cryptas

we establish trust.

intercede

Zertifikats- und Credential Management

Grundpfeiler von ZeroTrust

24.04.2024

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

Document Version: 1.0
Creation Date: 04/2024

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

cryptas
we protect identities.

intercede

NIS2 @CRYPTAS

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

cryptas
we protect identities.

intercede

- DIREKT betroffen

  → qTSP

- INDIREKT betroffen

  → viele DIREKT betroffenen Kunden

- DIREKT betroffen

  → Managed (Security) Services

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

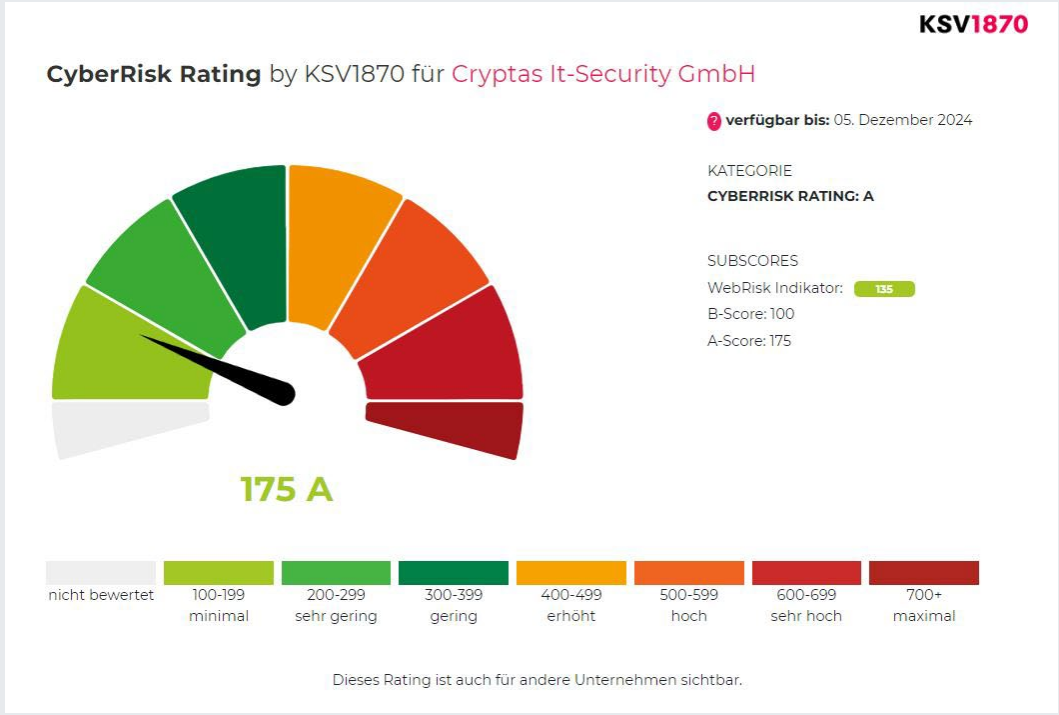
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm

cryptas
we protect identities.

intercede

Nach dem Audit ist...
...vor dem Audit

TÜV AUSTRIA
ZERTIFIZIERT
ISO/IEC 27001
ZERTIFIKAT NR. TA420223013993
TÜV AUSTRIA GMBH



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

cryptas
we protect identities.

intercede

EU

NIS2 Artikel 21: Cybersecurity risk-management measures

- Policies on risk analysis and information system security
- Incident handling
- Business continuity (backup management, disaster recovery and crisis management)
- Supply chain security
- Security in network and information systems acquisition, development and maintenance
- Cyber hygiene and training
- Procedures to assess the effectiveness
- Procedures regarding the use of cryptography and encryption
- Human resources security, access control
- Multi-factor authentication, secured communication systems

Organizational Measures

Management systems like ISMS and BCMS

Technological Measures

Implementing "State of the Art" mechanisms

Operational Measures

including SIEM or CSIRT/SOC

→ Level: "State-of-the-art" and relevant 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.

intercede

EU

Konkretes Beispiel: Kryptografie und MFA

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

...

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

...

