Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

SR 816.111.1
Anhang 8 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier

Erläuterungen zu den Anpassungen in Ausgabe 2

(Ausgabe 2 vom 26. Februar 2018, Inkrafttreten 1. April 2018)

Technische und organisatorische Zertifizierungsvoraussetzungen für Identifikationsmittel und deren Herausgeber (Schutzprofil für Identifikationsmittel)

Technical and organizational Certification Requirements for Electronic Authentication Means and Their Issuers (Protection Profile for Authentication Means)

Anpassungen

Kapitel	
1.2.2 „TOE Usage“	**Ausgabe 1**: Beschreibung und sicherheitsrelevante Vorgaben zum Kommunikationskanal fehlen. **Ausgabe 2**: IdP und RP müssen für ihre Kommunikation (Autorisierung, Erneuerung von Authentifizierungsnachweisen; Token Renewal) einen direkten und abgesicherten Rück-Kanal nutzen. **Veränderung**: - Die Beschreibung der Kommunikation hinsichtlich Authentifizierung und Erneuerung von Authentifizierungsnachweisen (Token Renewal) zwischen Identity Provider (IdP) und Relying Party (RP) wurde konkretisiert und erweitert. - Im Rahmen des Authentifizierungsprozesses ist sichergestellt, dass die Kommunikation zwischen IdP und RP immer abgesichert und direkt erfolgt und kein Ausweichen auf potentiell unsichere Elemente zulässt.
1.5 / Table 1 „TSF data: Claimant ID“	**Ausgabe 1**: A unique ID provided by the IdP to identify the claimant unambiguously. **Ausgabe 2**: A unique ID of the authenticator issued by the IdP to identify the claimant unambiguously. **Veränderung**: - Die Beschreibung des Begriffs „Claimant ID“ wurde dahingehend präzisiert, dass es sich um den Identifikator des physischen Identifikationsmittels (Authenticator) handelt.
1.6 / Table 2 “External Entities and Subjects: Attacker”	**Ausgabe 1**: A human or a process acting on his behalf, located outside the TOE. The main goal of the attacker is to access or modify security relevant data. **Ausgabe 2**: A party who acts with malicious intent to compromise an information system. **Veränderung**: - Die Umschreibung des Begriffs „Attacker“ wurde allgemeiner gefasst, um möglichst alle Ausprägungen begrifflich zu fassen.

5.2.7 “Cryptographic operation (FCS_COP.1.1)”	**Ausgabe 1**: - **Ausgabe 2**: Es sind andere kryptografische Algorithmen zugelassen, sofern deren Verschlüsselungsstärke mindestens gleich hoch ist wie in der bisherigen Definition. **Veränderung**: - Die Vorgabe bezüglich der Verschlüsselungs-/Entschlüsselungsverfahren wurde erweitert, so dass auch andere Verfahren gleicher Stärke zugelassen werden können. - Es können auch von der Vorgabe abweichende Verschlüsselungs-/Entschlüsselungsverfahren angewendet werden sofern deren Verschlüsselungsstärke der bisherigen Regelung entspricht.
6.2 “Indirect and direct RP-Initiated Authentication-Sequences”	**Ausgabe 1**: - **Ausgabe 2**: Ergänzung um Punkte 3 und 4 **Veränderung**: - Die Vorgaben zur Kommunikation zwischen Identity Provider (IdP) und Relying Party (RP) bezüglich der Abläufe und Authentizifierungsnachweise wurden präzisiert. - Die Kommunikationsabläufe und die Authentifizierung richten sich nach klareren Vorgaben.
6.3 “SAML Recommendations”	**Ausgabe 1**: - **Ausgabe 2**: Die Empfehlungen wurden um die Begriffe „ID“ und „ID Reference Values ergänzt. **Veränderung**: - Der Umgang mit dem Identifikator ist bezüglich Eindeutigkeit, Länge und Referenzierung präziser definiert. .