

essendi xc – Zertifikatsmanagement neu gedacht

**im Kontext der DIN ISO 27001**

- **DIN 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 DIN ISO 27001: 2017-03 erfordert **Richtlinien** für den Gebrauch kryptografischer Maßnahmen und eine angemessene **Schlüsselerzeugung und -verwaltung**.

**Tabelle A.1 – Maßnahmenziele und Maßnahmen**

| A.10 Kryptographie                                                                                                                                              |                                                         |                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.10.1 Kryptographische Maßnahmen                                                                                                                               |                                                         |                                                                                                                                                                                      |
| Ziel: Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt. |                                                         |                                                                                                                                                                                      |
| A.10.1.1                                                                                                                                                        | Richtlinie zum Gebrauch von kryptographischen Maßnahmen | <i>Maßnahme</i><br>Eine Richtlinie für den Gebrauch von kryptographischen Maßnahmen zum Schutz von Information ist entwickelt und umgesetzt.                                         |
| A.10.1.2                                                                                                                                                        | Schlüsselverwaltung                                     | <i>Maßnahme</i><br>Eine Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln ist entwickelt und wird über deren gesamten Lebenszyklus umgesetzt. |

Quelle: DIN 27001:2017-03, Seite 21

Wiedergabe gestattet mit freundlicher Genehmigung durch DIN Deutsches Institut für Normung e.V.

## 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

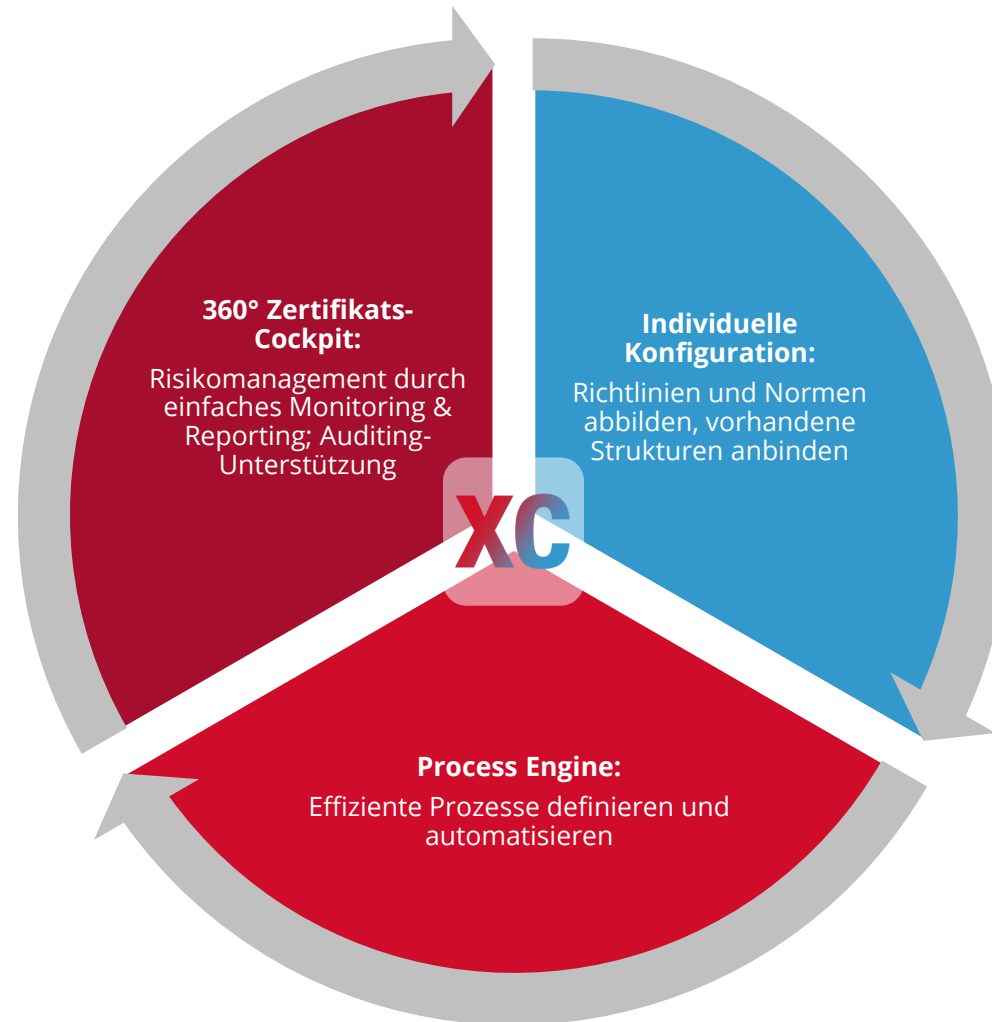
- Welches Verschlüsselungsverfahren soll genutzt werden?
- Management und Transparenz über vorhandene Schlüssel?
- Definierte Prozesse im Umgang mit Schlüsseln, z.B. für Ausstellung, Verteilen, Erneuerung etc.?
- Wer ist für die Einhaltung der Vorgaben zuständig?
- Verhalten bei Verlust der Schlüssel?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

The logo "XC" in a large, bold, sans-serif font. The "X" is red and the "C" is blue, with a gradient effect between them.

unterstützt Sie dabei im Bereich Zertifikatsmanagement.

# 1. essendi xc:

## Krypto-Richtlinien erfolgreich und effizient umsetzen





## 2. Key Management with 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





Besseres Zertifikatsmanagement





ist ISO-konform, auch in anderen,  
informationssicherheitsrelevanten  
Bereichen.  
Sprechen Sie uns an.

# Unsere Partner

**PSW GROUP**



**securosys**

**SwissSign**

**digicert®**

**digicert® + QuoVadis**

**utimaco®**



**intercede**







Trust Seal  
[www.teletrust.de/itsmig](http://www.teletrust.de/itsmig)

# Thank you

## EU Kontakt

essendi it GmbH

Dolanallee 19

DE-74523 Schwäbisch Hall

xc@essendi.de

xc.essendi.de

Tel.: +49 791 94 30 70 11

## Internationaler Kontakt

essendi it AG

Bahnhofplatz 1

CH-6460 Altdorf

xc@essendi.ch

xc.essendi.ch

Tel.: +41 41 874 27 30



## 27001:2017

- Informationstechnik-Sicherheitsverfahren-Informationssicherheitsmanagementsystem – Anforderungen (DIN ISO 27001:2013 einschließlich Cor 1:2014 und Cor 2: 2015); Deutsche Fassung EN ISO 27001:2017-03
- Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO 27002:2016-11
- [https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS\\_Zertifizierung\\_node.html](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](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](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](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](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](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> (retrieved: 27.11.2017)