

Whitepaper

Leistungsbeschreibung & Funktionsübersicht des bitkasten



Datum: August 2023

Version: 2.6

Inhalt

Überblick	3
Funktionsübersicht	4
bitkasten Prinzip	4
Prozessablauf im bitkasten	5
Registrierung Empfänger:in	6
Registrierung mit neuem Personalausweis	6
Identifizierung mit IDnow Autolent	6
Registrierung (kundenspezifisch)	6
User-Import (kundenspezifisch)	7
Login bitkasten	7
2-Faktor-Authentifizierung	7
Biometrische Anmeldung (Face-ID, Fingerprint)	7
Digitaler Postversand	8
Bereitstellung von Dokumenten	8
Identifizierung & digitale Zustellung	8
Analoger Postversand	8
bitkasten Archiv	9
Digitalisierung und bidirektionaler rechtssicherer Informationsaustausch	10
Qualifizierte elektronische Signatur nach eIDAS	10
Digitalisierung Eingabeprozesse & Input Management	11
Integration in Bestandssysteme	11
Sicherheit	12
DSGVO-Konformität	12
Kein Opt-in/ Opt-out notwendig	13
Darstellung Datenschutzmanagementsystem/-organisation	13
Technische und organisatorische Maßnahmen (TOM) zum Datenschutz	14
Auszug der technischen Maßnahmen	14
Auszug der organisatorischen Maßnahmen	14
Rechenzentren in Deutschland	14
Berechtigungszertifikate	15

Berechtigungszertifikat Bundesverwaltungsamt.....	15
Berechtigungszertifikat eID-Service Bundesdruckerei	15
Informationssicherheit.....	16
Unsere Informationssicherheitsleitlinie.....	16
Software Hosted in Germany!	16
Qualitätsmanagement.....	17
Unsere Qualitätspolitik.....	17
Software Made in Germany!.....	17
Lizenzmodell und Service-Nutzung.....	18

Überblick

Die bitkasten AG ist ein deutscher Software-as-a-Service (SaaS) und Green Tech Anbieter für die vollständige Digitalisierung der Briefkommunikation und des Informationsaustauschs. Die Lösung ist der bitkasten, eine Digitalisierungs- und Kommunikationsplattform – ökologisch, nachhaltig und smart.

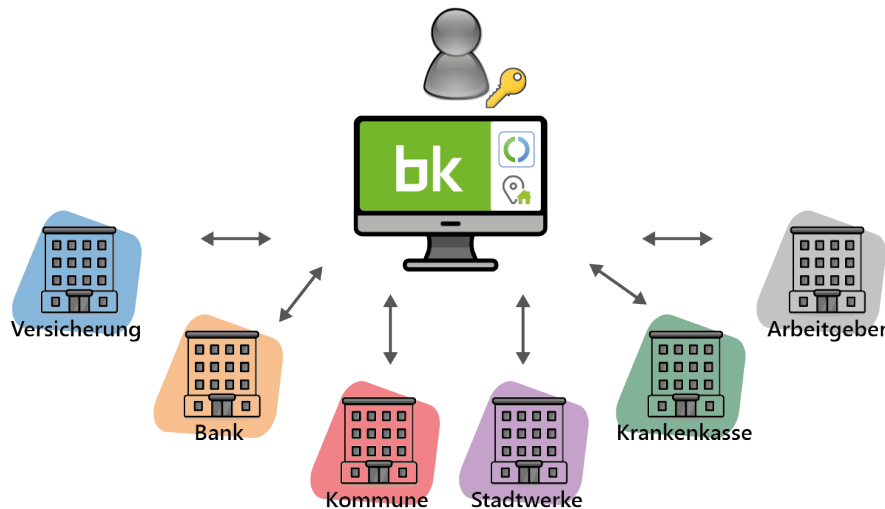
Der bitkasten sorgt für eine sichere, digitale Vernetzung der Kommunikationspartner. Durch verschlüsselte Transportwege und einem eindeutig identifizierten Nutzerkreis wird eine DSGVO-konforme Dokumentenzustellung sichergestellt. Zudem überbrücken Unternehmen die „letzte Meile“ zu Kund:innen und Mitarbeitenden durch die Digitalisierung der Input- und Output-Prozesse. Dies erfolgt ohne aufwändiges IT-Projekt innerhalb kurzer Zeit durch Verwendung bestehender Druckdaten und bekannte Postadressen. Die nachhaltige Briefkommunikation, digital und ohne Druck & Transport, führt zu einer Halbierung der Druck-, Porto- und Prozesskosten mit einem ROI innerhalb von wenigen Wochen.

Briefe werden rechtssicher an den digitalen, smarten Briefkasten zugestellt. Der bitkasten steht für schnelle Kommunikation wie E-Mail, aber ohne E-Mail-Adresse, dafür sicher und DSGVO-konform. Die Identifizierung und digitale Zustellung der Kommunikation erfolgen mittels der bekannten Postadresse über den elektronischen Personalausweis (eID) oder Kennung. Für Empfänger:innen funktioniert die Kommunikation im bitkasten ohne Medienbruch via App oder Web.

Funktionsübersicht

bitkasten Prinzip

Den bitkasten kann man mit dem Briefkasten an der Hauswand vergleichen – nur eben digital. Im Briefkasten erhalten Empfänger:innen adressierte Post, wie beispielsweise die der Versicherung, der Bank, des Stromversorgers, des Arbeitgebers etc. Der digitale Briefkasten funktioniert nicht anders – nur, dass Empfänger:innen Post der Absender digital im bitkasten finden.



