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

Die Sicht des QTSPs

24.05.2023

Enrico Entschew

Was muss heute ein QTSP beachten hinsichtlich:

- Basics
- Systemen, Services und Prozesse
- Produktdefinition,
- Produkt aufsetzen,
- Auditierung und Zertifizierung
- Beantragung Status QTSP
- Eintritt als QTSP
- Aufrechterhaltung des QTSP-Status
- Aktuelle Herausforderungen eines QTSP

Was wird sich mit eIDAS 2.0 ändern?

- Neue Vertrauensdienste
- Einfluss der EUDI und angrenzende Systeme
- Änderung von Teilen der Regulatorik

- **Benennung der verantwortlichen Akteure** (Leiter, Vertreter, Revisor)
- **Erfüllung der Antragsanforderungen des Supervisory Body (zuständige Stelle)**
- **Etablierung der Basismanagementsysteme** (u.a. für Erfüllung von Sicherheitsanforderungen nach Artikel 19 der eIDAS-VO)

Die Basics

https://www.bundesnetzagentur.de/cln_122/EVD/DE%2520alt/Fachkreis/AntragQuali/AntragQuali-start.html

- Handelsregisterauszug oder vergleichbarer Nachweis
- Ggf. Bevollmächtigung der verantwortlichen Personen (Leiter, Stellvertreter des Vertrauensdienstes sowie Revisor)
- Konformitätsbewertungsbericht mit der Registriernummer
- Certificate Policy (CP) und Certification Practice Statement (CPS)
- Beendigungsplan
- Deckungsvorsorge/Versicherungsnachweis
- Bei Übertragung von Aufgaben an Dritte: Auflistung dieser Dritten Fachkundenachweise der mit den Aufgaben betrauten Personen
- Allgemeine Geschäftsbedingungen für Kunde

Bundesnetzagentur

Ort, Datum

Bundesnetzagentur
Referat IS15
Canisiusstr. 21
55122 Mainz

E-Mail: eidas@bnetza.de

Antrag auf Qualifikation als qualifizierter Vertrauensdiensteanbieter

gemäß Artikel 21 Verordnung (EU) Nr. 910/2014

Qualifizierungsart wählen

- qualifizierter Dienst zur Erstellung qualifizierter Zertifikate für elektronische Signaturen (Art. 28)
  - *Option: Verwaltung der Signaturerstellungsdaten im Auftrag des Unterzeichners (Fernsignatur)*
- qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen (Art. 33)
- qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen (Art. 34)
- qualifizierter Dienst zur Erstellung qualifizierter Zertifikate für elektronische Siegel (Art. 38)
  - *Option: Verwaltung der Siegelerstellungsdaten im Auftrag des Siegelerstellers (Fernsiegel)*
- qualifizierter Validierungsdienst für qualifizierte elektronische Siegel (Art. 40 i.V.m. Art. 33)
- qualifizierter Bewahrungsdienst für qualifizierte elektronische Siegel (Art. 40 i.V.m. Art. 34)
- qualifizierter Dienst für die Zustellung elektronischer Einschreiben (Art. 44)
- qualifizierter Dienst zur Erstellung qualifizierter elektronische Zeitstempel (Art. 42)

Anbieter Angaben

Name des Anbieters
Name des Dienstes
Straße
PLZ, Ort
ggf. Rechtsform
ggf. Handelsregistereintrag
ggf. Umsatzsteuer-IdNr.

Seite 1 / 4

Basismanagementsysteme

(machen das Leben leichter, vor allem im Hinblick auf die anstehenden Zertifizierungen)

- Data Privacy (DSGVO konform)
- IT-Sicherheit
- Risikomanagement
- Informationssicherheitsmanagement (ISO 27001)
- Business Continuity Management
- Infrastruktursicherheit (TSI Level 3 und EN50600)
- ISO 9001-Zertizierung
- Arbeitssicherheit, Umweltschutz, Energieeffizienz etc.

Welche Infrastruktur brauche ich, um ein Produkt anbieten zu können?

- Prozesse

  (Antragstellung, Identifizierung, Überprüfung der Angaben, Schlüsselmanagement, Schlüsselerzeugung, Sperrung etc.)

- Systeme

  (Antragsportal, Prüfsystem, Produktionssystem, Archivsystem etc.)

- Service

  (Statusauskunft, Sperrdienst, Support, Verzeichnisse etc.)

- Produktdefinition

  Auf Basis einer bestehenden Policy, z.B. qcp-l

  Auf Basis der bestehenden Systeme, Services und Prozesse des QTSP

- Produkt aufsetzen

  PKI etablieren

  Produkt setup

  Nutzungsbedingungen

  Freigabe

  Veröffentlichung notwendiger Informationen

- Dokumentenaudit
- Vorortaudit
- Audit Report (ETSI 319 401, ETSI 319 411-1, ETSI 319 411-2)
- Conformity Assessment Report (eIDAS, VDG, VDV)
- Zertifikat

Beantragung beim SB durch den QTSP mit

- Audit Report
- Conformity Assessment Report
- Zertifikat
- Informationen zur ausstellenden CA
- CP/ CPS/ TSPS, Subscriber Agreement, PKI disclosure statement
- Etc.

Prüfung und Veröffentlichung des QTSP mit seinem qualifizierten Vertrauensdienst auf TSL

- Interner Prüfprozess
- Ggf. zusätzliche Auditierung
- Entscheidung
- Veröffentlichung auf der nationalen Trusted List (TSL)
- https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

- Jährlich: Überwachungsaudit
- Jedes zweite Jahr: Rezertifizierung der qualifizierten Vertrauensdienste
- Kontinuierliche Arbeit eines Compliance Teams mit dem Focus auf Monitoring, Sicherheitsfallmanagement (z.B. Meldung jedes Verdachtsfalls eines Betrugsversuchs bei einem Identifikationsverfahrens) bzw. Weiterentwicklung von Standards und Normen, Audit- und Zertifizierungsmanagement, Gremienarbeit, Produktdefinition für PKI und Identity-proofing-Verfahren

- Abhängigkeit von zertifizierten Drittmodulen (z.B. Identity Proofing Module)
- Abhängigkeit von Zertifizierungen (z.B. QSEE, HSM), die die Basis für die Zertifizierung des QTSP sind
- Unterschiedliche Handhabung der Auditierung im europäischen Wettbewerb

Was wird sich mit eIDAS 2.0 ändern?

- These: Nicht alle Vertrauensdienste werden von einem QTSP zentral angeboten
- Vertrauensdienste benötigen ggf. starke Spezialisierung, um wirtschaftlich erfolgreich zu sein
- Rahmen muss ggf. durch Regulierung geschaffen werden (Bedarf für einen Vertrauensdienst)

- Durch EUDI werden Identifizierungsprozesse deutlich einfacher
- Nutzungsmöglichkeit von Authentic Sources durch QTSP über elektronische Schnittstellen
- Möglichkeit des Antragsstellers Nachweise mit Hilfe von Qualified Attestations of Attribute (QEAA) einzureichen

- Einfluss der NIS 2 Richtlinie
  - Gefahr, dass auf nationaler Ebene über die Anforderung der NIS 2 hinausgegangen wird
  - Aktuelles Beispiel Referentenentwurf NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)

Vielen Dank.

Enrico Entschew
Principal Industrial Standardization and Compliance
Email: e.entschew@d-trust.net

Teil der Bundesdruckerei-Gruppe