cryptas

we protect identities.

NIS2 – Praxisbeispiel: Umsetzung Kryptografie

10.8.2023

Author: DI (FH) Stefan Bumerl
stefan.bumerl@cryptas.com

Document Version: 1.0
Creation Date: 3/2023

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

About CRYPTAS

SPECIALIST FOR PKI, STRONG AUTHENTICATION, ENCRYPTION, LAWFUL SIGNATURES AND DIGITAL IDENTITIES

Own solutions around Digital Signatures, Virtual Smart Card, clientless Smart Card access, Self-Service Processes, PKI, OCSP++...

CONSULTING, DEVELOPMENT, INTEGRATION, SERVICES

Topics: eSignature, Smart Cards, PKI, FIM, Key Management, HSM, Encryption...

WIEN, GRAZ, DÜSSELDORF, HENGELO AND STOCKHOLM

Successful in crypto-business since 2003; main markets D/A/CH, Typical Project Size: 1.000 to 300.000 Users

> 50.000 CUSTOMERS / ~100 COUNTRIES /

Verticals: banking, insurance, energy provider, health, industry, government...

eIDAS TRUST CENTER

Qualified Trust Center with focus on Qualified Onboarding, eIDAS Online Contracting, Video-Legitimation, eIDAS Remote Services

Millions Transactions per Day

Thousands Enrollments per Day

> 3 Millions qualified certificates issued to 163 nationalities

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

NIS2 (EU 2022/2555) Verordnung - Inhalt

+ Kapitelüberisicht

I. ALLGEMEINE BESTIMMUNGEN
II. KOORDINIERTE RAHMEN FÜR DIE CYBERSICHERHEIT
III. ZUSAMMENARBEIT AUF UNIONS- UND INTERNATIONALER EBENE
IV. RISIKOMANAGEMENTMAßNAHMEN UND BERICHTSPFLICHTEN IM BEREICH DER CYBERSICHERHEIT
V. ZUSTÄNDIGKEIT UND REGISTRIERUNG
VI. INFORMATIONSAUSTAUSCH
VII. AUFSICHT UND DURCHSETZUNG
VIII. DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE
IX. SCHLUSSBESTIMMUNGEN

+ Anhänge

I. SEKTOREN MIT HOHER KRITIKALITÄT ("Wesentliche Dienste" / "Essential")
II. SONSTIGE KRITISCHE SEKTOREN ("Wichtige Dienste" / "Important")
III. ENTSPRECHUNGSTABELLE

Pflicht für Mitgliedstaaten:
Einrichten von Anlaufstellen, CSIRT...

Pflicht für Betroffene:
Cybersicherheitsrisikomanagement

Pflichten zum Austausch von
Cybersicherheitsinformationen

Pflicht für Mitgliedstaaten:
Aufsichts- und Durchsetzungspflichten

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

Artikel 21: Risikomanagementmaßnahmen im Bereich der Cybersicherheit

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Business Continuity (Backup-Mangement, Notfall- und Krisenmangement
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen
- Cyberhygiene and Schulungen
- Verfahren zur Bewertung der Wirksamkeit
- Verfahren für den Einsatz von Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Zugriffskontrolle
- Multi-Faktor-Authentifizierung, gesicherte Kommunikationswege

Organizational Measures

Management systems like ISMS and BCMS

Technological Measures

Implementing "State of the Art" mechanisms

Attack detection

Utilizing SIEM or CSIRT/SOC

→ Niveau: "Stand der Technik" und ggf. einschlägige Standards

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

Technikklausel „Stand der Technik"

- Generell:
  Die Anforderungsschwelle des Standes der Technik gilt als erreicht, wenn das tatsächlich gesetzte Verhalten fortschrittlich ist, auf einschlägigen wissenschaftlichen Erkenntnissen beruht, und seine Funktionstüchtigkeit erprobt und erwiesen ist."

- Fortschrittlichkeit:
  - macht den Vergleich mit alternativen Verhaltensweisen notwendig
  - ... wenn das damit verfolgte Ziel im konkreten Fall besser erreicht werden kann...
  - Verhältnismäßigkeit ist zu berücksichtigen

- ISO 27000 – Reihe als Stand der Technik anerkannt

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

Konkretes Beispiel: „Einsatz von Kryptografie"

