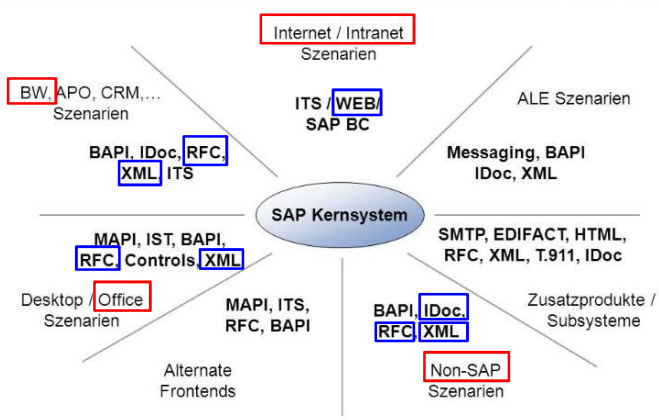
1. Hintergrund

Ein SAP-System besitzt eine Vielzahl von Schnittstellen, um beispielsweise den Datenaustausch zwischen SAP-Systemen oder aber auch zwischen einem SAP-System und einem Non-SAP-System zu ermöglichen.

Mitunter haben Schnittstellen für die ordnungsgemäße Durchführung von Geschäftsprozessen eine sehr große Bedeutung. So werden beispielsweise Informationen aus der Zeitwirtschaft für die Durchführung der Lohn- und Gehaltsabrechnung in SAP oder Informationen aus einem angebundenen proprietären (Non-SAP-) Warenwirtschaftssystem zur Bewertung des Umlaufvermögens benötigt.

Daneben kann auch die Wartung bzw. die Erbringung von externen Beratungs- und Unterstützungsleistungen über eine Schnittstelle zum SAP-System erfolgen.

Die nachfolgende Darstellung 1 ordnet exemplarisch einzelne Schnittstellen –Formate (z.B. Web, IDoc, XML, RFC, etc.) möglichen „Zugriffs-Szenarien“ (z.B. Zugriff über Internet, (SAP-) Business Warehouse, MS Office, Non-SAP-Systeme, etc.) zu.[1]



Darstellung 1

Die wichtigsten Schnittstellen eines SAP-Systems sind:

- Manuelle Schnittstelle,
- IDocs,
- Remote Function Calls (RFC),
- XML,
- Business API (BAPI),
- SAP Java Connector (JCo),
- SAP Exchange Infrastructure (SAP XI).

Aufgrund der **Bedeutung** der Schnittstellen für den **ordnungsgemäßen Betrieb** eines SAP-Systems und aus Gründen der **Übersicht** sind die gewährten System-Zugriffe zunächst **konzeptionell** zu planen. Die mit der Erstellung eines SAP-Schnittstellen-Konzepts generierte **Dokumentation** ist von den **Verantwortlichen** aktuell zu halten und regelmäßig auf **Richtigkeit** und **Vollständigkeit** zu **überprüfen**.

Nicht dokumentierte oder **obsolete Schnittstellen** stellen mitunter ein erhebliches **Sicherheitsrisiko** für ein SAP-System dar. Veraltete und inkompatible Schnittstellen können zu empfindlichen **Störungen** im Betriebsablauf führen.

Eine aktuelle und vollständige **Schnittstellendokumentation** ist darüber hinaus **Grundvoraussetzung** für

- eine effiziente und effektive Schnittstellenüberwachung,
- die Planung und Umsetzung von Änderungen[2],
- die Erfüllung datenschutzrechtlicher Anforderungen.

[1] Die Darstellung erhebt keinen Anspruch auf Vollständigkeit.

[2] Zum Beispiel im Rahmen von technischen oder betriebswirtschaftlichen Transformationsprojekten

2. Geltungsbereich (Rev.)

Die im Zusammenhang mit dem SAP-Schnittstellen-Konzept nachfolgend dargestellten Soll-Vorgaben sind grundsätzlich für alle Prüfungen der SAP-Schnittstellen in der Diehl-Gruppe – ergänzend zu den bereits vorhandenen Schnittstellen-Vorgaben - heranzuziehen.

