

DEP – malédiction ou bénédictio

David Fiaux
Senior Sales HIN / Responsable SR

Grangeneuve, le 26.11.2018, symposium RAI-NH
2018

Une excursion, un positionnement, une impulsion...

- HIN
- Stratégie eHealth
- LDEP
- DEP prise de conscience
- Infrastructure de base
- Fournisseur d'identité

HIN

Protection et disponibilité des données

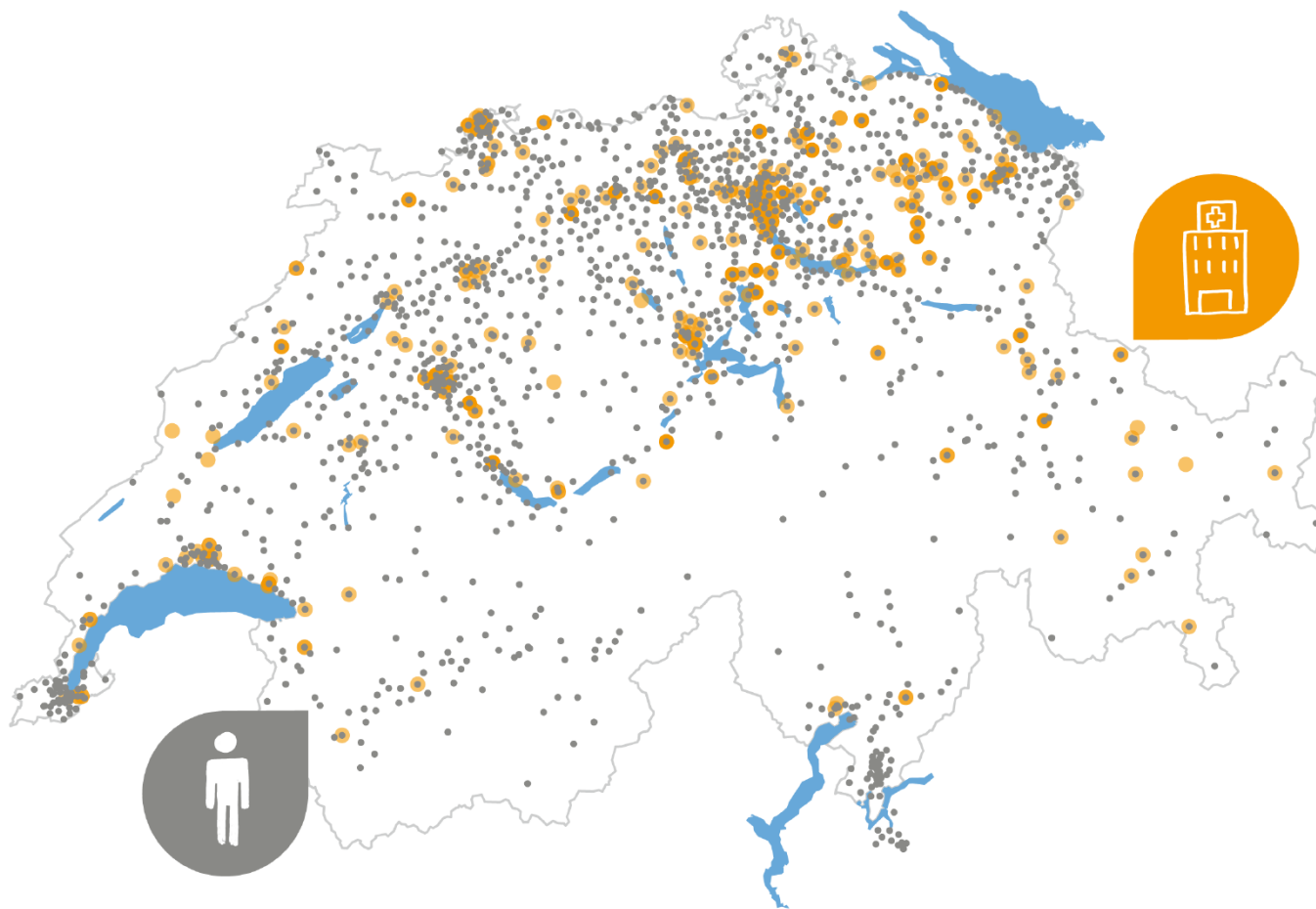
HIN a été fondé en 1996 sur l'initiative du corps médical