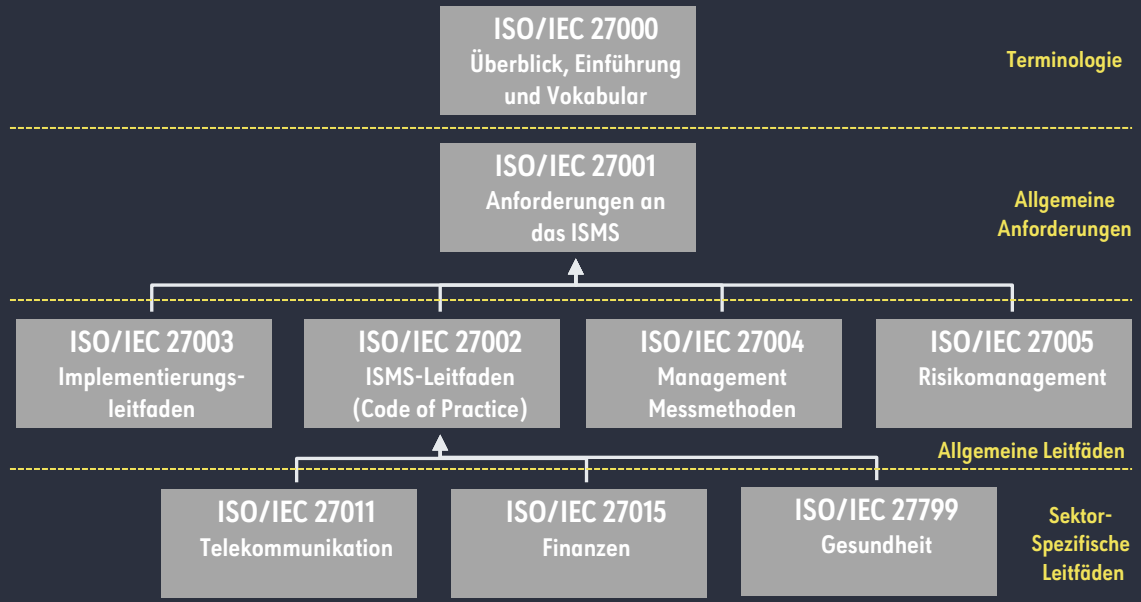
... wesentliche und wichtige Einrichtungen ... ergreifen geeignete und verhältnismäßige Maßnahmen ... unter Berücksichtigung des Stands der Technik und einschlägigen Normen ... beruhend auf einem gefahrenübergreifenden Ansatz ... welche umfassen:

...
h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
...

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

ISO 27000-Reihe als Grundlage



Unterstützende Normen

ISO/IEC 27010 Inter-sector Communication	ISO/IEC 27014 Governance Framework
ISO/IEC 27031 Business Continuity	ISO/IEC 27032 Cyber Security
ISO/IEC 27033 Network Security	ISO/IEC 27034 Application Security
ISO/IEC 27035 Security Incident Management	ISO/IEC 27036 Outsourcing
ISO/IEC 27037 Digital Evidence	ISO/IEC 27099 PKI Trust Services

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

Was sagt die ISO27001 dazu?

A.10 Cryptography		
A.10.1 Cryptographic controls		
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.		
A.10.1.1	Policy on the use of cryptographic controls	*Control* A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
A.10.1.2	Key management	*Control* A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

Mehr dazu in ISO 27002 -> Section 10 Cryptography!

10.1.1 Policy on the use of cryptographic controls

When developing a cryptographic policy the following should be considered:

a) the management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected;

b) based on a risk assessment, the required level of protection should be identified taking into account the type, strength and quality of the encryption algorithm required;

(...)

Cryptographic controls can be used to achieve different information security objectives, e.g.:

a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;

b) integrity/authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information;

c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or nonoccurrence of an event or action;

d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

Mehr dazu in ISO 27002 -> Section 10 Cryptography!

10.1.2 Key management

The policy should include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys. (...)

A key management system should be based on an agreed set of standards, procedures and secure methods for:
a) generating keys for different cryptographic systems and different applications;
b) issuing and obtaining public key certificates;
c) distributing keys to intended entities, including how keys should be activated when received;
d) storing keys, including how authorized users obtain access to keys;
e) changing or updating keys including rules on when keys should be changed and how this will be done;
f) dealing with compromised keys;
g) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);
h) recovering keys that are lost or corrupted;
(...)

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

BSI – Gesetz: §30 Risikomanagementaufgaben

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf ihre oder andere Dienste zu verhindern oder möglichst gering zu halten.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe der Einrichtung oder des Betreibers sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen.

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

Themenumfang...

	User	Device	Service	Software	Data
Authenticity	MFA	Certificates	Certificates	Code Signing	Dig Signatur
Integrity	Onboarding	Cert Mgmt.	Cert Mgmt.	Code Signing	Dig Signatur
Confidentiality	Certificates	Certificates	Certificates	Encryption	Encryption
Accountability	Cred Mgmt.	Cert Mgmt.	Cert Mgmt.	Cert Mgmt.	Cert Mgmt.
Availability	Decoupling	Validation	Validation	X	Backup

→ (Qualified) Trust Service – PKI als zentrale Basis!

