



## **Leitfaden zur Sicherheit**

### **SAP® Business ByDesign FP3.0**

#### **Zielgruppe**

- Berater
- Administratoren
- Sonstige

Öffentlich  
Dokumentversion 1.0 – 01.08.11

© 2011 SAP AG. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung der SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Die von SAP AG oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten.

Microsoft, Windows, Excel, Outlook und PowerPoint sind eingetragene Marken der Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli und Informix sind Marken oder eingetragene Marken der IBM Corporation.

Linux ist die eingetragene Marke von Linus Torvalds in den USA und anderen Ländern.

Adobe, das Adobe-Logo, Acrobat, PostScript und Reader sind Marken oder eingetragene Marken von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Oracle und Java sind eingetragene Marken von Oracle und/oder ihrer Tochtergesellschaften.

UNIX, X/Open, OSF/1 und Motif sind eingetragene Marken von Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame und MultiWin sind Marken oder eingetragene Marken von Citrix Systems, Inc.

HTML, XML, XHTML und W3C sind Marken oder eingetragene Marken von W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer und weitere im Text erwähnte SAP-Produkte und Dienstleistungen sowie die entsprechenden Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und anderen Ländern.

Business Objects und das Business-Objects-Logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius und andere im Text erwähnte Business-Objects-Produkte und Dienstleistungen sowie die

entsprechenden Logos sind Marken oder eingetragene Marken von Business Objects Software Ltd. Business Objects ist ein Unternehmen der SAP AG.

Sybase und Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere und andere im Text erwähnte Sybase-Projekte und -Dienstleistungen sowie die entsprechenden Logos sind Marken oder eingetragene Marken von Sybase, Inc. Sybase ist ein Unternehmen der SAP AG.

Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen. Die Angaben im Text sind unverbindlich und dienen lediglich Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die vorliegenden Unterlagen werden von der SAP AG und ihren Konzernunternehmen („SAP-Konzern“) bereitgestellt und dienen ausschließlich Informationszwecken. Der SAP-Konzern übernimmt keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Der SAP-Konzern steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

## Bedingungen für inbegriffene Open Source Software

Diese SAP-Software umfasst auch die im Folgenden aufgelisteten Open-Source-Software-Produkte von Fremdanbietern. Beachten Sie, dass für diese Fremdprodukte die folgenden besonderen Bestimmungen und Bedingungen gelten.

1. Diese Software wurde unter Verwendung von ANTLR entwickelt.
2. gSOAP

Bei einem Teil der in dieses Produkt integrierten Software handelt es sich um gSOAP-Software. Für Software-Teile, die unter Verwendung von gSOAP angelegt wurden, gilt Folgendes: Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. Alle Rechte vorbehalten. DIE IN DIESEM PRODUKT ENTHALTENE SOFTWARE WURDE ZUM TEIL VON GENIVIA BEREITGESTELLT, JEDWEDE GEWÄHRLEISTUNG, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTTAUGLICHKEIT SOWIE DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK WIRD AUSGESCHLOSSEN. DER AUTOR ÜBERNIMMT UNTER KEINEN UMSTÄNDEN DIE VERTRAGLICHE, DELIKTISCHE ODER VERSCHULDENSUNABHÄNGIGE HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE ODER BESONDERE SCHÄDEN, STRAFSCHADENERSATZ BEGRÜNDENDE SCHÄDEN SOWIE FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE ERSATZBESCHAFFUNG VON GÜTERN ODER DIENSTLEISTUNGEN, DEN VERLUST DES GEBRAUCHSWERTS ODER VON DATEN, ENTGANENEM GEWINN ODER BETRIEBSUNTERBRECHUNG), DIE IM ZUSAMMENHANG MIT DER BENUTZUNG DIESER SOFTWARE STEHEN, SELBST WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

3. SAP-Lizenzvereinbarung für STLport zwischen der SAP Aktiengesellschaft Systems, Applications, Products in Data Processing Neurtottstrasse 16 69190 Walldorf, Deutschland (nachfolgend: SAP) und Ihnen (nachfolgend: Kunde)

a) Vertragsgegenstand

A) SAP stellt dem Kunden eine nicht exklusive, nicht übertragbare und gebührenfreie Lizenz zur Verwendung der STLport.org-C++-

Bibliothek (STLport) sowie deren zugehöriger Dokumentation kostenfrei zur Verfügung.

B) Durch das Herunterladen, Verwenden oder Kopieren von STLport oder Teilen davon stimmt der Kunde zu, sich an die Gesetze zum Schutz des geistigen Eigentums sowie alle Geschäftsbedingungen dieser Vereinbarung zu halten.

C) Der Kunde kann mit STLport kompilierte Binärdateien (ob unverändert oder modifiziert) ohne Lizenzgebühren oder Einschränkungen vertreiben.

D) Der Kunde muss die folgenden Urheberrechts- und Erlaubnishinweise für STLport-Quellen und die zugehörige Dokumentation unverändert beibehalten:

Copyright 2001 SAP AG

E) Der Kunde darf unveränderte oder modifizierte STLport-Quellen vertreiben, sofern:

o die in dem oben stehenden Erlaubnishinweis genannten Bedingungen erfüllt sind;

o die folgenden Urheberrechtshinweise beibehalten werden und die in den begleitenden Erlaubnishinweisen genannten Bedingungen erfüllt sind:

**Copyright 1994 Hewlett-Packard Company**

**Copyright 1996,97 Silicon Graphics Computer Systems Inc.**

**Copyright 1997 Moscow Center for SPARC Technology.**

**Copyright 1999,2000 Boris Fomitchev Copyright 2001 SAP AG**

Hiermit wird die Erlaubnis erteilt, diese Software und ihre Dokumentation kostenfrei zu verwenden, zu kopieren, zu modifizieren, zu vertreiben und zu verkaufen, vorausgesetzt, dass der obige Urheberrechtshinweis in allen Kopien der Software enthalten ist und dass sowohl der Urheberrechtshinweis als auch diese Erlaubnis in der dazugehörigen Dokumentation erscheinen. Hewlett-Packard Company gibt keine Gewährleistung hinsichtlich der Eignung dieser Software für irgendeinen Zweck.

Sie wird „wie besehen“ bereitgestellt, ohne ausdrückliche oder stillschweigende Gewährleistung.

Hiermit wird die Erlaubnis erteilt, diese Software und ihre Dokumentation kostenfrei zu verwenden, zu kopieren, zu modifizieren, zu vertreiben und zu verkaufen, vorausgesetzt, dass der obige Urheberrechtshinweis in allen Kopien der Software enthalten ist

und dass sowohl der Urheberrechtshinweis als auch diese Erlaubnis in der dazugehörigen Dokumentation erscheinen. Silicon Graphics gibt keine Gewährleistung hinsichtlich der Eignung dieser Software für irgendeinen Zweck. Sie wird „wie besehen“ bereitgestellt, ohne ausdrückliche oder stillschweigende Gewährleistung.

Hiermit wird die Erlaubnis erteilt, diese Software und ihre Dokumentation kostenfrei zu verwenden, zu kopieren, zu modifizieren, zu vertreiben und zu verkaufen, vorausgesetzt, dass der obige Urheberrechtshinweis in allen Kopien der Software enthalten ist und dass sowohl der Urheberrechtshinweis als auch diese Erlaubnis in der dazugehörigen Dokumentation erscheinen. Moscow Center for SPARC gibt keine Gewährleistung hinsichtlich der Eignung dieser Software für irgendeinen Zweck. Sie wird „wie besehen“ bereitgestellt, ohne ausdrückliche oder stillschweigende Gewährleistung.

Boris Fomitchev gibt keine Gewährleistung hinsichtlich der Eignung dieser Software für irgendeinen Zweck. Dieses Material wird „wie besehen“ bereitgestellt, ohne ausdrückliche oder stillschweigende Gewährleistung.

Die Nutzung erfolgt auf eigenes Risiko. Hiermit wird die Erlaubnis erteilt, diese Software kostenfrei für jeden Zweck zu nutzen oder zu kopieren, sofern die oben stehenden Hinweise in allen Kopien beibehalten werden.

Es wird die Erlaubnis erteilt, den Code zu modifizieren und modifizierten Code zu vertreiben, sofern die oben stehenden Hinweise beibehalten werden und der oben stehende Urheberrechtshinweis mit einem Zusatz versehen wird, dass der Code modifiziert wurde.

