technischen und organisatorischen Prozesse eines Unternehmens
- Unterstützung der rechtlichen Anforderungen der Schweizer Gesetze
- Unterstützung unterschiedlicher Dokumentenformate
- Unterstützung moderner Algorithmen und standardisierter Verfahren
- Software Lebenszyklen vs. Aufbewahrungspflicht



Technische Umsetzung

keyon

Ein wichtiges Entscheidungskriterium für die Signaturlösung true-Sign war die kompromisslose Unterstützung gängiger Signaturstandards und modernster Signaturverfahren, die flexiblen Schnittstellen für eine nahtlose technische und organisatorische Integration sowie die Unabhängigkeit zu einem Archivanbieter.

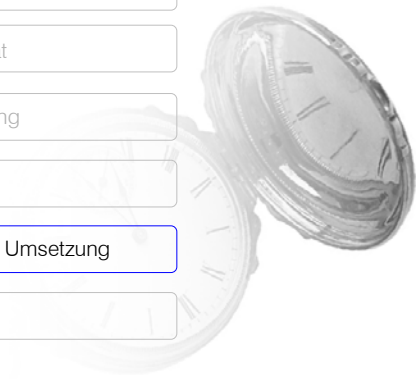
Technische Umsetzung

keyon

- **Vorteile der elektronischen Signatur**
  - Einfache und schnelle Migration der Datenträger und grosser Datenvolumen
    - Einfaches periodisches Prüfen der Integrität
    - Einfaches Vervielfältigen der Daten
    - Löschen der Daten nach Ablauf der Aufbewahrungsfrist
  - Einfaches auslagern (kopieren) von Daten an einen Drittstandort
  - Kostengünstige Lösung, rasche Amortisation
- **Nachteile der elektronischen Signatur**
  - Anpassen der bestehenden Revisionsprozesse
  - Hilfsmittel für die Sicherstellung der Integrität

Agenda

keyon



Organisatorische und Betriebliche Umsetzung

keyon

Welche organisatorischen und betrieblichen Massnahmen müssen umgesetzt werden und warum?

Organisatorische und Betriebliche Umsetzung

keyon

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.
- Alle Dokumente, welche zu einer Entscheidungsfindung führten, sollten aufbewahrt werden. Sie können für die Interpretation einer Vertragsklausel hinzugezogen werden und zeigen auf, was der Wille der Parteien ursprünglich war.
- Die Einhaltung der definierten technischen und organisatorischen IT Prozesse sind integraler Bestandteil der kaufmännischen Buchführung.

Organisatorische und Betriebliche Umsetzung

keyon

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.
- **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.

Organisatorische und Betriebliche Umsetzung

keyon

Bausteine

- IT-Sicherheitsmanagement
- Organisation und Personal
- Notfallvorsorge-Konzept und Behandlung von Sicherheitsvorfällen
- Datensicherungskonzept
- Zugriffskonzept
- Change Management
- IT-Sicherheitssensibilisierung und -schulung
- Migrationskonzept
- etc.

Erfolgsfaktor Mensch!

Organisatorische Umsetzung

keyon

Revisionsprozesse

- Unterscheidung zwischen Revision der IT-Prozesse und Revision des Geschäftsfalles
- Unterscheidung zwischen handels- und steuerrechtlicher Revision
  - Bei der steuerrechtlicher Revision müssen weitere Bedingungen erfüllt werden wie z.B. das Sicherstellen eines progressiven und retrograden Prüfpfads.
- Nachweis der Einhaltung der in der Verfahrensdokumentation beschriebenen technischen und organisatorischen Prozesse
- Periodische Überprüfung der Integrität der archivierten Dokumente

Organisatorische Umsetzung

keyon

Revisionsprozesse

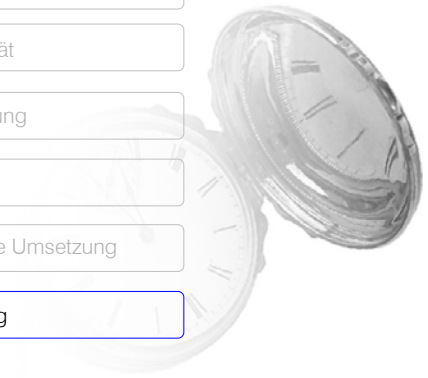
- Nachweis der Integrität bei einer Revision
  - Validierungsprotokoll über alle revisionsrelevanten Dokumente
  - Dedizierter Validierungsservice für Einsichtsberechtigte, Partner und Kunden
  - Validierungstools für Partner und Kunden
- Bereitstellen aller Hilfsmittel für den Zugriff der Daten
- Konsolidieren der Protokolle

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

Agenda

keyon

- Über Keyon
- Der Erste Eindruck und die Realität
- Rechtssicherheit bei der Umsetzung
- Technische Umsetzung
- Organisatorische und Betriebliche Umsetzung
- Rückblick auf vier Jahre Erfahrung

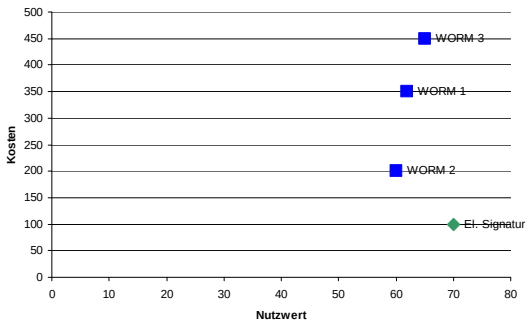


Rückblick auf vier Jahre Erfahrung

keyon

Kosten – Nutzen überzeugen

- Nutzwertanalyse (Integrität, Performance, Management, Schnittstellen, Administration, Skalierbarkeit, Nachhaltigkeit, etc.)
- Kostenanalyse (Beschaffung, Integration, Betrieb über ca. 5 Jahre, etc.)



Rückblick auf vier Jahre Erfahrung

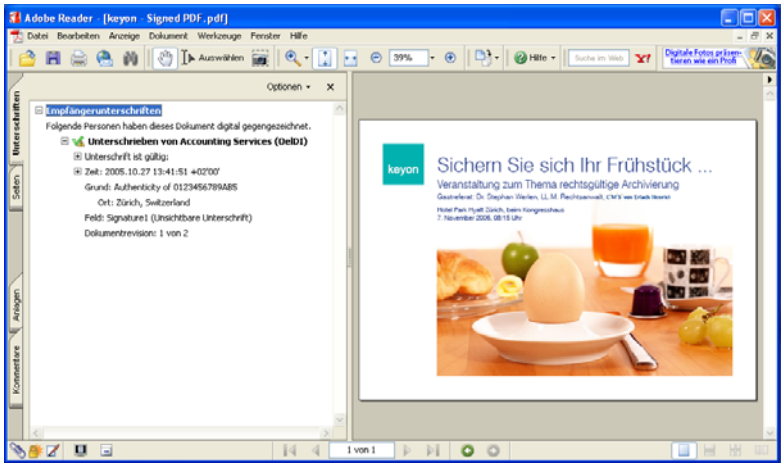
keyon

- **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

Rückblick auf vier Jahre Erfahrung

keyon

- **Bank- und Rechnungsbelege für Partner und Kunden**



Rückblick auf vier Jahre Erfahrung

keyon

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

keyon

Bei Fragen stehe ich Ihnen gerne zur Verfügung.

keyon Aus Gründen Ihrer Sicherheit