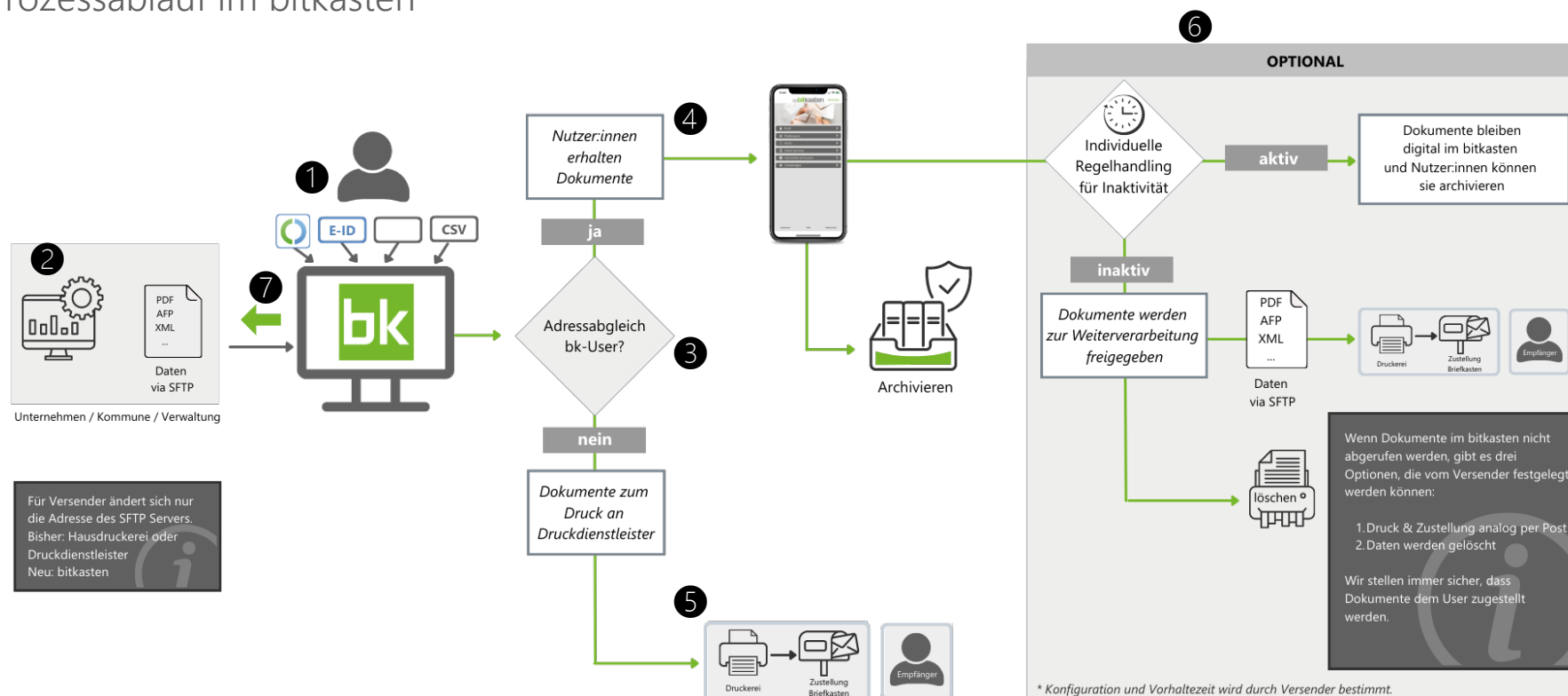
Der bitkasten empfängt und archiviert digitale Post von allen teilnehmenden Versendern, stellt die Möglichkeit einer digitalen Signatur bereit und übermittelt Daten digital an ERP,- CRM-, HR-Systeme oder direkt an Fachverfahren. Durch die Abbildung von Prozessen, Eingabemöglichkeiten oder Formularen im geschlossenen System des bitkasten, sind Empfänger:innen sicher mit dem Unternehmen oder der Verwaltung verbunden.

Die Implementierung des bitkasten erfolgt nahezu ohne IT-Aufwand, da die **bestehenden Druckdatenströme der dokumentenerzeugenden Systeme** übernommen werden. Dokumente müssen also nicht kanalspezifisch aufbereitet werden. Dies gilt einerseits für transaktionale Daten und Druckdatenformate, wie PDF, AFP, IPDS, etc. aber auch für individuelle Dokumente oder Tagespost. Es kommt kein zu installierender Druckertreiber zum Einsatz, sondern die fertigen Druckdaten werden via SFTP anstatt zum Druckdienstleister an den bitkasten gesendet.

Das Prinzip der digitalen Zustellung ist **sicher und einfach**: Anstatt der Druckerei empfängt der bitkasten die Druckdaten, stellt digital an bitkasten Nutzer:innen zu und die verbleibenden, nicht zugestellten Dokumente werden im ursprünglichen Format an die Druckerei angesteuert, um sicherzustellen, dass alle erreicht werden. Der Versender muss Dokumente also nicht kanalspezifisch aufbereiten und muss vorher auch nicht wissen, wer es digital empfangen kann oder nicht. Ein „Opt-In“ ist dafür nicht notwendig, wie zum Beispiel für E-Mail.

Der bitkasten sorgt für eine sichere, digitale Vernetzung der Kommunikationspartner. Durch verschlüsselte Transportwege und einem eindeutig identifizierten Nutzerkreis stellen wir eine DSGVO-konforme Dokumentenzustellung sicher.

