Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

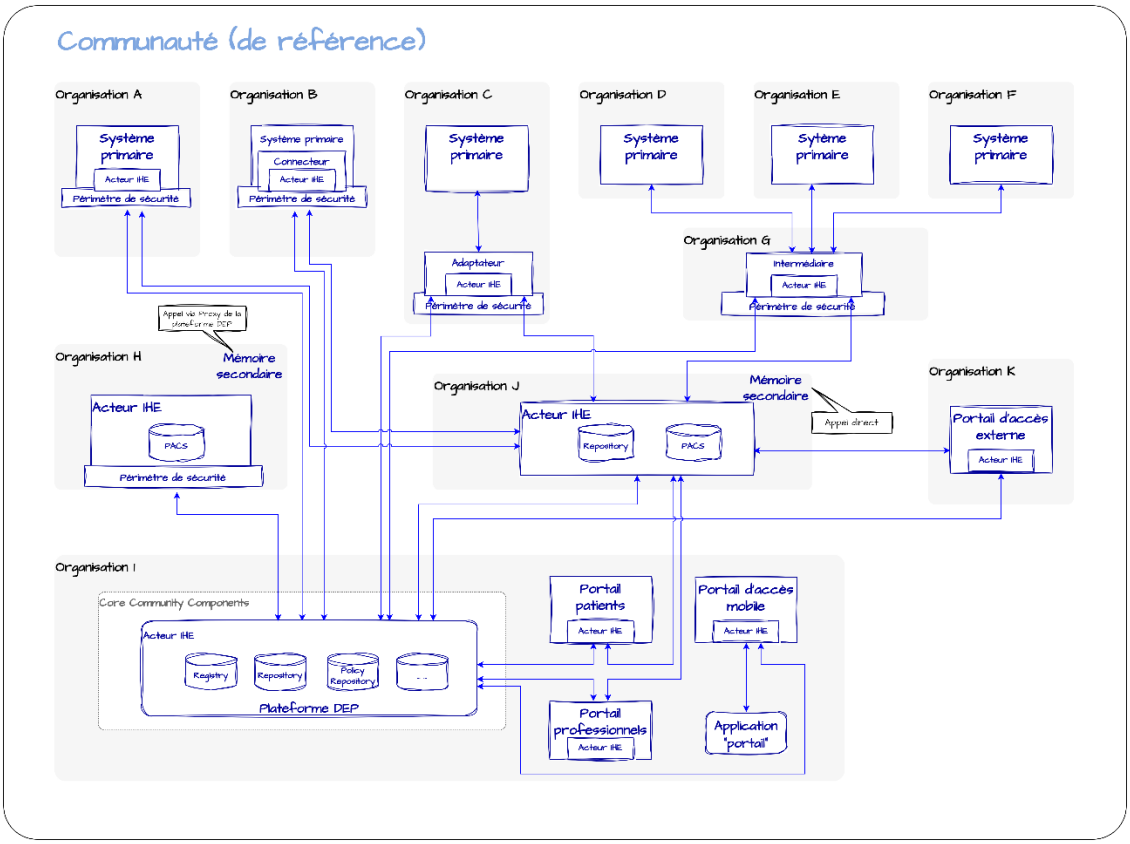
Office fédéral de la santé publique OFSP
Division Transformation numérique

Fiche d'information

Date : 25.11.2024

Certification des systèmes externes dans le cadre du DEP

L'acceptation et la diffusion du dossier électronique du patient (DEP) au sein de la population, dans les institutions de santé et parmi les professionnels de la santé dépendent essentiellement des bénéfices et de la confiance de la population dans la sécurité du DEP. Par conséquent, le raccordement de systèmes externes apportant une plus-value à l'espace de confiance du DEP[1] est souhaité, dans la mesure où le respect de la protection et de la sécurité des données ainsi que l'interopérabilité au sein du DEP sont garantis. De nombreux systèmes techniques ont accès au DEP en mode lecture ou écriture. Ils peuvent être représentés ainsi dans le paysage informatique :



[1] Dans la présente fiche d'information, l'espace de confiance du DEP correspond à la plateforme DEP et à ses interfaces avec les systèmes externes. Dans d'autres contextes, cet espace de confiance du DEP comprend la plateforme DEP et tous les systèmes raccordés au DEP ; dans la présente fiche d'information il ne s'agit pas explicitement de cela.

Plus d'informations :
Cette publication paraît également en allemand et en italien.