3. Definitionen

Application-Link-Enabling-Schnittstelle (ALE)	Die Application-Link-Enabling-Schnittstelle (ALE) wird als Kommunikationsmechanismus zur Integration von Geschäftsprozessen über mehrere SAP Systeme oder andere externe Systeme hinweg genutzt. Über die Schnittstelle werden Geschäftsdaten und Systemdaten (z. B. beim Einsatz der Zentralen Benutzerverwaltung) zwischen Sender- und Empfänger-System transportiert. Die Verarbeitung erfolgt in den Empfänger-Systemen automatisiert. Daher muss die ALE-Schnittstelle abgesichert werden. Dabei ist Folgendes zu beachten:
Batch-Input	Batch-Input ist eine der wesentlichen Arten, auf die Daten in das SAP-System übertragen werden. Batch-Input wird für Massendatenübernahmen und nicht für fast Realtime-Datenübernahmen verwendet.
Business Application Programming Interface (BAPI)	BAPIs (Business Application Programming Interface) sind SAP-Standard-Schnittstellen. Sie spielen eine wesentliche Rolle bei der technischen Integration und den betriebswirtschaftlichen Datenaustausch zwischen SAP-Komponenten untereinander und zwischen SAP- und Nicht-SAP-Komponenten.
GUI	Mit der GUI-Schnittstelle (Graphical User Interface) zu R/3 können Sie ein Client-Programm schreiben, das auf den Datenstrom zugreift, der zwischen der R/3-Anwendungsserver und seinem SAPgui ausgetauscht wird. Mit der GUI-Schnittstelle kann Ihr externes Client-Programm eine Alternativschnittstelle zum Standard-SAPgui anbieten. Diese Alternativschnittstelle kann entweder grafisch oder nicht grafisch sein (z.B. sprachgesteuert oder auf Web-Basis). Die Programmierung über die GUI-Schnittstelle ermöglicht es Ihrem Client-Programm außerdem, einen Benutzerdialog mit SAPgui-Bildern zu überwachen oder aufzuzeichnen.

IDocs	IDoc steht für Intermediate Document und dient als Schnittstelle für den Nachrichtenaustausch zwischen SAP-Systemen als auch von SAP-Systemen und Fremdsystemen. IDocs beinhalten Verwaltungsinformationen für die technische Verarbeitung sowie die eigentlichen Daten der Anwendung in den sogenannten Segmenten. Segmente bestehen aus Segmentfeldern als kleinsten Sinneinheiten des IDocs, vergleichbar etwa mit den Datenelementen des EDIFACT-Standards.
IDoc-Schnittstelle	Über die IDoc-Schnittstelle werden betriebswirtschaftliche Daten mit einem Fremdsystem ausgetauscht. Die IDoc-Schnittstelle besteht aus der Definition einer Datenstruktur und einer Verarbeitungslogik für diese Datenstruktur. Die Datenstruktur ist das IDoc. Es ist das Austauschformat, auf das sich die kommunizierenden Systeme einigen. Mit IDocs können Sie eine Ausnahmebehandlung innerhalb des SAP-Systems über SAP Business Workflow definieren, ohne dass die Daten bereits als SAP-Anwendungsbeleg vorliegen müssen
Remote Function Call (RFC)	Der Remote Function Call (RFC) Mechanismus ist für den ABAP -Stack die primäre Kommunikationsschnittstelle für die System-zu-System-Kommunikation. Auch der Java-Stack unterstützt die RFC-Kommunikation über den Java Connector (JCo).
SAP Exchange Infrastructure (SAP XI)	Mit der Exchange Infrastructure, kurz SAP NetWeaver XI, können systemübergreifende Geschäftsprozesse realisiert werden. Dabei können Systeme unterschiedlicher Hersteller (nicht-SAP und SAP) in unterschiedlichen Versionen und implementiert in unterschiedlichen Programmiersprachen (Java, ABAP, usw.) miteinander verbunden werden.
SAP Java Connector (JCo)	Der SAP Java Connector (SAP JCo) ist eine Middleware-Komponente, die die Entwicklung von SAP-fähigen Komponenten und Anwendungen in Java ermöglicht. SAP JCo unterstützt die Kommunikation mit dem SAP Server in beiden Richtungen: inbound (Java ruft ABAP) und outbound calls (ABAP ruft Java).
XML	Die erweiterbare Auszeichnungssprache (englisch Extensible Markup Language), abgekürzt XML, ist

eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten im Format einer Textdatei, die sowohl von Menschen als auch von Maschinen lesbar ist.

4. Zielsetzung

Mit dem Erstellen eines **SAP-Schnittstellen-Konzepts** sind grundsätzlich folgende **Zielsetzungen** verbunden:

- Abbildung von einschlägigen Rechtsnormen und unternehmensinternen Regelungen auf die technischen Schutzmöglichkeiten innerhalb eines SAP-Systems,
- (Vorab-) Festlegung von Rahmenbedingungen,3
- Berücksichtigung und Einhaltung von unternehmensinternen Funktionstrennungen, gesetzlichen Anforderungen und IKS-Vorgaben,
- Schaffung von Transparenz,
- Erleichterung der Administration,
- Verbesserung der Nachvollzieh- und Kontrollierbarkeit.[4]

5. Normative Anforderungsgrundlagen

1. GoBS, GDPdU (bis 2014),
2. GoBD (ab 2014),
3. HGB, KonTraG,
4. Prüfungsstandard des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW, PS 330),
5. Anforderungen aus der „Datenschutzgrundverordnung“ (DSGVO, ab 25. Mai 2018),
6. Hier: insbesondere Art. 5 Abs. 1f), Art. 24 und Art. 32.
7. Datenschutzleitfäden der Deutschsprachige SAP® Anwender-gruppe (DSAG) e. V,
8. Prüfleitfäden der Deutschsprachige SAP® Anwender-gruppe (DSAG) e. V.

6. Verantwortlichkeiten

Die Verantwortung für die **Initiierung** eines SAP-Schnittstellen-Konzepts liegt zunächst bei den **gesetzlichen Vertretern** der Unternehmenseinheit. Die konkrete **Erstellung** und **Ausprägung** eines SAP-Schnittstellen-Konzepts erfolgt regelmäßig durch die **IT-Sicherheitsbeauftragten** bzw. durch den **IT-Leiter**.

Die Verantwortung für die **Umsetzung** des SAP-Schnittstellen-Konzepts liegt regelmäßig bei dem zuständigen (System-) **Administrator** bzw. dem **IT-Leiter**.

Die konkreten Verantwortlichkeiten sind mit den eineindeutigen Funktionsnamen in dem Konzept aufzuführen.

[3] Vorab festgelegte Rahmenbedingungen – wie z.B. Vermeidung von Funktionstrennungskonflikten, Trennung von Bewegungs- und Stammdatenpflege - sind innerhalb des Berechtigungskonzeptes einzuhalten. Die festgelegten Rahmenbedingungen definieren das Berechtigungssystem, bevor die Systemanpassung durchgeführt und das System produktiv gesetzt wird.

[4] Insbesondere im Zusammenhang mit dem Transparenzgebot des Art.5 Abs. 1a) DSGVO sowie mit dem Grundsatz der Zweckbindung in Art. 5 Abs. 1b) DSGVO.