Hiermit wird die Erlaubnis erteilt, diese Software und ihre Dokumentation kostenfrei zu verwenden, zu kopieren, zu modifizieren, zu vertreiben und zu verkaufen, vorausgesetzt, dass der obige Urheberrechtshinweis in allen Kopien der Software enthalten ist und dass sowohl der Urheberrechtshinweis als auch diese Erlaubnis in der dazugehörigen Dokumentation erscheinen. SAP gibt keine Gewährleistung hinsichtlich der Eignung dieser Software für irgendeinen Zweck. Sie wird gemäß der mit dieser Kopie verteilten Lizenzvereinbarung mit beschränkter Gewährleistung und Haftung bereitgestellt.

SAP bietet diese Haftungs- und Gewährleistungspflichten ausschließlich für Kunden und nur mit Blick auf von SAP vorgenommene Modifikationen an.

b) Support und Wartung SAP stellt keine Software-Wartungsleistungen für STLport bereit. Die Software-Wartung von STLport ist daher nicht Teil dieser Vereinbarung.

Alle anderen Dienstleistungen werden zu den in der SAP-Preis- und Konditionenliste ausgewiesenen Dienstleistungssätzen abgerechnet und sind Gegenstand eines separaten Vertrags.

#### c) Haftungsausschluss

Da STLport dem Kunden leihweise und kostenfrei zur Verfügung gestellt wird, kann SAP nicht garantieren, dass STLport fehlerfrei, ohne Materialfehler oder für eine bestimmte Anwendung im Hinblick auf Rechte Dritter geeignet ist. Von SAP erstellte technische Daten, Verkaufsbroschüren, Werbetexte und Qualitätsbeschreibungen stellen keine Zusicherung besonderer Eigenschaften dar.

#### d) Haftungsbeschränkung

A) Gleich aus welchem Rechtsgrund haftet SAP nur dann für Schäden, einschließlich der Bedienung ohne Befugnis, wenn diese (i) nach dem Produkthaftungsgesetz gutgemacht werden können, (ii) durch Vorsatz oder grobe Fahrlässigkeit seitens SAP verursacht wurden oder (iii) aus dem Fehlen einer garantierten Eigenschaft resultieren.

B) Die Haftbarkeit von SAP für Schäden, die vorsätzlich oder grob fahrlässig von Mitarbeitern verursacht wurden, bei denen es sich weder um Betreuer noch um leitende Angestellte von SAP handelt, beschränkt sich insgesamt maximal auf den Umfang, der von SAP bei Vertragsabschluss mit Blick auf den Eintritt eines solchen Vorfalls vorausgesehen werden konnte (infolge der SAP zu diesem Zeitpunkt bekannten Umstände im Rahmen einer typischen Software-Weitergabe).

C) Im Falle des oben genannten Art. 4.2 haftet SAP nicht für indirekte Schäden und Folgeschäden, die sich aus einem Fehler oder entgangenem Gewinn ergeben.

D) SAP und der Kunde vereinbaren, dass das Ausmaß des typischen, vorhersehbaren Schadens unter keinen Umständen EUR 5.000 überschreiten darf.

E) Der Kunde verpflichtet sich, hinreichende Maßnahmen zum Schutz von Daten und Programmen zu ergreifen, insbesondere durch das Erstellen von Sicherungskopien in den von SAP empfohlenen Mindestabständen. SAP haftet nicht für den Verlust von Daten und deren Wiederherstellung, unbeschadet der übrigen Einschränkungen von Art. 4, wenn dieser Verlust durch Einhaltung der zuvor genannten Verpflichtung hätte vermieden werden können.

F) Der Ausschluss oder die Verjährung von Ansprüchen gemäß Art. 4 schließt Ansprüche gegen Mitarbeiter oder Betreuer von SAP ein.








4. Adobe Document Services Adobe, das Adobe-Logo, Acrobat, PostScript und Reader sind entweder eingetragene Marken oder Marken von Adobe Systems Incorporated in den USA und/oder

anderen Ländern. Informationen zur Drittanbietersoftware, die mit Adobe Document Services und Adobe LiveCycle Designer ausgeliefert wird, finden Sie im SAP-Hinweis 854621.

## Typografische Konventionen

Format	Beschreibung
<i>Beispieltext</i>	Wörter oder Zeichen, die von der Oberfläche zitiert werden. Dazu gehören Feldbezeichner, Bildtitel, Drucktastenbezeichner sowie Menünamen, Menüpfade und Menüeinträge. Verweise auf andere Dokumentationen.
<b>Beispieltext</b>	Hervorgehobene Wörter oder Ausdrücke im Fließtext, Titel von Grafiken und Tabellen.
BEISPIELTEXT	Technische Namen von Systemobjekten. Dazu gehören Reportnamen, Programmnamen, Transaktionscodes, Tabellennamen und Schlüsselbegriffe einer Programmiersprache, die von Fließtext umrahmt sind, z. B. SELECT und INCLUDE.
Beispieltext	Ausgabe auf der Oberfläche. Dazu gehören Datei- und Verzeichnisnamen und ihre Pfade, Meldungen, Namen von Variablen und Parametern, Quelltext und Namen von Installations-, Upgrade- und Datenbankwerkzeugen.
<b>Beispieltext</b>	Exakte Benutzereingabe. Dazu gehören Wörter oder Zeichen, die Sie genau so in das System eingeben, wie es in der Dokumentation angegeben ist.
<Beispieltext>	Variable Benutzereingabe. Die Wörter und Zeichen in spitzen Klammern müssen Sie durch entsprechende Eingaben ersetzen, bevor Sie sie in das System eingeben.
BEISPIELTEXT	Tasten auf der Tastatur, wie z. B. die Funktionstaste F2 oder die ENTER-Taste

## Symbole

Symbol	Bedeutung
	Achtung
	Beispiel
	Notiz
	Empfehlung
	Syntax

In der SAP-Dokumentation werden weitere Symbole verwendet, die verdeutlichen, welche Art von Informationen ein Text enthält. Weitere Informationen finden Sie auf der Startseite jeder Version der *SAP-Bibliothek* unter *Hilfe zur Hilfe* → *Allgemeine Informationsklassen und Informationsklassen für das Business Information Warehouse*.

# Inhalt

Einführung.....	1
Warum ist Sicherheit notwendig? .....	1
Über dieses Dokument.....	1
Technische Systemlandschaft .....	3
Sicherer Systemzugang / Authentifizierung.....	5
Authentifizierung .....	5
Kennwortrichtlinie .....	5
Identitäts- und Zugriffsverwaltung .....	7
Berechtigung .....	7
Benutzerattribute .....	7
Zuordnung von Berechtigungen.....	8
Zugriffseinschränkung.....	8
Funktionstrennung .....	9
Benutzertypen .....	9
Standardbenutzer .....	9
Frontend-Sicherheit .....	11
Business-to-Business-Kommunikation .....	12
Sicherheit der Datenablage / Sicherheit des Rechenzentrums.....	13
Anlagenschutz und Datenintegrität .....	13
Redundante und ausfallsichere Stromversorgung.....	13
Eingeschränkter physischer Zugang.....	13
Kommunikationssicherheit .....	13
Netzwerksicherheit.....	13
Sonstige sicherheitsrelevante Informationen.....	15
Servicekomposition .....	15
URL-Mashup-Integration .....	15
HTML-Mashup-Integration .....	16
Karten-Mashup-Integration.....	16
Webdienstkomposition .....	17
Lokal installierte Komponenten.....	18
Sicherheitsprotokollierung und Nachverfolgung .....	20



## Einführung



Dieser Leitfaden ersetzt nicht die Lektüre des Administrationsleitfadens und des Lösungsbetriebsleitfadens, die für den Produktivbetrieb verfügbar sind.

### Warum ist Sicherheit notwendig?

Mit zunehmender Verwendung verteilter Systeme und des Internets beim Verwalten von Geschäftsdaten steigen auch die Anforderungen an die Sicherheit. Wenn Sie ein verteiltes System verwenden, müssen Sie sicherstellen, dass Ihre Daten und Prozesse Ihre Geschäftsanforderungen unterstützen, ohne unberechtigten Zugriff auf wichtige Informationen zu ermöglichen. Fehler der Benutzer, Nachlässigkeit oder Manipulationsversuche an Ihrem System dürfen keine Daten- oder Verarbeitungsverluste nach sich ziehen. Diese Sicherheitsanforderungen gelten ebenso für SAP Business ByDesign. Wir stellen Ihnen diesen Sicherheitsleitfaden zur Verfügung, um Business ByDesign sicher zu machen.

### Über dieses Dokument

Der Sicherheitsleitfaden bietet einen Überblick über die sicherheitsrelevanten Informationen, die SAP Business ByDesign betreffen. SAP Business ByDesign setzt sich aus mehreren Anwendungen zusammen; daher enthält dieser Leitfaden einen Überblick über die Lösung in ihrer Gesamtheit.