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

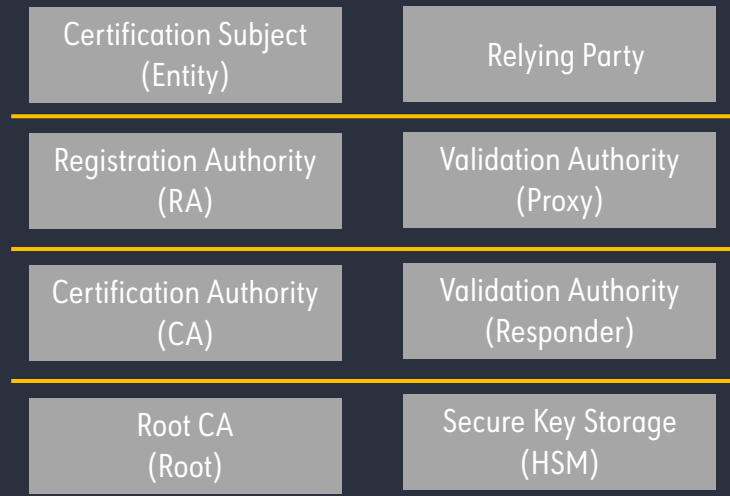
cryptas
we protect identities.

ISO 27099:2022 Public key infrastructures – Practices and policy

- Rahmen von Anforderungen um die Informationssicherheit von PKI Trust Services umzusetzen
- Standard beschreibt die Verwendung eines ISO27001 ISMS als PKI Management Framework
- Section 7: CA objectives and controls inkl. Anforderungen an den Betrieb (>300!)

z.B. Trennung der Netzwerke:

Sensitive systems (e.g. root CA) shall require a dedicated (isolated) computing environment.
Controls (e.g. firewalls) shall be in place to protect the CA's internal network domain from any unauthorized access from any other domain.
The network relating to the process of certificate-management shall be separated from all other networks. The separation of the network should rely on an appropriate physical or logical separation from untrusted networks. For example, physical separation or appropriate firewall, switch and routing capability shall be utilized.



CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

ISO 27099:2022 Public key infrastructures – Objectives and Controls

- z.B. Anforderungen an die Betriebsumgebung

The CA shall employ personnel who possess the relevant skills, knowledge, and experience appropriate for the job function.

Procedures shall exist and be followed to control physical and logical access to CA facilities and systems by third parties (e.g. on-site contractors, trading partners and joint ventures).

Physical access to CA facilities shall be limited to authorized individuals or, in the case of virtualised environment, CA software shall be isolated from other software and cannot be accessed by unauthorised individuals.

- z.B. Anforderungen an Schlüsselspeicherung (HSM)

The CA's private (signing and confidentiality) keys shall be stored and used within a secure cryptographic device meeting requirements based on a risk assessment and the business requirements of the CA and in accordance with the CA's CPS and applicable certificate policies. When defining the requirements, an appropriate ISO/IEC 15408 / common criteria protection profile EAL 4 AVA_VAN.5 (or higher), ISO/IEC 19790 / FIPS 140-2 level 3 (or higher), or equivalent standards should be considered and taken into account.

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

ISO 27099:2022 Public key infrastructures – Objectives and Controls

- z.B. Anforderungen an die Zugriffskontrolle

Business requirements for access control shall be defined and documented in an access control policy which includes at least the following:

a) roles and corresponding access permissions;

b) identification and authentication process for each user;

c) segregation of duties;

d) number of persons required to perform specific CA operations (i.e. *m* of *n* rule where *m* represents the number of key shareholders required to perform an operation and *n* represents the total number of key shares).

- z.B. Anforderungen an Betriebsführung

Development and testing facilities shall have a physical or logical separation from operational facilities.

cryptographic devices used for storage of back-up CA private keys shall be securely stored at an off-site location in order to be recovered by the CA in the event of a disaster at the primary CA facility;

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

ISO 27099:2022 Public key infrastructures – Objectives and Controls

- z.B. Anforderungen an den Zertifikatslebenszyklus

To maintain controls to provide reasonable assurance that certificates are revoked in a timely manner and information about revoked certificates is published as dictated by risk, based on authorized and validated certificate revocation requests.

- z.B. Anforderungen wenn HW-Token verwendet werden

If the CA (or RA) distributes subject key pairs and certificates to minimize the risk of key compromise during hardware token preparation and dissemination that is, to provide reasonable assurance for:

a) securely controlling hardware token procurement, preparation, and personalization;

b) enabling hardware token usage by the CA (or RA or other authorized third party) prior to hardware token issuance;

c) securely storing and distribute hardware tokens;

d) securely replacing hardware tokens;

e) securely terminating hardware tokens returned to the CA (or RA or other authorized third party).

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

Weitere wichtige Betrachtungen im Umfeld PKI

- Sperrinformationen: Blacklist (CRL) vs. Whitelist (OCSP)
- Verfügbarkeit bei DDoS
- Disaster Recovery: Primary Identity Konzept (Entkoppelung)
- Performance – insbesondere bei globalen Deployments
- ...

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com