



ISO 27001 ist eine internationale Zertifizierungsnorm, mit deren Hilfe die **Informationssicherheit** gewährleistet werden soll (Vertraulichkeit, Authentizität, Integrität etc.).

Ziel: Einführung eines Informationssicherheitsmanagementsystems (ISMS) in Unternehmen.

Kryptografie

Ein Bestandteil des Maßnahmenkatalogs ist der Bereich „Kryptografie“



Die Umsetzung von Kryptografiemaßnahmen im Rahmen der ISO 27001 erfordert **Richtlinien** für den Gebrauch kryptografischer Maßnahmen und eine angemessene **Schlüsselerzeugung und –verwaltung**.

1. Kryptografische Richtlinien

- Welche Informationen müssen geschützt werden?
- Wann müssen die Informationen wie intensiv geschützt werden?
- Sind für den Schutz / Signierung gewisser Informationen externe Authentifizierungsstellen (CA's) erforderlich?
- Prozesse: Wer macht was?
- Wer ist für die Einhaltung der Konventionen verantwortlich?
- Wie sieht ein nachhaltiges Controlling aus?
- etc.

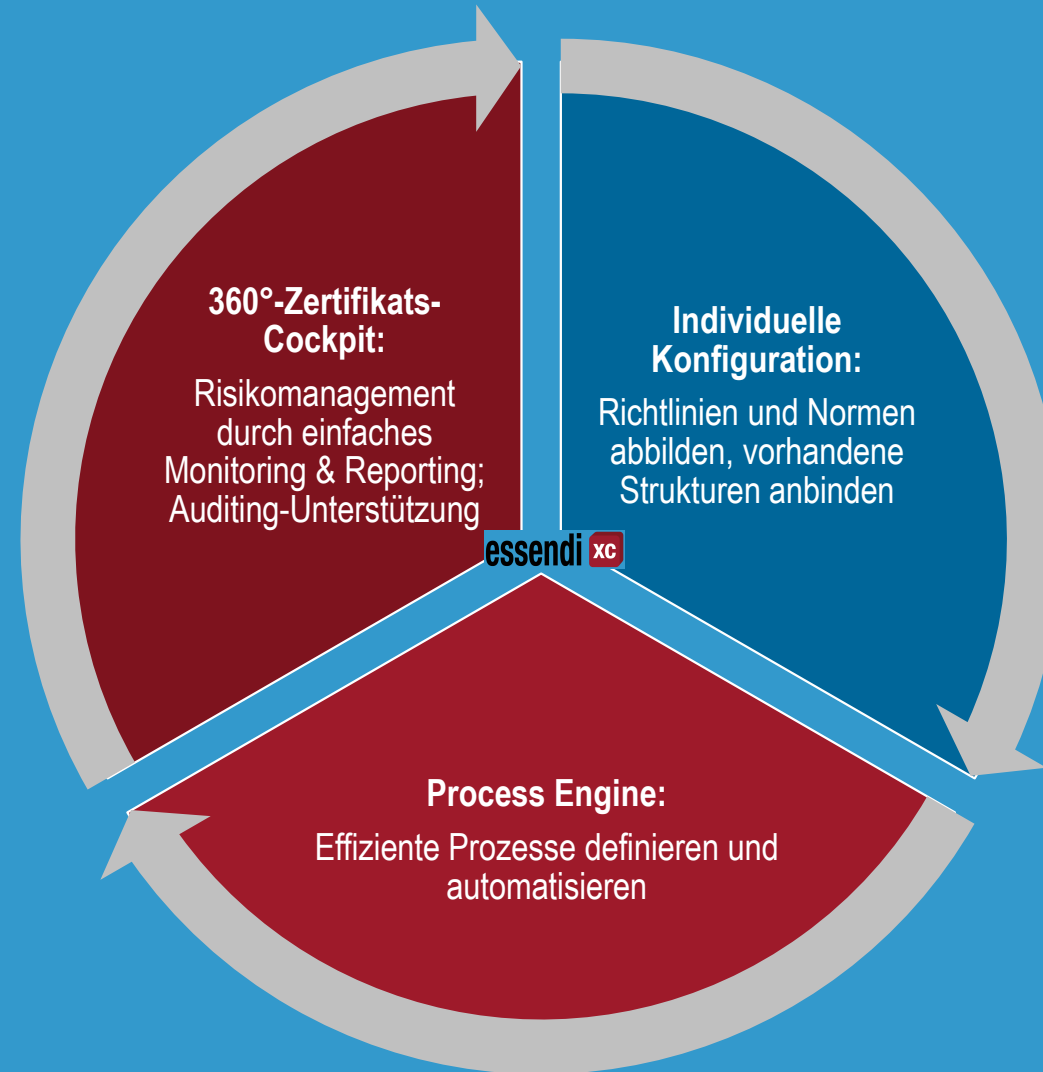
2. Schlüsselverwaltung

- Welches Verschlüsselungsverfahren soll genutzt werden?
- Management und Transparenz über vorhandene Schlüssel?
- Definierte Prozesse im Umgang mit Schlüsseln, z.B. für Ausstellung, Verteilen, Erneuerung etc.?
- Wer ist für die Einhaltung der Vorgaben zuständig?
- Verhalten bei Verlust der Schlüssel?
- Lebensdauer der Schlüssel?
- Wer hat Zugriff auf die Schlüssel, inkl. archivierter Schlüssel?
- etc.

essendi

unterstützt Sie dabei im Bereich Zertifikatsmanagement.