#### Überblick über die Hauptabschnitte

Der Sicherheitsleitfaden besteht aus den folgenden Hauptabschnitten:

- Technische Systemlandschaft  
Dieser Abschnitt bietet einen Überblick über die technischen Komponenten und Kommunikationspfade, die von der SAP-Business-ByDesign-Anwendung verwendet werden.
- Sicherer Systemzugang / Authentifizierung  
Dieser Abschnitt bietet einen Überblick über den Systemzugang und das für SAP Business ByDesign geltende Authentifizierungskonzept.
- Benutzerverwaltung und -authentifizierung  
Dieser Abschnitt bietet einen Überblick über folgende Aspekte der Benutzerverwaltung und -authentifizierung:
  - für die Benutzerverwaltung empfohlene Werkzeuge
  - für die verschiedenen Features von SAP Business ByDesign erforderliche Benutzertypen
  - mit SAP Business ByDesign ausgelieferte Standardbenutzer
  - Überblick über die Benutzersynchronisationsstrategie, wenn mehrere Komponenten oder Produkte eingebunden sind
  - Überblick über die Integrationsmöglichkeiten in Single-Sign-On-Umgebungen
- Frontend-Sicherheit  
Dieser Abschnitt bietet einen Überblick über die von SAP Business ByDesign verwendeten Frontend- und Kommunikationspfade sowie die geltenden Sicherheitsmechanismen.
- Business-to-Business-Kommunikation  
Dieser Abschnitt stellt Sicherheitsinformationen bereit, die für gemeinsam mit SAP Business ByDesign verwendete Fremd- oder Zusatzanwendungen gelten.
- Sicherheit der Datenablage / Sicherheit des Rechenzentrums  
Dieser Abschnitt bietet einen Überblick über alle kritischen Daten, die von SAP Business ByDesign verwendet werden, sowie über die anzuwendenden Sicherheitsmechanismen.

## Einführung

- Sonstige sicherheitsrelevante Informationen

Dieser Abschnitt enthält Informationen zu Folgendem:

- Audits und Zertifizierung
  - Servicekomposition
  - Lokal installierte Komponenten
- Sicherheitsprotokollierung und Nachverfolgung
- Dieser Abschnitt bietet einen Überblick über die Trace- und Protokolldateien, die sicherheitsrelevante Informationen enthalten, damit Sie z. B. im Falle einer Sicherheitslücke Aktivitäten reproduzieren können.

## Technische Systemlandschaft

Bei SAP Business ByDesign handelt es sich um ein SaaS-Angebot (Software as a Service), das in der SAP Private Cloud ausgeführt wird.

Sie umfasst eine vollständige Enterprise Resource Planning (ERP) Suite, einschließlich Serverlandschaft und Systemwartung.

Da SAP Business ByDesign mit den Geschäftsdaten aus den Kernprozessen Ihres Unternehmens arbeitet, muss SAP höchste Anforderungen an die Sicherheit und Qualität erfüllen:

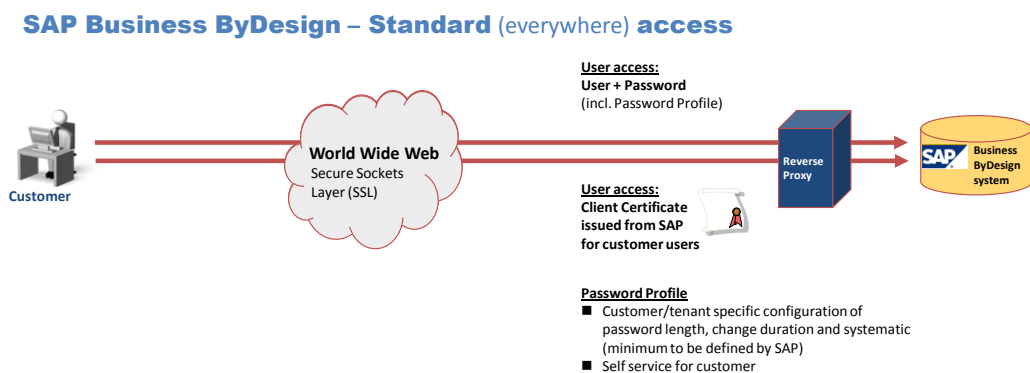
- Die Geschäftsdaten werden sicher in einem SAP-Rechenzentrum abgelegt.
- Kunden verwenden physische Hardwareressourcen gemeinsam, aber ihre Daten werden in Mandanten aufgeteilt.
- Benutzer, die auf die Geschäftsdaten zugreifen möchten, müssen sich authentifizieren, und ihre Identität muss unter Verwendung der Identitäts- und Zugriffsverwaltung verifiziert werden.
- Kundendaten gehören stets nur dem Kunden

Sie können wie folgt auf SAP Business ByDesign zugreifen:

- Desktop-Computer: browserbasierter Zugriff über das Internet aus dem Kundennetzwerk heraus
- Tragbare Computer
- Mobile Geräte

Branchenweit bewährte Verfahren („Best Practices“) und modernste offene kryptografische Standards sichern bzw. schützen die Kommunikation zwischen dem Gerät eines Kunden und der SAP-Business-By-Design-Systemlandschaft im SAP-Rechenzentrum.

Die folgende Grafik bietet einen Überblick über die technische Systemlandschaft für den Standardzugriff.



Um auf Ihr SAP-Business-ByDesign-System zuzugreifen, müssen Sie eine eindeutige, kundenspezifische URL eingeben.

Die Kommunikation durchläuft die Reverse-Proxy-Komponente (RP) im SAP-Rechenzentrum.

Das Reverse Proxy stellt den SAP Web Dispatcher dar, der von SAP entwickelt wurde und gewartet wird.

Durch die Verwendung des TLS/SSL-Internetstandards (Transport Layer Security/Secure Socket Layer) werden die Kommunikationskanäle gesichert, indem eine gegenseitige Authentifizierung erforderlich ist.

Die folgenden Authentifizierungsmechanismen werden unterstützt:

- Benutzername + Kennwort
- X.509-Client-Zertifikat

## **Technische Systemlandschaft**

Die Kommunikationskanäle zur Überwachung und Verwaltung von SAP-Business-ByDesign-Instanzen im SAP-Rechenzentrum-Netzwerk sind ebenfalls verschlüsselt und erfordern eine Authentifizierung.

Sie können Anhangsdateien in mehreren Anwendungsszenarios in SAP Business ByDesign hochladen, z. B. bei der Fakturierung oder der Datenmigration. Regelmäßig aktualisierte Antiviren-Software prüft die hochgeladenen Dateien auf Viren und andere Arten von Malware.

## Sicherer Systemzugang / Authentifizierung

### Authentifizierung

Jeder Benutzertyp muss sich für den regulären, browserbasierten Frontend-Zugriff sowie für die Business-to-Business-Kommunikation gegenüber SAP Business ByDesign authentifizieren.

SAP Business ByDesign unterstützt keinen anonymen Zugriff.

Die folgenden Authentifizierungsmechanismen werden unterstützt:

- Anmeldung mit Benutzername und Kennwort
- Anmeldung mit Client-Zertifikat (X.509)

Wenn in SAP Business ByDesign ein neuer Benutzer angelegt wird, z. B. bei der Einstellung eines neuen Mitarbeiters, werden ein Benutzername und ein Kennwort angelegt.

Die Benutzer melden sich in SAP Business ByDesign mit ihrem zugeordneten Benutzernamen und Kennwort an. Standardmäßig ist in Kundensystemen eine solide Kennwortrichtlinie auf Basis des SAP-Produktsicherheitsstandards vorkonfiguriert. Als Anwendungsexperte können Sie die Sicherheitsstufe erhöhen, indem Sie die SAP-Kennwortrichtlinie ändern.

Ein Benutzer kann ein Client-Zertifikat zur Authentifizierung verwenden; im Anmeldebild kann er das Ankreuzfeld zum Anfordern der Generierung eines Client-Zertifikats oder zur Zuordnung eines vorhandenen Client-Zertifikats markieren.

- Sie können Ihr Client-Zertifikat Ihrer Benutzerkennung zuordnen, wenn Sie bereits über ein geeignetes Client-Zertifikat von einer vertrauenswürdigen SAP Certification Authority verfügen.
- Sie können ein Client-Zertifikat von SAP Business ByDesign anfordern, wenn kein geeignetes Client-Zertifikat verfügbar ist. Das angeforderte Zertifikat wird dann von einer SAP Certification Authority bereitgestellt. Diese Anforderung können Sie auf jedem beliebigen Computer wiederholen, auf dem Sie SAP Business ByDesign verwenden. Eine Anmeldung im System mit mehreren Benutzern unter Verwendung desselben Zertifikats ist nicht möglich.

