solventum

Technisches Konzept

Fluency Direct

Version 3.3 | 13.10.2025

Inhaltsverzeichnis

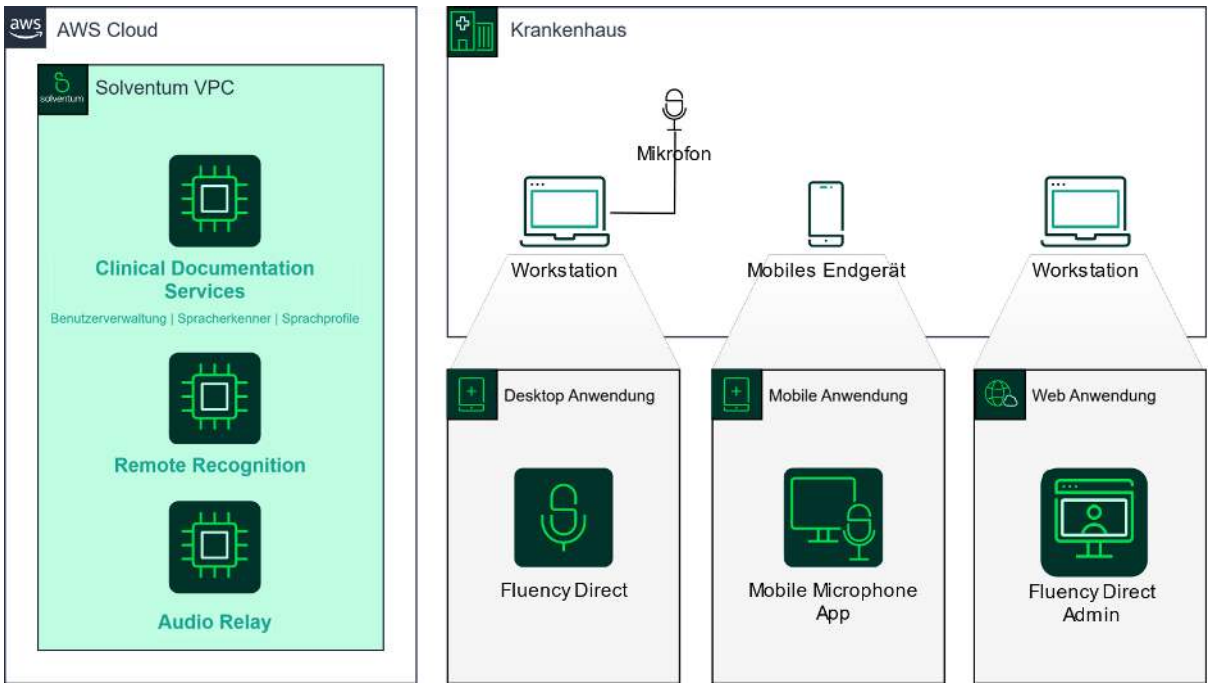
1 Übersicht

Solventum™ Fluency Direct™ ist eine KI-gestützte Spracherkennungssoftware, die speziell für den medizinischen Bereich entwickelt wurde. Sie unterstützt Ärztinnen, Ärzte und Pflegepersonal bei der effizienten und sicheren Dokumentation direkt im Krankenhausinformationssystem (KIS) oder anderen Anwendungen.

Kernfunktionen und Vorteile

- **KI-basierte Spracherkennung**: Fluency Direct nutzt fortschrittliche KI und Natural Language Understanding (NLU), um medizinische Sprache präzise zu erkennen und zu verarbeiten
- **Fachvokabular für alle Disziplinen**: Die Software enthält spezialisierte Vokabulare für über 30 medizinische Fachrichtungen – von Allgemeinmedizin über Radiologie bis hin zur Psychiatrie
- **Echtzeit-Dokumentation**: Ärztinnen und Ärzte können klinische Notizen direkt diktieren, bearbeiten und signieren – ohne Medienbrüche.
- **Cloud- und Offline-Betrieb**: Die Lösung ist cloudbasiert, funktioniert aber auch bis zu 30 Tage offline, z. B. bei Netzwerkausfällen
- **Mobile Nutzung**: Mit der **Fluency Mobile Microphone App** für iOS und Android ist ortsunabhängiges Diktieren möglich.
- **Individuelle Sprachprofile**: Persönliche Profile sorgen für eine hohe Erkennungsgenauigkeit und kontinuierliche Verbesserung durch automatisches Training.
- **Kompatibilität**: Fluency Direct ist mit über 300 Systemen kompatibel, darunter auch Microsoft Office
- **Datenschutz & Sicherheit**: Die Software ist DSGVO-konform und nach den C5-Kriterien des BSI zertifiziert.

2 Systemarchitektur



Das obige Architekturdiagramm zeigt einen Überblick über die Systemstruktur und die einzelnen Komponenten der angebotenen Lösung.

Die zentralen Dienste der cloudbasierten Technologie werden in der privaten Solventum Cloud gehostet und stehen somit jederzeit zur Verfügung. Serverseitige Komponenten müssen in der Kundenumgebung für den Betrieb nicht installiert werden.

Desktopbasierte Client Anwendungen können neben der direkten Installation auf den Workstations auch in virtualisierten Umgebungen bereitgestellt werden.

Abhängig von den tatsächlichen Anforderungen während der tatsächlichen Implementierung werden einige der gezeigten Komponenten nicht relevant sein.

3 Hardwareanforderungen

3.1 Anforderungen an Arbeitsplätze

Im Folgenden sind die Hardware-, Software- und Netzwerkanforderungen für den Betrieb der Desktop-Client-Anwendungen für Kliniker aufgeführt:

Hardware/Software Anforderungen

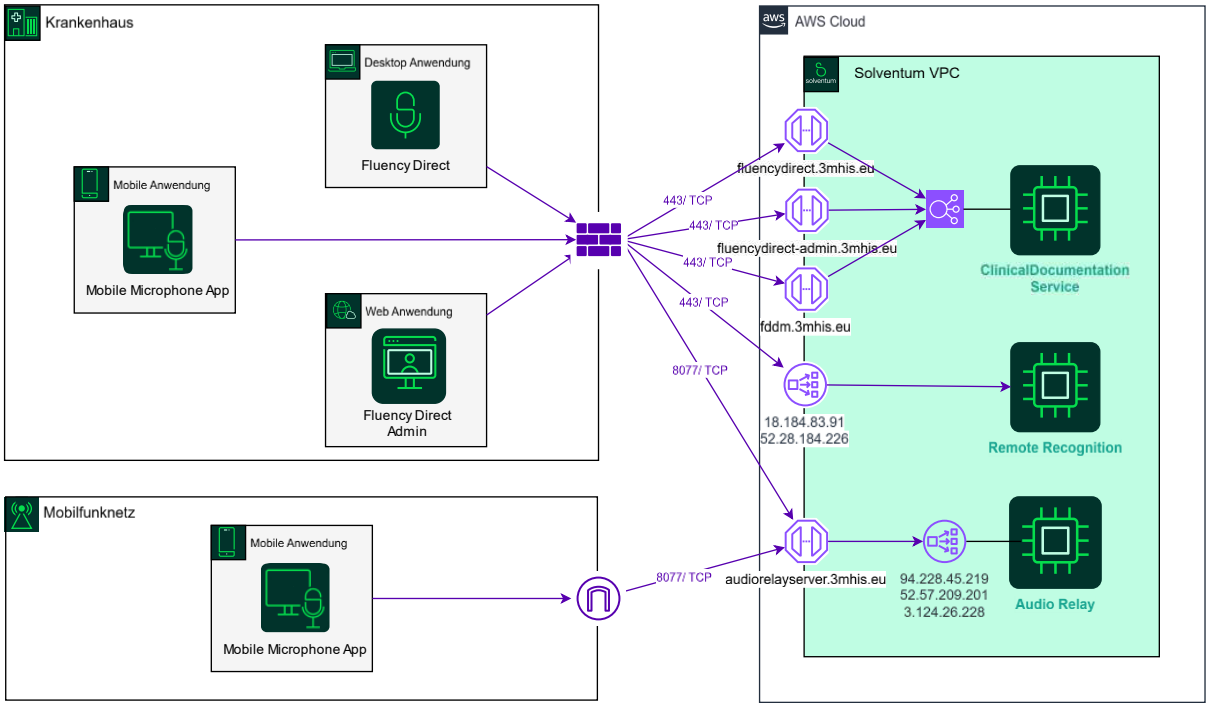
- Microsoft® Windows® 10 oder höher
- Prozessor: Intel Core 2 CPU, 2,0 GHz, 2 GB empfohlen für die lokale Erkennung
- Prozessor: Intel Core 2 CPU, 2,0 GHz, 1 GB empfohlen für die Remote-Erkennung
- Festplattenspeicher: 4 GB für die lokale Erkennung, 1 GB für die entfernte Erkennung
- Microsoft® Edge, Internet Explorer ab Version 8 oder Google Chrome
- .Net Framework 4.6.1
- Wenn in Java-basierte Anwendungen diktiert werden soll: JRE 1.7 u6 (32 bit) oder höher muss auf dem Computer installiert sein, bevor Fluency Direct installiert wird.
- Für Citrix XenApp-Unterstützung: Citrix Client 10, 11, 12 (oder höher) oder der Citrix Receiver

