



SST AG-Ergebnis Guide

Auskunftsportal & SFTP Datenabruf



SST AG-Ergebnis Guide






Contents

- 1 Übersicht..... 6**
- 1.1 Zielgruppe..... 6
- 1.2 Glossar 6
- 2 Auskunftsportal..... 7**
- 2.1 Voraussetzungen 7
- 2.2 URL..... 7
- 2.3 Login..... 7
- 2.4 Suche..... 8
- 2.5 Datei Download 9
- 2.6 Bereitgestellte Dateien 10
- 2.6.1 ZIP-Archiv-Datei 10
- 2.6.2 Ergebnisdateien im ZIP-Archiv 10
- 2.7 Aufbewahrungsdauer abgeschlossener Vorgänge und automatisches Löschen im POSTIDENT-System 10
- 2.8 Benachrichtigungs-E-Mail bei Betrugsverdachtsfällen..... 11
- 2.9 Benutzerverwaltung 12
- 2.9.1 Erläuterungen zu den Benutzerrollen 13
- 2.9.2 Erläuterungen zu den Rollen der System-Accounts 14
- 2.9.3 Einrichtung der Mehrfachauthentifizierung 14
- 2.9.4 Deaktivierung und Löschung von Benutzern und System-Accounts..... 15
- 3 SFTP..... 16**
- 3.1 Voraussetzungen 16
- 3.2 Protokoll 16
- 3.3 Host..... 17
- 3.4 Bereitgestellte Dateien 17
- 3.4.1 Ergebnisdateien 17
 - ZIP-Archiv-Datei 17
 - Ergebnisdateien im ZIP-Archiv 18
 - Bereitstellungsintervall 18
- 3.4.2 Audiovisuelle Aufzeichnungen 18
 - Namenskonvention der Dateien 18
 - Dateien in ZIP-Archiv-Datei 19
 - Bereitstellungszeit..... 19
- 3.5 Abholen und Löschen von Dateien durch den Geschäftskunden auf dem SFTP-Laufwerk 19
- 3.6 Aufbewahrungsdauer abgeschlossener Vorgänge und automatisches Löschen auf dem SFTP-Laufwerk..... 19
- 4 Ergebnisdateien..... 20**

4.1	Ergebnisdatendatei	20
4.2	Ergebnis-PDF	20
4.3	Weitere Ergebnisdateien (Nachweisdaten)	20
4.4	Signaturdatei.....	21
4.4.1	Überprüfung der Signatur mit RSAPSS.....	21
5	Datenformate und Datenfelder.....	22
5.1	JSON Version v1 (empfohlen)	22
5.2	CSV Version v2.0	22
5.2.1	CSV Version 2.0	22
	Format & Encoding	22
	Datenstruktur.....	22
	Beispiel	23
5.2.2	Datenstruktur CSV	23
5.2.3	Liste der weiteren Ergebnisdateien	31

Änderungshistorie

Datum	Änderung
09.08.2024	Ergänzung Hinweise zu erweiterter Suche
08.07.2024	Ergänzung SFTP Block Cipher um AES GCM Varianten
13.05.2024	Entfernung Ergebnisformat XML
04.04.2024	Dokumentation der SFTP Hostkeys im Kapitel 3. SFTP ergänzt
15.05.2023	eID-Karte für Unionsbürger und EWR-Staatsangehörige ergänzt
25.04.2022	Neues Identverfahren AutoID hinzugefügt
09.08.2021	Kennzeichnung XML als obsolet
18.02.2021	<ul style="list-style-type: none"> Details zur ZIP-Verschlüsselung ergänzt Vom SFTP-Server unterstützte kryptographische Verfahren ergänzt
16.02.2021	Dokumentation zur Benutzerverwaltung im Kapitel 2 ergänzt
23.11.2020	CSV Version 1.3 entfernt, Scan Services entfernt
05.11.2020	Ergänzender Hinweis beim Feld Ausweisnummer
08.05.2020	SHA1DSA Verfahren entfernt
20.04.2020	Ergänzung Identifikationsstatus 205 bei eID-Ident
14.01.2020	Entfernung CSV 1.3, Entfernung Comfort und Special, Markierung Scan als "nur noch unterstützt bis 30.09.2020" Neue Signpad Unterschrift Dateilieferung
19.11.2019	SFTP: Hinweis zur Integritätsprüfung und Löschung überarbeitet
05.08.2019	Anpassungen bei der Datenauslieferung und Portraitfoto für TKG
04.06.2019	Änderungen zum Release 5.3 ab dem 2. Juli 2019 ergänzt: <ul style="list-style-type: none"> Neuer Substatus 19 in den Identifiergebnisdateien Umbenennung nPA in eID
05.04.2019	Änderungen zum Release 5.2 ab dem 7. Mai 2019 ergänzt: Neue Substatus 17 und 18 in den Identifiergebnisdateien
28.03.2019	Neues Signaturverfahren RSAPSS beschrieben SHA1DSA Verfahrens auf obsolet gesetzt
01.02.2019	Wertebereich "Ausweisart" in Identifikationsdaten ergänzt
12.12.2018	Erläuterung zur Signaturdatei ergänzt
14.11.2018	Maximale Aufbewahrungsdauer der Identifizierungsergebnisse auf 90 Tage angepasst
06.08.2018	Abruf via SFTP angepasst: es wird der Zugriff über SHAFB beschrieben Beschreibung der Bereitstellung von audiovisuellen Aufzeichnungen

Datum	Änderung
 26.04.2018	Überarbeitung Neu: weitere Ergebnisdatei 'Unterschrift aus PI-Formular' (ab R4.6)
 16.06.2017	Fraud Manager: kann Betrugsverdachtsfälle im Auskunftsportaal abrufen
 19.04.2017	Fraud Manager: Hinweis auf E-Mail-Benachrichtigung ergänzt
 10.01.2017	Anlagen > Übergreifende Datenstruktur: Statusliste überarbeitet
 02.01.2017	SFTP: Hinweis zur Löschung überarbeitet

1 Übersicht

Geschäftskunden können die Ergebnisdateien Ihrer Identifikationsvorgänge mit POSTIDENT auf folgenden Wegen abholen:

1. **Auskunftsportal:** Manueller Abruf in einem Web-Portal; Beschreibung in diesem Dokument
2. **SFTP-Schnittstelle:** Automatisierter Abruf via SFTP; Beschreibung in diesem Dokument
3. **REST API SCR-Ident:** Automatisierter Abruf via REST; Beschreibung im Dokument "SCR-Ident API Guide"; den Download finden Sie unter dieser URL: <http://www.postident.de/handbuch>

Die Bereitstellung ist abhängig vom Status des Vorgangs und Ihrer POSTIDENT Konfiguration.

Außerdem werden über die **SFTP-Schnittstelle** die audiovisuellen Aufzeichnungen der Videochats für die Geschäftskunden bereitgestellt. Diese audiovisuellen Aufzeichnungen sind für eine GwG-konforme Identifikation per Videochat erforderlich und sind somit für Geschäftskunden, die GwG verpflichtet sind, obligatorisch. Beschreibung im Kapitel 3. SFTP.

1.1 Zielgruppe

Dieses Dokument richtet sich an Nutzer des Auskunftsportals und Entwickler, die Identifikationen mit POSTIDENT in ihre Anwendung integrieren möchten.