### Kennwortrichtlinie

Die Kennwortrichtlinie kann über den Kennwortrichtlinien-Editor bearbeitet werden. Sie können die Komplexität und Gültigkeit für alle Kennwörter entsprechend den Sicherheitsanforderungen Ihres Unternehmens ändern.

1. Rufen Sie in Ihrem SAP-Business-ByDesign-System das Work Center *Anwendungs- und Benutzerverwaltung* auf.
2. Wählen Sie die Sicht *Benutzer- und Zugriffsverwaltung*.
3. Wählen Sie *Sicherheitsrichtlinien*.
4. Wählen Sie die Untersicht *Sicherheitsrichtlinie bearbeiten*.

Daraufhin wird das folgende Bild angezeigt, in dem Sie die Ihren Anforderungen entsprechenden Angaben machen können:

The screenshot shows the SAP Security Policy configuration interface for the user 'S\_BUSINESS\_USER'. The interface includes a top navigation bar with 'SAP Business ByDesign', user 'Oliver Adams', and options for 'Personalize', 'Adapt', and 'Help'. The main title is 'Security Policy: S\_BUSINESS\_USER', with a close button. Below the title, it shows 'Changed On: 08/01/2011 08:20' and 'Changed By: SAP\_SYSTEM'. A toolbar contains buttons for 'Save and Close', 'Save', 'Close', 'New', and 'Reset'. A sidebar on the left has search and user icons. A vertical 'HELP CENTER' button is on the right. The main content area has a heading 'You can edit the rules of password complexity and validity.' followed by a 'General Information' section with fields for 'Name' (S\_BUSINESS\_USER) and 'Description' (Default Password Policy for Business Users). Below this are two sections: 'Complexity' and 'Validity', each with several numeric input fields and their units.

**Complexity**

Minimum Number of Characters:	8
Minimum Number of Changed Characters:	1
Minimum Number of Lowercase Letters:	1
Minimum Number of Uppercase Letters:	1
Minimum Number of Digits:	1
Minimum Number of Special Characters:	0

**Validity**

Password History:	5
Minimum Password Change Waiting Time:	1 Day(s)
Maximum Password Validity:	90 Day(s)
Unused Initial Password Validity:	30 Day(s)
Unused Productive Password Validity:	0 Day(s)

# Identitäts- und Zugriffsverwaltung

## Berechtigung

Als Anwendungsexperte können Sie in der Work-Center-Sicht *Benutzer- und Zugriffsverwaltung* die nachfolgend genannten Aufgaben ausführen.

- Benutzer durch das Sperren und Entsperrern verwalten
- Benutzern Zugriffsrechte für Work Center und Work-Center-Sichten zuordnen
- Benutzern den Lese- und Schreibzugriff auf spezielle Daten einschränken

## Benutzerattribute

In der Work-Center-Sicht *Benutzer- und Zugriffsverwaltung* können Sie benutzerspezifische Attribute anlegen und ändern. Dies umfasst z. B. die folgenden Attribute:

- Benutzerkennung
- Kennwort
- Sperrstatus
- Gültigkeit

SAP Business ByDesign Oliver Adams | Personalize | Adapt | Help | ⏻

**Business User: KJACOB** ✕

Technical ID: JACOBKATEMC2 Employee ID: MC2471 Location: NY01 E3.01-02  
 Department: MC42110 New York Office

Save and Close Save Close Edit Access Rights

Employee Data	User Data
Name: <a href="#">Jacob, Kate</a>	User ID: * KJACOB
Employee ID: MC2471	Technical ID: JACOBKATEMC2
E-Mail: <a href="mailto:kate.jacob@akron.com">kate.jacob@akron.com</a>	Valid From/To: 01/01/0001 / Unlimited
Phone: +1 (6227) 7-42720	Locked: <input type="checkbox"/>
Location: NY01 E3.01-02	Password Locked: <input type="checkbox"/>
Department: MC42110 New York Office	Security Policy: S_TEST_USER - View Details
Company: MC10000 Akron Heating Technologies INC.	Password: <input type="password"/>
Manager: <a href="#">Menson, Bob</a>	Confirm Password: <input type="password"/>
Internal Comment	Password Changed On: 07/18/2008
No note history exists	Language: English
	Decimal Notation: 1.234.567,89
	Date Format: DD.MM.YYYY
	Time Format: 24-Hour Time
	Time Zone: * (UTC-05:00) Eastern Time (New Yi

Application and User Man... Business User: K...

## Zuordnung von Berechtigungen

Sie können jedem Mitarbeiter, der in SAP Business ByDesign über eine Benutzerkennung verfügt, Berechtigungen zuordnen.

Ein Mitarbeiter wird einer Organisationseinheit im Organisationsmanagement zugeordnet.

Die zugeordnete Organisationseinheit bestimmt die Funktionen, die verwendet werden können.

Basierend auf diesen Funktionen werden Work Center und Work-Center-Sichten für die Benutzer vorgeschlagen. Sie können den Benutzern dann die vorgeschlagenen sowie zusätzliche Work Center und Work-Center-Sichten zuordnen.

SAP Business ByDesign prüft, ob die zugeordneten Sichten im Widerspruch zur Funktionstrennung stehen, wenn der Benutzer mehreren Sichten zugeordnet wurde.

Mithilfe der Funktionstrennung sollen das Missbrauchs- und Fehlerrisiko minimiert und das Unternehmensvermögen (wie Daten oder Bestände) geschützt werden.

Die Funktionstrennungsprüfung in der Work-Center-Untersicht *Anwender* der Work-Center-Sicht *Benutzer- und Zugriffsverwaltung* unterstützt Sie bei der Zuordnung konfliktfreier Zugriffsrechte. Im Falle von Konflikten stellt SAP Business ByDesign eine detaillierte Konfliktbeschreibung bereit und schlägt eine angemessene Lösung vor (siehe auch „Funktionstrennung“).

Einige Geschäftsprozesse erfordern, dass eine Sicht nur in Kombination mit einer oder mehreren anderen Sichten zugeordnet werden kann. Wenn Sie als Anwendungsexperte einem Benutzer eine solche Sicht zuordnen, ordnet SAP Business ByDesign dem Benutzer automatisch diese zusätzlichen Sichten zu.

## Zugriffseinschränkung

Sie können definieren, ob ein Benutzer Lese- oder Schreibzugriff auf die in einer Work-Center-Sicht enthaltenen Daten besitzt.

Wenn Sie die Zuordnung zu einer Sicht vornehmen, gewährt SAP Business ByDesign dem Benutzer Zugriff auf alle Geschäftsbelege und Aufgabensteuerungspositionen in dieser Sicht.

Sie können den Zugriff auf spezielle Daten auf der Grundlage des Berechtigungskontexts, welcher der Work-Center-Sicht, in der die Daten angezeigt werden, zugeordnet ist, einschränken.

### Funktionstrennung

Mithilfe der **Funktionstrennung** sollen das Missbrauchs- und Fehlerrisiko minimiert und das Unternehmensvermögen (wie Daten oder Bestände) geschützt werden.

Durch die zweckmäßige Zuordnung von Zugriffsrechten wird die Verantwortlichkeit für Geschäftsprozesse und -verfahren auf mehrere Benutzer verteilt.

In Ihrem Unternehmen ist es z. B. erforderlich, dass zwei Mitarbeiter für den Zahlungsprozess zuständig sind. Mitarbeiter A legt einen Scheck an, und Mitarbeiter B unterzeichnet diesen. Durch diese Anforderung wird sichergestellt, dass die Verantwortlichkeit mit Blick auf die Unternehmensausgaben auf zwei Mitarbeiter verteilt wird.

Bei der **Funktionstrennungsprüfung** werden Funktionstrennungskonflikte ermittelt, nachdem Sie Zugriffsrechte zugeordnet haben.

Ein **Funktionstrennungskonflikt** tritt auf, wenn ein Benutzer Zugriff auf eine Gruppe von Work-Center-Sichten besitzt, über die er Fehler machen oder einen Betrug begehen und damit das Unternehmensvermögen schädigen könnte. Wenn die Anwendung einen Konflikt ermittelt, gibt sie diesen auf der Benutzungsoberfläche an und schlägt mögliche Lösungen vor.

Auf der Grundlage dieser Informationen können Sie Geschäftsprozessverantwortliche auf vorhandene Konflikte aufmerksam machen, sodass diese abschwächende Prozesssteuerungen implementieren können.

### Benutzertypen


Oft ist es erforderlich, für verschiedene Arten von Benutzern unterschiedliche Sicherheitsrichtlinien zu erstellen. Ihre Richtlinie erfordert z. B., dass einzelne, interaktiv arbeitende Benutzer ihre Kennwörter regelmäßig ändern müssen, nicht jedoch Benutzer, unter denen Hintergrundverarbeitungsprozesse ausgeführt werden.