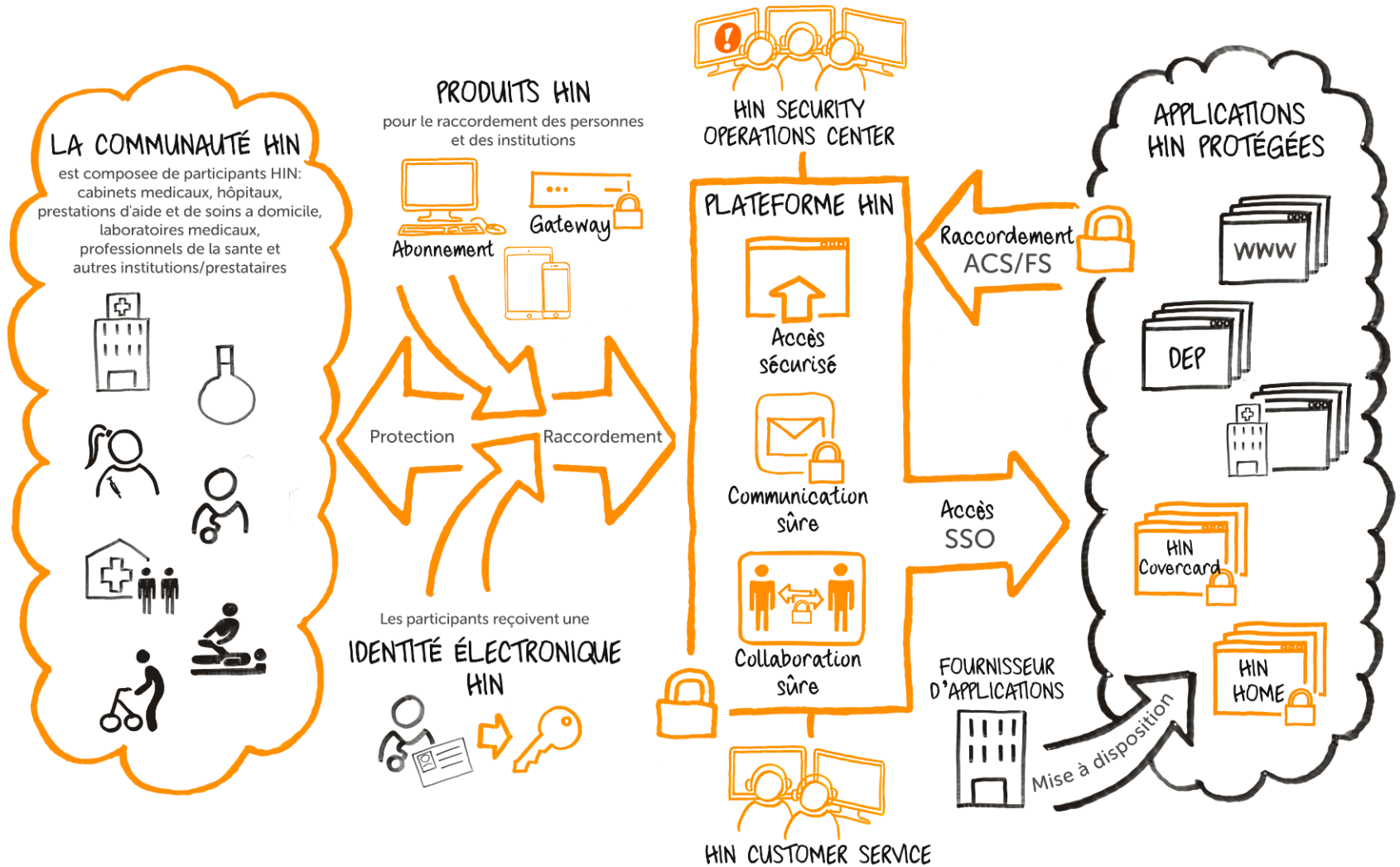
ofac



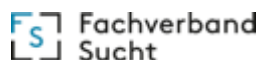
22'000 ID, 800 établissements et 60 services protégés par HIN



L'univers HIN plus sûr



HIN est soutenu par les associations professionnelles et les associations faitières concernées



FONDEMENT I/II

eHealth Suisse stratégie

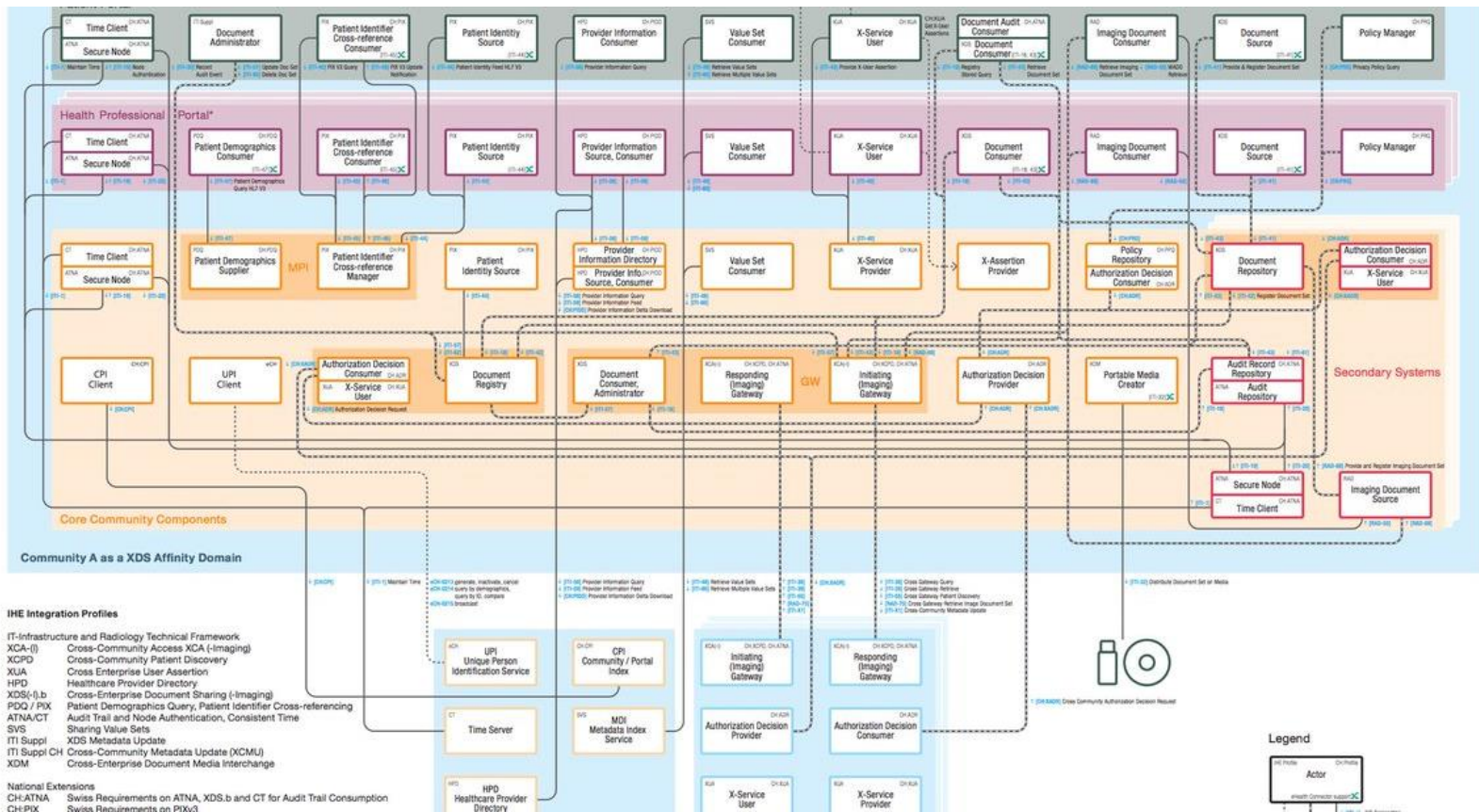
"Steve en avait assez" - Mais après seulement trois ans, le premier iPhone a été lancé en 2007.