1.2 Glossar

Begriff	Beschreibung
Geschäftskunde	Auftraggeber (AG) für die Identifikation mit POSTIDENT
Abrechnungsnummer / ClientId	Identifier für die POSTIDENT Konfiguration und die Abrechnung von Identifikationsvorgängen
Nutzer	Endkunde, der identifiziert werden möchte
Identifikationsvorgang, Vorgang	Container für eine oder mehrere Identifikationen eines Nutzers
Identifikation	Identifikation eines Nutzers mit einem Verfahren
Verfahren	POSTIDENT kann von Nutzern mit folgenden Verfahren durchgeführt werden (in alphabet. Reihenfolge): <ul style="list-style-type: none"> • POSTIDENT durch AutoID • POSTIDENT durch Foto (kurz Foto) • POSTIDENT durch Postfiliale (kurz Basic) • POSTIDENT durch Videochat (kurz Video) • POSTIDENT mit neuem Personalausweis (kurz eID)
Audiovisuelle Aufzeichnungen	Bei einer Videoidentifizierung nach GWG ist die audiovisuelle Aufzeichnung des Videochats erforderlich. Diese Aufzeichnung muss GK samt Identifiergebnissen aufbewahren (s. BaFin Rundschreiben von 2017 https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.htm)

2 Auskunftsportal

Manueller Abruf der Ergebnisdaten von POSTIDENT Vorgängen in einem Web-Portal durch Ihre Mitarbeiter.

2.1 Voraussetzungen

Jeder Ihrer Mitarbeiter oder Mitarbeiterinnen, der/die das Auskunftsportal benutzen soll, benötigt zum Login einen Benutzer-Account mit Benutzername und Passwort. Die Benutzer-Accounts richtet das DPAG-Service-Team ein. Für jeden Benutzer-Account erhält der jeweilige Benutzer / die jeweilige Benutzerin zudem ein Datenpasswort, mit dem er / sie die verschlüsselt bereitgestellten Daten nach dem Abruf entschlüsseln kann. Die Verschlüsselung verwendet die sogenannte WinZip-AES Verschlüsselung (basierend auf AES256 CTR), die von gebräuchlicher Zip-Software unterstützt wird.

2.2 URL

<https://postident.deutschepost.de/auskunftsportal>

2.3 Login

Bei Aufruf der o.g. URL wird der Login des Auskunftsportals angezeigt.

Dort geben Sie bitte den Benutzernamen und das Passwort des Auskunftsportalnutzers ein. Bestätigen Sie dann mit Enter bzw. durch Drücken des "Login"-Buttons.



Login

[> Passwort vergessen?](#)

[> Passwort ändern](#)

Kontakt: 06151/908-8000 oder serviceteam.postident@deutschepost.de - Geschäftszeiten: Mo-Do 8-17 Uhr, Fr 8-16 Uhr

© 2016 Deutsche Post AG

[Über die Deutsche Post](#) | [Impressum](#) | [Datenschutz](#) | [Rechtliche Hinweise](#)

2.4 Suche

Nach erfolgreichem Login wird eine Vorgangssuche angezeigt. Hier ist eine einfache und eine erweiterte Suche möglich.

Kontakt: 06151/908-8000 oder serviceteam.postident@deutschepost.de - Geschäftszeiten: Mo-Do 8-17 Uhr, Fr 8-16 Uhr

© 2016 Deutsche Post AG

[Über die Deutsche Post](#) | [Impressum](#) | [Datenschutz](#) | [Rechtliche Hinweise](#)

Der Suchbereich

Hier kann die Ergebnismenge eingeschränkt werden. Hierzu stehen folgende Möglichkeiten zur Verfügung:

- **Abrechnungsnummer (ClientID)**
Die Suche kann auf einzelne Abrechnungsnummern (ClientIDs) begrenzt oder Ergebnisse für alle ausgewählten Abrechnungsnummern angezeigt werden. Die Mehrfachauswahl ist durch Klick auf die entsprechenden Abrechnungsnummern und gleichzeitigem Drücken der Strg-Taste möglich.
- **Zeitraum**
Definition des gewünschten Suchzeitraums bezogen auf das Änderungsdatum der Vorgänge. Die Eingabe des "von"-Feldes ist obligatorisch. Das Ende des Suchzeitraums ("bis"-Feld) muss größer oder gleich dem Beginn sein. Beide Datums-Eingaben dürfen nicht in der Zukunft liegen und müssen im Format TT.MM.JJJJ HH:MM angegeben werden.

Bei Nutzung der **erweiterten Suche** haben Sie zusätzlich Zugriff auf die folgenden Suchfelder:


- Vorgangsnummer
- Referenznummer
- Nachname
- Vorname

Sie haben bei allen oben genannten Feldern die Möglichkeit, mit "%" eine Wildcard-Suche durchzuführen, d.h. einen Platzhalter für Teile Ihres Suchbegriffs zu verwenden:

- <Suchstring>% : Alle Identifiergebnisse, die mit <Suchstring> anfangen, werden gesucht.
 - z.B. Ann% → Ann, Anné, Anna, Anna Maria, Anne-Sophie
- %<Suchstring>: Alle Identifiergebnisse, die mit <Suchstring> enden, werden gesucht.
 - z.B. %lina → Alina, Paulina
- %<Suchstring>%: Alle Identifiergebnisse, die <Suchstring> beinhalten, werden gesucht.
 - z.B. %man% → Mustermann, Manfred, Manuela


Der Ergebnisbereich


Nach Betätigen des "Suche"-Buttons werden die Ergebnisse in Form einer Tabelle angezeigt. Die Tabelle beinhaltet folgende Spalten:

- Vorgangsnummer
- Referenznummer
- Nachname
- Vorname
- Änderungszeitpunkt
- Vorgangstatus
- Verfahren
- Ident-Status
- Ident-Substatus
-  (Vorgang herunterladen)

Hinweis: Weitere Informationen über die genannten Datenfeldern finden Sie im Kapitel 5. Datenformate und Datenfelder.

2.5 Datei Download

Durch Betätigen des Buttons  hinter jedem Vorgang, können Ergebnisdaten und weitere Dateien heruntergeladen werden.


POSTIDENT Auskunftportal
A.ABNAHME



Suche

Abrechnungsnummer (ClientID) ?

50747250573701 (50747250573701)

50747250573703 (CAB051FF)

50747250573710 (50747250573710)

Zeitraum von  bis  ?






Erweiterte Suche ▾

Suchen

Downloadoptionen Identifikationsdaten Nachweisdaten Ergebnis-PDF

Ausgewählte Einträge (2) Herunterladen

4 Ergebnisse

<input type="checkbox"/>	Vorgangsnummer	Referenznummer	Nachname	Vorname	Änderungszeitpunkt ▾	Vorgangstatus	Verfahren	Ident-Status	Ident-Substatus	
<input type="checkbox"/>	B81HYXVD2VYX	1426948528	Blanko	Frank	24.06.2016 12:14 Uhr	geschlossen	Video	erfolgreich		
<input checked="" type="checkbox"/>	QVZAPHJBEBYC	446366307	Vorl	Max	24.06.2016 10:08 Uhr	geschlossen	Video	erfolgreich		
<input type="checkbox"/>	0VAZ6954Z680	1770185383	Seid	Frank	24.06.2016 09:46 Uhr	geschlossen	Video	erfolgreich		
<input checked="" type="checkbox"/>	FY0RHQE4ZBYX	1483515924	Mustermann	Max	24.06.2016 09:38 Uhr	geschlossen	Video	erfolgreich		

Kontakt: 06151/908-8000 oder serviceteam.postident@deutschepost.de - Geschäftszeiten: Mo-Do 8-17 Uhr, Fr 8-16 Uhr

© 2016 Deutsche Post AG

Über die Deutsche Post | Impressum | Datenschutz | Rechtliche Hinweise

Neben dem Download einzelner Vorgänge können auch mehrere oder alle angezeigten Vorgänge gemeinsam heruntergeladen werden. Die Auswahl von Vorgängen erfolgt über Auswahlhaken vor jedem Eintrag in der Ergebnisliste bzw. mit dem Auswahlhaken in der ersten Spalte Tabellenüberschrift, um alle angezeigten Einträge auszuwählen. Mithilfe des

Download-Buttons oberhalb des Suchergebnisses () werden alle ausgewählten Vorgänge herunter geladen.