Terminologie

Adaptateur	Applications qui mettent à disposition des interfaces de conversion des protocoles pour rendre les interfaces propriétaires conformes au DEP et qui sont utilisées dans les systèmes primaires pour le raccordement au DEP (relation 1 : 1 entre le système primaire et le DEP).
Application « portail »	Client mobile de l'application web qui communique avec le portail d'accès mobile et permet ainsi l'accès à la plateforme DEP.
Connecteur	Bibliothèques et composants de logiciels qui mettent à disposition des fonctions prédéfinies pour accéder au DEP et qui sont intégrés aux produits (système primaire, adaptateur, utilisateur technique, etc.).
Intermédiaire	Applications qui permettent à un nombre quelconque d'institutions de raccorder leur système primaire au DEP pour disposer d'un accès en mode lecture ou écriture (relation n : 1 entre le système primaire et le DEP).
Mémoire secondaire	Applications exploitées par les institutions et dans lesquelles les données du DEP sont enregistrées.
Périmètre de sécurité	Dans la présente fiche d'information, les systèmes de sécurité suivants sont concernés : routeur de bordure, pare-feu d'applications web avec serveur proxy, protection antivirus, système de détection d'intrusion (IDS), système de prévention d'intrusion (IPS), zone démilitarisée (DMZ).
Plateforme DEP	Toutes les applications ou leurs composants utilisés par une communauté (de référence) pour l'exploitation du DEP.
Portail d'accès	Applications exploitées par les communautés (de référence) qui permettent aux utilisateurs du DEP (p. ex. professionnels de la santé, patients) d'accéder au DEP en lecture ou écriture.
Portail d'accès externe	Applications exploitées par des tiers qui permettent aux patients d'accéder au DEP en lecture.
Portail d'accès mobile	Partie serveur d'une application web exploitée par la communauté (de référence) qui permet à une application « portail » d'accéder à la plateforme DEP via des interfaces conformes au DEP.
Système primaire	Système utilisé dans un cabinet médical ou un hôpital pour traiter les données médicales, par exemple un système informatique de cabinet ou de clinique.
Utilisateur technique	Fonctionnalité dans un système qui permet le téléversement automatique de documents dans le DEP.

Plus d'informations :
Cette publication paraît également en allemand et en italien.

Limites de la certification

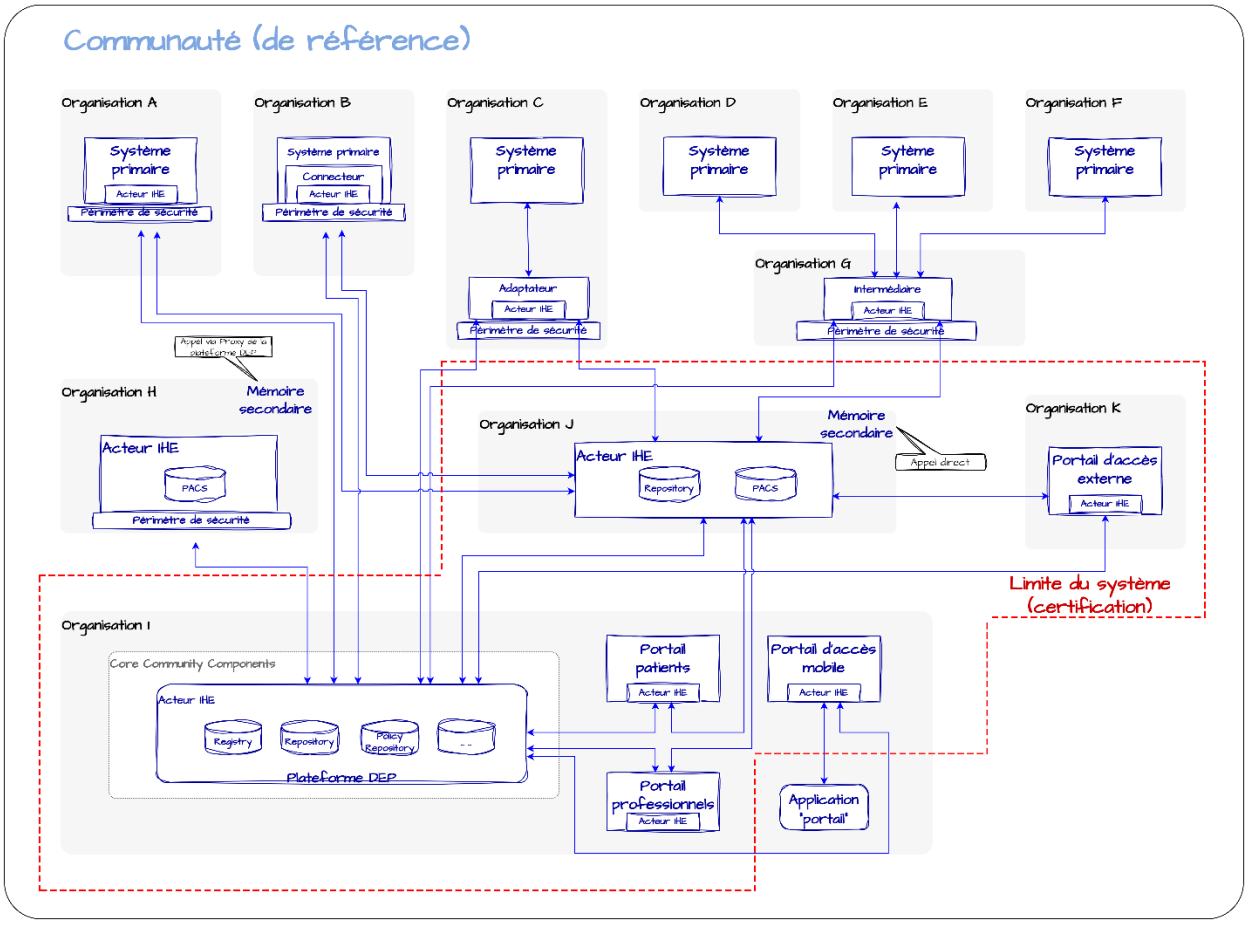
En évaluant les risques et les bénéfices du raccordement des systèmes externes au DEP, l'Office fédéral de la santé publique (OFSP) a décidé de ne pas soumettre les systèmes suivants à la certification au sens de la LDEP jusqu'à nouvel avis[2,3] :