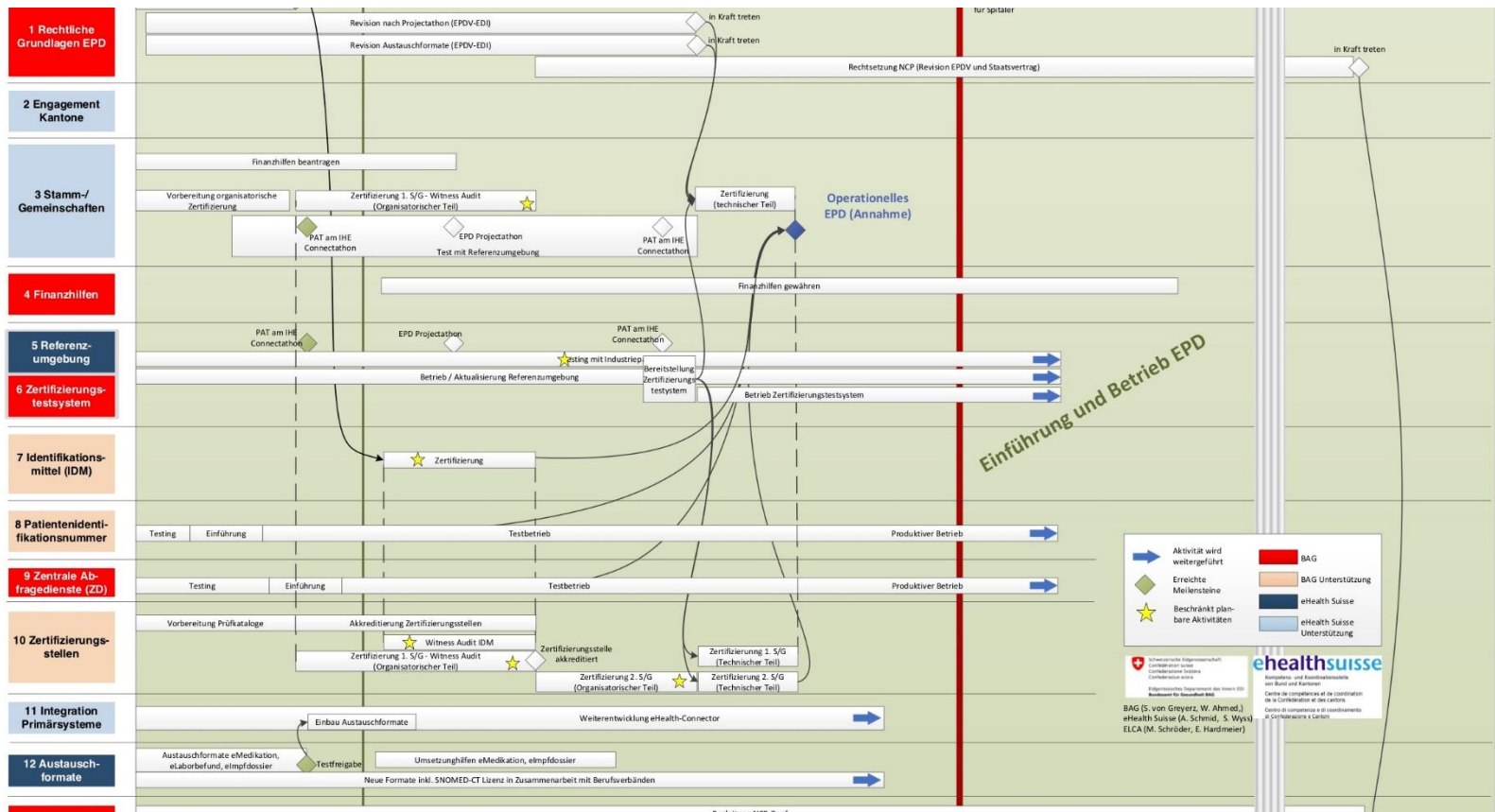
Accès à un système de soins de haute qualité, efficace, sécuritaire et rentable



Avec le DEP, les patients fournissent aux professionnels de la santé les documents les plus importants relatifs à leur santé



La Confédération et les cantons partent du principe que Le DEP sera disponible dans toutes les régions de Suisse comme prévu au printemps 2020



„Un Big Mac c'est un Big Mac mais ils disent « le » Big Mac.“

John Travolta dans le rôle de Vincent Vega dans Pulp Fiction (USA 1994)



FONDEMENT II/II

LDEP

L'accès à au DEP nécessite une identité électronique ainsi que l'appartenance à une communauté (- de référence)

Loi fédérale LDEP

- Art. 7: Tout les professionnels de la santé et les patients doivent disposer d'une eID
- Art 10: Accès-DEP par les communauté (- de référence)

Droit d'exécution

- ODEP
- ODEP-DFI
- OFDEP

LAMal

- Art 39 f: Hôpitaux, foyers, centres de naissance s'affilient à une communauté (- de référence)



-  **Art. 7 Identité électronique**

¹ Les personnes suivantes doivent disposer d'une identité électronique sécurisée pour traiter des données dans le dossier électronique:

- a. les patients;
- b. les professionnels de la santé.

² Le Conseil fédéral définit les critères de l'identité électronique et fixe les moyens d'identification; il règle la procédure d'émission des moyens d'identification.

-  **Art. 11 Portail d'accès pour les professionnels de la santé**

Le DFI fixe les exigences applicables au portail d'accès destiné aux professionnels de la santé, notamment pour la mise à disposition et la consultation des données ainsi que pour l'accessibilité.

-  **Art. 12 Protection et sécurité des données**

¹ Les communautés doivent se doter d'un système de gestion de la protection et de la sécurité des données adapté aux risques. Ce système doit comprendre les éléments suivants en particulier:

- a. un système de détection et de gestion des incidents de sécurité;
- b. un inventaire des moyens informatiques et des recueils de données;
- c. les exigences relatives à la protection et à la sécurité des données imposées aux institutions de santé et aux tiers affiliés à la communauté.

² Les communautés désignent un responsable de la protection et de la sécurité des données.

³ Elles sont tenues de signaler à l'OFSP tout incident ayant une influence sur la sécurité survenu dans le système de gestion de la protection et de la sécurité des données.

⁴ Le DFI fixe les exigences techniques et organisationnelles applicables à la protection et à la sécurité des données.

⁵ Les supports de données doivent se trouver en Suisse et être régis par le droit suisse.

Comme moyen d'identification :

Le traitement sécurisé des données nécessite l'identification et l'authentification claires et sécurisées des patients et des professionnels de santé. Cela se fait au moyen d'identification d'un éditeur certifié.