Die Downloadoptionen steuern, welche Ergebnisdateien in welchem Format heruntergeladen werden sollen. Dies betrifft sowohl den Download einzelner als auch mehrerer Vorgänge.

2.6 Bereitgestellte Dateien

2.6.1 ZIP-Archiv-Datei


Alle Dateien werden in ein Archiv (ZIP) verpackt, mit dem Datenpasswort des eingeloggten Users verschlüsselt und heruntergeladen. Die Verschlüsselung verwendet die sogenannte WinZip-AES Verschlüsselung (basierend auf AES256 CTR), die von gebräuchlicher Zip-Software unterstützt wird.

2.6.2 Ergebnisdateien im ZIP-Archiv

Abhängig von Ihrer POSTIDENT Konfiguration und den genutzten Verfahren können im ZIP-Archiv je Vorgang folgende Ergebnisdateien enthalten sein:


- **Ergebnisdatendatei** in einem der verfügbaren Datenformate
- **Ergebnis-PDF-Datei(en)** in einer oder mehreren verfügbaren PDF-Varianten
- **Nachweisdatendatei(en)** wie Bilder von Nutzer, Ausweis, Unterschrift

Datenformat, PDF-Varianten und Nachweisdateien werden vom DPAG-Service-Team nach Ihren Wünschen in Ihrer POSTIDENT Konfiguration eingestellt und aktiviert.

 Die Ergebnisdateien werden erst ab dem Zeitpunkt der Aktivierung in Ihrer POSTIDENT Konfiguration erstellt. Einige PDF-Varianten und Nachweisdaten unterliegen gesetzlichen Beschränkungen (bspw. Ausweisbilder) und können nur erstellt/ausgeliefert werden, sofern die gesetzlichen Voraussetzungen erfüllt sind.

2.7 Aufbewahrungsdauer abgeschlossener Vorgänge und automatisches Löschen im POSTIDENT-System

Aus Datenschutzgründen müssen abgeschlossene Vorgänge nach Ablauf einer max. Aufbewahrungsdauer von 90 Tagen vom POSTIDENT-System gelöscht werden. Sie können die Aufbewahrungsdauer für jede Ihre POSTIDENT-Konfigurationen auch kürzer festlegen. Einstellbar sind 5-90 Tage nach Abschluss des Vorgangs. Danach werden die Vorgänge inkl. aller Daten unwiderruflich aus dem POSTIDENT-System gelöscht.

 Nach Ablauf der Aufbewahrungsdauer stehen die Ergebnisdaten der Vorgänge auch nicht mehr via Auskunftportal zur Verfügung.

2.8 Benachrichtigungs-E-Mail bei Betrugsverdachtsfällen

Sie können für einen oder mehrere Ihrer Mitarbeiter jeweils einen Benutzer-Account mit der Rolle "Fraud Manager" anlegen lassen. Diese Benutzer sind berechtigt, Vorgänge abzurufen, die als "Betrugsverdacht" oder als "Identifikation mit Auffälligkeiten" markiert wurden.

Nutzer mit dieser Rolle werden automatisch per E-Mail informiert, sobald neue Betrugsverdachtsfälle vorliegen. Der Versand der E-Mail erfolgt aggregiert alle 4 Stunden.

Die E-Mail enthält einen Deeplink in das Auskunftportal, der (nach dem erfolgreichen Login) die Suchkriterien mit Abrechnungsnummer/ClientId und Zeitraum vorbelegt. Die Suche wird automatisch ausgeführt, so dass sofort die in der E-Mail aufgeführten Vorgänge eingeblendet werden.



Guten Tag Max Mustermann,

im POSTIDENT System wurden im Zeitraum von 02.05.2022, 08:01 Uhr bis 02.05.2022, 12:01 Uhr neue Betrugsverdachtsfälle festgestellt:

Geschäftskunde:	Demobank24
Abrechnungsnummer:	50747250573744
POSTIDENT durch Foto	1 Vorgang
POSTIDENT durch Videochat	2 Vorgänge
POSTIDENT in der Filiale	1 Vorgang
Postident durch Online-Ausweisfunktion	1 Vorgang
POSTIDENT durch AutoID	1 Vorgang

Vorgänge im Auskunftportal öffnen

Bei Rückfragen wenden Sie sich bitte an das Serviceteam Postident:
 E-Mail: serviceteam.postident@deutschepost.de
 Telefon: +49 228 / 182 - 19444

Mit freundlichen Grüßen
 Ihr Kundenservice BRIEF

© 2022 Deutsche Post AG
 Impressum

2.9 Benutzerverwaltung

Sie haben die Möglichkeit im Auskunftsportal eigene Benutzer und System-Accounts für das Postident System zu verwalten. Dafür wird ein Benutzer in der Rolle "Benutzer-Verwaltung" benötigt. Die erstmalige Berechtigung eigene Benutzer zu verwalten, wird durch das Postident Serviceteam vergeben. Der Benutzer in der Rolle "Benutzer-Verwaltung" kann die Daten aller Benutzer und System-Accounts einer EKP verwalten, unabhängig davon, welchen Abrechnungsnummern diese zugeordnet sind.

The screenshot shows the 'Benutzerverwaltung' page in the POSTIDENT Auskunftsportal. The page has a yellow header with the logo and the user 'K.NORDMANN'. A left sidebar contains navigation options: 'Identergebnisse', 'Konfigurationen', and 'Benutzerverwaltung'. The main content area is titled 'Benutzerverwaltung' and is split into two sections:

- Benutzer-Accounts:** A table with one entry:

Benutzername	Rolle(n)	Vorname	Nachname	Ort	Anzahl GK-Konfigurationen
K.NORDMANN	Benutzer-Verwaltung, Portal Ergebnisdaten	Kari	Nordmann	Engelskirchen	2

 Below the table is a '+ Neuer Account' button.
- System-Accounts:** A table with two entries:

Benutzername	Rolle(n)	Vorname	Nachname	Ort	Anzahl GK-Konfigurationen
NORDMANN.SFTP	SFTP Ergebnisdaten	Kari	Nordmann	Engelskirchen	1
BD.SCR	REST SCR-Ident	Brigitte	Dörrenberg	Engelskirchen	2

 Below the table is a '+ Neuer Account' button.