7. Mindestanforderungen

7.1 Vorgabe ist vorhanden

- Aktuelle Übersichten der vorhandenen Schnittstellen liegen in schriftlicher Form unter Berücksichtigung von rechnungsrelevanten und datenschutzkonformen Anforderungen vor. Es gibt eine Vorgabe zur Dokumentation der ordnungsgemäßen Schnittstellenverarbeitung sowie deren Aufbewahrung

Hinweis I

Die Anforderung, ein SAP-Schnittstellen-Konzept zu erstellen, erstreckt sich nicht nur auf ein produktives SAP-Systems bzw. auf Produktiv-Mandanten. Vielmehr sind für **alle** eingesetzten SAP-Systeme, das heißt einschließlich der Entwicklungs- und Qualitätssicherungssysteme mit sämtlichen dort angelegten Mandanten zu berücksichtigen.

Hinweis II

Grundsätzlich sind für alle in einer Unternehmenseinheit eingesetzten DV-Systeme (einschließlich der Non-SAP-Systeme) die vorhandenen Schnittstellen ausreichend zu dokumentieren.

7.2 Formale Kriterien werden erfüllt

Das Berechtigungskonzept erfüllt folgende **formalen Anforderungen** bzw. **Dokumentationsstandards**:

- **Schriftform**: Das Schnittstellen-Konzept liegt in Schriftform vor.
- **Freigabe**: Das Schnittstellen-Konzept ist von den Verantwortlichen freigegeben.
- **Aktualität**: Das Schnittstellen-Konzept ist aktuell.
- **Kommunikation**: Das Schnittstellen-Konzept wird an die relevanten Stellen kommuniziert.
- **Vollständigkeit**: Das Konzept umfasst alle Im- und Export-Schnittstellen.

Das schriftliche **SAP-Schnittstellen-Konzept** muss derart verfasst sein, dass es

- verständlich, zuverlässig, nachvollziehbar, administrierbar, umsetzbar sowie überprüfbar und
- „ordnungsgemäß“ gemäß den zugrundeliegenden rechtlichen Normen ist. Die Ordnungsmäßigkeit ist gegeben, wenn die
  - Einhaltung gesetzlicher Anforderungen[5],
  - Gewährleistung der – teilweise gesetzlich geforderten – Nachvollziehbarkeit,
  - Gewährleistung der Datenintegrität,
  - Gewährleistung der Überprüfbarkeit der Wirksamkeit von Datenschutzkontrollmaßnahmen, frühzeitige Erkennung und Beseitigung von potenziellen Schwachstellen, sowie das
  - Möglichkeit, Verstöße gegen Sicherheitsvorgaben zu erkennen,

  gegeben ist.

[5] Abbildung von einschlägigen Rechtsnormen und unternehmensinternen Regelungen auf die technischen Schutzmöglichkeiten innerhalb eines SAP-Systems.

7.3 Inhaltliche Vorgaben werden erfüllt

- **Schnittstellenübersicht**
  - Graphische Darstellung der Schnittstellen
  - Auflistung der Schnittstellen (in Listenform)

Hinweis:
Berücksichtigung **aller** im Einsatz befindlicher sowohl **interner als auch externer Im- und Export-schnittstellen**.

- **Beschreibung aller** in der Schnittstellenübersicht aufgeführten **Schnittstellen**
  - Bezeichnung / Name der Schnittstelle
  - Zweck der Schnittstelle
  - Verantwortlicher
  - Datenarten- und Datenkategorien die Übertragen werden (§ 4e BDSG, Stichwort “Beschreibung der Daten oder Datenkategorien“)
  - Schnittstelleninformationen wie
    - Sender- und Empfängersystem
    - Richtung der Übertragung
    - Übertragungsart (ALE, Datei, RFC-Aufruf, ...)
    - Übertragungsweg (BAPI, IDOC, ...)
    - Häufigkeit der Übertragung
    - Verschlüsselung
  - Schnittstellenverarbeitung
    - Datenübernahme
    - PC -Verarbeitung
    - Kommunikationsschnittstellen
    - SAP -Automation
    - Job-Auftragsverfahren und –Dokumentation
  - Systemschnittstellen
    - Batch-Input
    - RFC , ALE, BAPI
    - PC -Download
    - ABAP -Listviewer
    - Risiken und zu ergreifende Maßnahmen zur Absicherung

Alle Schnittstellen sind im Falle der Übermittlung / Weitergabe entsprechend den **datenschutzrechtlichen Anforderungen** zu dokumentieren. Aus dem Schnittstellennachweis geht eine vollständige Übersicht über die Schnittstellen und entsprechenden Übertragungswegen hervor. Daraus sollten Nutzen und Zecke der Nutzung ersichtlich sein.

