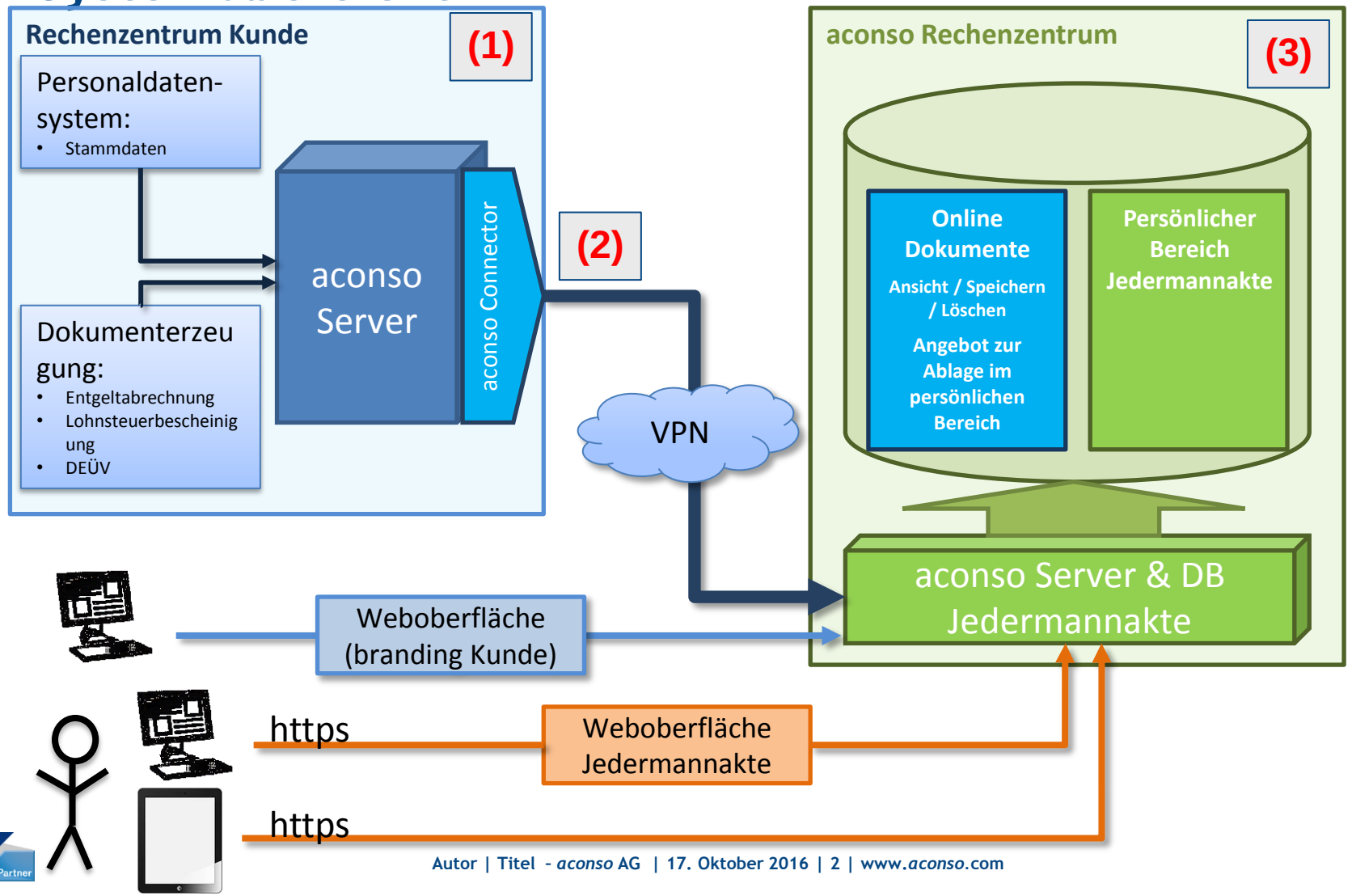
aconso

Jedermann-Akte

Systemübersicht & Security

Systemübersicht



(1) Verarbeitung auf dem aconso Server

Mitarbeiter-individueller Sicherheitsschlüssel

1. Mittels Secure Random wird pro Mitarbeiter eine konfigurierbare Anzahl von Bytes erzeugt. Dieser zufällig erzeugte Schlüssel dient der Verschlüsselung der Dokumente. Pro Mitarbeiter wird ein einzigartiger Schlüssel verwendet.
2. Der Mitarbeiterindividuelle Schlüssel wird in der aconso Datenbank gespeichert. Hierzu stehen zwei Verfahren zur Verfügung:
    a. aconsoJAMKv1: Aus einem konfigurierbaren Passwort und einem statischen Wert wird ein SHA256 Hash gebildet und dieser als Schlüssel für AES256 verwendet. Damit wird der Key in der DB abgelegt.
    b. aconsoJAMKv2: Aus einem konfigurierbaren Passwort und einem statischen Wert wird ein SHA256 Hash gebildet. Dieser wird 65.536 Mal# durch eine PBKDF2withHmacSHA1 laufen gelassen. Daraus ergibt sich ein Schlüssel und ein Initialisierungsvektor (IV). Dieses Paar wird in der DB abgelegt.