In der Benutzerverwaltung stehen Ihnen folgende Funktionalitäten zur Verfügung:

- Anlegen von neuen Benutzern und neuen System-Accounts
- Bearbeiten der Daten Ihrer Benutzer und System-Accounts
- Änderung der Berechtigungen der Benutzer und System-Accounts für die einzelnen Abrechnungsnummern
- Vergabe der Passwörter zur Authentifizierung
- Vergabe der Datenpasswörter zum Verschlüsseln der Ergebnisdaten
- Abfrage der Datenpasswörter einzelner Benutzer bzw. System-Accounts
- Löschen von Benutzer und System-Accounts

System-Account Brigitte Dörrenberg 🗑️ 🔧 Bearbeiten

System-Account

Rolle(n): REST SCR-Alive, REST SCR-Alive, REST SCR-Ident, REST SCR-Signing, REST SCR-Signing

Hauptansprechpartner: Hauptansprechpartner wird bei Ankündigungen von Änderungen bzgl. POSTIDENT informiert.

Gesperrt:

Benutzername:

Angaben zur Person

Vorname:

Nachname:

Name des Unternehmens:

Anschrift:

Telefonnummer:

Kommunikations-E-Mail-Adresse: Diese E-Mail-Adresse wird vom POSTIDENT Serviceteam genutzt, um Änderungen und Neuentwicklungen in POSTIDENT zu kommunizieren.

Passwort generieren

Datenpasswort generieren Mit dem Datenpasswort werden die Ergebnisdaten verschlüsselt.

Ident-Konfigurationen

	Abt.-Nr.	Client ID	Anzeigename	Klasse	Verfahren	Anbindung	Partner	Kurzbezeichnung
✓	77889900303701	e89FFE8C		GwG	eID	REST SCR		
✓	77889900303702	A695A85e		GwG	Video mit Ausweisbildern, eID, Postfiliale	Easy Connect REST SCR		

Signing-Konfigurationen

2.9.1 Erläuterungen zu den Benutzerrollen

Benutzerrolle	Erläuterung
Portal Ergebnisdaten	Der Benutzer hat die Berechtigung im Auskunftsportale Ergebnisse der Identifizierungen abzurufen.
Portal Fraudmanager	Der Benutzer hat die Berechtigung auf Detailinformationen zu Betrugsverdachtsfällen zuzugreifen. Aktivieren Sie dazu in den Downloadoptionen „Betrugsverdachtsmeldung-PDF“.
Benutzer-Verwaltung	<p>Der Benutzer hat die Berechtigung Benutzer- und System-Accounts für Ihren Geschäftskunden anzulegen, zu bearbeiten und zu löschen. Außerdem kann er Zugangsdaten für diese Benutzer erzeugen. Da die Benutzer dieser Rolle auf besonders sensible Daten (z.B. Passwörter) zugreifen können, muss der Zugang über einen 2. Faktor bei der Authentisierung geschützt werden. Weitere Details dazu finden Sie im Kapitel "Einrichtung der 2-Faktorauthentisierung".</p> <p>⚠️ Im Sinne der Funktionstrennung empfehlen wir es <u>nicht</u> Benutzern mit dieser Rolle noch weitere Rollen zuzuordnen.</p>

2.9.2 Erläuterungen zu den Rollen der System-Accounts


Benutzerrolle	Erläuterung
REST SCR-Ident	Der Benutzer hat die Berechtigung über REST SCR-Ident Schnittstelle Identifikationsvorgänge anzulegen und Ergebnisdaten dazu abzufragen, s. dazu die Dokumentationen "Standard Connect & Result Ident REST API Guide ..." unter https://www.deutschepost.de/de/p/postident/downloads.html
REST SCR-Signing	Der Benutzer hat die Berechtigung über REST SCR-Signing Schnittstelle Signaturvorgänge anzulegen, die signierten Dokumente abzufragen und die Identifiergebnisse dazu über REST SCR-Ident Schnittstelle abzufragen, siehe dazu auch die Dokumentation "Schnittstellenbeschreibung SCR-Signing für POSTIDENT E-Signing" unter https://www.deutschepost.de/de/p/postident/downloads.html
REST SCR-Alive	Der Benutzer hat die Berechtigung die Verfügbarkeit des Postident Systems über REST SCR-Ident Schnittstelle abzurufen, siehe Dokumentation "Standard Connect & Result Ident REST API Guide 1 Start" unter https://www.deutschepost.de/de/p/postident/downloads.html
SFTP Ergebnisdaten	Der Benutzer hat die Berechtigung die Identifizierungs- und Signaturergebnisse über SFTP abzurufen, siehe Abschnitt "3. SFTP". Dieser Benutzer authentifiziert sich nicht mit einem Passwort an unserem SFTP Server, sondern mittels RSA Keys. Den entsprechenden Public Key können Sie in der Benutzerverwaltung einsehen und ändern.
SOAP Heavy-Light-Connect	Der Benutzer hat die Berechtigung Identvorgänge über die SOAP Schnittstelle anzulegen.

2.9.3 Einrichtung der Mehrfachauthentifizierung

Als zweiter Faktor muss eine Authentisierungs-Applikation auf dem Smartphone des Benutzers verwendet werden. Die Einrichtung ist nachfolgend beschrieben:

1. Ein Benutzer installiert zunächst eine Authentisierungs-Applikation, z.B. Authy, FreeOTP, Google Authenticator, Microsoft Authenticator auf seinem Smartphone.
2. Der Benutzer meldet sich im Auskunftportal an und erhält nach der Eingabe des Passworts die Eingabemaske "Mehrfachauthentifizierung konfigurieren".
3. In der Authentisierungs-Applikation fügt der Benutzer einen neuen Account hinzu (z.B. "Add Account" in Authy) und scannt dafür den angezeigten QR Code.
Die Authentisierungs-Applikation gibt dann einen sechsstelligen Code aus, den der Benutzer in das Eingabefeld eintragen muss. Nach dem Absenden des Codes ist die Einrichtung abgeschlossen.

Mehrfachauthentifizierung konfigurieren

 Sie müssen eine Mehrfachauthentifizierung einrichten, um das Benutzerkonto zu aktivieren.

1. Installieren Sie eine der folgenden Applikationen auf Ihrem Smartphone:

- FreeOTP
- Google Authenticator

2. Öffnen Sie die Applikation und scannen Sie den Barcode.



Sie können den Barcode nicht scannen?

3. Geben Sie den von der Applikation generierten One-time Code ein und klicken Sie auf Speichern.

Absenden

2.9.4 Deaktivierung und Löschung von Benutzern und System-Accounts

Aus sicherheitstechnischen Gründen werden die Benutzer-Accounts nach 120 Tagen Inaktivität deaktiviert. Falls der Zugang nach der Deaktivierung noch benötigt wird, melden Sie sich bitte bei Ihrem Benutzerverwalter oder beim Serviceteam POSTIDENT um Ihren Zugang wieder aktivieren zu lassen. Wird der Zugang nicht wieder aktiviert, wird Ihr Account 60 Tage nach der Deaktivierung gelöscht. Die System-Accounts nach 180 Tagen Inaktivität deaktiviert.

3 SFTP

Automatisierter Abruf der Ergebnisdaten von POSTIDENT Vorgängen und audiovisuellen Aufzeichnungen des Videochats von einem SFTP Server.

3.1 Voraussetzungen

Die Bereitstellung via SFTP muss in Ihrer POSTIDENT Konfiguration durch das DPAG-Serviceteam aktiviert werden.

Jedes Ihrer IT-Systeme, das Daten via SFTP abrufen soll, benötigt für den Zugriff auf die SFTP-Schnittstelle einen System-Account mit Benutzernamen und Public Key (Vorgaben für den Key: RSA Public Key mit einer Länge von mindestens 3072bit im Open SSH-Format).