Quelle: Erläuterungen EPDV-EDI, Ausgangslage S. 5

Une brève introduction sur la conception du mode d'authentification



La personne prétend être X



Fournisseur d'identification (IDP)
vérifie l'authenticité de la personne

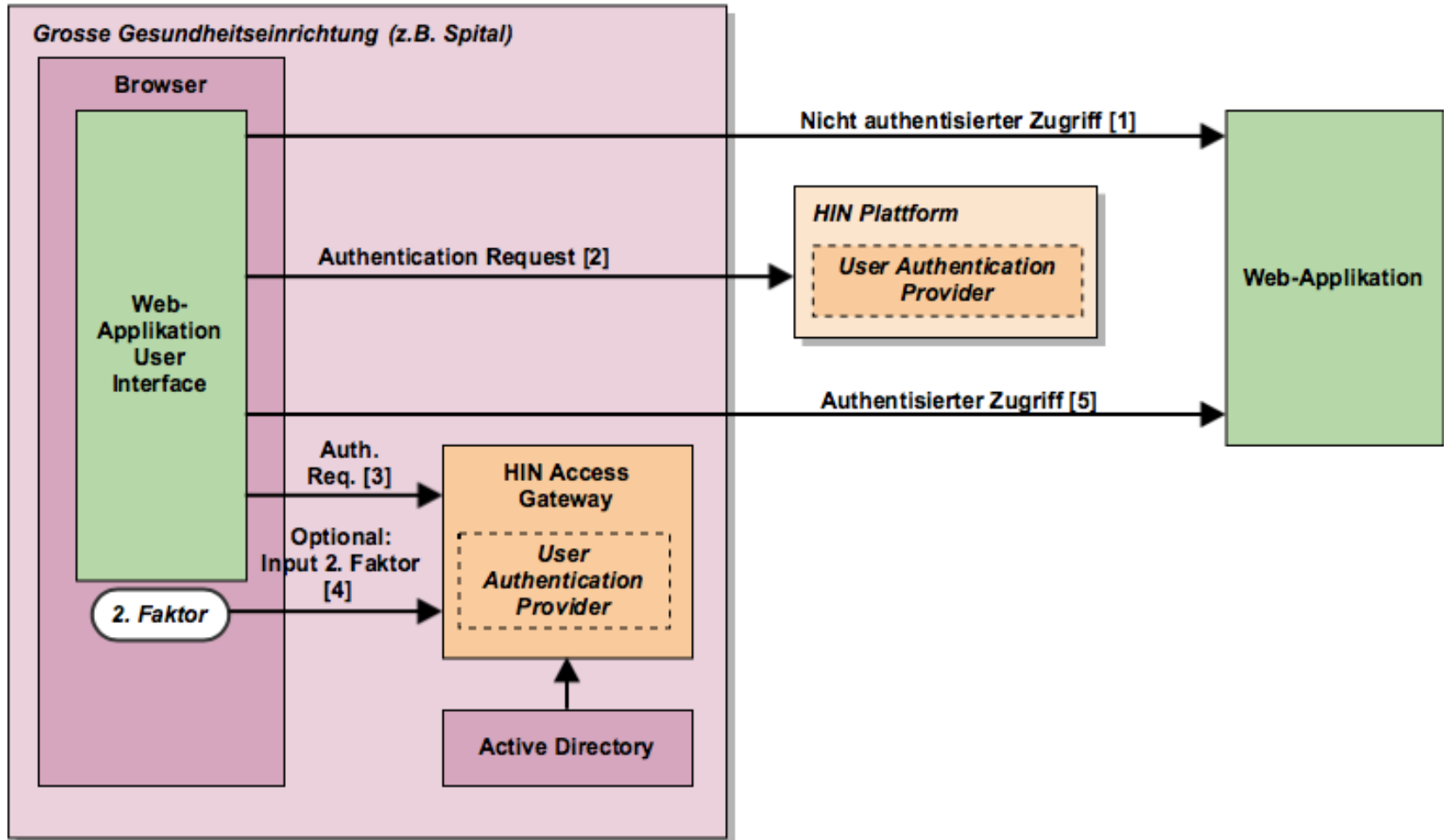


La personne reçoit un **moyen d'identification**, qui valide son identité



La personne **s'authentifie** avec son ID pour un accès

HIN Gateway utilise les moyens d'authentification internes



Avec la connexion HIN CURAVIVA, les gens travaillent et communiquent simplement en respectant les règles de protection des données.



[Raccordement HIN](#)

[Services](#)

[Produits](#)

[Portrait](#)

[Support](#)

[Contact](#)

[| de](#)

[News](#)



Gateway CURAVIVA HIN

[Home](#) > [Gateway CURAVIVA HIN](#)

sans

limitation

Nombre d'utilisateurs

illimité

Support / par année

@proprenom.ch

Mail

1 Identité

Access

de 3085 CHF

Taxe d'utilisation par
année

[Demande d'offre](#)

- Art. 7 Identité électronique

¹ Les personnes suivantes doivent disposer d'une identité électronique sécurisée pour traiter des données dans le dossier électronique:

- a. les patients;
- b. les professionnels de la santé.

² Le Conseil fédéral définit les critères de l'identité électronique et fixe les moyens d'identification; il règle la procédure d'émission des moyens d'identification.

- Art. 11 Portail d'accès pour les professionnels de la santé

Le DFI fixe les exigences applicables au portail d'accès destiné aux professionnels de la santé, notamment pour la mise à disposition et la consultation des données ainsi que pour l'accessibilité.

- Art. 12 Protection et sécurité des données

¹ Les communautés doivent se doter d'un système de gestion de la protection et de la sécurité des données adapté aux risques. Ce système doit comprendre les éléments suivants en particulier:

- a. un système de détection et de gestion des incidents de sécurité;
- b. un inventaire des moyens informatiques et des recueils de données;
- c. les exigences relatives à la protection et à la sécurité des données imposées aux institutions de santé et aux tiers affiliés à la communauté.

² Les communautés désignent un responsable de la protection et de la sécurité des données.

³ Elles sont tenues de signaler à l'OFSP tout incident ayant une influence sur la sécurité survenu dans le système de gestion de la protection et de la sécurité des données.

⁴ Le DFI fixe les exigences techniques et organisationnelles applicables à la protection et à la sécurité des données.

⁵ Les supports de données doivent se trouver en Suisse et être régis par le droit suisse.