CPU-Benchmarks

Die obigen CPU-Richtlinien dienen als gute allgemeine Regel für die Systemanforderungen. Es ist oft hilfreich, bestimmte Computer in Ihrem Unternehmen anhand einer idealen CPU-Geschwindigkeit zu bewerten. Websites wie www.cpubenchmark.net bieten objektive Bewertungen für einzelne Prozessoren. Wenn Sie eine Website wie www.cpubenchmark.net besuchen, können Sie einen Benchmark-Wert für Ihre(n) Prozessor(en) erhalten und ihn mit dem Mindestwert von 5000 vergleichen. Jeder Computer mit einem Benchmark-Score unter 5000 sollte eine Clouderkennungskonfiguration in Erwägung ziehen, um eine maximale und konsistente Leistung bei der Spracherkennung zu gewährleisten. Wenn ein PACS oder andere ressourcenintensive Systeme verwendet werden, empfehlen wir einen Mindestwert von 5000 und einen empfohlenen Benchmark von 8000 oder höher.

4 Netzwerkanforderungen

4.1 URLs und TCP Ports



4.2 Internet-Bandbreite

Für jeden gleichzeitigen/aktiven Diktierenden wird eine Bandbreite von ~55 Kbits/sec benötigt. Daher kann eine Verbindung mit 10 MB/Sek. 180 gleichzeitige Diktierende unterstützen. Bitte bedenken Sie, dass die Anwender nicht ununterbrochen diktieren, so dass die Anzahl der gleichzeitigen Diktierenden auch in Spitzenzeiten typischerweise weniger als 12 % der Gesamtzahl der lizenzierten Benutzer beträgt. Der größte Teil der Bandbreite wird durch den Daten-Upload verbraucht, wenn Audio zwischen den Geräten im Netzwerk gestreamt wird. Deutlich weniger Daten werden zwischen der Client-Software und den Citrix-Sitzungs- oder Remote Recognition-Servern übertragen. Der Download-Verkehr vom Datenzentrum ist im Vergleich zum Upload minimal.

4.3 Firewall / Proxy

Die folgenden Domänen müssen von den Arbeitsstationen und mobilen Geräten aus erreichbar sein, ohne dass ein Proxy verwendet wird:

3mhis.de
3mhis.eu

Die folgenden Adressen müssen ohne die Verwendung eines Proxys erreicht werden können. Diese Adressen befinden sich hinter Application Load Balancern, so dass mehrere Dienste über den/die gleichen Endpunkt(e) ausgeführt werden:

Purpose	Endpoint	IP(s)	Port (outbound)
Standard Web Services	fluencydirect.3mhis.eu fluencydirect-admin.3mhis.eu fddm.3mhis.eu production.3mhis.eu	Siehe (1)	443
Mobile Microphone	audiorelayserver.3mhis.eu	94.228.45.219 52.57.209.201 3.124.26.228	8077
Remote Recognition	Siehe (2)	18.184.83.91 52.28.184.226	443
CloudFront	d3ars4xsbl6uaf.cloudfront.net	Siehe (3)	443
SSL Verification	ocsp.comodoca.com crl.comodoca.com ocsp.usertrust.com crl.usertrust.com ocsp.sectigo.com crl.sectigo.com	151.139.128.14 151.139.128.10	80

(1) Diese Dienste werden mit AWS Application Load-Balancers (ALBs) bereitgestellt. Aufgrund der Funktionsweise von AWS ALBs ändert sich die zugewiesene IP-Adresse im Laufe der Zeit, daher kann in diesem Dokument keine statische IP-Adresse angegeben werden. Bitte nehmen Sie stattdessen die FQDNs in Ihrer Firewall in die Whitelist auf.

(2) Wenn Fluency Direct die Remote-Erkennung nutzt, wird die Verbindung über die IP-Adresse und nicht über den FQDN hergestellt.

(3) Amazon CloudFront wird verwendet, um die aktualisierte Version der Spracherkennungs-Engine an die Clients zu verteilen. Aufgrund der Natur von Amazon CloudFront ist dem FQDN keine statische IP zugewiesen. Amazon CloudFront wird nur zum Herunterladen neuer Versionen und niemals zum Hochladen von Daten vom Kunden verwendet.

Key Features of a Content Delivery Network| Performance, Security | Amazon CloudFront

(4) Sectigo (ehemals Comodo) ist eine Trust Root Certification Authority. Aufgrund der Art und Weise, wie SSLÜberprüfungen funktionieren, erfolgt die Kommunikation über Port 80. Es werden keine sensiblen Informationen gesendet: Bei einer Widerrufsprüfung geht es darum, die Trust Root Certification Authority zu fragen, ob einem bestimmten, von ihr ausgestellten Zertifikat noch vertraut werden kann. Die Überprüfung von Zertifikaten wird vom Betriebssystem und dem Browser durchgeführt, nicht von der/den Solventum-Anwendung(en). Die von Sectigo verwendeten IP-Adressen sind nicht statisch und können sich daher ändern. Es wird empfohlen, Firewall-Regeln auf der Grundlage des DNS-Hostnamens in die Whitelist aufzunehmen. Weitere Informationen finden Sie unter https://sectigo.com/knowledge-base/detail/OCSP-and-CRL-access-information/kA01N000000zFJr

5 Virtualisierung

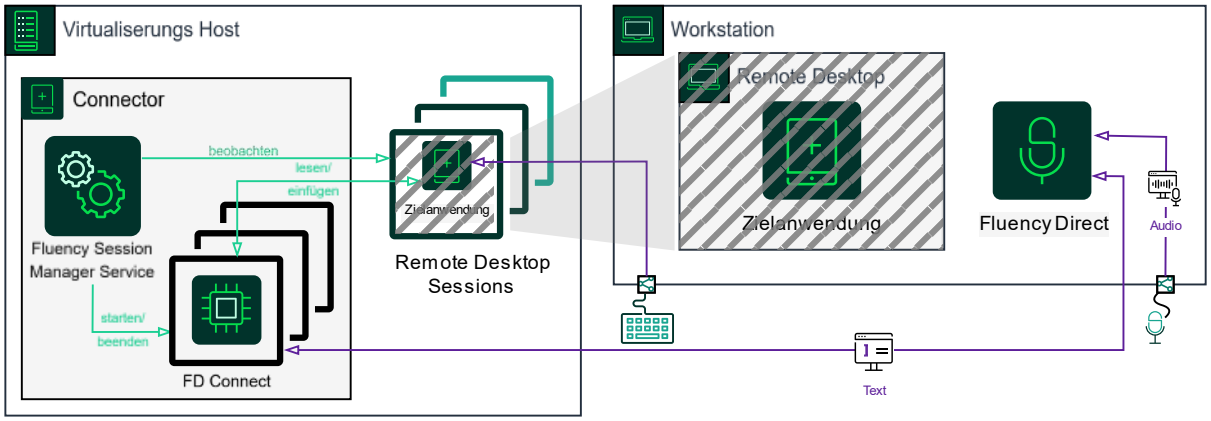
Fluency Direct ist eine Windows-basierte Anwendung, kann aber auch in virtualisierten Umgebungen eingesetzt werden. **Solventum** unterstützt derzeit **Citrix XenApp, XenDesktop, Remote Desktop, Parallels und VMWare Horizon View**, aber auch andere können unterstützt werden (wenn dies gewünscht wird).