Den System-Account richtet entweder das DPAG-Serviceteam ein, oder Sie selber, sofern Sie Ihre Benutzer im Auskunftsportal administrieren. Für jeden System-Account erhalten Sie zudem ein Datenpasswort, mit dem Sie die verschlüsselt bereitgestellten Daten nach dem Abruf entschlüsseln können.

3.2 Protokoll

Es wird das Secure File Transfer Protocol (SFTP) verwendet.

Die folgenden kryptographischen Verfahren werden vom Server unterstützt:

Block Encryption:

- AEAD_AES_256_GCM (aes256-gcm@openssh.com) (**recommended**)
- AEAD_AES_128_GCM (aes128-gcm@openssh.com)
- aes256-ctr
- aes128-ctr
- aes192-ctr

Key Exchange:

- diffie-hellman-group14-sha256 (**recommended**)
- diffie-hellman-group15-sha512
- diffie-hellman-group16-sha512
- diffie-hellman-group-exchange-sha256 (modulo size ≥ 2048 and ≤ 8192)

Message Authentication Code:

- hmac-sha2-256
- hmac-sha2-512

HostKey Algorithmus:

- ed-25519 (**recommended**)
- rsa-sha2-512
- rsa-sha2-256

Bekannte Hosts aktualisieren: Um den neuen Schlüssel sicher zu Ihrer Datei „known_hosts“ hinzuzufügen, entfernen Sie zunächst den alten Eintrag für unseren Server aus der Datei (dieser befindet sich normalerweise in `~/.ssh/known_hosts`) und stellen Sie dann über Ihren SFTP-Client eine Verbindung zum Server her, um den neuen Schlüssel zu akzeptieren, oder fügen Sie den von ssh-keyscan erhaltenen Schlüssel manuell zur Datei „known_hosts“ hinzu.

Stellen Sie unbedingt sicher, dass Sie der Quelle des SSH-Schlüssels vertrauen. Die manuelle Überprüfung des Schlüsselfingerabdrucks mit dem von uns bereitgestellten Fingerabdruck erhöht Ihre Sicherheit, indem bestätigt wird, dass Sie eine sichere Verbindung zum echten Server herstellen.

Überprüfen Sie den neuen SSH-Schlüssel: Nach dem Update erhalten Sie bei der ersten Verbindung zum SFTP-Server eine Benachrichtigung, dass sich der Hostschlüssel geändert hat, sofern Sie die Datei „known_hosts“ nicht zuvor manuell

aktualisiert haben. Um die Sicherheit Ihrer Verbindung zu gewährleisten, ist es wichtig, dass Sie den Fingerabdruck des neuen SSH-Schlüssels überprüfen, bevor Sie fortfahren.

Der neue Fingerabdruck des öffentlichen SSH-Schlüssels lautet:

Integrations- und Testumgebung

```
Ed25519 Public Key MCowBQYDK2VwAyEApyD7vMQe5osn0a659RBF7Hs5dtCBvk08ZdggYdy9FQ=
```

```
Ed25519 Public Key Fingerprint SHA256:+tmHr71+iqWQBtluwH5y1HJgSrUI0ucIAmwbIJSldCo
```

```
Ed25519 Public Key Fingerprint MD5:74:a4:e1:0c:57:81:ff:44:b0:d6:89:d3:72:66:c2:3f
```

```
RSA Public Key Fingerprint SHA256:vzYyGqkYQIfcVjmhKlXe1QU7PuZPiGzrvlW9r0vQvRs
```

```
RSA Public Key Fingerprint MD5:3b:07:f9:92:ca:20:6e:61:7f:00:ad:1e:7b:61:16:84
```

Produktionsumgebung ab Release 21, 09.07.24:

```
Ed25519 Public Key MCowBQYDK2VwAyEA9gq9TjaFjxo9i6MFeCRxUAZzhgZErEbMubndkthxDmc=
```

```
Ed25519 Public Key Fingerprint SHA256:MzIEMQ6Vq+bAJ5X1CuCBbVo7pkAw0PHOakAwLK+79/Y
```

```
Ed25519 Public Key Fingerprint MD5:9a:74:4d:36:73:93:3b:6a:de:d0:7b:40:9e:c1:11:ac
```

```
RSA Public Key Fingerprint SHA256:MRA6iDLbCXc/l/cx5u0GZbYMa/cjL+dFYOM2PFAGIdA
```

```
RSA Public Key Fingerprint MD5:bb:35:08:a4:79:c5:bd:d6:d6:4a:91:ff:24:1b:89:2c
```

3.3 Host

```
postident-transfer.deutschepost.de (149.239.125.97) Port 22
```

3.4 Bereitgestellte Dateien

Über SFTP werden den Geschäftskunden Ergebnisdateien zu den durchgeführten Identvorgängen und audiovisuellen Aufzeichnungen des Videochats im Fall von Videoidentifikation nach GWG bereitgestellt. Alle Dateien werden in ein Archiv (ZIP) verpackt, mit dem Datenpasswort des SFTP System-Accounts verschlüsselt und im SFTP-Laufwerk bereitgestellt. Die Verschlüsselung verwendet die sogenannte WinZip-AES Verschlüsselung (basierend auf AES256 CTR), die von gebräuchlicher Zip-Software unterstützt wird.

3.4.1 Ergebnisdateien

ZIP-Archiv-Datei

Namensschema:

```
POSTIDENT_<BENUTZERNAME>_<ABRECHNUNGSNUMMER>_<DATUM_VON>_<UHRZEIT_VON>_<DATUM_BIS>_<UHRZEIT_BIS>.zip
```

Parametername	Beschreibung	Beispiel
BENUTZERNAME	System-Benutzername für den SFTP Zugriff	NUTZER.SFTP
ABRECHNUNGSNUMMER	Abrechnungsnummer der ausgelieferten Vorgänge	50747250573701
DATUM_VON	Anfangszeitpunkt zur Auswahl der Vorgänge in der Auslieferung	20160406
UHRZEIT_VON	dito	113000
DATUM_BIS	Endzeitpunkt zur Auswahl der Vorgänge in der Auslieferung	20160406
UHRZEIT_BIS	dito	123000

z.B. `POSTIDENT_NUTZER.SFTP_50747250573701_20160406_113000_20160406_123000.zip`


Ergebnisdateien im ZIP-Archiv

Abhängig von Ihrer POSTIDENT Konfiguration und den genutzten Verfahren können im ZIP-Archiv je Vorgang folgende Ergebnisdateien enthalten sein:

- **Ergebnisdatendatei** in einem der verfügbaren Datenformate
- **Ergebnis-PDF-Datei(en)** in einer oder mehreren verfügbaren PDF-Varianten
- **Nachweisdatendatei(en)** wie Bilder von Nutzer, Ausweis, Unterschrift
- **Signaturdateien**, falls konfiguriert

Ausführliche Informationen zu den Ergebnisdateien finden Sie im Kapitel [4. Ergebnisdateien](#)

Datenformat, PDF-Varianten und Nachweisdateien werden vom DPAG-Serviceteam nach Ihren Wünschen in Ihrer POSTIDENT Konfiguration eingestellt und aktiviert.

 Alle Dateien werden erst ab dem Zeitpunkt der Aktivierung in Ihrer POSTIDENT Konfiguration erstellt. Einige PDF-Varianten und Nachweisdaten unterliegen gesetzlichen Beschränkungen (bspw. Ausweisbilder) und können nur erstellt/ausgeliefert werden, sofern die gesetzlichen Voraussetzungen erfüllt sind.