Prozessablauf im bitkasten



Registrierung Empfänger:in

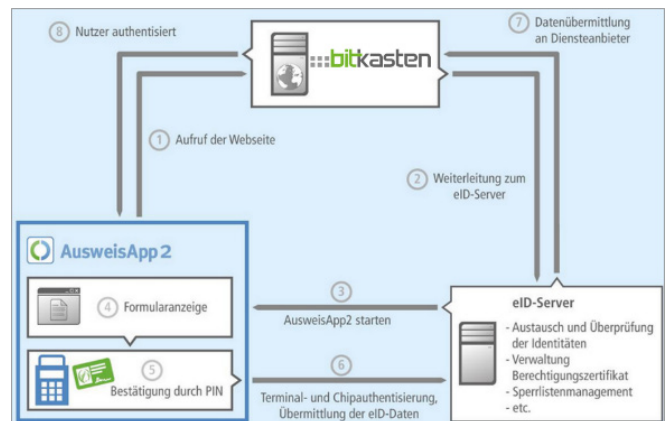
Empfänger:innen können sich kostenfrei für den persönlichen bitkasten registrieren. Persönliche Zugangsdaten haben sich früher lediglich aus einem Anmeldenamen in Kombination mit einem Passwort zusammengesetzt. Heutzutage gibt es viele weitere und sichere Möglichkeiten der Anmeldung im Internet. Da wir auf Sicherheit im bitkasten setzen und verifizierte Daten für die Zustellung über die Postanschrift benötigen, haben wir diesen durch unterschiedliche Identifizierungsverfahren ausgestattet.

Folgende Optionen werden auf der Registrierungs- bzw. Login-Seite aufgezeigt:

Registrierung mit neuem Personalausweis

Dies ist eine Standardfunktion des bitkasten. Der neue Personalausweis beinhaltet einen sogenannten RFID-Chip. Empfänger:innen können die Identität mit dem Ausweis und einem persönlichen Passwort eindeutig online bestätigen. Die Online-Authentifizierung erfolgt über die AusweisApp2 des Bundes, die man sich kostenfrei im Internet herunterladen kann.

Die Authentifizierung mit dem neuen Personalausweis lässt sowohl über das Smartphone (iOS und Android) als auch über den PC durchgeführt werden.



Alles, was dafür benötigt wird:

- Neuer Personalausweis mit aktivierter eID-Funktion
- Passender Kartenleser (z.B. Smartphone mit NFC Funktion)
- Installierte BSI-zertifizierte AusweisApp2

Identifizierung mit IDnow Autolident

Nach der Auswahl des Identifizierungsverfahrens IDnow Autolident wird das jeweilige Ausweis- oder Führerscheindokument auf Echtheit überprüft. Zudem erfolgt eine biometrische Erkennung, um zu prüfen, ob die Person hinter einer Transaktion auch diejenige ist, für die sie sich ausgibt. Der Prozess dauert nur wenige Minuten und die Identität wird innerhalb kürzester Zeit bestätigt.

Autolident überprüft das Selfie mit dem Lichtbild, welches zusammen mit dem Ausweis im Rahmen der Dokumentenüberprüfung aufgezeichnet wurde. Eine Ähnlichkeitsprüfung wird durchgeführt. Empfänger:innen erhalten anschließend eine digitale Identität und können sich damit eindeutig im bitkasten identifizieren.

Registrierung (kundenspezifisch)

Neben der Registrierung mit Identifizierungsverfahren gibt es auch ein kundenspezifisches Onboarding von bitkasten Empfänger:innen. Über eine individuell eingerichtete Registrierungsseite können sich

Empfänger:innen für den bitkasten registrieren. Die dort eingegebenen Daten werden von uns verarbeitet und ein bitkasten Account angelegt. Die Zugangsdaten erhalten die Empfänger:innen auf dem Postweg.

User-Import (kundenspezifisch)

Alternativ zu der individuell eingerichteten Registrierungsseite kann die Einrichtung der bitkasten Zugänge über einen User-Import erfolgen. Das Unternehmen stellt dafür alle relevanten User-Informationen in Form einer Excel-Liste bereit.

Relevant für die Einrichtung sind folgende Angaben:

- Eindeutige Kennung (Personalnummer, Kundennummer, Versicherungsnummer etc.)
- Vorname und Nachname
- Vollständige Adresse

Die Integration weiterer eID-Identifikationslösungen ist in Planung und durch unser offenes Schnittstellenkonzept und die Erfahrung aus den bestehenden Integrationen schnell durchführbar.

Login bitkasten

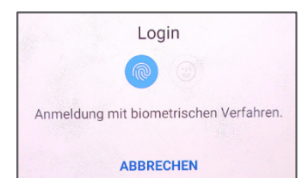
Empfänger:innen können sich mit dem neuen Personalausweis oder persönlichen Zugangsdaten im bitkasten anmelden. Dies kann über den Webclient oder per App (iOS, Android) erfolgen. Sie haben Zugriff auf ihre Dokumente, das persönliche Archiv und auf die vom Versender bereitgestellten Services.

2-Faktor-Authentifizierung

Für noch mehr Sicherheit können der Empfänger:innen den bitkasten mit einem zweiten Sicherheitsschritt schützen. Neben der Eingabe des Passwortes wird zusätzlich einen einmaligen Zugangscode eingegeben. Empfänger:innen müssen für den Erhalt dieses einmaligen Codes auf dem mobilen Endgerät eine Authentifizierungs-App, wie zum Beispiel Authy, Google-Authenticator, Microsoft Authenticator etc. installieren. Die Zweifaktor-Authentifizierung kann in den Einstellungen unter Login & Sicherheit aktiviert werden. Nach Aktivierung ist der bitkasten zweifach geschützt. Bei jedem Login müssen Empfänger:innen einen einmaligen Code, den der bitkasten an die Authentifizierungs-App senden, eingeben.