Gegebenenfalls können die Produkte als Zero-Client eingesetzt werden. Ein Zero-Client erfordert keine Installation der Software auf dem lokalen Rechner und kann daher auf Thin Clients, Linux-, Windows- und OSX-Workstations eingesetzt werden.

Speziell für Fluency Direct, da es sich hierbei um eine Anwendung handelt, die zum Diktieren in Anwendungen von Drittanbietern - wie z. B. Ihrem KIS - verwendet wird, werden zwei Virtualisierungsbereitstellungsmodelle unterstützt:

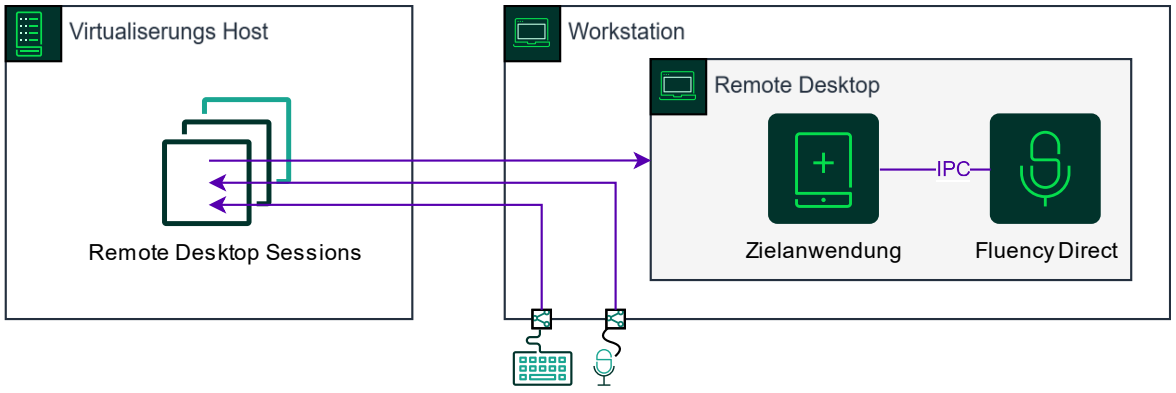
5.1 Fluency Direct lokal

Ein lokal installiertes Fluency Direct (FD), das mit einer virtualisierten KIS-Sitzung durch den Einsatz eines "Connectors" interagiert:



5.2 Fluency Direct remote

Sowohl Fluency Direct als auch das KIS laufen in einer virtualisierten Sitzung



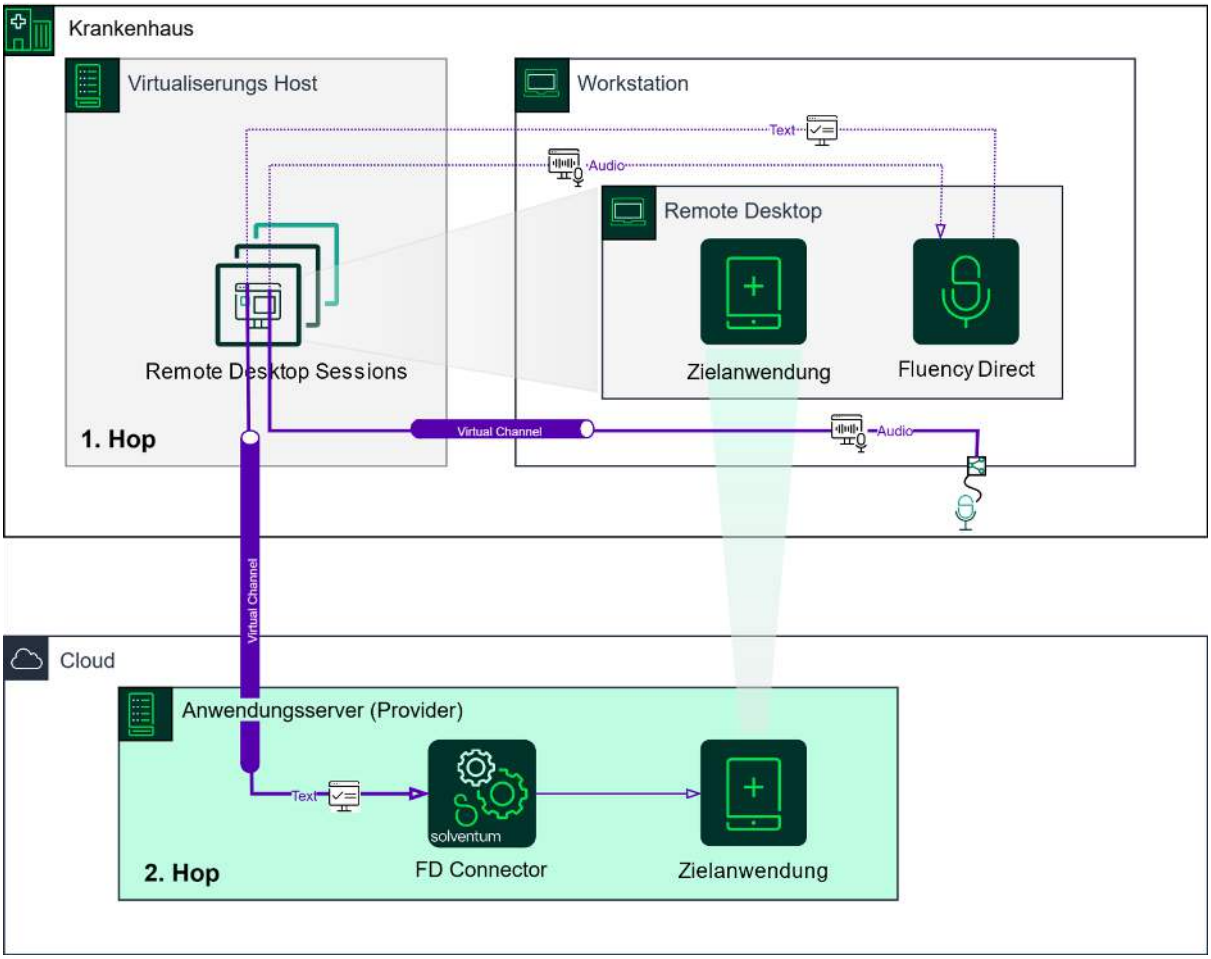
5.3 Double-Hops

Ähnlich wie bei einer Desktop-Installation von Fluency Direct, bei welcher in eine virtuelle Anwendung diktiert werden soll, wird Fluency Connector auf den virtuellen Servern (z.B. Citrix) installiert. Dort wird eine virtuelle Anwendung gehostet, was in diesem Fall dem zweiten Hop entspricht.

Der erste Hop ist ein virtueller Desktop, auf dem Fluency Direct installiert ist. Dieses virtualisierte Fluency Direct kann mit den virtuellen Anwendungen auf dem 2. Hop über die Fluency Connector-Komponente kommunizieren (benutzerdefinierter ICA-Kanal).