Für SAP Business ByDesign erforderliche Benutzertypen sind z. B.:

- Einzelne Benutzer:
  - Dialogbenutzer werden für den Internetzugriff und normale Anwendungsinteraktionen verwendet.
- Technische Benutzer:
  - Systembenutzer werden bei Remote Function Calls und bei der Hintergrundverarbeitung verwendet.
  - Servicebenutzer werden für den anonymen Systemzugang verwendet.
  - Kommunikationsbenutzer werden für die Business-to-Business- oder Anwendungskommunikation verwendet.

### Standardbenutzer

Die nachfolgende Tabelle zeigt die Standardbenutzer, die für den Betrieb von SAP Business ByDesign erforderlich sind.

System	Typ	Beschreibung
Business ByDesign	Dialogbenutzer	Ein Benutzertyp für normale interaktive Benutzer.
Business ByDesign	Systembenutzer	Ein Benutzertyp für die dialogfreie Kommunikation in einem System.
Business ByDesign	Servicebenutzer	<p>Ein Benutzertyp, der von einer großen Gruppe anonymer Benutzer mit stark eingeschränkten Berechtigungen verwendet werden kann.</p> <p>Eine Sitzung, die als anonyme Servicebenutzersitzung beginnt, kann im Anschluss an die Authentifizierung als persönliche Dialogbenutzersitzung fortgesetzt werden.</p> <p> Servicebenutzer können für einen anonymen Systemzugang über einen ITS-Service (Internet Transaction Server) verwendet werden.</p>
Business ByDesign	Kommunikationsbenutzer	Ein Benutzertyp, der von Kommunikationspartnern verwendet wird, um in einem Business-to-Business- oder Anwendungsintegrationsszenario ihre Identität nachzuweisen.

Alle diese Benutzer werden mit SAP Business ByDesign ausgeliefert. Ein Kommunikationsbenutzer muss vor der Festlegung des Lösungsumfangs angelegt werden; alle anderen Benutzer werden nach der Festlegung des Lösungsumfangs und dem Fine-Tuning der Lösung angelegt.



Es wird empfohlen, die automatisch bei der Installation angelegten Benutzerkennungen und Kennwörter zu ändern.

## Frontend-Sicherheit

Das SAP-Business-ByDesign-Frontend besteht aus einer Webanwendungs-Benutzungsoberfläche auf Basis der Microsoft-Silverlight-Technologie. Bei Microsoft Silverlight handelt es sich um eine Entwicklungsplattform für Webanwendungen.

Sie können Microsoft-Silverlight-Anwendungen in Ihrem Web-Browser ausführen und direkt von den Sicherheitsmechanismen des Browsers profitieren. Zu Beispielen für Browser-Sicherheitsmechanismen zählen die sichere Cookie-Behandlung und die Same-Origin-Policy. Mit der Same-Origin-Policy wird sichergestellt, dass der Austausch vertraulicher Daten ausschließlich mit der Herkunftsdomäne erfolgt und dass diese Daten nach Beendigung der aktuellen Sitzung nicht auf dem Client abgelegt werden.

Microsoft-Silverlight-Anwendungen aus unterschiedlichen Herkunftsdomänen werden unabhängig voneinander ausgeführt. Ressourcen wie Geschäftsdaten werden von ihnen nicht gemeinsam verwendet. Die Anwendungen haben nur einen stark begrenzten Zugriff auf die Client-Ressourcen, z. B. das lokale Dateisystem.

Mit Blick auf die Sicherheit profitiert die Benutzungsoberfläche von SAP Business ByDesign von den Sicherheitsmechanismen und -konzepten, die bereits im Framework selbst von Microsoft realisiert wurden:

- Microsoft Silverlight Application Sandbox und Ressourcenisolation
- Cross-Site-Scripting-Gegenmaßnahmen
- Microsofts sichere Standardkonfiguration im Framework
- Development Guide zu sicheren Webanwendungen

Weitere Informationen finden Sie im Microsoft Silverlight Security Guide unter [www.silverlight.net](http://www.silverlight.net).

## Business-to-Business-Kommunikation

Die Business-To-Business-Kommunikation (B2B) bezieht sich auf den Austausch unternehmensbezogener Daten zwischen Administratordomänen. Diese Domänen müssen nicht notwendigerweise zu unterschiedlichen Entitäten gehören; sie können z. B. durch verschiedene Niederlassungsstandorte desselben Unternehmens repräsentiert werden. Die Endpunkte einer solchen Kommunikation werden in SAP Business ByDesign als Kommunikationssysteme bezeichnet. Sie können Kommunikationssysteme anlegen und bearbeiten, um Geschäftsbelege elektronisch auszutauschen.

Kommunikationssysteme stellen Endpunkte für Kommunikationsvereinbarungen dar. Ein Kommunikationssystem repräsentiert ein externes System zur Kommunikation, das von mehreren Geschäftsbelegen und Kommunikationsmethoden verwendet wird. Beispiele für Kommunikationssysteme umfassen externe Zeiterfassungs- oder Stammdatensysteme.

Mithilfe von Kommunikationsvereinbarungen können Sie den Austausch von Geschäftsbelegen zwischen Ihrem Unternehmen und seinen Geschäftspartnern und Kommunikationssystemen konfigurieren.

Sie müssen die Kommunikationsvereinbarungen aktivieren und die Details konfigurieren, bevor Sie mit der Arbeit beginnen können. Die B2B-Sicherheitskonfiguration erfolgt auch auf Kommunikationsvereinbarungsebene. Hier können Sie die Authentifizierungsmethode und Kommunikationssicherheit konfigurieren.

Ähnlich der Endbenutzerauthentifizierung kann die Authentifizierung der B2B-Kommunikation über die beiden Mechanismen Benutzername/Kennwort und X.509-Client-Zertifikat erfolgen. Für die eingehende Kommunikation können Sie das Client-Zertifikat des Geschäftspartners in die Konfigurationsbenutzungsoberfläche (UI) hochladen und es dem Kommunikationsbenutzer zuordnen. Weitere Informationen zu Zertifikaten erhalten Sie unter [www.sme.sap.com/irj/sme/community/collaboration/wiki?path=/display/AMI/FP2.6+ByDesign+Pilot+Installation+Guide](http://www.sme.sap.com/irj/sme/community/collaboration/wiki?path=/display/AMI/FP2.6+ByDesign+Pilot+Installation+Guide).

Für die ausgehende Kommunikation können Sie eine Containerdatei im PKCS#12-Format hochladen, die sich aus einem privaten Schlüssel und dem entsprechenden Client-Zertifikat zusammensetzt, dem der Geschäftspartner vertraut und das von ihm zugeordnet werden muss.

Beachten Sie, dass Zertifikate einen Gültigkeitszeitraum aufweisen und dass ihre Gültigkeit zu einem definierten Zeitpunkt abläuft. Vor dem Ablauf muss das Zertifikat erneuert werden. Bei einer Änderung des Zertifikatantragstellers oder -ausstellers muss der Prozess des Hochladens und Zuordnens wiederholt werden. Kommunikationsvereinbarungen fallen in den Verantwortungsbereich des Kunden, da ihre Konfiguration Kundendaten und deren geschäftspartnerspezifische Details widerspiegelt. In der Folge können ablaufende Zertifikate nicht automatisch von SAP ersetzt werden. Diese Aufgabe obliegt dem Kunden.

Im Falle der ausgehenden Kommunikation überwacht SAP das Ablaufdatum von Client-Zertifikaten und informiert Sie im Rahmen eines Health-Check-Ereignisses einen Monat vor Ablauf der Gültigkeit.

Es wird empfohlen, anstelle der Benutzername-Kennwort-Kombination Client-Zertifikate zu Authentifizierungszwecken zu verwenden. Ein gutes Sicherheitskonzept auf Ihrer Seite erfordert darüber hinaus in regelmäßigen Abständen eine Kennwortänderung. Diese Änderungen müssen an beiden Kommunikationsebenen synchron erfolgen. Wenn ein abgelaufenes Client-Zertifikat mit demselben Attribut erneuert wird, können die Zertifikatsinformationen asynchron ausgetauscht werden.

## Sicherheit der Datenablage / Sicherheit des Rechenzentrums

Die SAP Business ByDesign unterstützenden Rechenzentren umfassen eine Vielzahl von Sicherheitsmaßnahmen für die physische Datensicherheit und -integrität. Durch die Verwendung von redundanten Netzwerken und Netzsystemen sorgen sie ebenfalls für eine hohe Verfügbarkeit Ihrer Geschäftsdaten.