Biometrische Anmeldung (Face-ID, Fingerprint)

In den bitkasten Einstellungen haben Empfänger:innen die Möglichkeit, die biometrische Anmeldung zu nutzen. Vorher sind allerdings die Geräteeinstellungen zu prüfen, ob die biometrische Anmeldung generell eingerichtet und auch aktiviert ist. In den Einstellungen unter „App-Anmeldung“ wird die Funktion aufgezeigt. Bei erfolgreicher Aktivierung färbt sich der Schieber grün. Bei der nächsten Anmeldung im bitkasten wird gefragt, welches biometrische Authentifizierungsverfahren genutzt werden soll. Empfänger:innen haben die Auswahl zwischen Face ID und Fingerprint (wenn das Endgerät beides unterstützt).



Digitaler Postversand

Bereitstellung von Dokumenten

Der Informationsaustausch im bitkasten funktioniert grundsätzlich rein digital. Er beginnt mit der Bereitstellung der Dokumente durch den Versender (Absender). Diese erhalten wir über einen gesicherten elektronischen Weg per SFTP, VPN oder REST-Schnittstelle. Hier setzen wir auf bestehende Druckdaten auf, die nicht aufbereitet werden müssen. Der Versender teilt uns zudem auf Dokumentenbasis mit, wie lange die Dokumente digital für Empfänger:innen im bitkasten bereitstehen sollen.

Identifizierung & digitale Zustellung

Die Identifizierung und digitale Zustellung an Empfänger:innen erfolgen mittels der bekannten Postadresse oder einer eindeutigen Kennung, wie zum Beispiel Personalnummer, Versicherungsnummer, Kundennummer etc. Für Empfänger:innen funktioniert die Kommunikation im bitkasten ohne Medienbruch via App oder Web.

Für den Adressabgleich kommt eine Technologie zum Einsatz, mit der wir die geografischen Daten überprüfen bzw. mit einer Datenbank abgleichen. Damit können unterschiedliche Schreibweisen bzw. Abkürzungen oder Ortsteile entsprechend gematcht werden. Beim Adressatennamen achten wir auf die identische Schreibweise bzw. stellen nur dann digital zu, wenn diese eineindeutig ist. Nicht zuordenbare Dokumente werden angesteuert und entsprechend einem definierten Fehlerhandling bearbeitet.

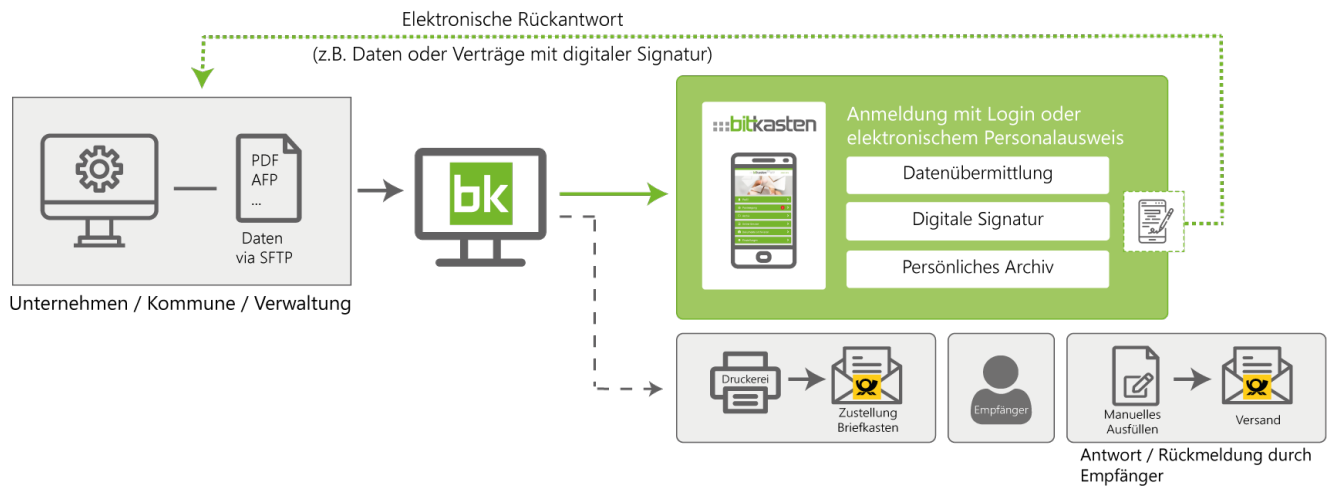
Analoger Postversand

Sollte ein Dokument einmal nicht digital zugestellt werden können, wird dieses automatisch dem Prozess des analogen Postversands zugeführt. Hier kann die bestehende Druckerei - basierend auf dem bestehenden Workflow - genutzt werden. So geht nichts verloren und wir stellen eine 100%ige Zustellung der Dokumente sicher.

Bei inaktiven Nutzer:innen geben wir Versendern die Möglichkeit, basierend auf dem Dokumententyp, eine sogenannte Vorhaltezeit einzurichten. Diese ermöglicht ein definiertes Fehlerhandling nach Ablauf der Zeit und ausbleibender Reaktion wie Öffnen, Speichern oder Herunterladen durch Nutzer:innen. Das Fehlerhandling kann beispielsweise das Löschen der Dokumente im bitkasten oder der zusätzliche Druck dieser sein.

Die Druckerei erhält die Dokumente, die nicht digital zugestellt werden konnten, weil Empfänger:innen keinen bitkasten haben oder das Fehlerhandling ein Druck vorsieht. Hierfür wird entweder direkt eine sichere Verbindung zwischen der bitkasten AG und dem jeweiligen Druckzentrum hergestellt oder die Daten gehen an den Versender zurück, der dann seinen bisherigen Prozess bedient.