- **Beschreibung der Kontroll- und Abstimmverfahren**
  - Sicherstellen der Funktionalität und Integrität
  - Vollständige und fehlerfreie Verarbeitung
  - Schutz vor Manipulation während der Datenübertragung
  - Schutz vor Einsichtnahme in personenbezogene Daten
  - Schutz vor unkontrollierter Weitergabe von Daten
  - Datenschutzkonformer Umgang (§ 4g BDSG, Stichwort “Überwachung der ordnungsgemäßen Anwendung”)
  - Festlegung von Verfahrensweisen bei Auftreten von Fehlern

- **Datenschutzrechtliche Anforderungen**
  - Werden SAP-Daten mit Personenbezug[6] mittels einer Schnittstelle in ein anderes IT-System exportiert, können die für das SAP-System vormals festgelegten datenschutzrechtlich relevanten Sachverhalte wie z.B. die Zweckbindung, Löschfristen oder andere datenschutzrechtliche Anforderungen unter Umständen für das „Zielsystem“ nicht ohne weiteres übernommen werden.

    Bei jeder Form der Schnittstellenverarbeitung liegen die damit verbundenen Risiken vorrangig in
    - o der unvollständigen bzw. fehlerhaften Verarbeitung,
    - o der möglichen Manipulation während der Datenübertragung bzw. des Programmablaufs,
    - o der unzulässigen Einsichtnahme in personenbezogene Daten,
    - o der unkontrollierten Weitergabe der exportierten Daten.
  - Diesen Risiken ist durch geeignete Maßnahmen zu begegnen. Als organisatorische Maßnahmen sind daher zu beschreiben, wie
    - o alle Schnittstellendateien und die genutzten Verfahren entsprechend den Anforderungen des BDSG bzw. der DSGVO dokumentiert werden[7],
    - o die Dokumentation der vorhandenen Schnittstellen mit dem entsprechenden Verfahrensverzeichnis bzw. Verarbeitungsverzeichnis zu verbinden ist,
  - Die zur Risikominimierung eingesetzten technischen Maßnahmen sind im SAP-System geeignete interne Kontrollstufen zuzuordnen. Dabei ist jede einzelne Kontrollstufe hinsichtlich ihrer ordnungsgemäßen Einstellung, insbesondere auch in dem Zusammenspiel mit einzelnen Kontrollen, regelmäßig zu überwachen.

[6] Schließt auch die „Personen beziehbaren“ Daten mit ein.

[7] Gemäß § 4g BDSG, Stichwort „Überwachung der ordnungsgemäßen Anwendung“ und gemäß § 4e BDSG, Stichwort „Beschreibung der Daten oder Datenkategorien“.

8. Reports, Tabellen und Transaktionen zu SAP-Berechtigungen

Werkzeug	Beschreibung
Tabelle RFCDES	Tabelle der RFC-Verbindungen
Transaktion SM59	Verwalten von RFC-Verbindungen
Transaktion SM35	Batch-Input-Mappen abspielen
Transaktion WE02	IDoc anzeigen
Transaktion WE05	IDoc-Liste
Transaktion SM54	CPIC-Destination
Transaktion BD64	Verteilungsmodellpflege
Transaktion BD87	Statusmonitor für ALE-Nachrichten
Transaktion SALE	ALE-Customizing anzeigen

♦ ♦ ♦