### Anlagenschutz und Datenintegrität

SAP hält sich beim Betrieb der Rechenzentren an die Best Practices der Branche: Die Bereiche für Rechenleistungen und die Datenspeicher befinden sich in räumlich getrennten, vor Feuer geschützten Bereichen. So können sämtliche Daten auch nach einem Brand wiederhergestellt werden.

Das Speichersystem selbst ist redundant ausgelegt, und es werden regelmäßige Datensicherungen durchgeführt. Die für SAP Business ByDesign verwendete hochmoderne Datenbankverwaltungslösung isoliert die Geschäftsdaten der einzelnen Kunden jeweils in einer eigenen Datenbankinstanz und speichert sie mit einem Maximum an Datenintegrität.

### Redundante und ausfallsichere Stromversorgung

Die Rechenzentren unterhalten mehrere Leitungen zu unterschiedlichen Energieversorgungsunternehmen, sodass ein kompletter Stromausfall extrem unwahrscheinlich ist. Sollte das örtliche Energieversorgungsnetz doch einmal komplett ausfallen, so verfügen die Rechenzentren für SAP Business ByDesign über eine unterbrechungsfreie Stromversorgung für kurzfristige Stromausfälle und einen Dieselgenerator als zusätzliche Energieversorgung für längerfristige Ausfälle. Eine Unterbrechung oder ein Ausfall der Stromversorgung hat also normalerweise keine Auswirkungen auf den Zugang zu den Anwendungen oder die Kundendaten.

### Eingeschränkter physischer Zugang

Derzeit nutzt SAP rund um die Uhr besetzte Rechenzentren in der Nähe des Hauptsitzes der SAP AG in Deutschland sowie in Pennsylvania (USA). Ein biometrisches Sicherheitssystem beschränkt den Zugang auf befugte Mitarbeiter. Außerdem sind die Rechenzentren in verschiedene Bereiche unterteilt, zu denen nur die jeweils dafür zuständigen Mitarbeiter Zutritt haben.

### Kommunikationssicherheit

SAP verwendet eine Transport-Layer-Security-Verschlüsselung via HTTPS, um Unbefugte am Abhören des Netzwerkverkehrs zu hindern. Die Verschlüsselung ist TLS-basiert (Transport Layer Security). Die benötigte Verschlüsselungssoftware ist bereits in aktuellen Clientbetriebssystemen und -browsern enthalten.

### Netzwerksicherheit

Im Netzwerk für SAP Business ByDesign werden verschiedene Technologien genutzt. Die proprietäre Netzwerkarchitektur setzt sich aus mehreren Ebenen und Teilen zusammen. Sie ermöglicht nur autorisierten Zugriff auf die SAP Business ByDesign unterstützenden Rechenzentren und zeichnet sich durch Folgendes aus:

- Eine Web-Dispatcher-Farm macht die Netzwerktopologie nach außen unsichtbar.
- Mehrere Internetanbindungen minimieren die Auswirkungen dezentraler Denial-of-Service-Angriffe (DDoS).
- Ein modernes Angriffserkennungssystem überwacht den Netzwerkverkehr ständig auf mögliche Angriffe.
- Mehrere Firewalls unterteilen das Netzwerk in geschützte Abschnitte und schützen das interne Netzwerk vor unbefugtem Internet-Datenverkehr.

## **Sicherheit** der Datenablage / Sicherheit des Rechenzentrums

- Über das ganze Jahr verteilte Prüfungen durch unabhängige Experten sorgen für eine frühzeitige Erkennung neuer Sicherheitsrisiken.

Beim Zuordnen von Benutzern zu Work Centern erhalten die betreffenden Benutzer Zugriffsrechte für die Funktionen und Daten des jeweiligen Work Centers. Den Benutzern werden genau die Funktionen angezeigt, die ihren Rechten entsprechen. Das senkt den Schulungsbedarf.

## Sonstige sicherheitsrelevante Informationen

Um unseren Kunden die dem neuesten Stand der Technik entsprechende Sicherheit bieten zu können, wird SAP Business ByDesign mehreren internen und externen Audits unterzogen (Zertifizierung nach SAS70/ISAE3402 oder ISO27001).

### Statement on Auditing Standards No.70, Type II

Der Umfang des SAS-70-Type-II-Berichts beinhaltet u. a. die physische Sicherheit der SAP-Einrichtungen, Datensicherungsverfahren sowie die Infrastruktur der SAP-Business-ByDesign-Systemlandschaft.

### ISO/IEC 27001

ISO/IEC 27001 fungiert als allumfassendes Verwaltungs- und Steuerungs-Framework zum Verwalten der Datensicherheitsrisiken eines Unternehmens.

ISO/IEC 27001 stellt eine erhöhte Sicherheit und Zuverlässigkeit von Informationssystemen sowie ein hohes Maß an Sicherheitsbewusstsein der SAP-Mitarbeiter sicher und veranschaulicht die entsprechende Sorgfaltspflicht.

Den aktuellen Stand der Zertifizierungen können Sie der Solutions-Site unter folgender URL entnehmen:

[www.sme.sap.com/irj/sme/solutions?rid=/webcontent/uuid/30f7e866-fe58-2c10-5780-f056f2d71ed2&language=de](http://www.sme.sap.com/irj/sme/solutions?rid=/webcontent/uuid/30f7e866-fe58-2c10-5780-f056f2d71ed2&language=de)

## Servicekomposition

Dieser Abschnitt bietet einen Überblick über die Sicherheitsaspekte, die für die vordefinierten Mashup-Integrations- und Webdienstkompositions-Funktionen von SAP Business ByDesign gelten. Mashups und Servicekomposition haben eine domänenübergreifende Kommunikation zwischen verschiedenen Internetdomänen zur Folge, z. B. zwischen den Domänen bydesign.com und google.com.

Inhalte aus unterschiedlichen Domänen, insbesondere aktive Inhalte (z. B. JavaScripts), werden im Browser immer auf die entsprechende Domäne beschränkt.

Eine in den Browsern vorhandene Same-Origin-Sicherheitsrichtlinie, die den Zugriff auf domänenübergreifende Inhalte verbietet, wird aktiviert.

## URL-Mashup-Integration

Sowohl Partner als auch Anwendungsexperten können URL-Mashups erstellen, um Folgendes zu tun:

- Öffnen einer Webseite
- Öffnen einer Ressource (z. B. Microsoft-Office-Dokument, Adobe-PDF-, Adobe-Flash-, Multimedivideo-Datei usw.)
- Öffnen einer benutzerdefinierten URL einer Frontend-Anwendung (z. B. Microsoft Outlook, Instant Messenger oder Apple iTunes usw.)

Sie können diese Positionen in einem SAP-Business-ByDesign-Bild öffnen, indem Sie die URL mit dynamischen Parametern aus dem Out-Port-Interface des SAP-Business-ByDesign-Bilds konfigurieren.



- Einige URLs können Ihre Geschäftsdaten an eine externe Anwendung Dritter weitergeben. Bei der Inverssuche in einem Online-Adressbuch werden z. B. Kundendaten an eine Web-Suchmaschine übergeben. Aus diesem Grund sollten Sie vor der Verwendung eines URL-Mashups sicherstellen, dass dieser mit den Sicherheits- und Datenschutzrichtlinien Ihres Unternehmens übereinstimmt.
- Einige Browsereinstellungen (z. B. Popup-Blocker) verhindern möglicherweise, dass das neue Browserfenster im URL-Mashup angezeigt wird. Es wird daher empfohlen zu überprüfen, ob Popup-Fenster in Ihren Browsereinstellungen zulässig sind.