Bereitstellungsintervall

Das Bereitstellungsintervall wird mit Ihnen abgestimmt, bspw. stündlich oder täglich. Sollten in einen Zeitraum **keine** Vorgänge fallen, so wird ein leeres Archiv (Größe 0 Byte) bereitgestellt. Dadurch können Sie Ihre Verbindung und Bereitstellung einfach validieren.

3.4.2 Audiovisuelle Aufzeichnungen

Namenskonvention der Dateien

Namensschema der ZIP-Dateien: VIDEOCHATRECORDING_< BENUTZERNAME >_< ABRECHNUNGSNUMMER >_<VORGANGS_NR>.zip

Namensschema der Videodatei: VIDEOCHATRECORDING_<BENUTZERNAME>_<ABRECHNUNGSNUMMER>_<VORGANGS_NR>.webm

Parametername	Beschreibung	Beispiel
BENUTZERNAME	System-Benutzername für den SFTP Zugriff	NUTZER.SFTP
ABRECHNUNGSNUMMER	Abrechnungsnummer der ausgelieferten Vorgänge	50747250573701
VORGANGS_NR	Vorgangs-Nr der Videoidentifikation	YTCZ29ZUZVYC

z.B. VIDEOCHATRECORDING_PIFTDEMOBANK24_11235813523701_YTCZ29ZUZVYC.zip und VIDEOCHATRECORDING_PIFTDEMOBANK24_11235813523701_YTCZ29ZUZVYC.webm

Dateien in ZIP-Archiv-Datei

Eine ZIP-Archiv-Datei enthält eine audiovisuelle Aufzeichnung für genau eine Videoidentifikation, eine webm-Datei im VP8 Format. Die Dateigröße kann zwischen 80 und 150 MB liegen. Zum Anschauen der Videoaufzeichnungen empfehlen wir als Player den Firefox Browser.


Außerdem befindet sich die Signatur der Videodatei (*.sig) in dem ZIP-Archiv, siehe auch Abschnitt [Signaturdatei](#).

Bereitstellungszeit

Die audiovisuellen Aufzeichnungen werden pro Vorgang kurz nach der Durchführung der Videoidentifikation ausgeliefert, dies kann einige Minuten dauern und auch einige Minuten (aber maximal 1 Tag) nach dem Empfang von dem finalen Webhook (falls konfiguriert) erfolgen.

3.5 Abholen und Löschen von Dateien durch den Geschäftskunden auf dem SFTP-Laufwerk

Die auf dem SFTP-Laufwerk bereitgestellten Dateien werden **nicht automatisch** nach dem Abholen gelöscht. Somit behalten Sie die volle Kontrolle über das Löschen Ihrer Dateien.

 Bitte überprüfen Sie direkt nach dem Herunterladen die Integrität der Dateien (durch Entschlüsselung des Zip-Archivs und die Überprüfung der enthaltenen Signatur-Dateien, sofern diese in Ihrer Konfiguration aktiviert sind). Nach erfolgreicher Prüfung der Integrität sollten Sie die Dateien zudem **umgehend** von unserem SFTP-Laufwerk löschen. Dies ist nötig, um nicht die für Sie reservierten Speicherplatzgrenzen zu überschreiten, Ihre spezifischen Datenschutzlöschfristen zu erfüllen und mehrfaches Herunterladen und Verarbeiten derselben Datei zu verhindern.

3.6 Aufbewahrungsdauer abgeschlossener Vorgänge und automatisches Löschen auf dem SFTP-Laufwerk

Aus Datenschutzgründen müssen abgeschlossene Vorgänge nach Ablauf einer Aufbewahrungsdauer von max. 90 Tagen vom POSTIDENT-System gelöscht werden. Alle Dateien auf dem SFTP-Laufwerk, die älter als 90 Tage sind, werden automatisch gelöscht.

Eine Ausnahme stellen die audiovisuellen Aufzeichnungen dar, diese werden bereits 30 Tage nach Bereitstellung auf dem SFTP-Laufwerk gelöscht und diese Aufbewahrungsdauer ist nicht konfigurierbar.

4 Ergebnisdateien

4.1 Ergebnisdatendatei

Die Ergebnisdatendatei enthält die Daten zu einem oder mehreren Identvorgängen. Sie können in folgenden Formaten bereitgestellt werden:

Datenformat	Versionen	Beschreibung
JSON (empfohlen)	v1	Die Daten der ausgewählten Vorgänge in Form <i>mehrerer</i> JSON-Dateien (eine Datei je Vorgang). Beschreibung der Datenstruktur siehe Dokument "SCR-Ident API Guide" (Download-Link siehe Kapitel 1 Übersicht oben)
CSV	2.0	Die Daten der ausgewählten Vorgänge in Form <i>einer</i> CSV-Datei. Beschreibung der Datenstruktur siehe Kapitel 5 Datenformate und Datenfelder. Falls bei Anbindung mit der REST API SCR an Stelle von JSON das Datenformat CSV konfiguriert sein sollte, werden die Daten auf das Format CSV 2.0 gemapped.

i Das empfohlene Datenformat ist JSON v1. Anders als bei CSV ist die Datenstruktur von JSON v1 modernisiert und enthält die kompletten Ergebnisdaten eines Vorgangs. Außerdem sind die Dateinamen der weiteren Ergebnisdateien einheitlich.

4.2 Ergebnis-PDF

Zu jedem abgeschlossenen Vorgang kann auf Wunsch ein Ergebnis-PDF erstellt werden. Das Ergebnis-PDF enthält die wichtigsten Ergebnisdaten sowie auf Wunsch weitere Nachweisdaten wie Bilder von Person, Ausweis und Unterschrift. Eine detaillierte Beschreibung des Ergebnis-PDFs finden Sie im Dokument "Result PDF Guide".

Sie können das Ergebnis-PDF in drei Varianten erhalten:

1. komplett, d.h. Daten und Bilder
2. nur Daten
3. nur Bilder

Die Varianten 2 und 3 können aus Datenschutzgründen für die Bearbeitung in Ihrem Hause erforderlich sein.

Die Erstellung und Bereitstellung der Ergebnis-PDF-Dateien muss vom DPAG-Serviceteam für ihre POSTIDENT-Konfiguration aktiviert werden.

i Die Ergebnis-PDFs werden erst ab dem Zeitpunkt der Aktivierung in Ihrer POSTIDENT-Konfiguration erzeugt. Einige Nachweisdaten unterliegen gesetzlichen Beschränkungen (bspw. Ausweisbilder) und können nur erstellt/ausgeliefert werden, sofern die gesetzlichen Voraussetzungen erfüllt sind.

4.3 Weitere Ergebnisdateien (Nachweisdaten)

Je nach Verfahren, Konfiguration und gesetzlichen Vorschriften (bspw. Einschränkungen für Ausweisbilder) können in der Bereitstellung/Lieferung auf Wunsch folgende weitere Dateien enthalten sein:

- Portraitfoto des Nutzers (nur bei Video)
- Ausweisbilder (nur bei Basic, eID, Video)
- Unterschrift aus Ausweis (nur bei Video)
- Unterschrift von Signpad (nur bei Basic)

Die Erstellung und Bereitstellung/Lieferung dieser Dateien muss vom DPAG-Serviceteam für ihre POSTIDENT-Konfiguration aktiviert werden.

i Die Nachweisdaten werden erst ab dem Zeitpunkt der Aktivierung in Ihrer POSTIDENT-Konfiguration erzeugt. Einige Nachweisdaten unterliegen gesetzlichen Beschränkungen (bspw. Ausweisbilder) und können nur erstellt/ausgeliefert werden, wenn die gesetzlichen Voraussetzungen erfüllt sind.