L'authentification est de nouveau réglée à l'art. 9 al. 2 let. e de l'ODEP-DFI

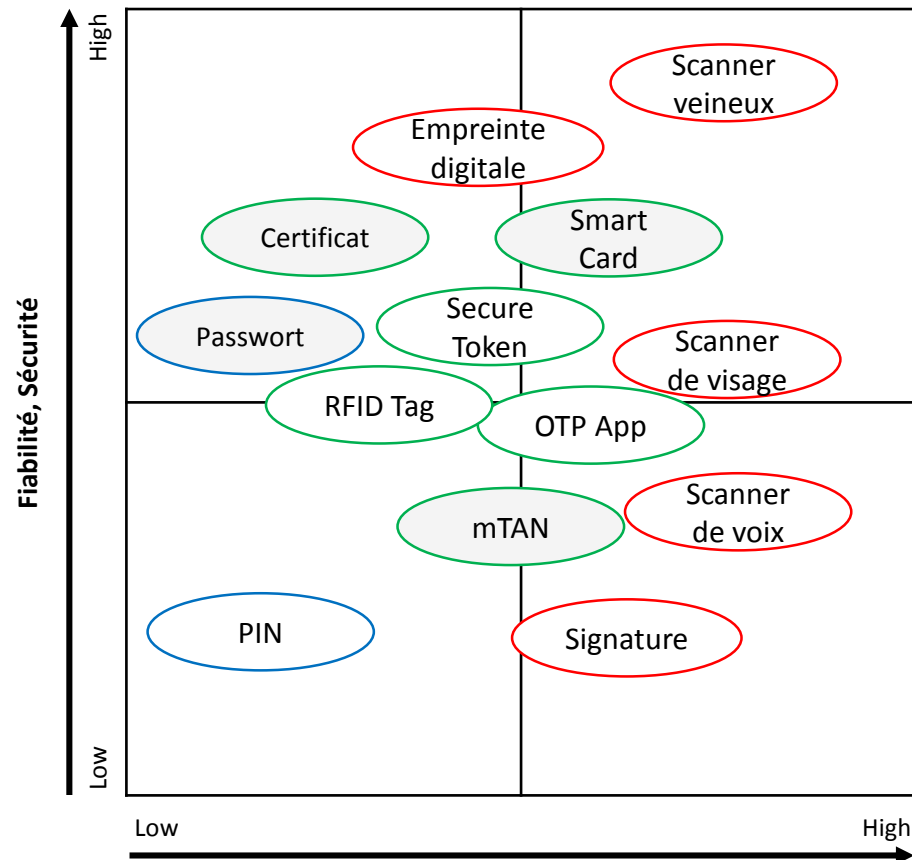
Les professionnels de santé doivent s'authentifier pour accéder au dossier électronique du patient en utilisant des moyens d'identification valides délivrés par un éditeur certifié selon l'article 31 ODEP.

Quelle: Anhang 2 der EPDV-EDI, Identifizierung und Authentifizierung
S. 5

Il y a beaucoup de solution à 2 facteurs avec une fiabilité variable

Facteurs possibles

- Catégorie : Connaissances
- Catégorie : Etre
- Catégorie : Avoir



- Art. 7 Identité électronique

¹ Les personnes suivantes doivent disposer d'une identité électronique sécurisée pour traiter des données dans le dossier électronique:

- a. les patients;
- b. les professionnels de la santé.

² Le Conseil fédéral définit les critères de l'identité électronique et fixe les moyens d'identification; il règle la procédure d'émission des moyens d'identification.

- Art. 11 Portail d'accès pour les professionnels de la santé

Le DFI fixe les exigences applicables au portail d'accès destiné aux professionnels de la santé, notamment pour la mise à disposition et la consultation des données ainsi que pour l'accessibilité.

- Art. 12 Protection et sécurité des données

¹ Les communautés doivent se doter d'un système de gestion de la protection et de la sécurité des données adapté aux risques. Ce système doit comprendre les éléments suivants en particulier:

- a. un système de détection et de gestion des incidents de sécurité;
- b. un inventaire des moyens informatiques et des recueils de données;
- c. les exigences relatives à la protection et à la sécurité des données imposées aux institutions de santé et aux tiers affiliés à la communauté.

² Les communautés désignent un responsable de la protection et de la sécurité des données.

³ Elles sont tenues de signaler à l'OFSP tout incident ayant une influence sur la sécurité survenu dans le système de gestion de la protection et de la sécurité des données.

⁴ Le DFI fixe les exigences techniques et organisationnelles applicables à la protection et à la sécurité des données.

⁵ Les supports de données doivent se trouver en Suisse et être régis par le droit suisse.

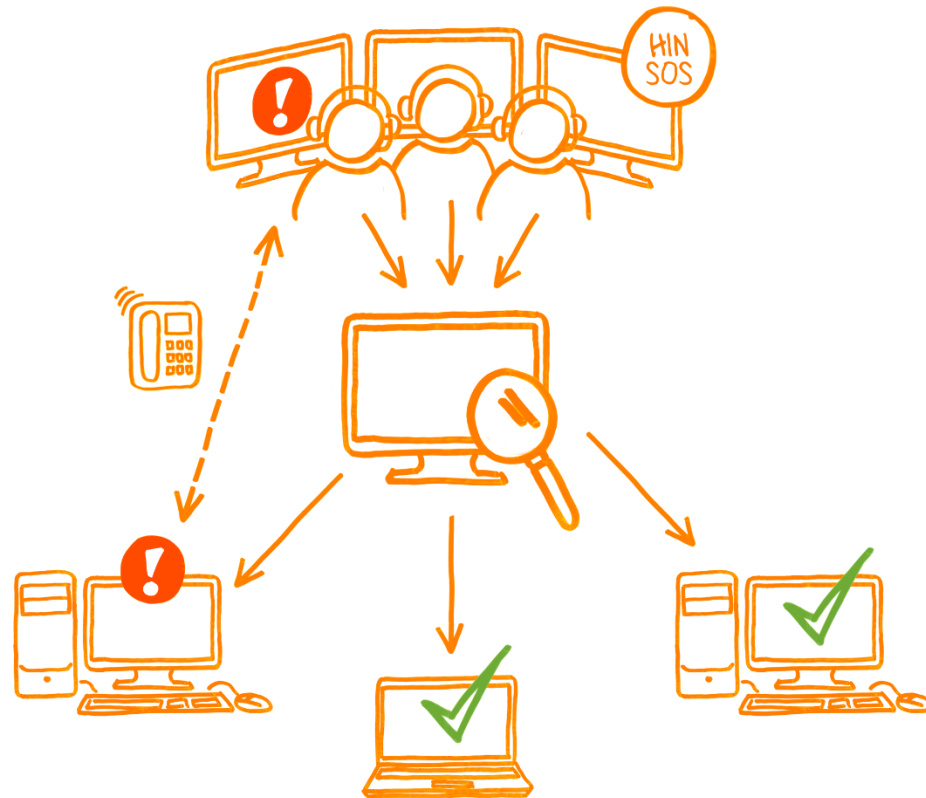
Les communautés doivent : a) prendre des mesures pour se protéger ... de logiciels malveillants, d'avoir les moyens notamment de détecter et de supprimer de tels logiciels

Source: Anhang 2 der EPDV-EDI, Schutz vor Schadsoftware
S. 15

Les communautés doivent :
... c) exiger que la configuration sécurisée des équipements finaux soit assurée...