Wenn gewünscht kann die bitkasten AG mit Partnern auch die Druck- und Versanddienstleistung zusammen mit einem Partner übernehmen.



Neben der digitalen Dokumentenzustellung bietet der bitkasten noch viel mehr.

- bitkasten Archiv
- Formulare und Anträge inkl. digitaler Signatur
- Online-Services – kundenindividuelle Formulare im bitkasten

bitkasten Archiv

Wenn Briefpost elektronisch in einem digitalen Briefkasten empfangen wird, dann sollte diese auch direkt archiviert werden können – ganz, ohne den Briefkasten zu verlassen. Dabei stellen wir sicher, dass nur die jeweiligen Benutzer:innen Zugriff auf die Briefpost haben. Die Dokumente können mittels PC oder Smartphone abgerufen werden – und das orts- und zeitunabhängig. Es können eigene Ordnerstrukturen angelegt und digital empfangene Dokumente einfach und bequem abgelegt werden. Selbst eingescannte Dokumente können einfach in das Archiv hochgeladen werden.

Das bitkasten Archiv ist ein Archiv der Nutzer:innen und nicht der Versender. Es ermöglicht eine beweiswerterhaltende, sichere sowie revisionssichere Langzeitaufbewahrung von Dokumenten. Das Ziel und die Herausforderung der rechtssicheren Ablage elektronischer Unterlagen ist es, sowohl für die digitalen Inhalte als auch deren Metadatenätze die folgenden Punkte für lange Zeiträume (mehrere Jahrzehnte) zu gewährleisten:

- Verfügbarkeit und Lesbarkeit
- Integrität (Unversehrtheit)
- Beweiswerterhaltung von Signaturen/Siegeln und Zeitstempeln, Authentizität (daraus folgt auch die Nichtabstreitbarkeit) sowie
- Datenschutz, Datensicherheit und Vertraulichkeit

Aus diesem Grund hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Technische Richtlinie für die sogenannte beweiswerterhaltende Langzeitaufbewahrung kryptografisch signierter Dokumente herausgegeben: die TR-03125, auch TR-ESOR genannt. Das Archiv des bitkasten erfüllt die Anforderungen dieser Technischen Richtlinie. Es wurde konform der TR-03125 implementiert und ist für einen möglichst generischen Einsatz ausgelegt.

Die Sicherheit bzw. der Beweiswert wird hierbei in Software und nicht in Hardware „konserviert“. Somit ist eine hohe Unabhängigkeit hinsichtlich Einsatzszenarien und verwendeter Speicher- und Hardware-schichten gegeben. Durch diese Vorgehensweise ist das Archiv auch unabhängig hinsichtlich der zu sichernden Datenformate/Inhaltsdaten.

Digitalisierung und bidirektionaler rechtssicherer Informationsaustausch

Wir digitalisieren Formulare und Prozesse (z.B. Anträge oder Arbeitsverträge) und erstellen einen automatisierten Workflow. Die Informationen können direkt digital weiterverarbeitet werden. Mittels integrierter Qualifizierter elektronischer Unterschrift (QES) können Verträge digital rechtssicher abgeschlossen werden.

Qualifizierte elektronische Signatur nach eIDAS

Mit der integrierten bitkasten Signatur können Dokumente digital und rechtsverbindlich unterschrieben werden. Die rechtliche Grundlage bildet dafür die eIDAS-Verordnung. Unsere Lösung unterstützt unterschiedliche Arten von Signaturen:

- Einfache / fortgeschrittene elektronische Signatur (SES)
- Qualifizierte elektronische Signatur (QES)

Die qualifizierte elektronische Signatur (QES) hat die höchste Qualität und ist der händischen Unterschrift rechtlich gleichgestellt. Damit können alle unterschriftspflichtigen Dokumente, wie zum Beispiel Verträge und auch Arbeitsverträge verarbeitet werden.



Um die Signaturlösung als Erstellender zu nutzen, ist keine Installation einer Software erforderlich. Der Signatur-Client kann über jeglichen Browser (Mozilla Firefox, Chrome, Edge etc.) aufgerufen werden und der Erstellende kann sofort loslegen:

- Dokument hochladen
- Empfänger:in via Postadresse auswählen
- Digital signieren
- Abschicken

Über den bitkasten Signatur-Client wird der Vertrag vom Ersteller signiert und anschließend in den bitkasten der Empfänger:innen übertragen. Sie können den Vertrag im bitkasten aufrufen und signieren. Anschließend wird der komplett signierte Vertrag automatisch an den Ersteller zurückgeschickt.

Anhand der integrierten Unterschriftenmappe im Signatur-Client können alle offenen, laufenden und abgeschlossenen Vorgänge eingesehen und verwaltet werden. Zusätzlich gibt es die Möglichkeit den signierten Vertrag direkt in eine digitale Personalakte zu überführen.

Digitalisierung Eingabeprozesse & Input Management

Wir digitalisieren bestehende Eingabeprozesse (z.B. Krankmeldung, Urlaubsantrag, Adressänderung) und erstellen einen automatisierten Workflow. Am Beispiel Urlaubsantrag und Adressänderung: Diese werden unter dem Menüpunkt „Online-Service“ für Empfänger:innen in Form von Formularen bereitgestellt, sind 24/7 verfügbar, können online ausgefüllt, ggf. unterschrieben und an den Arbeitgeber zur weiteren Bearbeitung zurückgeschickt werden. Die Erstellung und Bereitstellung von Formularen erfolgen durch die Beauftragung sowie Spezifizierung durch den Versender.

