TÜVIT

Omnisecure 2023

Auf dem besten Wege zum Qualifizierten Vertrauensdienst gemäß eIDAS 2014 und 2024

Matthias Wiedenhorst | Omnisecure 2023 | 24.05.2023

eIDAS – Arten von Vertrauensdiensteanbietern

Vertrauensdiensteanbieter
(VDA / TSP)

- Müssen die Anforderungen der eIDAS einhalten
- Unterliegen einer ex-post Aufsicht durch die national zuständige Aufsichtsbehörde
- Sicherheitsmaßnahmen / ISMS nach dem Stand der Technik
- Mitteilungspflicht über Sicherheitsvorfälle an die national zuständigen Stellen

Qualifizierter Vertrauensdiensteanbieter
(QVDA / QTSP)

- Nationale Qualifizierung
- Eintrag auf der ‘trusted list’
- Konformitätsbewertung erforderlich
- ex-ante Aufsicht durch die national zuständige Aufsichtsbehörde

TÜVIT

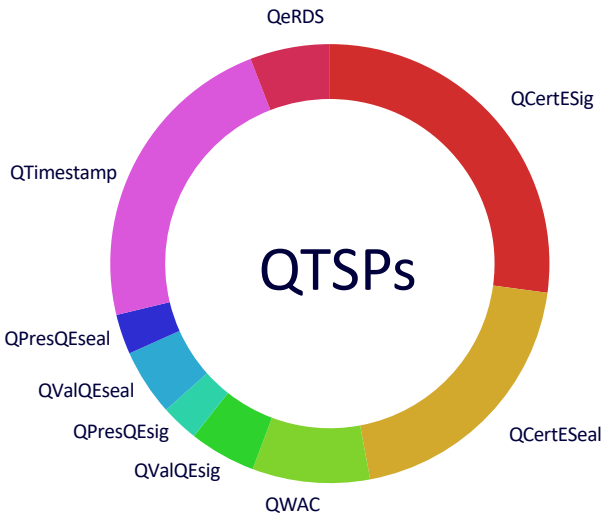
Arten von qualifizierten Vertrauensdiensten

eIDAS 2014

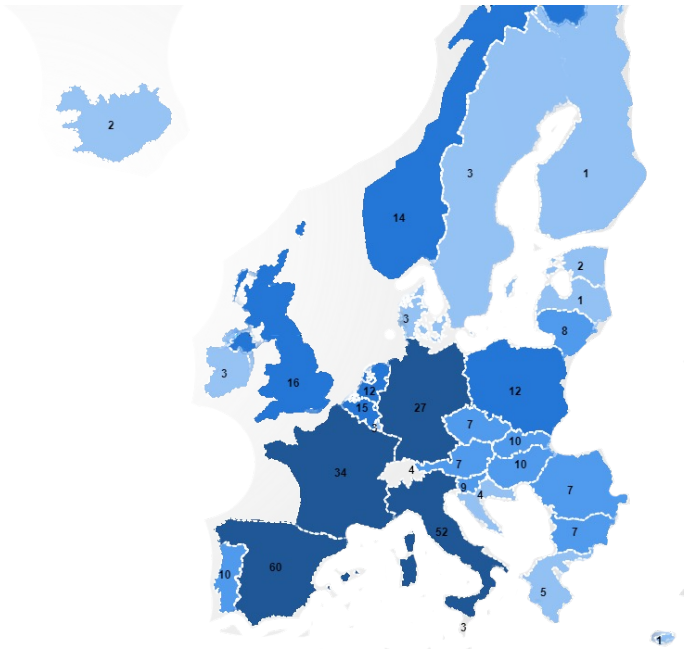
Mögliche Vertrauensdienste der Qualitätsstufe “EU qualified”

- Erstellung von Zertifikaten für elektronische Signaturen
- Erstellung von Zertifikaten für elektronische Siegel
- Erstellung von elektronischen Zeitstempeln
- Validierung von Signaturen und Siegeln
- Elektronische Zustelldienste
- Bewahrung von Signaturen und Siegeln
- Erstellung von Zertifikate für Website-Authentisierung

Anzahl der aktiven qualifizierten Trust Service Provider (QTSPs) nach Typ



Anzahl der aktiven Trust Service Provider (TSPs)



TÜVIT

Zusätzliche qualifizierte Vertrauensdienste

eIDAS 2024

Derzeit vorgesehene zusätzliche Vertrauensdienste der Qualitätsstufe “EU qualified”

- Management of remote qualified electronic signature creation devices
- Management of remote qualified electronic seal creation devices
- Issuance of qualified electronic attestation of attributes
- Qualified electronic archiving services