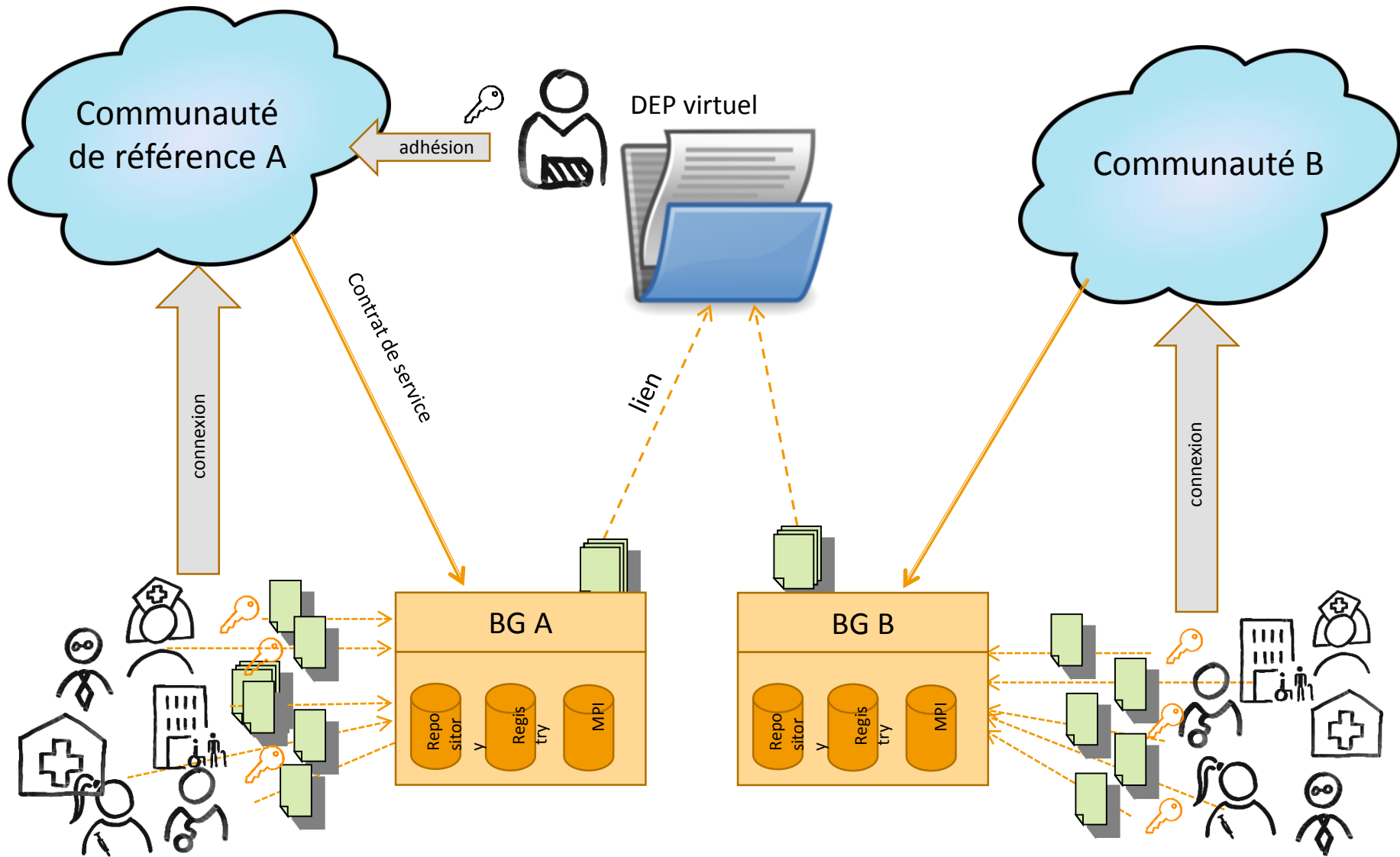
Source: Anhang 2 der EPDV-EDI, Schutz vor Schadsoftware
S. 17

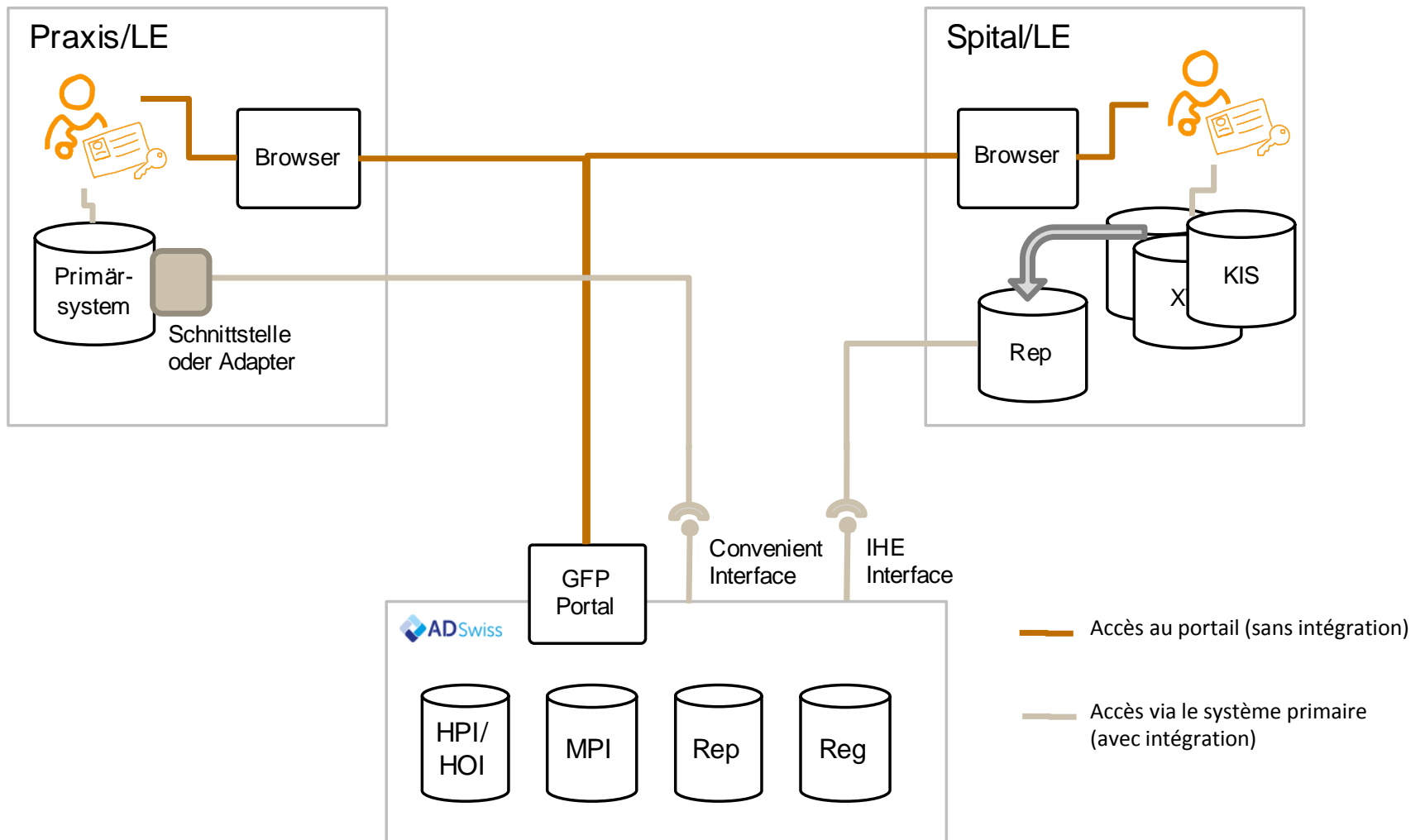
HIN Endpoint Security : améliorer la disponibilité, la sécurité et la protection des données sensibles