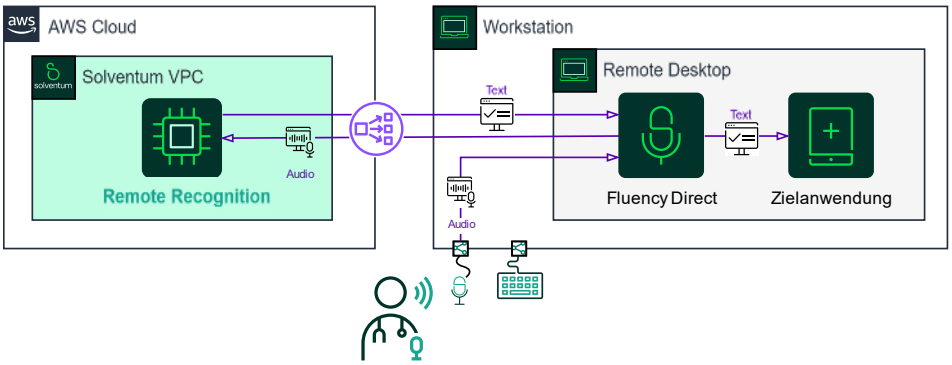
Aus Sicht des Fluency Connectors ist es egal, ob Fluency Direct nativ (d.h. auf dem Desktop installiert) oder virtuell (d.h. auf einem virtuellen Desktop installiert) ist.

Der Benutzer verwendet dann Fluency Direct auf Hop 1, genau wie bei jeder anderen Zero-Client-Integration wo Fluency Direct verwendet wird.



6 Remote Recognition

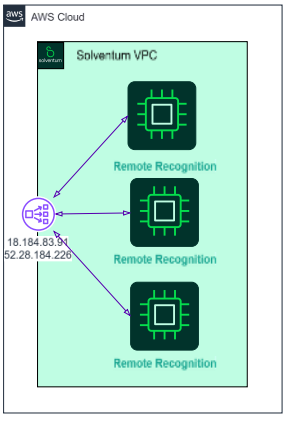
Als SaaS Anwendung muss kein Server in der Einrichtung des Betreibers installiert werden. Bei Zero Clients oder für den Fall, dass die Clients nicht die Mindestvoraussetzungen erfüllen, kann die Sprachengine auf einem Remote Recognition Server betrieben werden.



Beachten Sie, dass bei einer Zero-Client-Installation die Mikrofontreiber auf der Workstation installiert werden müssen und der Mikrofonhersteller muss das Virtualisierungsprodukt unterstützen. Dies ist bei den üblichen Philips-, und Olympus-Diktiergeräten der Fall. Als Alternative zur Verwendung eines physischen Mikrofongerätes bietet Solventum auch die Option, Solventum Mobile Microphone zu verwenden – eine Anwendung, die für iOS und Android verfügbar ist und Ihr iOS/Android-Gerät in ein Mikrofon verwandelt, das mit Fluency Direct in Verbindung steht. Für Citrix bietet Solventum auch eigene Remote-HID-Treiber an.

Beachten Sie auch, dass wir für Zero-Client-Implementierungen die Verwendung von Recognition Servern empfehlen – eine Recognition Server-Setup verlagert die teure CPU- und RAM-Verarbeitung auf dedizierte Hardware, wodurch der Fluency Direct Client weniger RAM und CPU auf dem Virtualisierungsserver beansprucht.

Recognition Server



Remote Recognition Server sind eine Sammlung von einer oder mehreren netzwerkbasierten Ressourcen, die dazu dienen die Erkennung von einem Fluency Direct-Client oder einer mobilen Anwendung auf eine zentrale Ressource zu verlagern. Dies ermöglicht eine Reduzierung der Gesamt-CPU- und Speicherressourcen des Fluency Direct-Clients, so dass er in Thin-Client-Umgebungen wirtschaftlich eingesetzt werden kann. Durch die Verwendung der Remote-Server für die Erkennung können Sie den Fluency Direct Client auf einer Workstation oder in einer virtuellen Desktop-Umgebung einsetzen und 2/3 weniger Speicher und einen Kern weniger als die normalen Mindestanforderungen von Fluency Direct an eine Workstation.

Der Remote-Erkennungsansatz ermöglicht auch eine genaue Spracherkennung, die auf einem mobilen Gerät aufgrund der Hardware nicht möglich wäre.

Remote Recognition Server werden von Solventum in Amazon AWS gehostet.

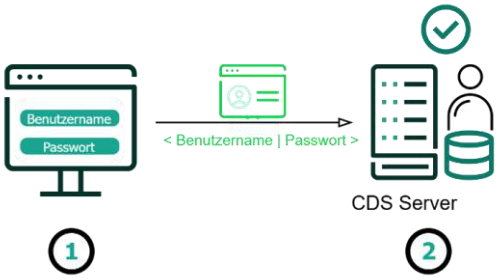
Remote HID

Beachten Sie, dass bei einer Zero-Client-Installation die Mikrofontreiber auf der Workstation installiert werden müssen und der Mikrofonhersteller muss das Virtualisierungsprodukt unterstützen. Dies ist bei den üblichen Philips-, und Olympus-Diktiergeräten der Fall. Als Alternative zur Verwendung eines physischen Mikrofongerätes bietet Solventum auch die Option, Solventum Mobile Microphone zu verwenden – eine Anwendung, die für iOS und Android verfügbar ist und Ihr iOS/Android-Gerät in ein Mikrofon verwandelt, das mit Fluency Direct in Verbindung steht. Für Citrix bietet Solventum auch eigene Remote-HID-Treiber an.

Beachten Sie auch, dass wir für Zero-Client-Implementierungen die Verwendung von Recognition Servern empfehlen – eine Recognition Server-Setup verlagert die CPU- und RAM-Verarbeitung auf dedizierte Hardware, wodurch der Fluency Direct Client weniger RAM und CPU auf dem Virtualisierungsserver beansprucht.

7 Benutzerauthentifizierung

Fluency Direct verwendet individuelle Sprachprofile, daher ist eine Authentifizierung des Benutzers erforderlich. Die Authentifizierung kann direkt gegen den Solventum CDS Service erfolgen. Der Benutzer authentifiziert sich durch Eingabe von Benutzernamen und Passwort, die Verifizierung erfolgt durch den CDS-Service.



7.1 Single Sign-On

Single Sign-on (SSO) ist eine Authentifizierungsmethode, die es Benutzern ermöglicht, sich bei mehreren Anwendungen zu authentifizieren ohne dabei ihre Anmeldeinformationen wiederholt eingeben zu müssen.

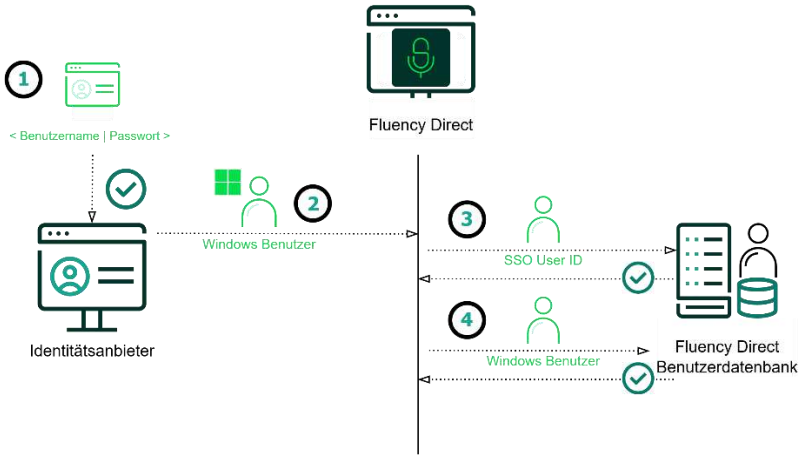
SSO basiert auf einer Vertrauensbeziehung zwischen einem Serviceanbieter, in diesem Fall Fluency Direct, und einen Identitätsanbieter. Innerhalb eines lokalen Netzwerks werden Benutzeridentitäten vielfach in Active Directory (AD) verwaltet. Fluency Direct vertraut in diesem Fall der Windows Anmeldung und setzt voraus, dass sich der aktuell angemeldete Windows Benutzer am Active Directory authentifiziert hat (1).