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung

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

cryptas
we protect identities.

intercede

ISO/IEC 29115 – Entity authentication assurance framework

	Technical		Management & Organizational
Enrolment phase	• Application and initiation • Identity proofing • Identity verification	• Record-keeping recording • Registration	• Service establishment • Legal and contractual compliance • Financial provisions • Information security management and audit • External service components • Operational infrastructure • Measuring operational capabilities
Credential management phase	• Credential creation • Credential pre-processing • Credential initialization • Credential binding • Credential issuance • Credential activation	• Credential storage • Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement • Record-keeping	
Entity authentication phase	• Authentication • Record-keeping		

Relevant criteria for Levels of Assurances (LoAs)

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Vienna . 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 TR-03107

Gefährdung	Potentieller Schaden bedingt Vertrauensniveau		
	Normal	**Substantiell**	**Hoch**
Verstoß gegen Gesetze/Vorschriften	Verstoß mit geringfügigen Konsequenzen	Verstoß mit substantiellen Konsequenzen	Verstoß mit erheblichen Konsequenzen Besondere Formvorschriften (*hoch +*) bei Gefahr eines Verstoßes mit schwerwiegenden Konsequenzen
Unrichtige Identifizierung oder Zuordnung zu einer Identität	Geringfügige Konsequenzen	Substantielle Konsequenzen	Erhebliche Konsequenzen Besondere Formvorschriften (*hoch +*) bei Gefahr von schwerwiegenden Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen beeinträchtigen können.	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen substantiell beeinträchtigen können.	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen können.
Beeinträchtigung körperlicher/persönlicher Unversehrtheit	Beeinträchtigung erscheint nicht möglich	Beeinträchtigung kann nicht vollständig ausgeschlossen werden	Beeinträchtigung kann nicht ausgeschlossen werden
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird von den Betroffenen als tolerabel eingeschätzt	Beeinträchtigung wird von einzelnen Betroffenen als tolerabel eingeschätzt	Beeinträchtigung wird als nicht tolerabel eingeschätzt
Negative Innen- oder Außenwirkung	Geringe/nur interne Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	Substantielle Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	Breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten
Finanzielle Auswirkungen	Finanzieller Schaden tolerabel	Substantieller finanzieller Schaden möglich	Beachtliche finanzielle Verluste, jedoch nicht existenzbedrohend
Zu beachten: Die Aggregation von Gefährdungen kann zur Erhöhung des notwendigen Vertrauensniveaus führen. Zum Beispiel kann die Verarbeitung personenbezogener Daten mit Schutzbedarf *substantiell* zu einem notwendigen Vertrauensniveau *hoch* führen, wenn viele Personen von einer Beeinträchtigung betroffen sind. Sind mehrere Gefährdungen relevant, so ist für die Gesamtbewertung das Maximum der einzeln ermittelten notwendigen Vertrauensniveaus anzunehmen.			

		Vertrauensniveau		
		normal	**substantiell**	**hoch**
Enrolment (Abschnitt 3.2)		Bekannte Stelle (vgl. Abschnitt 3.5.1)	Vertrauenswürdige Stelle (vgl. Abschnitt 3.5.2)	Vertrauenswürdige Stelle (vgl. Abschnitt 3.5.2) Für Formvorschriften (*hoch +*) ggf. besondere Anforderungen (vgl. Abschnitt 3.5.3)
	Identitätsprüfung (Abschnitt 3.2.1)	Nach [eIDAS LoA] bzw. [TR-03147]		
	Ausgabe (Abschnitt 3.2.2)	Nur an Berechtigte	Nur an Berechtigte Zwei Wege	Nur an Berechtigte Zwei Wege Explizite Aktivierung
Authentisierung (Abschnitt 3.3)		Sicher gegen Angriffspotential *enhanced-basic*	Sicher gegen Angriffspotential *moderate*	Sicher gegen Angriffspotential *high*
	Faktoren (Abschnitt 3.3.1)	Ein Faktor	Zwei Faktoren	Zwei Faktoren manipulationssicher
	Verfahren (Abschnitt 3.3.2)		Dynamische Authentisierung	Dynamische Authentisierung
Rückruf/Sperrung (Abschnitt 3.4)		≤ 24h	≤ 12h	≤ 1h
Alle relevante Stellen (Abschnitt 3.5)		Bekannte Stelle (vgl. Abschnitt 3.5.1)	Vertrauenswürdige Stelle (vgl. Abschnitt 3.5.2)	Vertrauenswürdige Stelle (vgl. Abschnitt 3.5.2) Für Formvorschriften (*hoch +*) ggf. besondere Anforderungen (vgl. Abschnitt 3.5.3)
Absicherung von Kommunikationsbeziehungen (Abschnitt 3.6)		Absicherung auf Transportebene	Ende-zu-Ende-Beziehung bzw. Absicherung durch vertrauenswürdige Stellen (vgl. Abschnitt 3.5.2)	Ende-zu-Ende-Beziehung bzw. Absicherung durch vertrauenswürdige Stellen (vgl. Abschnitt 3.5.2) Für Formvorschriften (*hoch +*) ggf. besondere Anforderungen (vgl. Abschnitt 3.5.3)
Beim Einsatz von Kryptographie (Abs. 3.7)	**Algorithmen / Schlüssellängen**	[TR-03116] / [TR-02102]		
	Schlüsselspeicherung	Vor unberechtigtem Zugriff geschützt	Vor unberechtigtem Zugriff geschützt	Nach geeignetem Common Criteria-Schutzprofil ~~zertifizierte Hardware~~ für private Schlüssel

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Vienna . 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.