Integration in Bestandssysteme

Der bitkasten kann in Kundenportale, Kunden-Apps, Fachverfahren, ERP-Systeme oder auch Web-Anwendungen integriert werden. Durch die moderne, offene Schnittstellenarchitektur ist dies meist problemlos möglich.

Sicherheit

Cyberangriffe haben in den kommenden Jahren verstärkt zugenommen. 67% der Angriffe in Deutschland im Jahr 2021 erfolgt durch Malware, Phishing und Ransomware, die über E-Mail verbreitet werden ¹. Durch den Verzicht von E-Mail adressiert der bitkasten diese Sicherheitsprobleme und minimiert die Risiken.

Der bitkasten sorgt für eine sichere, digitale Vernetzung der Kommunikationspartner. Durch verschlüsselte Transportwege und einem eindeutig identifizierten Nutzerkreis stellen wir eine DSGVO-konforme Dokumentenzustellung sicher.

Neben der Identifizierung und Authentifizierung bilden eine Reihe von Sicherheitsmaßnahmen das Fundament für sichere, medienbruchfreie Kommunikation und Informationsaustausch.

Sicherheit					
DSGVO-konform	Ende-zu-Ende verschlüsselt	Keine E-Mail Zustellung	Schutz vor SPAM, Ransomware, Phishing	Einfache IT-Integrierbarkeit	
	Kein Opt-In notwendig	Keine kanalspezifische Aufbereitung	TR-ESOR Archiv	Schutz gegen Identity Fraud	

DSGVO-Konformität

Mit dem bitkasten stellen wir eine sichere digitale Vernetzung zwischen Empfänger:innen und Versendern sicher. Es ist ein in sich geschlossenes System, in dem Informationen verschlüsselt, DSGVO-konform und ohne E-Mail ausgetauscht werden können.



¹ Quelle: Bitkom

Kein Opt-in/ Opt-out notwendig

Der bitkasten funktioniert vom Grundsatz her wie ein **Zustelldienst**. Es werden Daten entgegengenommen und an bitkasten Nutzer:innen zugestellt. Es gibt einen Auftragsverarbeitungsvertrag gemäß DSGVO (AVV) zwischen dem Versender und der bitkasten AG und der bitkasten AG und dem jeweiligen Empfänger der Post (bitkasten Nutzer:innen) via der Nutzungsbedingungen.

Der Gegenstand des Vertrages zwischen der bitkasten AG und den bitkasten Nutzer:innen, der in den Nutzungsbedingungen abgebildet ist, ist die digitale Zustellung von Briefkommunikation und Informationsaustausch (digitale Vernetzung) aller angeschlossenen Versender. Im Rahmen der Vertragserfüllung stellen wir jegliche Information und Briefpost der Versender zu. Wenn vom Versender gewünscht, stellen wir auch eine digitale Vernetzung zwischen ihm und dem Empfänger her. Hierdurch können Informationen bidirektional ausgetauscht und beispielsweise Formulare ausgefüllt oder Verträge digital abgeschlossen werden.

Im Rahmen der **Vertragserfüllung** ist ein dediziertes Opt-in für einzelne Versender nicht erforderlich. Das gleiche gilt auch für explizite Opt-out Möglichkeiten. Beides ist nicht notwendig, da wir andernfalls unseren Vertrag der Zustellung nicht erfüllen können.

Ein Opt-in/ Opt-out gemäß DSGVO ist für diese Form der Zustellung nicht notwendig.

Sofern Nutzer:innen Dokumente nicht mehr digital zugestellt haben möchten, müssen sie ihren Account komplett löschen lassen.

Darstellung Datenschutzmanagementsystem/-organisation

Grundlage von erfolgreichem Datenschutz ist eine gelebte Datenschutzkultur im gesamten Unternehmen und bei allen Lieferanten. Diese Kultur basiert sowohl auf dem richtigen Handeln im Umgang mit personenbezogenen Daten als auch darauf, neue Lösungen und Funktionen direkt mit dem Fokus der Einhaltung des Datenschutzes und – damit verbunden – der IT-Sicherheit zu planen und zu entwickeln. Beides sind u.a. architektonische Grundpfeiler auf denen der bitkasten entwickelt wurde.

Gemäß den Vorgaben aus der DSGVO und den auf die bitkasten AG ausgelegten Prozessen beinhaltet unser Datenschutzmanagementsystem die nachfolgenden Komponenten:

- Verzeichnis von Verarbeitungstätigkeiten: Es werden alle Verarbeitungen von personenbezogenen Daten nach den Vorgaben des Art. 30 DSGVO genau beschrieben.
- Auftragsverarbeitungsvertrag (AVV): Sowohl mit unseren Kunden (Versendern) als auch Dienstleistern schließen wir AVVs, die den Umgang mit personenbezogenen Daten definieren.
- Technische und organisatorische Maßnahmen: Sie definieren die Sicherheit der Daten und belegen die Implementierung angemessener Maßnahmen für einen ausreichenden Schutz.
- Aufbewahrungs-, Lösch- und Notfallkonzepte: Insbesondere die Aufbewahrungs- und Löschkonzepte sind ebenso Bestandteil unseres QMS. Gemäß den rechtlichen Anforderungen löschen wir Daten regelmäßig. Sofern es zu einer Datenpanne kommt, ist ein Meldeprozess implementiert. Zudem werden

Ursachen zur Vermeidung weiterer Vorfälle analysiert und behoben. Berichts- und Meldewege sind an die Mitarbeitenden kommuniziert.