In diesem Fall fungiert Windows als Identitätsanbieter, der auch als SSO-Quelle bezeichnet wird und einen Benutzernamen an Fluency Direct übergibt. Es können auch andere Systeme, wie z. B. das KIS mit einer seperaten Benutzerverwaltung, als SSO-Quelle verwendet werden.

Für die meisten SSO-Integrationen in Fluency Direct wird eine sogenannte SSO User ID benötigt. Die SSO User ID definiert einen einzelnen Satz von Anmeldeinformationen, der für die Authentifizierung an der Fluency Direct Benutzerdatenbank verwendet wird (3). Die Informationen über den SSO-User werden in verschlüsselter Form in der Konfiguration des Fluency Direct Clients hinterlegt.

Nach erfolgreicher Authentifizierung kann die übergebene Benutzer ID mit der Fluency Direct Benutzerdatenbank abgeglichen werden. Wenn der übergebene Benutzername in der Fluency Direct Benutzerdatenbank existiert und der Benutzer nicht gesperrt ist, wird das entsprechende Profil geladen und die Anmeldung war erfolgreich (4).

Die folgende Abbildung zeigt exemplarisch den Informationsaustauch während des Anmeldeprozesses zwischen Fluency Direct Client, der Fluency Direct Benutzerdatenbank und einem Identitätsanbieter, in diesem Fall Windows bzw. Active Directory.

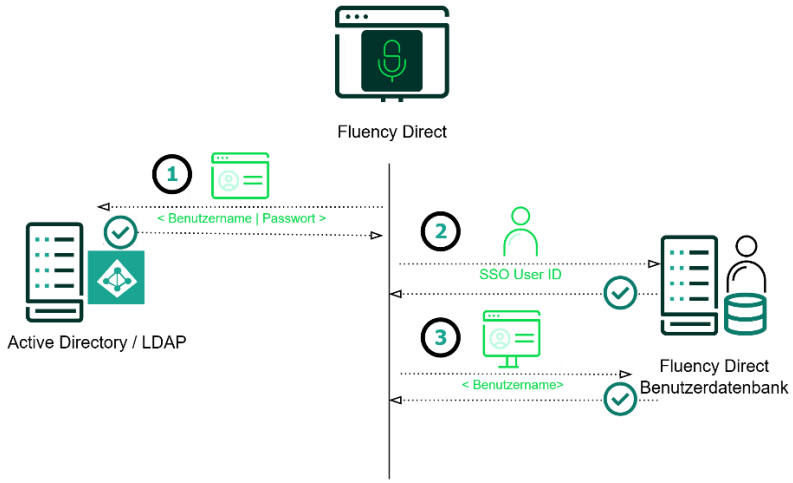


7.2 Benutzerauthentifizierung mittels LDAP

Fluency Direct unterstützt Active Directory-Integrationen. Der Fokus liegt hierbei auf der Authentifizierung. Das heißt, dass die Überprüfung der Anmeldeinformationen des Benutzers gegen das Active Directory des Kunden.

Bei dieser Konfiguration wird im ersten Schritt die vom Benutzer eingegebene Kombination aus Benutzername und Passwort mit dem Active Directory verifiziert. Wenn die Authentifizierung erfolgreich war, erfolgt in einem zweiten Schritt die Authentifizierung mit der Fluency Direct Benutzerdatenbank. Für diesen Schritt wird eine sogenannte SSO User ID benötigt (siehe 7.1).

War auch die Anmeldung an der Fluency Direct Benutzerdatendank erfolgreich, erfolgt in einem dritten Schritt der Abgleich der im ersten Schritt verifizierten Benutzer ID mit der Fluency Datenbank. Existiert in der Fluency Datenbank ein Benutzer mit der angegebenen ID wird dieser ohne Angabe eines Passwortes authentifiziert.



7.3 Benutzerverwaltung über REST-Schnittstelle

Die Verwaltung von Fluency Direct-Anwendern über die Fluency Direct Administrationsoberfläche ist standardmäßig enthalten.

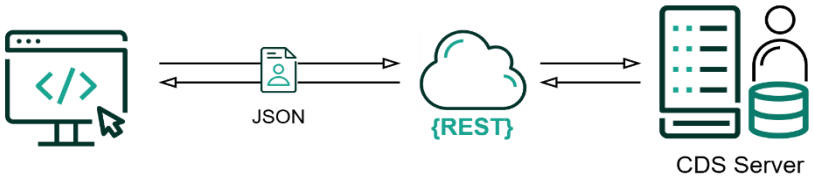
Optional kann die Benutzerverwaltung auch automatisiert über die Fluency Direct Web API erfolgen. Diese API basiert auf dem REST-Architekturstil und ermöglicht die programmgesteuerte Erstellung, Aktivierung, Deaktivierung und Verwaltung von Benutzerkonten.

7.3.1 Funktionsumfang der Web API

Die Fluency Direct Web API stellt mehrere Resourcen für verschiedene Anwendungsfälle bereit.

- Benutzer erstellen und aktivieren ('/user/activateFdUser')
- Benutzer deaktivieren ('/user/deactivateFdUser')
- Benutzerinformationen abrufen ('/user/getFdUser')
- Benutzergruppen verwalten ('/user/setFdUserGroupsMembership')
- Benutzername ändern ('/user/changeUserNameFdUser')
- Benutzerlisten abrufen ('/user/getFdUsersForCustomer')

Der Datenaustausch erfolgt im JSON-Format.



7.3.2 Authentifizierung

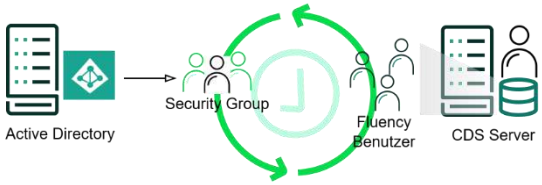
Die Authentifizierung gegenüber der Fluency Direct Web API erfolgt über zwei kombinierte Mechanismen:

- HTTP Basic Authentication – Benutzername und Passwort werden Base64-codiert im Header übermittelt.
- API-Key im Header – Ein API-Schlüssel unter dem Header-Feld `b2bUserAccount` identifiziert das B2B-Konto eindeutig.

Beide Mechanismen sind für jeden API-Aufruf erforderlich. Die Kommunikation erfolgt ausschließlich über HTTPS.

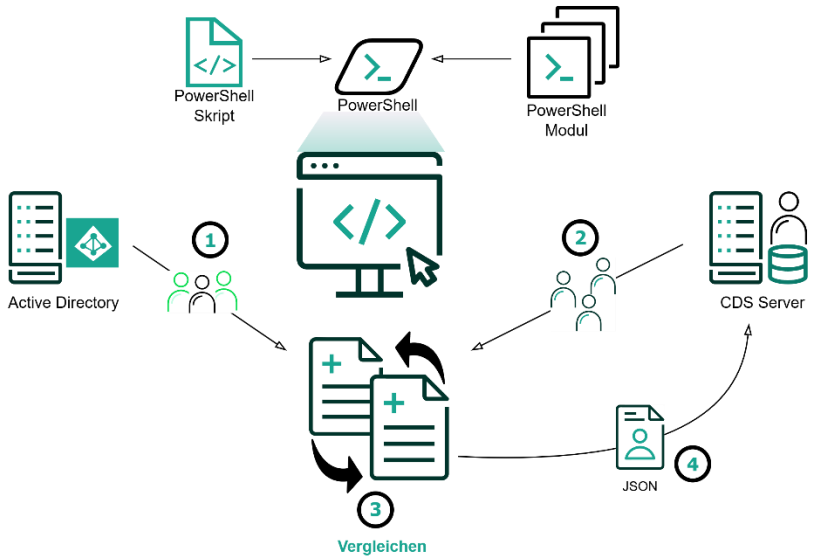
7.3.3 Integration in Krankenhaus-Systeme

Mittels der Fluency Direct Web API ist eine Integration in bestehende Benutzer-verwaltungssysteme des Krankenhauses möglich, z. B. in ein LDAP-basiertes Verzeichnis (wie Microsoft Active Directory) oder ein übergeordnetes Identity-Management-System. Die Integration kann über eine Middleware erfolgen, die regelmäßig Benutzerinformationen synchronisiert und API-Aufrufe ausführt.