Anforderungen an Faktoren

	Besitz	Wissen	Biometrie
Prävention			
Bindung an Inhaber	Einmaligkeit des Besitzes, Besitz darf nicht kopierbar sein und Inhaber darf Besitz nicht weitergeben	Nur Inhaber kennt das Wissen, Wissen darf nicht weitergegeben werden.	Inhaberspezifische biometrische Merkmale, Lebenderkennung
Kontrolle durch Inhaber setzt voraus:	Besitz unter physischer Kontrolle des Inhabers, Besitz wird nur zur Authentisierung genutzt	Wissen wird nur zur Authentisierung genutzt	Biometrisches Merkmal wird nur zur Authentisierung genutzt
Detektion			
Erkennen des Kontrollverlustes	Verlust des Besitzes; zusätzlich durch Missbrauchserkennung	Nur nachträglich durch Missbrauchserkennung in der Anwendung / heuristisches Profiling durch zentralen Server	
Reaktion			
Sperren der Mittel	Sperre über eindeutiges Merkmal des Besitzes	Sperren des zugehörigen Accounts (bei entfernter Verifikation durch Server) oder Besitzes (bei lokaler Verifikation durch Besitztoken)	
Ersatz für gesperrte Authentisierungsmittel	Ausstellen eines neuen Besitztokens	Setzen eines neuen Passworts / einer neuen PIN	Registrierung und Nutzung eines anderen biometrischen Merkmals

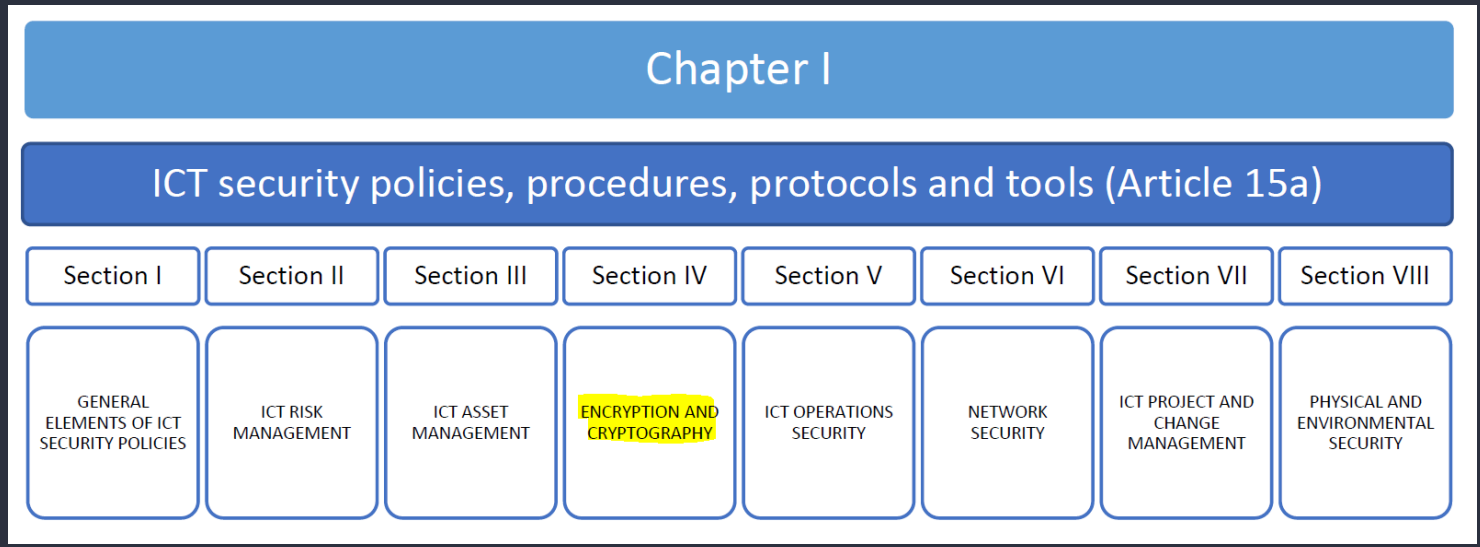
CRYPTAS International GmbH
Franzosengraben 8 . 1030 Vienna . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com

cryptas
we protect identities.