PRISE DE CONSCIENCE

Raccordement à une communauté (- de référence)

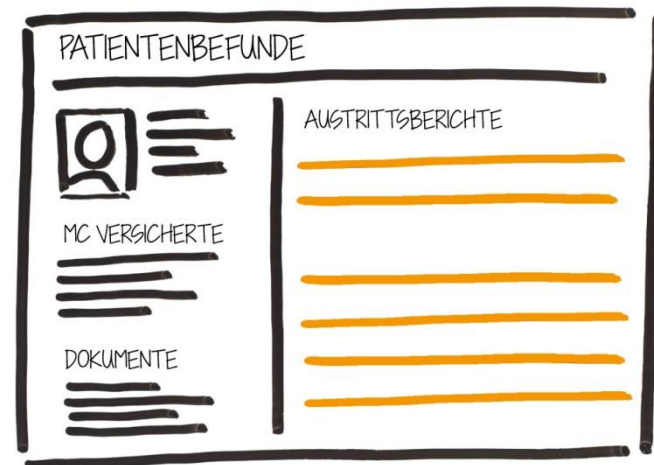
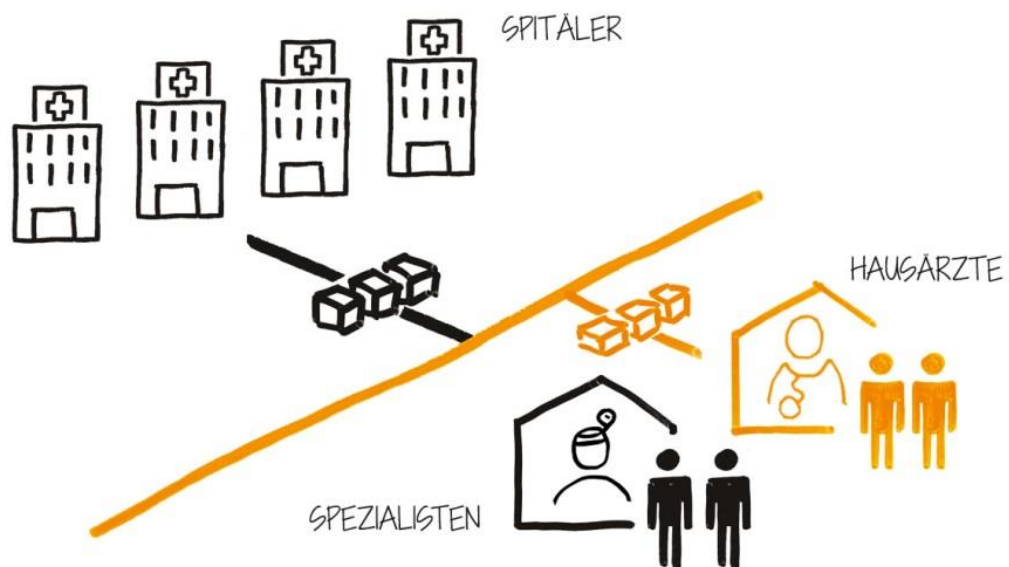




RAPPORT DE TERRAIN I/II

eHealth infrastructure de base

Expériences de projets pilotes : Ponte Vecchio, la première implantation intercommunautaire en Suisse



AD Swiss soutient les professionnels de la santé et ses établissements dans la communication dirigée et non dirigée.

Editorial FMH

Für eine digitale Zukunft der Gemeinschaft der Ärztinnen und Ärzte



In der ganzen Schweiz schenken eHealth-Projekte wie Flur an den Ärzten. Das sichere Austausch von Patientendaten zwischen primären, Sekundären, Spezialen, Kliniken und anderen Institutionen ist ein wichtiges Ziel. Im selben Aufwand unterstützen, Effizienz fördern, was alles aber die Patientensicherheit erhöhen soll. Die gemeinsame Behandlungssicht, die man genau hat, erkennt man jedoch, dass die Berücksichtigung der gesamten Behandlungssicht im ersten Moment entscheidend bleibt. Viele eHealth-Projekte werden auf Initiative von Kantonen oder Spitälern und Spezialkliniken betrieben und liefern sich mit einzelnen Dokumenten.

Wir müssen eine eigene Infrastruktur-Lösung aufbauen, welche die Kosten für den einzelnen Arzt minimiert und Anschluss an eHealth-Lösungen ermöglicht.