## HTML-Mashup-Integration

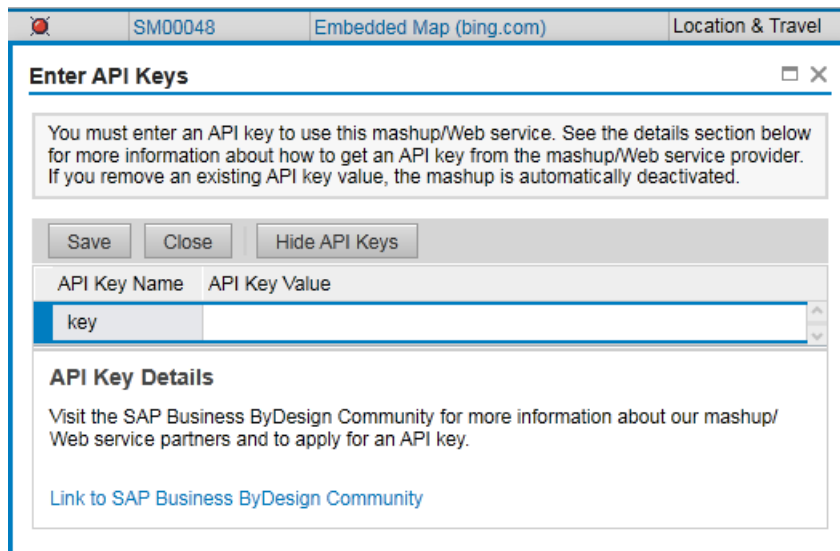
Sowohl Partner als auch Anwendungsexperten können HTML-Mashups anlegen, um eine HTML-basierte Webseite oder eine in einem Browser renderbare Ressource (z. B. Microsoft-Office-Dokument, Adobe-PDF-, Adobe-Flash-, Multimediateilvideo-Datei usw.) in ein Bild des SAP-Business-ByDesign-Systems einzubetten, indem sie die URL mit dynamischen Parametern aus dem SAP-Business-ByDesign-Screen-Out-Port-Interface konfigurieren.



- Einige URLs können Ihre Geschäftsdaten an eine externe Anwendung Dritter weitergeben. Beim Anzeigen eines Profils in einem sozialen Netzwerk werden z. B. Kunden- und Kontaktdaten an die Site des sozialen Netzwerks übergeben. Aus diesem Grund sollten Sie vor der Verwendung des HTML-Mashups sicherstellen, dass dieser mit den Sicherheits- und Datenschutzrichtlinien Ihres Unternehmens übereinstimmt.
- Einige HTML-basierte Webseiten werden über den Secure Sockets Layer (SSL), auf dem die Benutzungsoberfläche von SAP Business ByDesign läuft, möglicherweise nicht bedient. Im Browser wird unter Umständen eine Warnung zu unsicherem HTML-Content ausgegeben, bevor dieser auf der sicheren Benutzungsoberfläche von SAP Business ByDesign angezeigt wird. Es wird daher empfohlen zu prüfen, ob der SSL-Zugriff vom eingebetteten HTML-basierten Webseiten-Provider bereitgestellt wird. Sie können die URL darüber hinaus in Ihrem Browser der Liste vertrauenswürdiger Sites hinzufügen, wenn Sie dem Provider vertrauen. In diesem Fall wird kein Dialogfenster mit einer Warnung mehr angezeigt.
- Einige HTML-basierte Webseiten lassen ihre Einbettung in eine beliebige andere Anwendung aufgrund ihrer Nutzungsbedingungen oder rein technisch nicht zu (Sie sehen in diesem Fall lediglich eine leere Seite oder eine Webseite mit grau hinterlegten Einblendungen). Prüfen Sie daher, ob die Verwendung von eingebettetem HTML-Code zulässig ist.

## Karten-Mashup-Integration

SAP Business ByDesign verwendet Microsoft Bing Map als integrierten Kartendienstleister. Sowohl Anwendungsexperten als auch Endbenutzer können die Karten-Mashup-Verwendung für ein Bild von SAP Business ByDesign konfigurieren, um die visuellen Ortungs- oder Routeninformationen auf der Karte anzuzeigen. Bevor die Bing-Map-Mashups verwendet werden können, müssen Sie sie als Anwendungsexperte in der Sicht *Mashup-Bearbeitung* des Work Centers *Anwendungs- und Benutzerverwaltung* aktivieren, indem Sie den API-Schlüssel (Application Programming Interface) für die Bing-Map-Verwendung eingeben. Kunden können die SAP-Business-ByDesign-Community besuchen, um weitere Informationen zum Bing-Map-Webdienstpartner zu erhalten und einen API-Schlüssel anzufordern.



- Beachten Sie, dass der Karten-Mashup Ihre Geschäftsdaten an den Bing-Map-Webdienstleister weitergeben kann. So werden beispielsweise Liefer- und Rechnungsadressen an den Bing-Map-Webdienstleister übergeben, wenn die zugehörige visuelle Position auf der Karte angezeigt wird. Aus diesem Grund sollten Sie vor der Verwendung des Mashups sicherstellen, dass dieser mit den Sicherheits- und Datenschutzrichtlinien Ihres Unternehmens übereinstimmt.
- Die Bing-Map-Webdienstkommunikation findet direkt zwischen dem Browser des Benutzers und dem Webdienstleister über den SSL statt, wobei für jedes SAP-Business-ByDesign-Kundensystem der dedizierte API-Schlüssel angewendet wird. Beachten Sie, dass der Bing-Map-Webdienstleister die Bing-Map-Webdienst-API-Verwendung entsprechend den Lizenzbedingungen überwachen kann. Daher wird empfohlen, vor der Verwendung des Mashups die API-Verwendungs- und Lizenzdetails beim Bing-Map-Webdienstpartner zu erfragen.

## Webdienstkomposition

Sowohl Partner als auch Anwendungsexperten können Daten-Mashups zur Komposition von Webdiensten, die von einem externen Webdienstleister bereitgestellt werden, mit Geschäftsdaten aus SAP Business ByDesign erstellen. Mit dem integrierten Erstellungswerkzeug, dem Data Mashup Builder, können Sie externe Webdienste umwandeln oder mithilfe von Standard-Webdienst-Protokollen der Branche mit internen Geschäftsdaten zusammenführen (z. B. RSS-/ATOM-, REST- und SOAP-Webdienste).

Legen Sie Webdienste in SAP Business ByDesign an, bevor Sie die Webdienstkomposition im Data Mashup Builder erstellen. API-Schlüssel können zur Gewährleistung der Webdienstsicherheit mithilfe von in der Branche standardmäßig verwendeten oder Webdienst-spezifischen Authentifizierungsmethoden spezifiziert werden, z. B. Basisauthentifizierung, REST-Body-Credentials, SOAP-Serviceparameter-Credentials usw. Die von Partnern und Anwendungsexperten erfassten APIs werden in einem isolierten, sicheren Ablagebereich des SAP-Business-ByDesign-System-Backends abgelegt, der für das Frontend für Endbenutzer nicht offengelegt wird.



- Einige Webdienste können Ihre Geschäftsdaten an einen externen Webdienstleister Dritter weitergeben. So werden z. B. Kunden- oder Adressdaten an einen Datenqualität-Webdienstleister übergeben, wenn Sie in einer On-Demand-Anwendung einen Datenqualität-Bereinigungsvorgang ausführen. Aus diesem Grund sollten Sie vor der Verwendung des Mashups sicherstellen, dass der Webdienst mit den

## Sonstige sicherheitsrelevante Informationen

Sicherheits- und Datenschutzrichtlinien Ihres Unternehmens übereinstimmt.

- Die Webdienstkommunikation in Daten-Mashups findet nicht direkt zwischen dem Browser des Benutzers und dem Dienstleister statt. Stattdessen wird sie aufgrund der Einschränkung hinsichtlich der domänenübergreifenden Zugriffsrichtlinie des Browsers über das Webdienst-Proxy des Business-ByDesign-System-Backends getunnelt. Sämtliche Endbenutzer eines Kunden können über das Webdienst-Proxy des Business-ByDesign-System-Backends nur auf diejenigen Webdienst-Endpunkte zugreifen, die von Partnern und Anwendungsexperten bestätigt wurden. Aus diesem Grund sollten Sie sicherstellen, dass der Webdienst mit den Sicherheits- und Datenschutzrichtlinien Ihres Unternehmens und Landes übereinstimmt, bevor Sie ihn in SAP Business ByDesign hinzufügen und bestätigen.

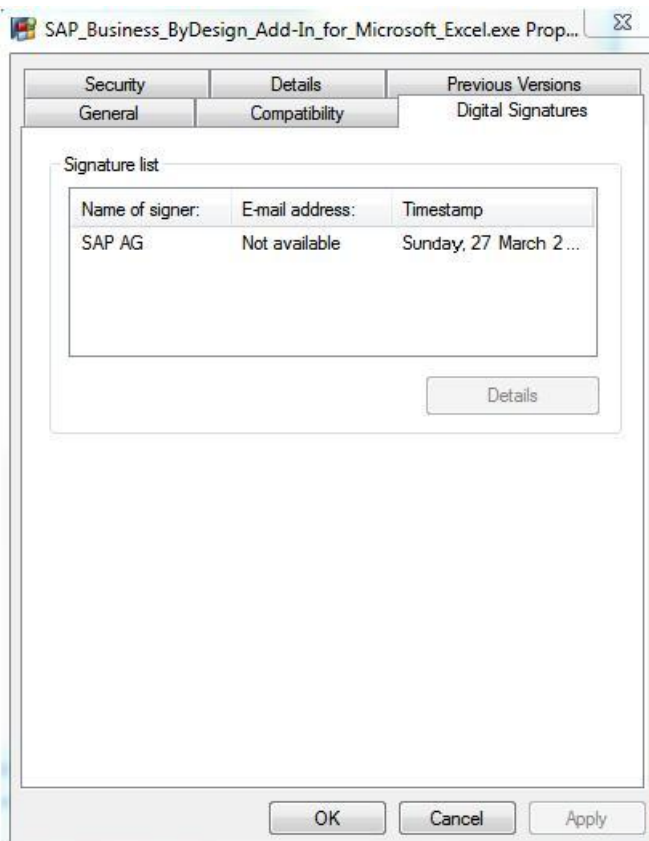
## Lokal installierte Komponenten

SAP bietet eine Gruppe von Softwarekomponenten an, die Sie zum Erlangen der Druckfunktion und anderer Funktionen auf Ihrem Desktop-Computer installieren können.

