

essendi xc – Redefining Certificate Management

**In the Context of DIN ISO 27001**

- **DIN ISO 27001** is an international certification standard designed to ensure **information security** (confidentiality, authenticity, integrity, etc.).
- **Goal:** Introduction of an information security management system (ISMS) in companies.

# Cryptography

One part of the list of measures is the area of "cryptoraphy".



The implementation of cryptographic measures within the framework of DIN ISO 27001 requires **guidelines** for the use of cryptographic measures and appropriate **key generation and management**.

Table A.1 – Goals and Actions

|  |   |  |
|--|---|--|
| <b>A.10 Cryptography</b>   |   |  |
| <b>A.10.1 Cryptographic Measures</b>   |   |  |
| Goal: The appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information is ensured. |   |  |
| A.10.1.1   | Guidelines on the use of cryptographic measures | Action:<br>A policy for the use of cryptographic measures to protect information has been developed and implemented.                   |
| A.10.1.2   | Key management                                  | Action:<br>A policy on the use, protection and lifetime of cryptographic keys is developed and implemented throughout their lifecycle. |

Source: inhouse translation of Table A.1 DIN ISO 27001, German Version

## 1. Cryptographic Guidelines

- What information needs to be protected?
- When does the information need to be protected and how intensively?
- Are external authentication authorities (CAs) required for the protection / signing of certain information?
- Processes: Who does what?
- Who is responsible for compliance with the conventions?
- What does sustainable controlling look like?
- etc.

## 2. Key Management

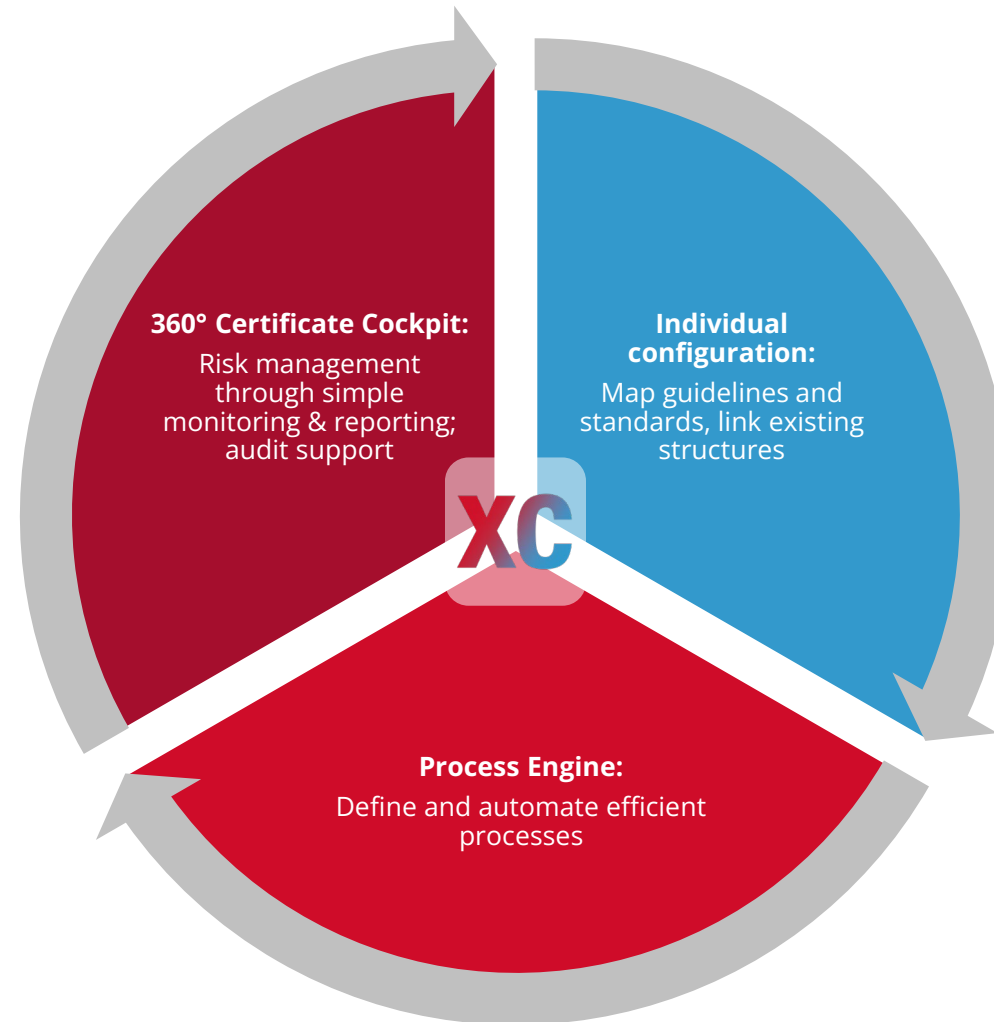
- Which encryption method should be used?
- Management and transparency about existing keys?
- Defined processes for handling keys, e.g. for issuing, distributing, renewing etc.?
- Who is responsible for compliance?
- What to do if the keys are lost?
- Lifespan of the keys?
- Who has access to the keys, including archived keys?
- etc.

The logo 'XC' is rendered in a large, bold, sans-serif font. The 'X' is solid red, and the 'C' is a gradient from purple to blue.

supports you in the area of certificate management.

# 1. essendi xc:

## Implementing crypto policies successfully and efficiently



## 2. Key Management with essendi xc

- ✓ Key generation: Fixed specifications for the keys that are generated (regarding algorithm, length, etc.).
- ✓ Key management: monitoring of service life and status, incl. alert function
- ✓ Certificate and key storage: in HSM and key vault
- ✓ Controlled recovery of keys in case of destruction or loss
- ✓ Certificate and key handling: generation, renewal, transport, etc. (structured according to standard processes and fixed, company-internal specifications)
- ✓ Forward-looking risk management
- ✓ Documentation





# Redefining Certificate Management



# XC

is ISO-compliant, also in other areas relevant to information security.

For more information, please get in touch.

# Business Partners

**PSW GROUP**



**securosys**

**SwissSign**

**digicert**

**digicert + QuoVadis**

**utimaco**



**intercede**



# SecurITy

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

made  
in  
Germany

# Thank you

## EU contact

essendi it GmbH

Dolanallee 19

DE-74523 Schwäbisch Hall

xc@essendi.de

xc.essendi.it

Tel.: +49 791 94 30 70 11

## International contact

essendi it AG

Bahnhofplatz 1

CH-6460 Altdorf

xc@essendi.ch

xc.essendi.it

Tel.: +41 41 874 27 30



## 27001:2017

- Information technology security procedures-Information security management system-Requirements (DIN ISO 27001:2013 including Cor 1:2014 and Cor 2: 2015); German version EN ISO 27001:2017-03.
- Information technology - Security procedures - Guidance for information security measures (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015); German version 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) (retrieved: 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) (retrieved: 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) (retrieved: 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) (retrieved: 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) (retrieved: 27.11.2017)
- <http://www.searchsecurity.de/meinung/In-fuenf-Schritten-zur-Einhaltung-der-EU-Datenschutz-Grundverordnung> (retrieved: 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) (retrieved: 27.11.2017)
- <https://www.projekt29.de/datenschutzblog29/umsetzung-der-eu-dsgvo-teil-20-datenschutz-folgenabschaetzung-leitlinien-zur-risikobewertung> (retrieved: 27.11.2017)