1. essendi xc: Krypto-Richtlinien erfolgreich und effizient umsetzen



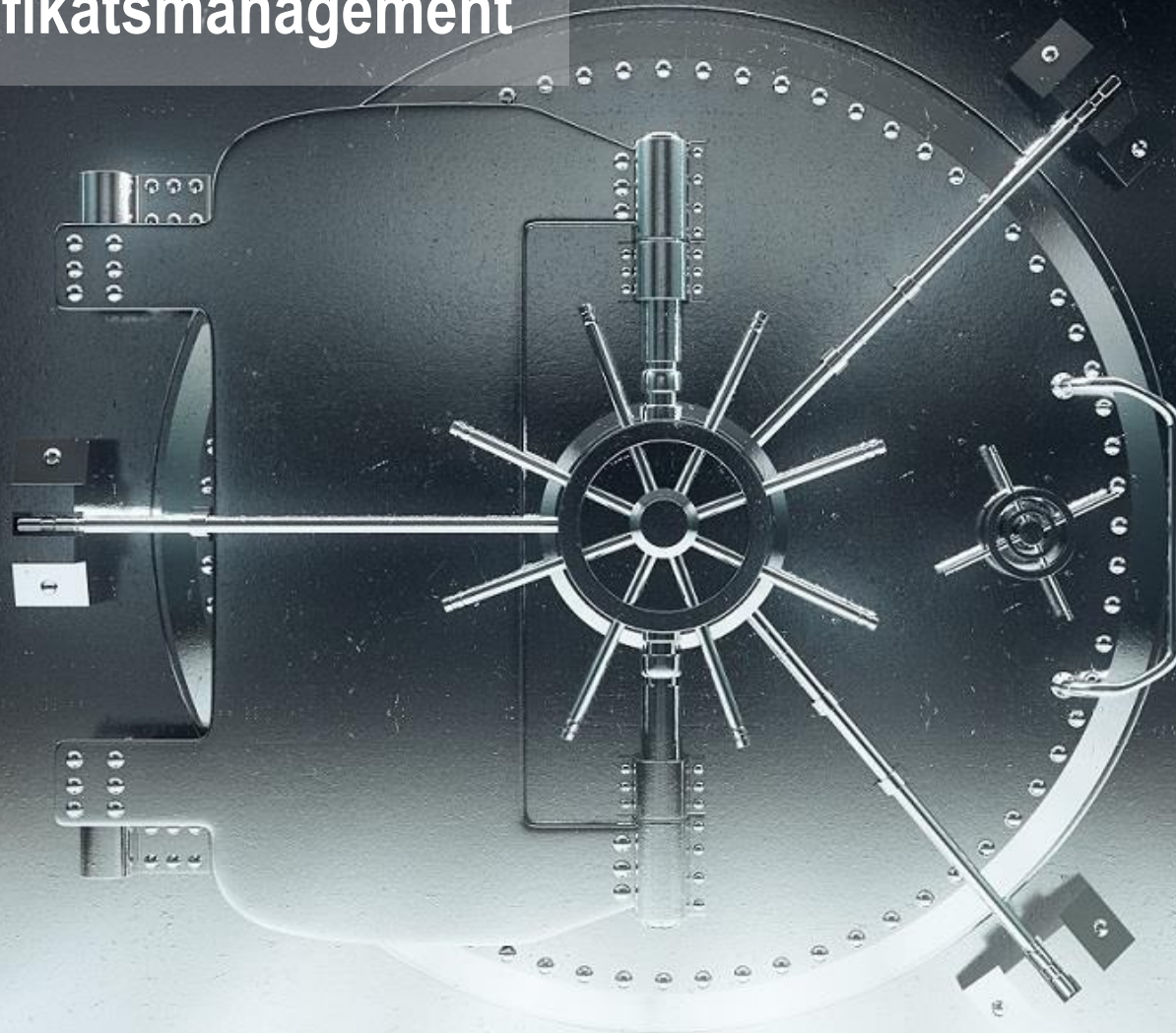
2. Schlüsselverwaltung mit essendi xc

- ✓ Schlüsselerzeugung: Feste Vorgaben für die Schlüssel, die generiert werden (bzgl. Algorithmus, Länge etc.)
- ✓ Schlüsselmanagement: Überwachung der Lebensdauer und des Status, inkl. Alertfunktion
- ✓ Zertifikats- und Schlüsselspeicherung: in HSM und Schlüsseltresor
- ✓ Kontrollierte Wiederherstellung von Schlüsseln im Falle von Vernichtung oder Verlust
- ✓ Zertifikats- und Schlüsselhandling : Erzeugen, Erneuern, Transport etc. (strukturiert nach Standardprozessen und festen, firmeninternen Vorgaben)
- ✓ Vorausschauendes Risikomanagement
- ✓ Dokumentation



essendi **xc**

Besseres Zertifikatsmanagement



essendi 

ist ISO-konform, auch in anderen,
informationssicherheitsrelevanten Bereichen.

Sprechen Sie uns an.

 **SwissSign**

securosys

TrustSeal – 100 % Software made in Germany

essendi 

SecurITy
made
in
Germany

Trust Seal
www.teletrust.de/itsmig



essendi **xc**

Ihr Kontakt:

Für Ihre
Rückfragen
oder eine Live-
Demo

Sarah Zügel

essendi it GmbH

Max-Planck-Str. 2

85609 Aschheim bei München

E-Mail: Sarah.Zuegel@essendi.de

Tel.: +49(0)89 944 697 71

HIER ENTSTEHT IT

- Informationstechnik-Sicherheitsverfahren-Informationssicherheitsmanagementsystem – Anforderungen (ISO / IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2: 2015); Deutsche Fassung EN ISO/IEC 27001:2017
- Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017
- https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html (abgerufen: 16.11.2017)
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02046.html (abgerufen: 16.11.2017)
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01007.html (abgerufen: 16.11.2017)
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05083.html (abgerufen: 27.11.2017)
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile (abgerufen: 27.11.2017)
- <http://www.searchsecurity.de/meinung/In-fuenf-Schritten-zur-Einhaltung-der-EU-Datenschutz-Grundverordnung> (abgerufen: 27.11.2017)
- https://www.datenschutz-hamburg.de/uploads/media/Hinweise_zur_Risikoanalyse_und_Vorabkontrolle.pdf (abgerufen: 27.11.2017)
- <https://www.projekt29.de/datenschutzblog29/umsetzung-der-eu-dsgvo-teil-20-datenschutz-folgenabschaetzung-leitlinien-zur-risikobewertung> (abgerufen: 27.11.2017)