Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

RS 816.111.1
Annexe 8 de l'ordonnance du DFI du 22 mars 2017 sur le dossier électronique du patient

Rapports explicatifs sur les ajustements dans la Version 2

(Version 2 du 26 février 2018, Entrée en vigeur 1 avril 2018)

Critères techniques et organisationnels de certification applicables aux moyens d'identification et à leurs éditeurs (profil de protection pour moyens d'identification)

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

Ajustements

Chapitre	
1.2.2 „TOE Usage“	**Version 1**: La description et les exigences de sécurité pour le canal de communication manquent. **Version 2**: IdP et RP doivent utiliser un canal inverse direct et sécurisé pour leur communication (autorisation, renouvellement des informations d'authentification, renouvellement des jetons). **Changement**: - La description de la communication concernant l'authentification et le renouvellement des informations d'authentification (Renouvellement de jeton) entre le fournisseur d'identité (IdP) et la partie fiante (RP) a été spécifiée et étendue. - Dans le cadre du processus d'authentification, il est garanti que la communication entre IdP et RP est toujours sécurisée et directe et ne permet pas d'utiliser les éléments potentiellement dangereux.
1.5 / Table 1 „TSF data: Claimant ID“	**Version 1**: A unique ID provided by the IdP to identify the claimant unambiguously. **Version 2**: A unique ID of the authenticator issued by the IdP to identify the claimant unambiguously. **Changement**: - La description du terme "Claimant ID" a été clarifiée afin de préciser qu'il s'agit de l'identifiant du moyen physique d'authentification (Authenticator).
1.6 / Table 2 “External Entities and Subjects: Attacker”	**Version 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. **Version 2**: A party who acts with malicious intent to compromise an information system. **Changement**: - Le terme "Attacker" a été généralisé afin d’inclure toutes les expressions possibles.

5.2.7 “Cryptographic operation (FCS_COP.1.1)”	**Version 1**: - **Version 2**: D'autres algorithmes cryptographiques sont autorisés, à condition que leur niveau de cryptage soit au moins aussi élevé que dans la définition précédente. **Changement**: - La procédure de cryptage / décryptage a été étendue pour permettre d'autres procédures de force égale. - Il est également possible d'utiliser des méthodes de cryptage / décryptage s'écartant de la spécification si la force de cryptage correspond à la régulation précédente.
6.2 “Indirect and direct RP-Initiated Authentication-Sequences”	**Version 1**: - **Version 2**: Complément aux points 3 et 4 **Changement**: - Les spécifications pour la communication entre le fournisseur d'identité (IdP) et la partie fiante (RP) en ce qui concerne les procédures et les preuves d'authentification ont été clarifiées. - Les processus de communication et l'authentification sont basés sur des spécifications plus claires.
6.3 “SAML Recommendations”	**Version 1**: - **Version 2**: Les recommandations ont été complétées par les termes "ID" et "ID Reference Values". **Changement**: - Le traitement de l'identifiant est défini plus précisément en ce qui concerne l'unicité, la longueur et le référencement.