4.4 Signaturdatei

Damit die Herkunft der Dateien nachgewiesen werden kann, werden alle in einem ZIP-Archiv enthaltenen Dateien signiert. Dadurch wird der Auftraggeber in die Lage versetzt zu überprüfen, ob die Datei tatsächlich von der Deutschen Post kommt und auf dem Transportweg nicht manipuliert wurde. Das Signieren wird unter Verwendung eines Private Key der Deutschen Post durchgeführt.

Verfahren	Beschreibung	Dateiextension
RSAPSS	Signaturverfahren "Probabilistic Signature Scheme" basierend auf einem RSA Schlüssel. Auch bekannt als: RSASSA-PSS und standardisiert in PKCS#1 ab v2.1 In Signaturbibliotheken wird dies auch als SHA256withRSAandMGF1 bezeichnet	.sig.rsapss

Es werden alle Dateien eines Archivs einzeln signiert. Die jeweilige Signaturdatei trägt den gleichen Namen wie die zugehörige Daten- bzw. Bilddatei, hat aber die in der obigen Tabelle angegebene Dateiendung. Beispiele: „data.csv.sig.rsapss“.

Die Überprüfung der Signaturen erfolgt mit einem durch die Deutsche Post bereitgestellten Zertifikat. Dieses Zertifikat enthält den Public Key mit der zusätzlichen Information zur Herkunft des Zertifikates (hier: Postident).

4.4.1 Überprüfung der Signatur mit RSAPSS

Folgende Dateien werden benötigt.

- dpdhl_postident_rsapss_2019-03-27.crt – Zertifikat der Deutschen Post für Postident RSAPSS
- dpdhl_postident_pubkey.pem – extrahierter Public Key
- data.csv– Inhaltsdatei (csv bzw. image)
- data.csv.sig.rsapss – Signatur der Inhaltsdatei

Die Zertifikate der Deutschen Post für Postident, mit dem die Echtheit der Datendateien verifiziert werden kann, können Sie unter www.postident.de/handbuch herunterladen.

Vor der ersten Prüfung muss aus dem Zertifikat der Public Key extrahiert werden, der für alle späteren Verifizierungen verwendet wird.

```
openssl x509 -inform der -pubkey -noout -in dpdhl_postident_rsapss_2019-03-27.crt > dpdhl_postident_pubkey.pem
```

Die eigentliche Prüfung erfolgt mit folgendem Kommando (dies erfordert openssl in Version > 1.1.x)

```
openssl dgst -sha256 -sigopt rsa_padding_mode:pss -verify dpdhl_postident_pubkey.pem -signature data.csv.sig.rsapss data.csv
```

5 Datenformate und Datenfelder

5.1 JSON Version v1 (empfohlen)

JSON v1 enthält die kompletten Ergebnisdaten und alle weiteren Dateien zu einem Vorgang.

Die Beschreibung der JSON-Datenstruktur finden Sie im Dokument "SCR-Ident API Guide" (Download-Link siehe Kapitel 1 Übersicht oben).

5.2 CSV Version v2.0

CSV ist ein älteres Datenformat, das nicht alle Ergebnisdaten enthält.

5.2.1 CSV Version 2.0

Format & Encoding

Format	CSV-Datei
Dateiname	data.csv
Separator	; (Semikolon)
Feldbegrenzerzeichen	" (Anführungszeichen)
Encoding	ISO-8859-15 (Fallback: ISO-8859-1)

Datenstruktur

Das Format CSV 2.0 unterstützt folgende Datenfelder:

Referenz- und Produktdaten

Vorgangsnummer, Abrechnungsnummer, Abrechnungsprodukt, Referenznummer, Sendungsnummer, Verarbeitungszeitpunkt, Kassenschlüssel, Kassentag, Journalsatznummer, Produkt, Status

Identifikationsdaten

Nachname, Vorname, Strasse und Hausnummer, PLZ, Ort, Ausweisart, Ausweisnummer, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Ausstellungsbehörde, Ausstellungsort, Ausstellungsdatum, Dienste- und kartenspezifische Kennzeichen

Sonstige Formularangaben (nie befüllt, da Scanservice nicht mehr angeboten wird)

Postvermerk, Empfaengeradresse, Paginiernummer

Anhang

Dateireferenz

Sonstige Merkmale

Merkmale Filiale, Merkmale eID, Merkmale Datenabgleich

Neue Datenfelder in der Version 2.0

Merkmale Einwohnermeldeamt, Gesamttreffergüte Schufa, Merkmale Kontotransaktion, Merkmale E-Postbrief

Substatus

Merkmale Video

Weitere Informationen zur Datenstruktur finden Sie im Kapitel Datenstruktur CSV.

Beispiel

1	"Vorgangsnummer";"Abrechnungsnummer";"Abrechnungsprodukt";"Referenznummer";"Sendung nummer";"Verarbeitungszeitpunkt";"Kassenschluessel";"Kassentag";"Journalatznummer";"Produkt";"Status";"Nachname";"Vorname";"Strasse und Hausnummer";"PLZ";"Ort";"Ausweisart";"Ausweisnummer";"Geburtsdatum";"Geburtsort";"Staatsangehoerigkeit";"Ausstellungsbehoerde";"Ausstellungsort";"Ausstellungsdatum";"Dienste- und kartenspezifische Kennzeichen";"Postvermerk";"Empfaengeradresse";"Paginiernummer";"Dateireferenz";"Merkmale Filiale";"Merkmale Scandienstleister";"Merkmale eID";"Merkmale Datenabgleich";"Merkmale Einwohnermeldeamt";"Gesamttrefferguete Schufa";"Merkmale Kontotransaktion";"Merkmale E-Postbrief";"Merkmale Video";
2	"9BGW449EM7YC";"11235813523701";"Postident Video";"9BGW449EM7YC";;"11.05.2016 19:36:02";;"Video";"411";"Muster geb. Müller";"Max";"Musterhausstr. 12";"56218";"Mülheim-Kärlich";"Personalausweis";"08154711XT9";"21.02.1977";"Koblenz";"DEUTSCH";"Landeshauptstadt Wiesbaden";;"20.05.2010";;"9BGW449EM7YC_0000000000_000000000000.tif";;"XZ7J38790000";"11235813523701";;"XZ7J38790000";;"11.05.2016 20:27:02";;"Basic";"130";"1B37P62WZ212";"11.05.2016 20:51:57";"85029310";"11.05.2016";"58";"Basic";"110";"Muster geb. Müller";"Max";"Musterhausstr. 35";"56218";"Mülheim-Kärlich";"Personalausweis";"08154711XT9";"21.04.1980";"Koblenz";"DEUTSCH";"Landeshauptstadt Wiesbaden";;"20.05.2010";;"1";;
3	
4	

5.2.2 Datenstruktur CSV

Die folgenden Tabelle zeigt die Datenstruktur von Vorgängen bei Ausgabe im Datenformat CSV.