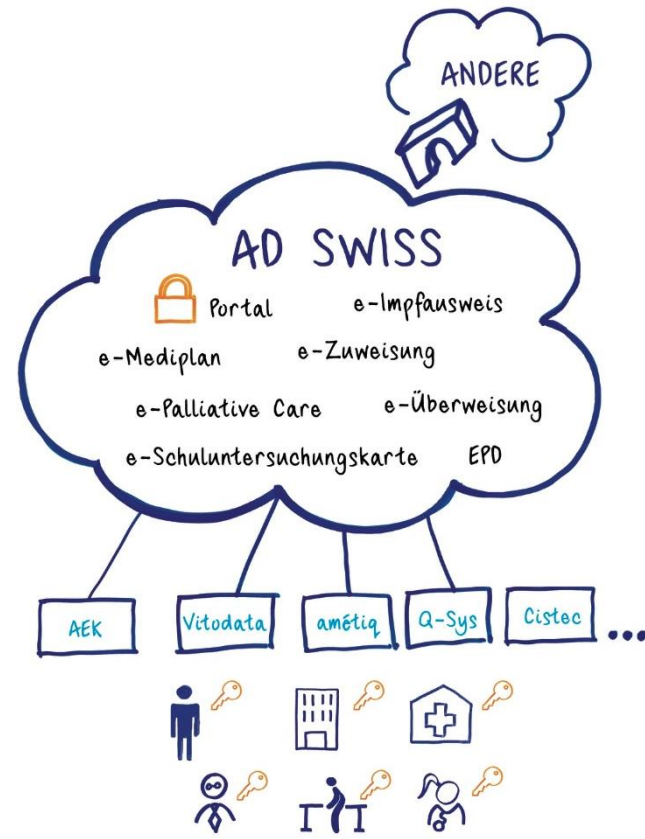
Nahe Investitionskosten und neue Bedürfnisse
Die bestehenden Systemen und Netzwerke eine zusätzliche Sicherheit bieten. Sie sind in einem oder zwei Jahren neu und nur selten an die verändernde Informationsstruktur einer professionellen Institution angepasst. Diese können sie sich nicht so leicht in eine bestehende sichere Netzwerkinfrastruktur einfügen. Eine eigene sichere Netzwerkinfrastruktur aufzubauen ist jedoch aufwändig, teuer und für einzelne Ärzte nicht immer eine gute Sache.

Die zu schaffende Infrastruktur muss eine Lösung von Ärzten für Ärzte sein, um die Möglichkeit von gemeinsamen Austausch vorzugeben. Die bestehende mündige Plattform für sichere Kommunikation und Vernetzung, die eHealth-Community, stellt bereits eine hervorragende Ausgangslage dar. Die bestehende eHealth-Infrastruktur und ihre Dienstleistungen zur Identifikation, sicheren Kommunikation und Interaktion im Netz bilden den Nukleus. Dieser lässt sich zur Infrastruktur der Gemeinschaft der Gesundheits-Angeboter - mit sehr geringen technischen Hindernissen und durch die eHealth-Community erweitert. Es ist in jedem eine Basis, auf welcher sich auch weitere Gemeinschaften bilden können.

Es entstehen so dabei die besten Anreize, an den die Partner anzukommen können und sollen. Die wichtigsten Patienten sind schließlich die der Schweiz die Partizipation und die Wahrung des Berufsgeheimnisses. Damit auch bestehende Ärzte an der digitalen Zukunft teilhaben können.

Dr. med. Urs Dähler, Mitglied des Zentralrats der FMH, Digitalisierungsbeauftragter und Chefarzt

Schweizerische Fachverbände | Bulletin des médecins suisses | Bulletin des medici svizzeri | 2014/05, 31 1171



RAPPORT DE TERRAIN II/II

HIN en tant que fournisseur d'identité

HIN eID est toujours utilisé avec l'authentification à 2 facteurs pour de nombreux services

Type d'utilisateurs



Produit / types d'accès



2ème facteur



Applications (par ex.)



HIN repose sur l'enregistrement électronique combiné à une identification vidéo

Einfach, sicher und bequem:
Identifizierung per Videochat

HIN

1. Persönliche Daten 2. Identifikation 3. Resultat

1 Persönliche Daten

Vielen Dank, dass Sie sich für die Online-Legitimation mit IDnow entschieden haben. Bitte geben Sie nun Ihre Daten für die Legitimation in das Formular unten ein, um die Identifizierung zu starten.

GLN-Nr. Person
Bitte geben Sie Ihre GLN-Nr. an

GLN-Nr. Person

ZSR-Nr. Person ✓

Gesundheitsberuf

Spezialisierung

Organisationsname (Praxis/Spital)

Berufsverband

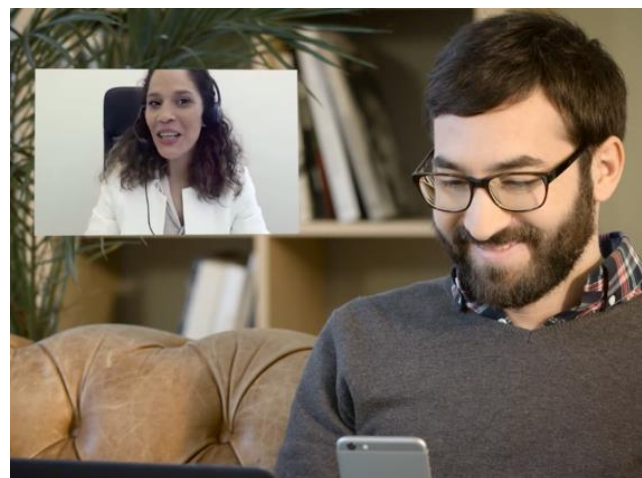
Ausweisdaten
Bitte geben Sie Ihre persönlichen Daten so ein, wie sie auf Ihrem Ausweis stehen.

Anrede*

Titel

Vorname(n)*

[Datenschutz](#) [Impressum](#) [Häufige gestellte Fragen](#) [Kundenservice](#)



- ✓ Inscription électronique
- ✓ Step-Up processus pour les eIDs existantes

TAKE AWAY

Pour finir

Ce qui nous semble être une épreuve difficile s'avère souvent être une bénédiction (Oscar Wilde)

- HIN en tant que IDP / AD Swiss en tant que plate-forme eHealth répondent aux exigences légales de la LDEP
- La technologie n'est pas un obstacle
- Les TIC favorisent la coordination des soins
- Les données améliorent la santé





Merci beaucoup de votre attention !

Nous serons heureux de répondre à vos questions.
N'hésitez pas à nous contacter :

HEALTH INFO NET AG
Grand-Rue 38
CH-2034 Peseux
Call Desk 0848 830 741
www.hin.ch

David.fiaux@hin.ch