intercede

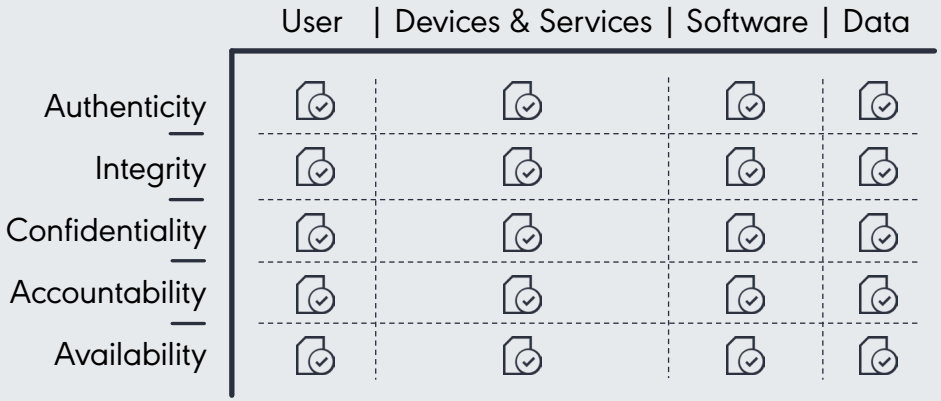
EU

DORA Regulatory Technical Standards (DRAFT)



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



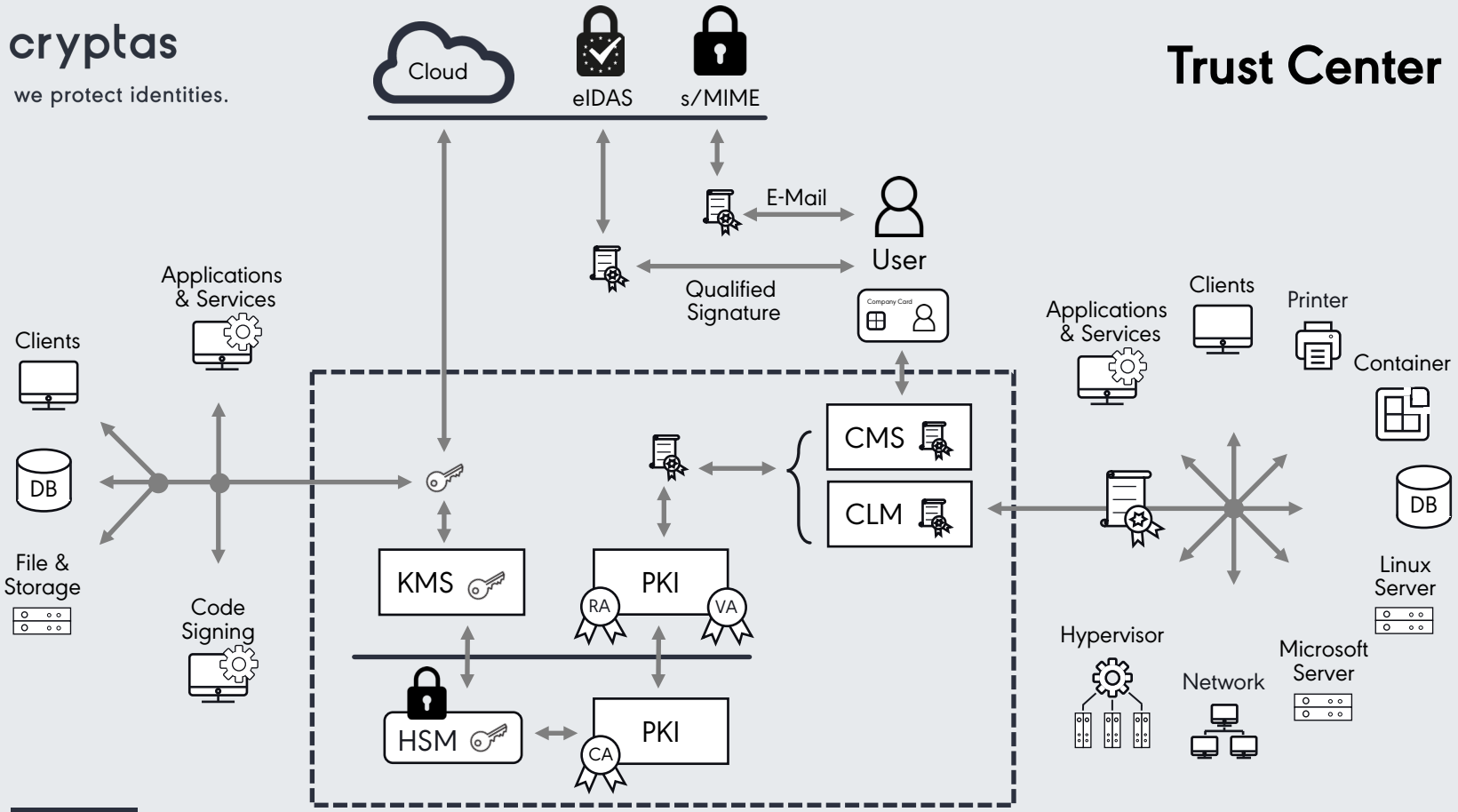
NIS-2
DORA
ISO 27001

CRYPTAS International GmbH
Franzosengraben 8 . 1030 Vienna . 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.