Die folgende Abblíldung zeigt eine mögliche Umsetzung der Middleware zur Synchronisierung von Benutzerkonten zwischen einem vorhandenen Verzeichnisdienst und der Fluency Direct Benutzerdatenbank.

Im dem gezeigten Beispiel wird Active Directy als Verzeichnisdienst angenommen und die Implemtierung basiert auf PowerShell.



Die PowerShell Lösung besteht aus zwei Komponenten. Einem Modul, das die Anfragen an die REST API kapselt und über Methoden bereitstellt und einem Skript in dem die verschiedenen Prozessschritte implementiert sind:

1. Daten aus dem AD auslesen
2. Daten aus der Fluency Direct Datenbank auslesen
3. Datensätze vergleichen
4. Änderungen über REST-Aufruf in die Fluency Datenbank übertragen

8 Unterbrechungsfreier Betrieb

Die vorgeschlagene Lösung wird als SaaS bereitgestellt. Desaster-Recovery- und Business-Continuity-Pläne sind im Rahmen des ISO27001 ISMS abgedeckt. Die in der Solventum Cloud gehosteten Dienste sind als hochverfügbares System ausgelegt, um eine Verfügbarkeit von 24x7x365 zu ermöglichen. Dies wird durch den Einsatz von Standby-Datenbanken, mehreren Anwendungsservern, RAID-Arrays, Load Balancern und Backup-Richtlinien erreicht.

Upgrades der gehosteten Lösung erfolgen in der Regel ohne Unterbrechung für die Kunden. Wenn eine Unterbrechung zu erwarten ist, wird dies in den geplanten Wartungsbenachrichtigungen mitgeteilt, die der Kunde im Vorfeld erhält.

Für den unwahrscheinlichen Fall eines Ausfalls verfügen alle lokal installierten Clients über einen Offline-Modus, der die Funktionalität möglichst uneingeschränkt bereitstellt und die Verbindung automatisch wiederhergestellt wird, wenn die Cloud-Infrastruktur wieder verfügbar ist.

Es ist möglich, dass nur bestimmte Funktionen nicht verfügbar sind, z. B. wenn es ein Problem mit unseren Servern gibt, die für das mobile Mikrofon benötigt werden, hat dies nicht unbedingt Auswirkungen auf die Server, die für CDI Engage usw. verwendet werden.

Bei Fluency Direct ist zu beachten, dass es sich im Wesentlichen um einen komfortablen Ersatz für die Tastatur handelt, so dass Sie Ihre Stimme verwenden können, anstatt zu tippen. Bei einem Ausfall kann der Benutzer auf die Tastatur/Maus zurückgreifen, um eine medizinische Dokumentation zu erstellen, d.h. selbst wenn Fluency Direct nicht verfügbar wäre, wird dies einen Arzt nicht davon abhalten, ein medizinisches Dokument zu erstellen.

Es wird nach zwei „Offline-Situationen“ unterschieden:

- Wenn ein Benutzer ein bestimmtes Gerät schon einmal erfolgreich verwendet hat, sind Informationen über diesen Benutzer im Benutzer-Cache auf diesem Gerät gespeichert. Wenn die Solventum Cloud nicht erreicht werden kann, wird eine Authentifizierung gegen den zuvor im Cache gespeicherten Zustand des Benutzers durchgeführt, und sobald die Authentifizierung erfolgreich war, wird der Cache vom System geladen. Wenn sich der Benutzer in diesem Offline-Zustand befindet, bemerkt er normalerweise nicht, dass er sich im Offline-Modus befindet. Das System erscheint so, als ob es mit dem Solventum Data Center verbunden wäre.
- Wenn Informationen zu einem bestimmten Benutzer nicht im Cache des Geräts gefunden werden, ermöglicht das System dem Benutzer dennoch den Zugriff auf das System in einem sichtbaren "Offline-Modus". Wenn sich das System im "Offline-Modus" befindet, wird ein ungeschultes Profil verwendet und es werden keine benutzerspezifischen Befehle, Wörterbucheinträge oder Abkürzungen geladen.

9 Datensicherheit

9.1 Rechenzentrum

Benutzereinstellungen, Benutzerprofile, Sprachdateien und Dokumente werden in der Cloud gehostet, ausschließlich in der AWS in Frankfurt Main, in redundanten Rechenzentren.

Alle an Solventum-Ressourcen gesendeten Informationen werden sicher mit TLS1.2 übertragen, einem verschlüsselten Übertragungsmechanismus nach Industriestandard. Innerhalb von TLS1.2 verwenden wir AES 256-Bit-Verschlüsselung (High) und RSA mit 2048-Bit-Austausch. Solventum-Ressourcen kommunizieren über Port 443 und 8077.

Hochverfügbar/-planbar	Datenschutzkonform	Sicher
Höchste Verfügbarkeit durch Nutzung cloudbasierter Infrastruktur: • Zentrales Releasemanagement • Sicherer 24x7x365 Betrieb • Keine On-Premise Kosten • Skalierbar • Entlastung der IT-Abteilung • Kosten planbar durch Abo, ohne Vorinvestition der Lizenzen • Optimiert für Citrix-Umgebung	Solventum und Amazon Web Service nutzen und unterstützen internationale und nationale Anforderungen: • EU-DSGVO & BDSG (neu) • In Frankfurt gehostet • BSI C5 zertifiziert • ISO 9001 • 27001 Sicherheitsmanagementkontrollen • 27017 Cloudspezifische Kontrollen • 27018 Schutz personenbezogener Daten • Jährliche Audits	Amazon Web Service ist Weltmarktführer von Infrastructure as a Service (IaaS) mit höchsten Anforderungen an die Sicherheit: • Nutzung von AWS als IaaS • Betrieb als Private Cloud, per VPN • Verschlüsselte Übertragung und Daten nach TLS, bzw. AES-256 • Striktes Sicherheitsregime/TOMs • Next Generation Firewall, sichere Authentisierung, Intrusion Detection System, Log Management System • Regelmäßige Risikoanalysen, Penetration Tests und Schulungsmaßnahmen

9.2 Speichermechanismen und Schutz personenbezogener Daten

Wie wird der Datenschutz gewährleistet?

- Jeder Mitarbeiter wird standardmäßig auf die Vertraulichkeit und Geheimhaltung verpflichtet.
- Datenschutzsystem wird regelmäßig überprüft
- Verpflichtende Schulungsmaßnahmen für die zuständigen Mitarbeiter werden durchgeführt
- Neben Datenschutzbeauftragten werden spezielle Datenschutzkoordinatoren für einzelne Geschäftsbereiche eingestellt, z.B. für HIS
- Sub-Unternehmer werden mit AV-Verträgen auf die Einhaltung gleichwertiger Datenschutzstandards verpflichtet

Benutzereinstellungen, Benutzerprofile, Quell-Audio und Text werden in proprietären Binärformaten gespeichert, die sowohl künstliche neuronale Netzwerke als auch faktorielle Modelle beinhalten. Da das System mandantenfähig ist, werden die kundenspezifischen Dateien in eindeutigen Speicherorten für jeden Kunden getrennt gespeichert. Innerhalb des Speicherortes des Kunden werden die individuellen Benutzerdaten weiter getrennt.

Letztendlich werden die Daten einem einzelnen Benutzer zugeordnet, mit einem Triple-DES-Algorithmus verschlüsselt und auf mit AES256 Bit verschlüsselten Festplatten gespeichert. Die proprietären Datenformate sind nur mit Solventum APIs mit den richtigen Verschlüsselungsschlüsseln zur Entschlüsselung lesbar. Sofern nicht vorgeschrieben, werden Patientennamen und Identifikatoren nicht vom System gespeichert.