- Datenschutzrichtlinien: Sowohl der Umgang mit personenbezogenen Daten als auch entsprechende Verpflichtungen sowie Nutzungsvereinbarungen sind vorhanden und gelebte Praxis.
- Prozesse zur Einhaltung von Betroffenenrechten: Prozesse zu den unterschiedlichen Rechten der Betroffenen sind definiert und implementiert.

Technische und organisatorische Maßnahmen (TOM) zum Datenschutz

In unseren TOM werden die implementierten Maßnahmen, zum Schutz vom personenbezogenen Daten oder Datenkategorien. Sie beinhalten Maßnahmen zu:

- Vertraulichkeit
- Integrität
- Verfügbarkeit & Belastbarkeit
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Auszug der technischen Maßnahmen

- Verschlüsselung aller Dokumente im Posteingang, Datenträgerverschlüsselung UND Verschlüsselung der einzelnen Dateien
- Einsatz eines Archivs (TR-ESOR-konform, BSI-konform)
- Schutz des bitkasten durch z.B. DDOS-Protection, IP filtering und limiting, Web Application Firewalls und klassische Firewalls
- Zugriff auf Datenbanken nur per VPN
- Regelmäßige Updates für Betriebssysteme, Server- und Client-Software sowie eingesetzte Software-Komponenten
- Regelmäßige Sicherheitsaudits intern und extern
- Regelmäßige Tests von Backups und Wiederherstellung (Disaster Recovery)

Auszug der organisatorischen Maßnahmen

- Regelmäßige Schulungen bzgl. Datenschutz und IT-Sicherheit
- Passwörter mit Komplexitätsanforderungen
- Zugriffsbeschränkung auf absolut notwendige, geschulte, vertrauensvolle Personen
- Sorgfältige Auswahl von Lieferanten
- Schriftliche Weisungen an Lieferanten
- Dauerhafte Überprüfung von Lieferanten

Rechenzentren in Deutschland

Für die Gewährleistung der sicheren Benutzer-Datenspeicherung haben wir uns für ein deutsches Rechenzentrum entschieden. Dieses bietet umfassende Transparenz in Bezug auf Richtlinien, betriebliche

Methoden und Technologien, mit denen der Datenschutz (DSGVO) sichergestellt wird. Die Speicherung der Daten erfolgt ausschließlich in Deutschland. Unser Rechenzentrum erfüllt die nationalen und internationalen Compliance Standards wie z. B. ISO/IEC 27001:2013.

Unser Rechenzentrum verfügt über zwei getrennte Cloud-Instanzen und Backup-Systeme, die in den Data-Centern in Nürnberg und Falkenstein gehostet werden.

- Hohe Ausfallsicherheit und hochverfügbare Infrastruktur
- Garantierte Verfügbarkeit der Systeme 99%
- Wiederanlaufzeit nach Systemausfall unter einer Stunde
- Tägliches, automatisiertes Systembackup

Hetzner Online wurde nach den Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) gemäß DIN ISO/IEC 27001 zertifiziert. Die Infrastruktur und der Betrieb des gesamten Datacenterparks in Nürnberg und Falkenstein/Vogtland wurde durch die FOX Certification geprüft. Dieser international anerkannte Standard bescheinigt der Hetzner Online GmbH, dass geeignete Sicherheitsmechanismen implementiert und adaptiert wurden. Es wird sichergestellt, dass unsere Daten in den Rechenzentren in verantwortungsvollen Händen sind und die Sicherheitsstandards kontinuierlich verbessert und nachhaltig kontrolliert werden.

Berechtigungszertifikate

Berechtigungszertifikat Bundesverwaltungsamt

Wir verfügen über ein Berechtigungszertifikat des Bundesverwaltungsamtes (BSI) zur Nutzung des neuen Personalausweises bzw. um Zugang zu den Ausweisdaten der Empfänger:innen zu erhalten.

Dieses international anerkannte und etablierte Verschlüsselungsverfahren garantiert einen sicheren Datentransfer zwischen Bürger:innen und dem Diensteanbieter.



Berechtigungszertifikat eID-Service Bundesdruckerei

Die Bundesdruckerei hat uns die Berechtigung über die Integration des elektronischen Identitätsnachweises durch die Bereitstellung des eID-Service, Berechtigungszertifikaten und SSL-/TLS-Zertifikaten des Bundesverwaltungsamtes erteilt. Dieses international anerkannte und etablierte Verschlüsselungsverfahren der Bundesdruckerei garantiert einen zuverlässigen und hochsicheren Datenaustausch zwischen Bürger:innen und dem Diensteanbieter.

Informationssicherheit

Unsere Informationssicherheitsleitlinie

Unser Informationssicherheitsmanagementsystem bildet die Grundlage für eine systematische Umsetzung von Informationssicherheit innerhalb des Unternehmens und die Einhaltung von Sicherheitsstandards.

Unsere Kunden vertrauen uns Ihre Daten an und erwarten eine solide IT-Sicherheit sowie entsprechende Prozesse. Wir wissen um die Gefahr von Sicherheitsmängeln für unseren Unternehmenserfolg. Unsere Informationssicherheitsleitlinie adressiert diese Erfordernisse im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb des Unternehmens.

Das Vertrauen unserer Kunden und unser Geschäftserfolg beruhen darauf, dass wir insbesondere:

- die gesetzlichen Vorgaben und nicht zuletzt die Datenschutzgesetze einhalten
- unsere Betriebsgeheimnisse schützen
- die Vertraulichkeit, Integrität und Verfügbarkeit der Daten unserer Kunden wahren
- integre Software sicher ausliefern und verwalten

Aus diesem Grund müssen wir bestehende Risiken für die genannten Ziele erkennen, durch geeignete Maßnahmen vermeiden bzw. mindern und Restrisiken geeignet behandeln.