Trust Center



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

cryptas

we establish trust.

intercede

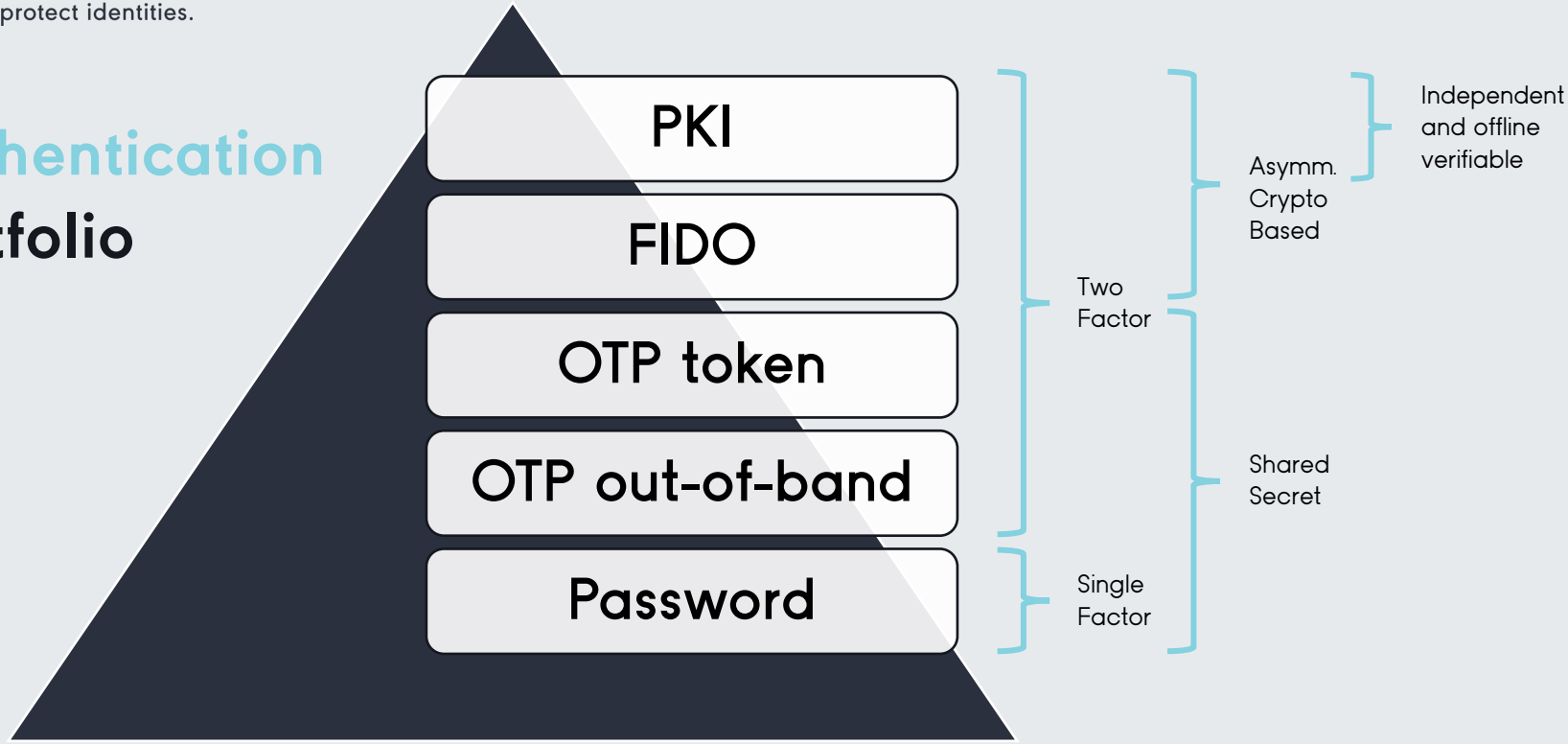
2-Faktor Authentifizierung

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

cryptas
we protect identities.