Da die Daten nach Benutzern getrennt und verschlüsselt sind, sind die Daten nicht benutzer- oder kundenübergreifend durchsuchbar. Der Zugriff erfordert Benutzeranmeldeinformationen, die mit Benutzerrollen verbunden sind.

Wie wird die Sicherheit überprüft?

Die Services und die Architektur, die wir einsetzen, wird auf Sicherheitslücken geprüft. Diese Kriterien werden durch unsere Security Assessment Process und Security Team kontrolliert (Assessment Reviews) und teilweise automatisiert überwacht (DivvyCloud und andere Tools/Policies). Darüber wird eine Dokumentation geführt, bzw. in Logs getrackt.

Organisatorische Maßnahmen

Solventum HIS hat in Übereinstimmung mit den Empfehlungen der Europäischen Datenschutzbehörde Mechanismen etabliert, die dem Datenschutz höchste Priorität einräumen. Aktivitäten, Datentransfers und Zugriffe werden dokumentiert. Standardvertragsklauseln nach § 46 der DSGVO bieten die Sicherheit auf einen integren Umgang mit personenbezogenen Daten. Zusätzliche technische und organisatorische Maßnahmen gehen zudem darüber hinaus. Zugangsbeschränkungen, Verschlüsselung bei der Übertragung und im Ruhezustand, die bewusste Minimierung der Datenmenge und regelmäßige Mitarbeiterschulungen sowie von Solventum HIS formulierte Zusatzklauseln im Verkehr mit Cloudanbietern heben das Schutzniveau weiter an.

9.3 Verschlüsselung

Solventum verwendet standardmäßig eine AES-256 Verschlüsselung für alle Daten in der Solventum Cloud, auf alle Speichermedien und Services, die zum Einsatz kommen. Verbindungen intern und extern in der Solventum Cloud werden von Solventum mit sicheren TLS/SSL-Verfahren und Versionen verschlüsselt. Beide Verschlüsselungs-Verfahren gelten als NSA sicher.

Die Verschlüsselungsverfahren im Detail:

- **Fluency Direct:** Alle Informationen werden sicher mit TLS1.2 AES 256-Bit-Verschlüsselung (High) und RSA mit 2048-Bit-Austausch über Port 443 übertragen.

- **Fluency Direct Mobiles Mikrofon:** Alle Informationen werden sicher mit TLS1.2 übertragen, einem verschlüsselten Übertragungsmechanismus nach Industriestandard. Innerhalb von TLS1.2 verwendet das System SHA oder AES 256-Bit-Verschlüsselung (High) und RSA mit 2048-Bit-Austausch. Dies wird über Port 8077 übertragen. Der Fluency Client öffnet auch einen Web-Socket auf demselben 8077-Port zum Solventum-Rechenzentrum mit TLS 1.2. Die beiden Websockets werden verwendet, um Daten zwischen Clients auszutauschen, wobei das Solventum-Rechenzentrum das ordnungsgemäße Routing übernimmt.

- **Clouderkennung:** Audio wird vom Client übertragen und auf dem Server verarbeitet. Alle an Remote-Erkennungsserver gesendeten Audiodaten werden sicher mit TLS1.2 mit SHA-256-Bit-Verschlüsselung (Hoch) und RSA mit 2048-Bit-Austausch auf Port 50001 übertragen.

- **Fluency Connector:** Wenn Fluency Direct verwendet wird, um in eine Citrix/RDP-Anwendung zu diktieren, erfolgt die Kommunikation über einen virtuellen Kanal. Dabei wird das ICA- oder RDP-Protokoll verwendet, das die Standardfunktionalität von Citrix und Remote Desktop ist. Alle Informationen werden sicher über einen benutzerdefinierten virtuellen Kanal übertragen und auf die sichere Kommunikation, die bereits zwischen dem Terminal\Citrix Client und dem Virtual Server über ICA- oder RDP-Protokolle besteht, huckepack genommen

9.4 Zertifikate

Wir sind zertifiziert nach:

- ISO 9001 (Health Information Systems, Berlin und Düsseldorf)
- ISO 27001 (Health Information Systems, Berlin)
- C5 Type 2

Die Zertifikate unseres Cloud-Anbieters AWS sind hier zu finden:
Compliance-Programme – Amazon Web Services (AWS)

10 Archivierungskonzept

Solventum Fluency ist nicht als Archivierungslösung gedacht, da das endgültige Dokument in einem System eines Drittanbieters wie dem KIS oder DMS gespeichert würde, aber natürlich werden Backups erstellt, um mit Disaster-Recovery-Ereignissen umgehen zu können. Solventum Fluency wird als SaaS angeboten, was auch bedeutet, dass die Backups von Solventum verwaltet werden. Es besteht keine Notwendigkeit für den Kunden, irgendwelche Backups durchzuführen. Die Backups werden verschlüsselt und nicht auf externen Geräten wie Bändern gespeichert. Es gibt formale Backup- und Recovery-Prozesse und -Verfahren.

10.1 Aufbewahrungsfristen

Die Produkte von Solventum werden nicht zur primären Dokumentenarchivierung genutzt, daher sehen wir die gesetzlichen Aufbewahrungsfristen durch den Einsatz des KIS und des Archivs abgedeckt. Nichtsdestotrotz bieten wir die Möglichkeit an, die Speicherzeiten in unseren Produkten auf die individuellen Anforderungen des Hauses anzupassen. Die mit Solventum gespeicherten Daten automatisch bereinigt, wobei die Aufbewahrung je nach Produkt konfigurierbar ist:

Fluency Direct: Die durch Fluency Direct generierten Audiodaten und Texte werden nicht in einem strukturierten Format gespeichert, da sie keine Metainformationen über den Patienten bzw. den Gesprächspartner enthalten: Die von Fluency Direct generierten Daten werden in Stücken von circa 45 Sekunden Audio gespeichert. Diese Daten werden gespeichert, um ein automatisches Profil-Training für den Sprecher zu ermöglichen, um seine Erkennungsqualität zu verbessern.

- Standardmäßig werden Sprachdaten (Audio + Text) für 12 Monate aufbewahrt, um eine optimale Spracherkennungsqualität zu gewährleisten. Für das Sprachprofil werden aufgrund der saisonalen Veränderungen in der Stimme die Sprachdateien über diesen Zeitraum genutzt.
- Nach den 12 Monaten werde die Textdaten pseudonymisiert und werden zu Entwicklungszwecken 5 Jahre aufbewahrt.
- CDI Engage-Daten werden standardmäßig für 2 Jahre aufbewahrt, sofern mit dem Kunden nichts anderes vereinbart wurde.
- Daten, die über Citrix ShareFile verarbeitet werden, werden für fünf Tage aufbewahrt. Citrix ShareFile wird verwendet, um einen sicheren Mechanismus zum Austausch von Dateien mit Kunden, wie z. B. Mitarbeiterlisten oder Altdaten, bereitzustellen; es ist nicht als Dateispeicher gedacht.
- Alle anderen Daten werden in der Regel für die Dauer des Vertrags oder bis zum ausdrücklichen Wunsch des Kunden sie zu löschen, aufbewahrt.

Fluency Align: Durch Fluency Align generierten Audiodateien werden in der Cloud gesichert, damit für jedes dokumentierte Gespräch ein Transkript und eine Zusammenfassung erstellt werden kann.

- Audiodaten, das Transkript und die Zusammenfassung werden standardmäßig für 90 Tage gespeichert, sofern mit dem Kunden keine andere Frist vereinbart wurde.
- Zu Entwicklungszwecken werden die Audiodaten für 12 Monate aufbewahrt, um ein optimales Training für den Spracherkenner zu gewährleisten.
- Nach den 12 Monaten werden die Daten automatisch und unwiederbringlich gelöscht.
- Daten, die über Citrix ShareFile verarbeitet werden, werden für fünf Tage aufbewahrt. Citrix ShareFile wird verwendet, um einen sicheren Mechanismus zum Austausch von Dateien mit Kunden, wie z. B. Mitarbeiterlisten oder Altdaten, bereitzustellen; es ist nicht als Dateispeicher gedacht.