Vor dem Hintergrund dieser Anforderungen ist Informationssicherheit ein integraler Bestandteil unserer Unternehmenskultur. Wir sind bestrebt, eine starke Informationssicherheitskultur aufzubauen und aufrechtzuerhalten, um die Vertraulichkeit, Integrität und Verfügbarkeit aller Daten und Informationen zu gewährleisten.



Wir leben Sicherheit – DIN EN ISO/IEC 27001:2017!

Im Juni 2023 hat uns die DEKRA bestätigt, dass wir einen großen Fokus auf Sicherheit haben und unser Informationssicherheitsmanagementsystem die Anforderungen bzw. die Normen der DIN EN ISO/IEC 27001:2017 entspricht.

Software Hosted in Germany!

Der Bundesverbands IT-Mittelstand e.V. hat uns im November 2021 das Qualitätssiegel "Software Hosted in Germany" verliehen. Die Auszeichnung zeichnet per Internet nutzbare Software aus, die deutsches Datenschutzrecht und weitere Kriterien berücksichtigt.



Qualitätsmanagement

Unsere Qualitätspolitik

Mit dem bitkasten haben wir, eine einfach zu implementierende Lösung entwickelt. Damit machen wir es Unternehmen einfach, die aktuellen Prozesse auf eine nachhaltige Kommunikation umzustellen und zu digitalisieren. Sie behalten alle Vorteile der Sicherheit (u.a. DSGVO-konform), aber leisten einen großen Beitrag zum Klimaschutz durch einen geringeren CO₂-Fußabdruck – Wegfall von Druck & Transport. Als Nebeneffekt werden Prozesskosten reduziert und eine höhere Kundenzufriedenheit erzielt.

Unsere Qualitätsvision beruht auf den folgenden Prinzipien

- Offenheit und Transparenz
- Mut, Wille und Neugier
- Schnelligkeit
- Flexibilität
- Exzellenter Support
- Fokussierung auf Kernkompetenzen

Um eine kontinuierliche Verbesserung und unseren Anspruch sicherzustellen, prüfen wir Qualität und Ergebnisse regelmäßig durch:

- Evaluation der Prozessqualität durch z.B. Ergebnisse der internen Audits, Erreichung festgelegter Ziele
- Evaluation der Ergebnisqualität durch z.B. Auswertung von Projektergebnissen
- Evaluation der Kundenzufriedenheit durch z.B. Kundenbefragung und der entsprechenden Auswertung

Von uns veranlasste Maßnahmen werden auf ihre Eignung zur Zielerfüllung überprüft und bei Bedarf angepasst. Das Erreichen der Qualitätsansprüche ist für die Geschäftsführung von höchster Priorität und diese stellt daher, die notwendigen materiellen und immateriellen Voraussetzungen zur Durchführung qualitätssichernder Maßnahmen und zur kontinuierlichen Verbesserung zur Verfügung.



Wir leben Qualität – DIN EN ISO 9001:2015!

Eine Zertifizierung mit Fokus auf Qualitätsmanagement, wie die DIN EN ISO 9001, war daher ein logischer Schritt. Im Januar 2022 hat uns die DEKRA unser Bestreben nach Qualität, Kundenzufriedenheit und kontinuierlicher Verbesserung mit der erfolgreichen Zertifizierung gemäß der Norm 9001:2015 bestätigt.

Software Made in Germany!

Der Bundesverbands IT-Mittelstand e.V. hat uns im Januar 2022 das Qualitätssiegel "Software Made in Germany" verliehen. Die Auszeichnung bestätigt, dass der bitkasten durch seine überragende Qualität und Sicherheitsstandards, hohe Investitionssicherheit sowie exzellente Kundenzufriedenheit überzeugt.



Lizenzmodell und Service-Nutzung

Der bitkasten ist ein reines Service-Angebot (SaaS). Das Preismodell für den bitkasten ist nutzungsabhängig.

Für Versender/ Einlieferer von Post:

- Transaktionales Geschäftsmodell
- 100% nutzungs- und nutzenbasiertes Erlösmodell
- Elektronisches Porto für Zustellung, nicht abgeholte Dokumente werden gemäß bestehenden Verträgen gedruckt und berechnet.
- Archivierung in persönlichem Archiv des Nutzers
- Keine Mindestlaufzeit
- Keine Abnahmemengen
- Geringe Anfangsinvestition
- ROI in wenigen Monaten

Die Bereitstellung und Nutzung des bitkasten für den „Empfänger“ via App oder Webzugang ist kostenlos. Die Gebühren trägt der Versender je nach Transaktion auf monatlicher Basis.

Sofern Dokumente nicht elektronisch zugestellt werden, greift Ihr bestehender Druck- und Versandvertrag. Durch das transaktionale Geschäftsmodell bezahlen Sie auch nur, was Sie tatsächlich nutzen. Die Kosten und die Einsparungen sind transparent und nachvollziehbar.

Eine Einführung des bitkasten geht schnell und ohne IT-Projekt – einfach und sicher in 4 Wochen sind Sie live und Ihre Nutzer an Bord. Da wir Ihre vorhandenen Standard-Prozesse und IT-Anwendungen nutzen, ist der Implementierungsaufwand gering.

Wir definieren zusammen einmalig, wie wir Ihr „User-Onboarding“ durchführen und unterstützen Sie bei der Einführung und der unternehmensweiten Kommunikation.

bitkasten AG

Wallensteinstraße 63

90431 Nürnberg

www.bitkasten.de

Kontakt

0911 | 6000 2874

E-Mail: <mailto:iris@bitkasten.de>info@bitkasten.de