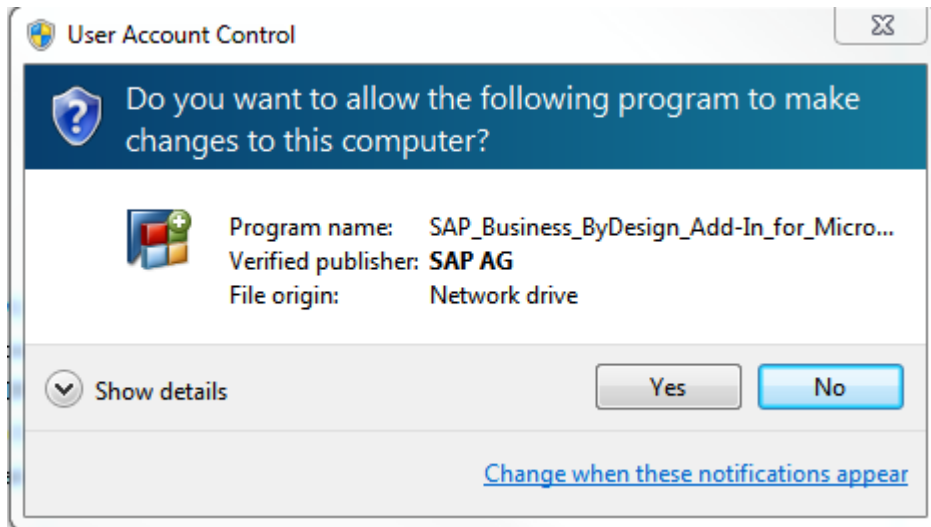
### Überprüfen der Signatur

Alle zum Download bereitgestellten Frontend-Komponenten von SAP Business ByDesign weisen eine digitale Signatur auf. Sie können diese Signatur wie folgt überprüfen:

- Klicken Sie mit der rechten Maustaste auf die Datei, die Sie heruntergeladen haben, und wählen Sie → *Eigenschaften*. Wählen Sie anschließend die Registerkarte *Digitale Signaturen*, und stellen Sie sicher, dass die Spalte *Name des Signaturgebers* den Wert *SAP AG* aufweist.



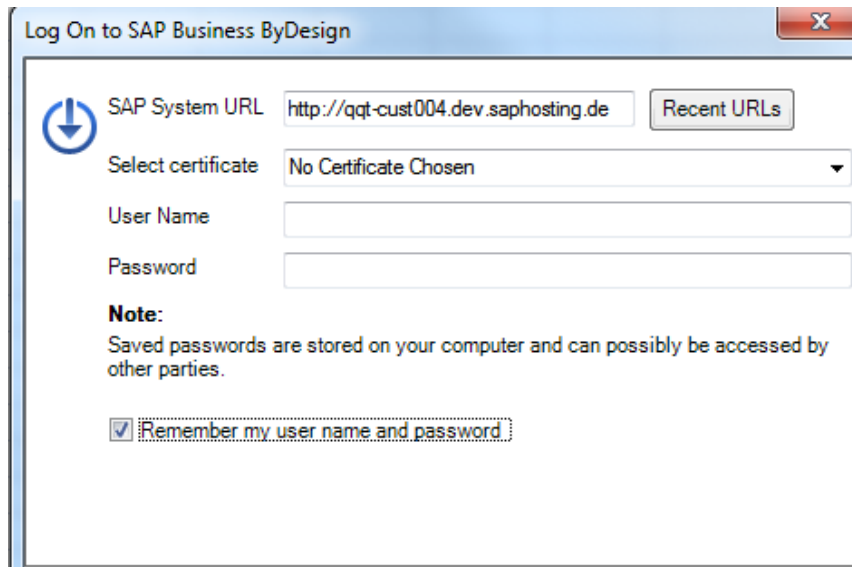
- Beim Installieren einer Datei wird ein Dialogfenster geöffnet, in dem der *verifizierte Herausgeber* angegeben ist. Im folgenden Beispiel handelt es sich ebenfalls um die *SAP AG*.



### Sichern von Anmeldedaten

SAP-Frontend-Komponenten verwenden eine vorhandene Authentifizierungssitzung für SAP Business ByDesign niemals gemeinsam, z. B. in einem Webbrowserfenster oder mit einer anderen Frontend-Komponente. Für den Aufbau eines vertraulichen, via SSL gesicherten Kommunikationskanals zu SAP Business ByDesign ist stets eine dedizierte Authentifizierung erforderlich.

Wenn Sie sich mit einem Benutzernamen und Kennwort im System anmelden, werden Sie gefragt, ob das Kennwort zu späteren Authentifizierungszwecken lokal auf dem Desktop-Computer gespeichert werden soll. Die Ablage des Kennworts erfolgt verschlüsselt und nicht als Klartext. Das Kennwort wird unter Verwendung der verfügbaren Schutzmechanismen des Betriebssystems gespeichert und kann ausschließlich von dem gegenwärtig im System angemeldeten Betriebssystembenutzer wiederverwendet werden. Die Verwendung dieser Funktion bleibt Ihnen überlassen. Sie sollte nur auf Ihrem eigenen Gerät und nicht auf öffentlichen Computern aktiviert werden.



## Sicherheitsprotokollierung und Nachverfolgung

Das Work Center *Anwendungs- und Benutzerverwaltung* bietet Ihnen eine Reihe von Berichten, die einen Einblick in das Systemverhalten ermöglichen. Beachten Sie, dass Sie in Abhängigkeit von Ihren Berechtigungen nicht auf alle Berichte Zugriff besitzen.

### **Zugriffsrechte – vor und nach der Systemaktualisierung**

Dieser Bericht zeigt alle Zugriffsrechte vor und nach der Systemaktualisierung von SAP Business ByDesign FP 2.0 auf FP 2.6 an (einschließlich der zugeordneten Work Center, Work-Center-Sichten und Einschränkungen). Diese Information ist nur dann für Sie relevant, wenn Sie Ihr SAP-Business-ByDesign-System von FP 2.0 auf FP 2.6 aktualisiert haben. Mithilfe des Berichts können Sie die Benutzer ermitteln, deren Zugriffsrechte Sie nach der Aktualisierung manuell anpassen müssen.

### **Änderungsprotokoll für Zugriffsrechte**

Dieser Bericht zeigt eine Liste mit allen im System vorhandenen Benutzern und den ihnen zugeordneten Zugriffsrechten an. Zudem wird aufgelistet, wann, wie und von wem die Zugriffsrechte geändert wurden. Diese Information ist aus Compliance-Gründen relevant und ermöglicht Ihnen, das System zu überwachen, um Betrugsfällen vorzubeugen, oder im Betrugsfall zurückzuverfolgen, von wem Änderungen vorgenommen wurden.

### **Alle aktuellen Zugriffsrechte**

Dieser Bericht zeigt eine Liste mit allen im System vorhandenen Benutzern und den ihnen gegenwärtig zugeordneten Zugriffsrechten an. Diese Information ist aus Compliance-Gründen relevant und ermöglicht Ihnen, das System zu überwachen, um Betrugsfällen vorzubeugen.

### **Alle aktuellen Benutzer**

Dieser Bericht zeigt eine Liste mit allen im System vorhandenen Benutzern an. Diese Information ist aus Compliance-Gründen relevant und ermöglicht Ihnen, das System zu überwachen, um Betrugsfällen vorzubeugen.

### **Benutzer – (De-)Aktivierungsprotokoll**

Dieser Bericht zeigt eine Liste mit allen im System vorhandenen Benutzern sowie dem Zeitpunkt an, zu dem diese aktiviert oder deaktiviert wurden. Diese Information ist aus Compliance-Gründen relevant und ermöglicht Ihnen, das System zu überwachen, um Betrugsfällen vorzubeugen.