10.2 Löschfunktionen

In Fluency Direct werden grundsätzlich keine Identifikatoren wie PatientenID oder Fallnummer gespeichert. Beim Diktieren werden Anwender angehalten, darauf zu verzichten, Patientennamen zu verwenden. Die Sprachdateien haben somit keinen unmittelbaren Patientenbezug. Daher muss das Löschen für diese Patienten durch Solventum mittels einer Liste erfolgen, die Solventum zur Verfügung gestellt wird und die die eindeutige Zuordnung zu den Sprachdaten ermöglicht.

Auf Wunsch kann der Kunde sich an Solventum wenden, sodass das Löschen der Daten dann im Auftrag des Kunden durch Solventum erfolgt.

Für Fluency Align wird bei individuellen Löschanfragen der Nutzername des Fluency Align-Anwenders sowie der Tag der Behandlung des Patienten benötigt. Dadurch können alle Audiodaten des Anwenders für diesen Zeitraum unwiederruflich gelöscht werden.

Eine Zwischenspeicherung (Caching) auf Endanwendergeräten findet nur für die Dauer einer Nutzersession (Aufnahme eines Gespräches) statt. Darüber hinaus findet keine lokale Speicherung von Audiodaten oder Metadaten statt.

Solventum hält sich an die Grundsätze, wie sie in der GDPR und DSGVO definiert sind.

Weitere Informationen finden Sie unter Datenschutz | Solventum Deutschland.

10.3 Recovery Time Objective (RTO) und Recovery Point Objectives (RPO)

Recovery Time Objective (RTO), also die angestrebte Wiederherstellungszeit bei einem IT-Ausfall und die **Recovery Point Objectives (RPO)**, die definierte Zeitspanne ab dem Datenwiederherstellungspunkt, werden entsprechend der nachfolgenden Standards definiert:

- Software die als End-Anwendung (FD, FFT-Editor, Flex) direkt durch ärztliches oder pflegerisches Personal verwendet wird: Diese wird als höchst kritische Komponente mit dem größten Einfluss auf Kunden und Patienten angesehen. Angemessene RTOs und RPOs wurden für diese Anwendungen definiert: 30 Minuten für die Wiederherstellungszeit und 0 Minuten für den Datenwiederherstellungspunkt.
- Software-Systeme (z.B. Prozesse für die Online-Spracherkennung und das Profil-Training) die nicht durch den End-Anwender direkt verwendet werden, aber für eine kontinuierliche Arbeit einen wesentlichen Bestandteil darstellen, haben per Definition eine 24 Stunden Wiederherstellungszeit und einen Datenwiederherstellungspunkt von unter 24 Stunden.
- Anwendungen (z.B. Support-Datenbank, Nutzer-Management) die nicht direkt mit der End-Anwendung in Verbindung stehen, also eine wichtige aber keine kritische Rolle spielen, werden per Definition mit einer 1-Wöchigen RTO und unter 24 Stunden RPO gehandhabt.

Das Design von unseren Produkten zur Spracherkennung- und dem Sprachverstehen ist auf höchste Erreichbarkeit und größtmögliche Robustheit durch Load-Balancing, Multi-Server und Standby-Datenbanken ausgerichtet. Lokal installierte Clients funktionieren durch den Offline-Modus ohne Unterbrechung und übernehmen den aktuellen Stand umgehend, sobald die Cloud-Verbindung wieder verfügbar ist. Backup-Pläne und Wiederherstellungsprozeduren sind ein elementarer Bestandteil von unserem Service.

Solventum stellt ein Response Team mit der Aufgabe zur Verfügung, sofort bei einem Ausfall die Organisation, den Support und alle in Verbindung stehenden Aktivitäten zu koordinieren. Das Response Team soll schnell und effektiv auf unvorhergesehene Zwischenfälle reagieren, welche die Produktivität und Aktivitäten von Solventum oder unserer Kunden einschränken. Dabei soll der finanzielle und operative Einfluss so gering wie möglich gehalten werden. Das Team ist autorisiert alle notwendigen Schritte zu unternehmen, die zur Lösung des Zwischenfalls notwendig sind.

Der Offline-Modus, bei welchem einige Features eingeschränkt funktionieren, stellt sicher, dass unsere Kunden stets weiterarbeiten können. Dabei konnten wir aus den vergangenen Jahren eine Erreichbarkeit unserer Server von 99,8% feststellen.
Als Einschränkung wird angesehen, dass die Echtzeithinweise (CDI Engage Nudges) für die Offline-Zeit nicht verfügbar sind.

11 Releases & Updates

Releases werden auf monatlicher Basis durchgeführt. Über ein Update und die entsprechenden neuen Funktionen wird die IT-Abteilung vorab per E-Mail informiert. Diese monatlichen Releases können beispielsweise Fehlerbehebungen und/oder Funktionalitätserweiterungen sein.

Updates werden unterschieden in:

- Minor Updates – diese dienen der fortwährenden Weiterentwicklung der Sprachengine sowie Bugfixes
- Major Updates – enthalten Neuentwicklungen und Bugfixes

Die Verteilung kann automatisiert per Skript auf die Clients erfolgen.

Minor Updates werden bei Ihren Geräten automatisch eingespielt. Nur so können wir sicherstellen, dass die Spracherkennungsrate die höchstmögliche ist.

Bei Major Updates entscheiden Sie, wann die neuesten Updates bei Ihren Geräten aktiviert werden, damit ihre Clients reibungslos und sicher funktionieren. Major Releases wie eine neue Version der Software werden in der Regel alle 6-9 Monate durchgeführt. Auch hierüber wird die zentrale IT-Abteilung per E-Mail vorab informiert.

Wenn Sie ein Update ausführen, erhalten Sie die neuesten Korrekturen und Sicherheitsverbesserungen, damit Ihr Gerät effizient arbeitet und stabil bleibt.

Die Software Release Struktur von Solventum sieht typischerweise wie folgt aus:

- VV.PP.XX (Beispiel: Fluency Direct™ 01.05.00)
- VV = Version der Software
- PP = Point release der Software
- XX = Patch release der Software

Solventum empfiehlt grundsätzlich die Verwendung der neuesten Version der Solventum Produkte.

12 Historie

Version	Datum	Autor	Änderung
1.0	10.08.2021	Andreas Kassner	Initiale Erstellung
1.1	02.09.2021	Anne Machura	Ergänzung um weitere Adressen für Remote Recognition
1.2	21.10.2021	Anne Machura	Anmerkung zu AWS Application Load Balancers hinzugefügt
1.3	24.03.2022	Leonie Schmitz	Releases & Updates hinzugefügt
1.5	21.08.2022	Andreas Kassner	Beschreibung Updates überarbeitet Zertifizierungsprozess ergänzt
1.5.1	19.01.2023	Raphael Graf	Erweiterung der Synchronisation der Benutzerautorisierung mit LDAP um die FD-Web-API
1.6	30.01.2023	Raphael Graf	Erweiterung Kapitel 6.3 (RTP und RPO)
1.7	15.02.2023	Andreas Kassner	Proxy-Server ergänzt
1.8	28.08.2023	Anne Machura	Überarbeitung Layout
1.9	23.11.2023	Anne Machura	IP-Adressen von AMCC zu Merlin geändert
2.0	10.05.2024	Anne Machura	Anpassung an Solventum-Design
3.0	29.10.2024	Anne Machura	Inhaltliche Anpassungen
3.2	12.06.2025	Markus Lierse	Anpassung Barrierefreiheit
3.3	13.10.2025	Anne Breuer/Thomas Bruckmann	Anpassung von Formuliereungen; Ergänzungen von Komponentendiagrammen