Initiales Anschreiben (Übermittlung Sicherheitsschlüssel an Mitarbeiter)

Das *aconso* Connector generiert pro Mitarbeiter ein individuelles Anschreiben. In dem Anschreiben erhält der Mitarbeiter Informationen zur Erst-Anmeldung an der Jedermann-Akte. In dem Anschreiben wird dem Mitarbeiter zusätzlich der individuelle Sicherheitsschlüssel mitgeteilt.

Entgegennahme von Dokumenten

Alle Dokumente, die für die Übertragung in die Jedermann-Akte vorgesehen sind, werden über die *aconso* Standard Import-Schnittstellen an den *aconso* Server im Rechenzentrum des Kunden übermittelt. Dort werden die Dokumente im Archiv des Personalakte-Servers (analog zu den Personalakte-Dokumenten) verschlüsselt zwischengespeichert.

(2) Übertragung der Dokumente

Übertragung der Dokumente

Vor der Übertragung der Dokumente ruft das Connector Modul jedes Dokument einzeln aus dem Archiv ab. Zu diesem Zeitpunkt ist das Dokument mit einem allgemeinen Schlüssel verschlüsselt. Das Connector Modul entschlüsselt das Dokument und verschlüsselt es unmittelbar im Anschluss erneut. Hierzu wird nochmals ein neuer Schlüssel erzeugt: Über den individuellen Sicherheitsschlüssel plus einer Benutzerspezifischen Information (z.B. Personalnummer) plus einen statischen Wert wird ein SHA256 Hash gebildet. Dies ist der Schlüssel für die AES256 Verschlüsselung des Dokuments. Während diesem Vorgang wird das Dokument lediglich im Cash des Servers gespeichert. Zu keinem Zeitpunkt liegt das Dokument unverschlüsselt z.B. im Dateisystem des Servers.

Sicherung der Übertragung

Die Übertragung der Dokumente an das *aconso* Rechenzentrum erfolgt 3-fach verschlüsselt:

- Die gesamte Kommunikation zwischen dem Rechenzentrum des Kunden und dem aconso Rechenzentrum wird durch einen VPN-Tunnel gesichert.
- Innerhalb des VPN-Tunnels erfolgt die Kommunikation über SSL
- Die übertragenen Dokumente selbst sind mit dem oben beschriebenen Verfahren verschlüsselt verschlüsselt

(3) Verarbeitung auf Jedermann-Akte Server

Speicherung der Dokumente

Die übertragenen Dokumente werden auf einem rechts-und revisionssicheren Archivsystem (Centerra) gespeichert. Der Jedermann-Akte Server nimmt die Dokumente bereits verschlüsselt entgegen und speichert diese (genau so wie sie entgegengenommen werden) im Archivsystem.

Zusätzliche wird das Archivsystem selbst üblicherweise nochmals zusätzlich mit AES 256 verschlüsselt.

Speicherung Sicherheitsschlüssel

Bei der erstmaligen Anmeldung am Jedermann-Akte Server muss der Mitarbeiter seinen postalisch erhaltenen individuellen Sicherheitsschlüssel eingeben. Gleichzeitig vergibt der Mitarbeiter ein Passwort (Passwortrichtlinien sind konfigurierbar). Der Sicherheitsschlüssel wird mit dem selben Verfahren wie auf dem sendenden System (aconsoJAMKv1 oder aconsoJAMKv2) gesichert in der Datenbank abgelegt. Auf dem Jedermann-Akte System wird jedoch anstelle des konfigurativ festgelegten allgemeinen Passwortes das vom Mitarbeiter selbst vergebene Passwort für die Verschlüsselung verwendet.

So ist sichergestellt, dass nur der Mitarbeiter selbst (mir Kenntnis des von Ihm vergebenen Passwortes) Zugriff auf den Schlüssel erhalten kann.

Datensicherheit im *aconso* Rechenzentrum

- ISO/IEC 27001 – Informationssicherheits-Managementsystem

Geltungsbereich:

Alle Prozesse, Mitarbeiter und Technologien zur Bereitstellung von IT-Services für die Kunden von OEDIV inklusive der zugehörigen IT-Infrastruktur an den Rechenzentrums-Standorten in Bielefeld.

- ISAE 3402 Typ 2

Nachweis über die Wirksamkeit der internen Kontrollsysteme zur Gewährleistung der Informationssicherheit.

aconso

Wir leben Dokumente.