- Système primaire
- Connecteur
- Adaptateur
- Intermédiaire
- Mémoire secondaire sans système d'autorisation d'accès (appel indirect via le proxy de la plateforme DEP)
- Utilisateur technique
- Application « portail »

Les systèmes suivants des communautés (de référence) sont, par conséquent, toujours soumis à la certification :

- Plateforme DEP
- Portail d'accès interne
- Portail d'accès mobile
- Mémoire secondaire avec système d'autorisation d'accès (appel direct)
- Portail d'accès externe

La limite de la certification est représentée dans le schéma ci-dessous :



[2] L'obligation de certification pour les systèmes déjà soumis à l'obligation de certification selon l'annexe 2 ODEP-DFI n'est pas affectée par cette décision.

[3] Selon l'évolution technologique, il pourrait se révéler nécessaire d'inscrire d'autres systèmes à l'annexe 2 ODEP-DFI et de les soumettre ainsi à l'obligation de certification.

Plus d'informations :
Cette publication paraît également en allemand et en italien.

Dans le cadre de l'évaluation des risques, l'OFSP part des affirmations suivantes :

- Grâce aux exigences légales de protection et de sécurité des données qui l'entourent, l'espace de confiance du DEP est considéré comme sûr d'après l'état actuel de la technique.
- Le titulaire du DEP ne met en danger que son propre DEP lorsqu'il y accède via une application « portail ». Les données des autres DEP ne sont donc pas menacées.
- Les institutions de santé et les professionnels de la santé sont responsables des systèmes qu'ils utilisent. Dans le cadre du contrat de raccordement à la communauté (de référence), les communautés (de référence) fixent des directives sur les systèmes autorisés selon les critères techniques et organisationnels (CTO) à l'intention des institutions de santé. Les fournisseurs tiers qui offrent des prestations aux institutions de santé ou aux professionnels de la santé travaillent toujours sur mandat d'une institution de santé ou d'un professionnel de la santé, et ces derniers sont, par principe, responsables des actes des mandataires.
- Tous les fournisseurs participants des systèmes mentionnés travaillent de manière responsable et gèrent la protection et la sécurité des données d'après le niveau actuel de la technique (p. ex. ISO/IEC 27001).
- Les communautés (de référence) imposent aux institutions de santé qui lui sont raccordées de transmettre les exigences de protection et de sécurité des données visées dans l'ODEP-DFI à tous les systèmes utilisés pour se raccorder au DEP, tels que les adaptateurs, les intermédiaires ou les utilisateurs techniques.
- Dans le cas d'éléments non couverts par la LDEP, d'autres règlementations s'en chargent, telles que les prescriptions en matière de protection des données (fédérales et cantonales), l'ODim et même les dispositions du droit du travail.

Plus d'informations :
Cette publication paraît également en allemand et en italien.