intercede

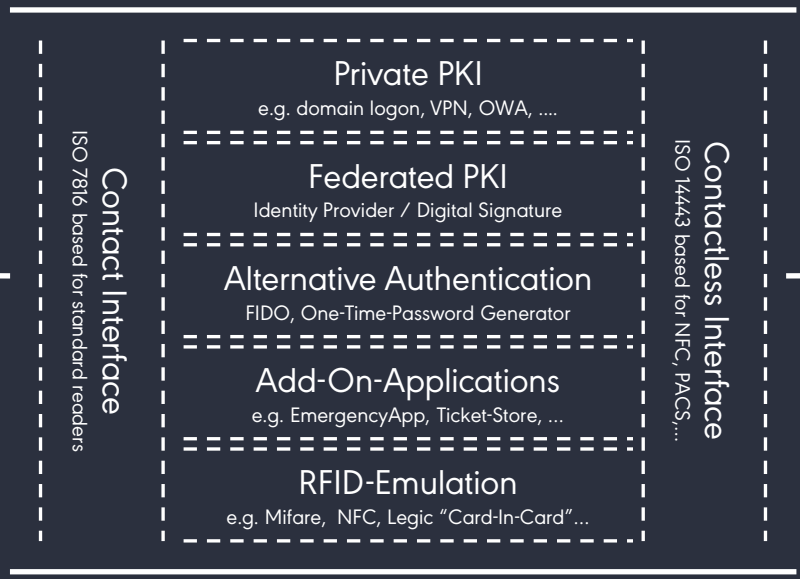
Authentication Portfolio



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

cryptas
we protect identities.

egofy CARD



Cost efficient
Existing environment
Reliability

Mobile Environments
Fast Transactions
NFC Compatibility

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

cryptas
we protect identities.

intercede

PKI Smart Cards "legacy" ?

+ 30 years of standardisation lead to broad integration of technlogogy
+ Technological independency (algorithms, systems, protocols...)
+ Long term proven in different significant application fields (payment, government, network...)
+ De-coupled, cross-organisational Identity Management System
+ interdisciplinary approach (from technology via von governance to legal)
+ Well established in European legal framework (eIDAS)

→ Much more than yet another authentication scheme!

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

cryptas

we establish trust.

intercede

Credential Management

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 | Stockholm

cryptas
we protect identities.

intercede

About Intercede

Focus
- Cybersecurity software company focused on digital identities, credential management and strong authentication

People
- 100 employees in UK and US
- All development in house
- Support
- Professional Services

Experience
- 20+ years of subject matter expertise
- Standards bodies and industry alliance cooperation

Certified
- ISO 27001
- ISO 9001
- Multiple ATOs granted

Customers
- Government, Military, Aerospace & Defense, Healthcare, Banking, Manufacturing...

Scalable
- From hundreds to millions of users

Products
- Commercial off-the-shelf product family
- Available standalone
- Integrated solution

Partners
- Technology partners
- Integration partners
- Reseller partners

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 | Stockholm

cryptas
we protect identities.

intercede

What is MyID?

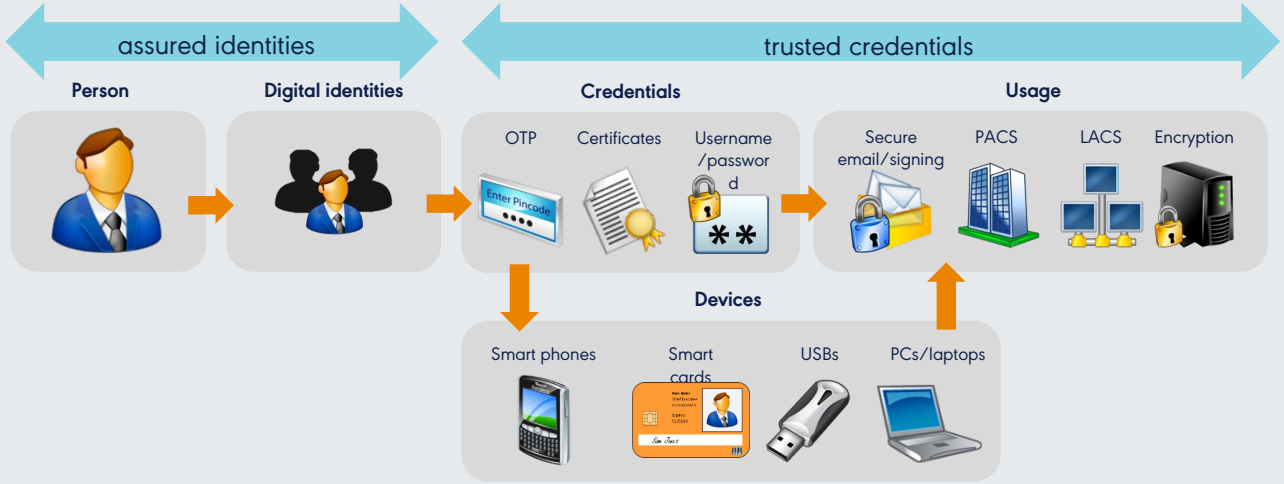
CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

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

cryptas
we protect identities.

intercede

What is MyID?