Nicht mehr zur Einführung vorgesehen

- Qualified electronic ledger

Weiterhin nicht als qual. Vertrauensdienst vorgesehen

- Creation of qualified electronic signatures / seals

NIS 2

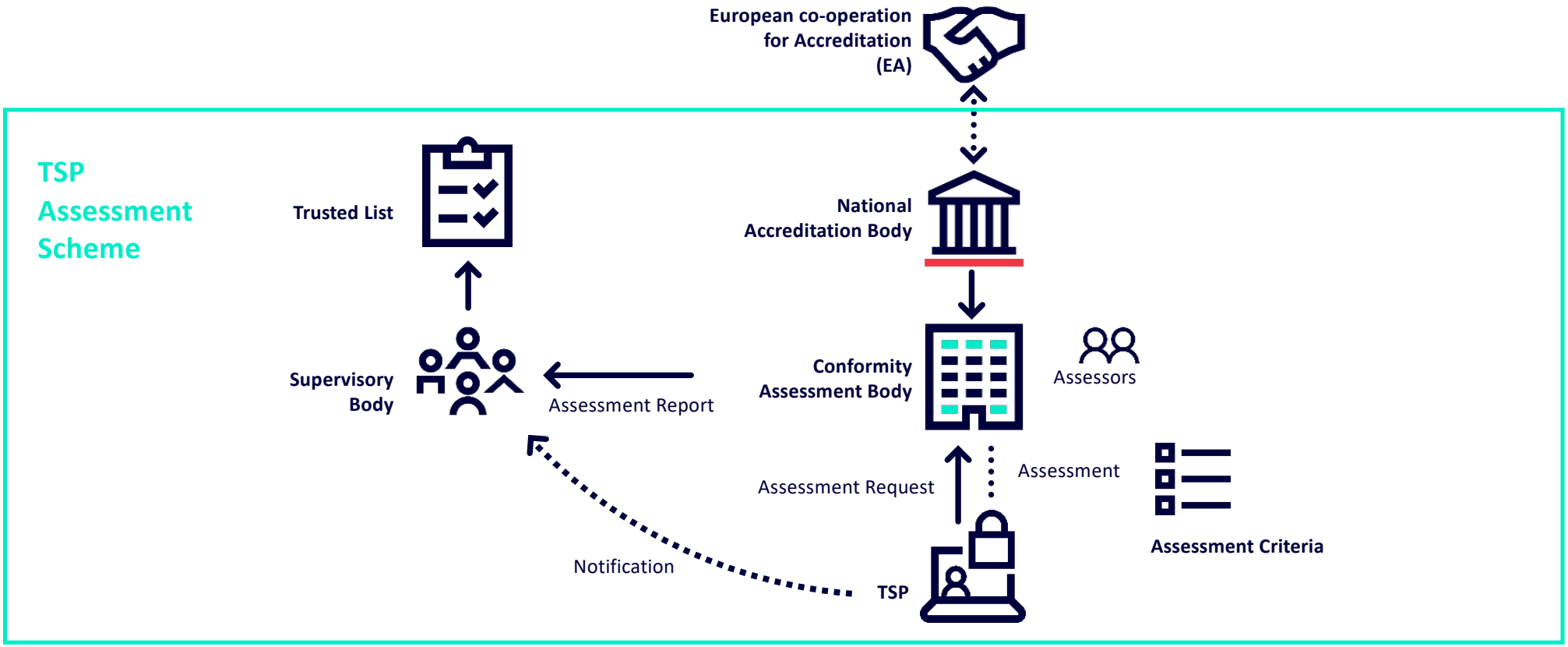
- **Artikel 19**, eIDAS („Sicherheitsanforderungen an Vertrauensdiensteanbieter“) wird mit **Wirkung zum 18.10.2024 gestrichen**. Stattdessen gelten dann die Anforderungen der jeweiligen nationalen NIS2-Umsetzung

- Die **Konformitätsbewertung** der qualifizierten Vertrauens-diensteanbieter soll sowohl die Erfüllung der relevanten **Anforderungen der eIDAS als auch der NIS2 umfassen**.

- Details über die **Anerkennung der eIDAS-Konformitäts-bewertungsstellen** und der von Ihnen durchgeführten Konformitätsbewertungen durch die für NIS2 zuständigen **Aufsichtsbehörden sind derzeit noch offen**.

TÜVIT

Konformitätsbewertung und beteiligte Stellen



TÜVIT

Prozess der Konformitätsbewertung





≈ **6 Monate** vom Kick-Off bis zur Zertifizierung

Projekt-Kick-Off
- Vorstellung der beteiligten Personen
- Abstimmung eines Meilensteinplans
- Klärung ggf. noch offener Fragen