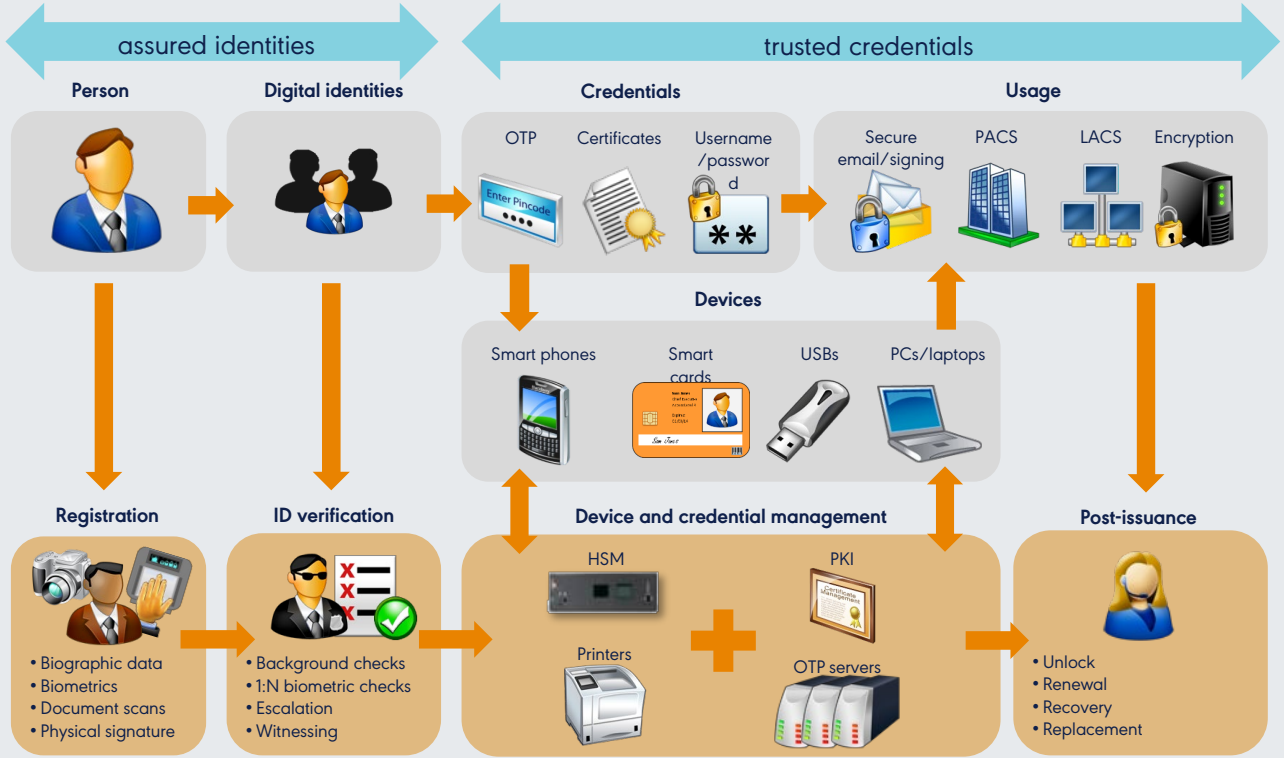
CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

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

cryptas
we protect identities.

intercede

What is MyID?



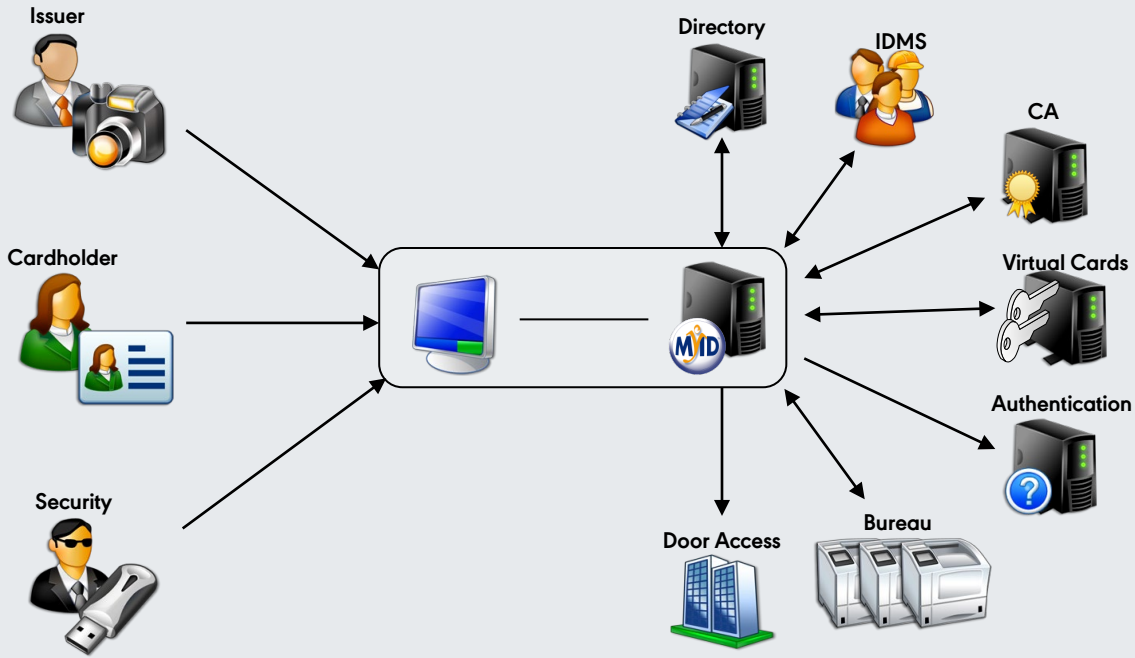
CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

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

cryptas
we protect identities.

intercede

Typical Credential Management Schema



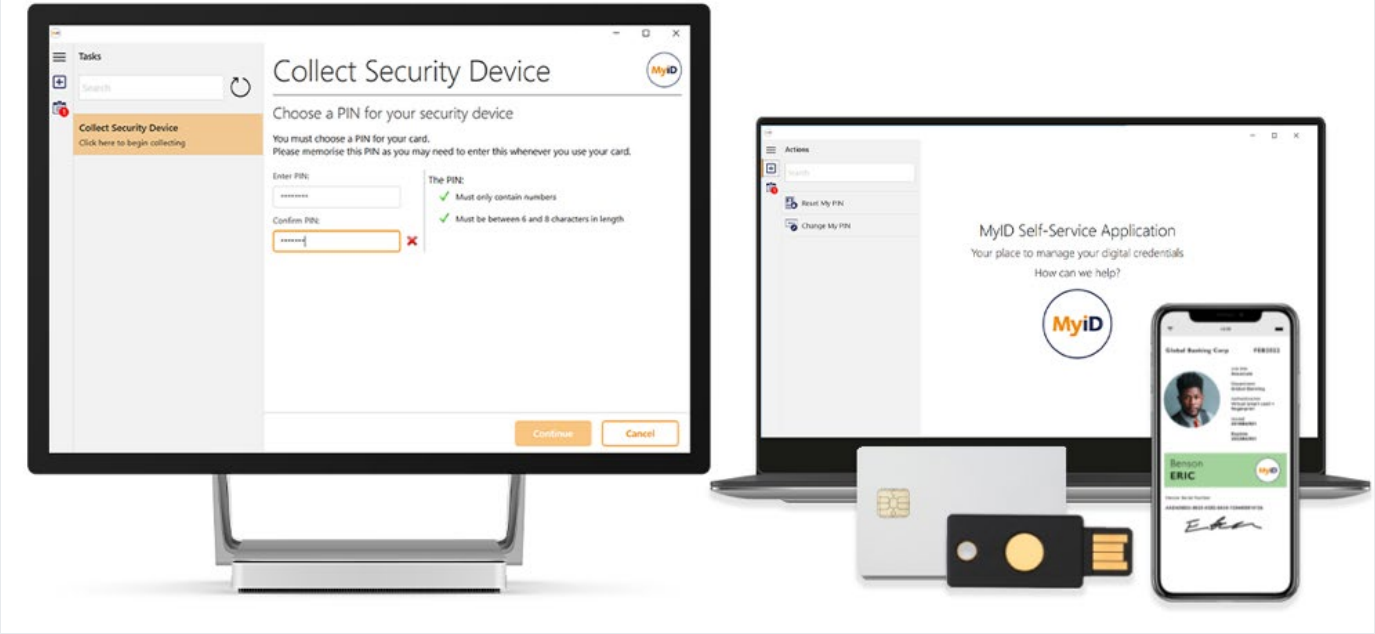
CRYPTAS International GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

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

cryptas
we protect identities.

intercede

Self Service!



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 | Stockholm

cryptas

we protect identities.

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