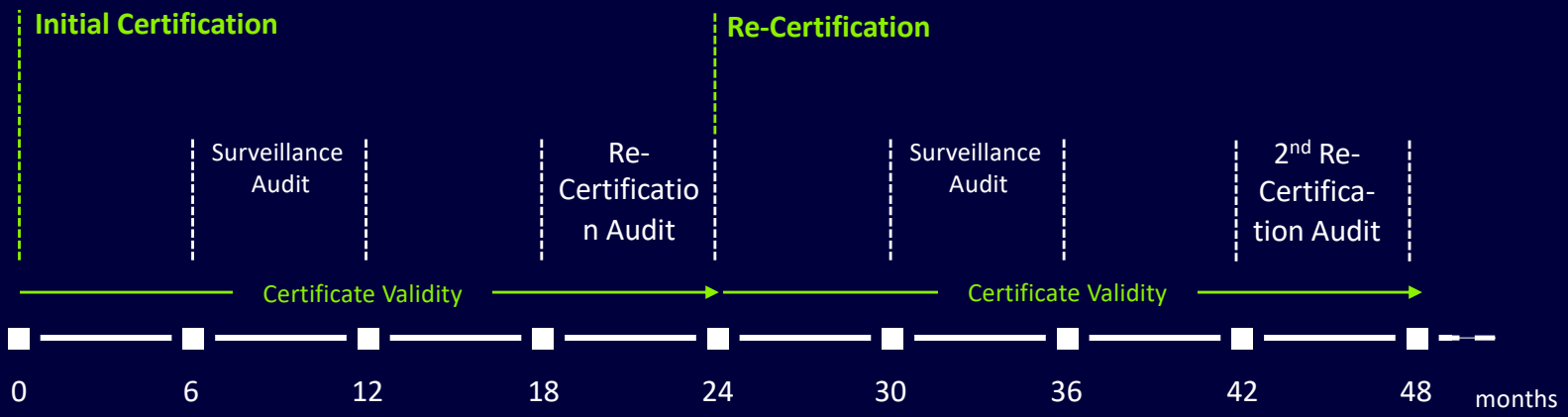
Dokumenten-Lieferung
Notwendige Dokumente, z.B.:
- CP/CPS/TSPS
- Policy Disclosure statement
- AGB
- Beendigungsplan

Stufe 1 Audit
- Prüfung der notwendigen Dokumente auf Einhaltung der definierten Kriterien und Anforderungen
- Bei Abweichungen, Erstellung eines Berichts und Behebung durch den Kunden

Stufe 2 Audit
- Vor-Ort Audit der organisatorischen, technischen und physischen Sicherheitsmaßnahmen und Prozesse

Berichtserstellung & Zertifizierung
- Berichtsentwürfe
- Freigabe durch den Kunden
- Zertifizierungsentscheidung

Gültigkeit des eIDAS Zertifikats/ der Konformitätsbewertung



Empfehlungen

Aus der Sicht einer Konformitätsbewertungsstelle (1)

Binden Sie die Konformitätsbewertungsstelle bereits in den Planungen mit ein

- Viele Entscheidungen bereits früh in der Planungs- und Realisierungsphase
- Fehler an dieser Stelle lassen sich später oft nur unter hohen Aufwänden korrigieren

Konformitätsbewertungsstellen dürfen nicht beraten, können aber trotzdem bereits im Vorfeld der eigentlichen Konformitätsbewertung unterstützen.

- Workshops (z.B. planungsbegleitend, zur Erarbeitung der relevanten Anforderungen)
- Konzeptbewertungen (z.B. Grobkonzept, Feinkonzept, Umsetzungskonzept)
- Vorprüfungen (z.B. von Dokumenten, von Dienste-Teilen oder der technischen Umsetzung)

Empfehlungen

Aus der Sicht einer Konformitätsbewertungsstelle (2)

Planen Sie ausreichend Zeit für die Konformitäts-bewertung ein

- Projektlaufzeit hängt stark von den Erfahrung des Anbieters ab
  - Komplette Neuentwicklung oder Upgrade eines bestehenden Dienstes
  - Wurden bereits andere Auditierungen absolviert
- Projektlaufzeiten von mehr als einem Jahr sind keine Seltenheit

Zeitdruck führt dazu, dass unfertige Dokumente eingereicht werden und Prozesse unvollständig umgesetzt sind

- zusätzliche Prüfzyklen, dadurch höhere Aufwände und Verzögerungen

TÜVIT

Empfehlungen

Aus der Sicht einer Konformitäts-bewertungsstelle (3)

Sehen Sie die Konformitätsbewertung als Chance

- Auditor als Partner, nicht als Gegner
- Gemeinsames Ziel ist ein sicherer und konformer Betrieb des Dienstes
- Möglichkeiten zur Verbesserung Ihres Dienstes

Gehen Sie offen und transparent mit der Konformitätsbewertungsstelle um

- Erhebliches Risiko, dass nicht besprochene oder bewusst vermiedene Punkte versteckte Nichtkonformitäten beinhalten
- Dies kann zu Verzögerungen führen, wenn diese erst später dennoch aufgedeckt werden

TÜVIT

TÜVIT

Vielen Dank für Ihre Aufmerksamkeit!

Matthias Wiedenhorst
Leiter des Zertifizierungsfachbereichs TSP

TÜV Informationstechnik GmbH
m.wiedenhorst@tuvit.de

tuvit.de