Feldname	Wertebereich / Beispiel	Beschreibung
Referenz- und Produktdaten		
Vorgangsnummer	ABC123DEF456	Identifizier des POSTIDENT-Systems für einen Identifikationsvorgang. Länge 12 Zeichen, Inhalt: alphanumerisch
Referenznummer		Identifizier des Auftraggebers (Geschäftskunde) für einen Identifikationsvorgang. Kann beim Start eines Vorgangs an das POSTIDENT-System übergeben werden. Länge: 14 Zeichen, Inhalt: alphanumerisch
Abrechnungsnummer	11223344556601	Identifizier des POSTIDENT-Systems für die POSTIDENT Konfiguration und die Abrechnung von Identifikationsvorgängen. Länge: 14 Zeichen, Inhalt: alphanumerisch. Schema: EKP (10 Stellen) + Verfahren (2 Stellen) + Teilnahme (2 Stellen)
Produkt	<ul style="list-style-type: none"> Basic Video Photo eID AutoID 	Verwendetes POSTIDENT Verfahren

Feldname	Wertebereich / Beispiel	Beschreibung												
Status	<p><u>Basic:</u></p> <ul style="list-style-type: none"> • 130 = Coupon wurde bereitgestellt / Kunde hat noch die Möglichkeit ein anderes Verfahren zu wählen. • 110 = Lieferung BasicIdent nach <i>erfolgreicher</i> Identifikation (Filialdaten) • 151 = Lieferung BasicIdent nach <i>erfolgloser</i> Identifikation (bspw. wg. Auffälligkeiten oder Betrugsverdacht) <p><u>Video:</u></p> <ul style="list-style-type: none"> • 400 = Lieferung Videoident, Identifikation vorläufig erfolgreich • 411 = Lieferung Videoident nach <i>erfolgreicher</i> Identifikation • 421 = Lieferung Videoident nach <i>erfolgloser</i> Identifikation <p><u>Foto</u></p> <ul style="list-style-type: none"> • 511 = Lieferung Fotoident nach <i>erfolgreicher</i> Identifikation • 521 = Lieferung Fotoident nach <i>erfolgloser</i> Identifikation <p><u>eID:</u></p> <ul style="list-style-type: none"> • 200 = Lieferung eID-Ident nach <i>erfolgreicher</i> Identifikation 	<p>Status der Identifikation</p> <p>Die möglichen Statuswerte hängen ab vom Verfahren und sind gruppiert in Statustypen:</p> <table border="1"> <thead> <tr> <th>Statustyp</th> <th>Auslieferung</th> <th>Beispiel (Basic)</th> </tr> </thead> <tbody> <tr> <td>Benachrichtigung (nur bei Basic)</td> <td>auf Wunsch</td> <td>130 Coupon bereitgestellt</td> </tr> <tr> <td>Vorläufiges Ergebnis (nur bei Video)</td> <td>auf Wunsch</td> <td>400 Lieferung Videoident, Identifikation vorläufig erfolgreich</td> </tr> <tr> <td>Finales Ergebnis</td> <td>immer</td> <td>110 Identifikation erfolgreich 151 Identifikation nicht erfolgreich 761 Identifikation nicht erfolgreich 771 Identifikation erfolgreich</td> </tr> </tbody> </table> <p>Weitere Details zu Ablauf und Statusmodell der einzelnen Verfahren finden Sie im Dokument "SCR-Ident API Guide" (Download-Link siehe Kapitel 1 Übersicht oben).</p>	Statustyp	Auslieferung	Beispiel (Basic)	Benachrichtigung (nur bei Basic)	auf Wunsch	130 Coupon bereitgestellt	Vorläufiges Ergebnis (nur bei Video)	auf Wunsch	400 Lieferung Videoident, Identifikation vorläufig erfolgreich	Finales Ergebnis	immer	110 Identifikation erfolgreich 151 Identifikation nicht erfolgreich 761 Identifikation nicht erfolgreich 771 Identifikation erfolgreich
Statustyp	Auslieferung	Beispiel (Basic)												
Benachrichtigung (nur bei Basic)	auf Wunsch	130 Coupon bereitgestellt												
Vorläufiges Ergebnis (nur bei Video)	auf Wunsch	400 Lieferung Videoident, Identifikation vorläufig erfolgreich												
Finales Ergebnis	immer	110 Identifikation erfolgreich 151 Identifikation nicht erfolgreich 761 Identifikation nicht erfolgreich 771 Identifikation erfolgreich												

Feldname	Wertebereich / Beispiel	Beschreibung
	<ul style="list-style-type: none"> 205 = Lieferung eID-Ident nach <i>erfolgloser</i> Identifikation AutoID: <ul style="list-style-type: none"> 761 = Lieferung Autoident nach erfolgloser Identifikation abgeschlossen 771 = Lieferung Autoident nach erfolgreicher Identifikation 	
Substatus	Abgelehnt: <ul style="list-style-type: none"> 11 = Betrugsverdacht 16 = Identifizierung mit Auffälligkeiten 17 = Identifizierung mit nicht behebbarem Datenproblem in Ausweisdaten 19 = Identifizierung mit nicht behebbarem Datenproblem in Videochat-Aufzeichnung 84 = sonstiger Ablehnungsgrund 	Ergänzender Substatus
Verarbeitungszeitpunkt	DD.MM.YYYY HH24:MM:SS (bei CSV)	Zeitpunkt der Verarbeitung abhängig vom Verfahren <ul style="list-style-type: none"> Basic: in der Filiale Video, Foto: im Service-Center eID: online-Verarbeitung mit Ausweislesegerät Nutzer
Kassenvermerk		Verfügbar bei Identifikation in der Filiale Kassenvermerk = Kassenschlüssel + Kassentag + Journalsatznummer
Kassenschlüssel		Verfügbar bei Identifikation in der Filiale Kassenschlüssel der Filialkasse, an der die Identifikation erfasst wurde.
Kassentag		Verfügbar bei Identifikation in der Filiale Tag, an dem die Identifikation an der Filialkasse erfasst wurde.
Journalsatznummer		Verfügbar bei Identifikation in der Filiale: Satznummer innerhalb des täglichen Kassenjournals, die die Erfassung der Identifikation an der Filialkasse identifiziert

Feldname	Wertebereich / Beispiel	Beschreibung
Abrechnungsprodukt	<u>„Wertebereich“/ Bedeutung:</u> <ul style="list-style-type: none"> • „Postident Basic Zusatzprodukt 1“/ Elektronische Formulardaten • „Postident Basic Zusatzprodukt 2“/ Elektronische Formulardaten und Anlagenhandling • „Postident Basic Zusatzprodukt 3“/ Elektronische Formulardaten und Anlagenimage bis 3 Seiten • „Postident Basic Zusatzprodukt 4“/ Elektronische Formulardaten und Anlagenimage bis 10 Seiten • „Postident Video“ Identifikation mit Postident Video • "Foto Mobility" Identifikation mit Postident Foto • „Postident eID“ Identifikation mit Postident eID 	Erbrachte Leistung, die für die Durchführung des Vorgangs in Rechnung gestellt wird.
Identifikationsdaten		
Nachname		Nachname auf dem Ausweis, ggf. inklusive Geburtsname Geburtsname wird bei TKG nicht ausgeliefert
Vorname		Alle Vornamen auf dem Ausweis
Strasse und Hausnummer		Strasse und Hausnummer aus dem Ausweis (falls auf Ausweis vorhanden) oder erfragt bei Nutzer (falls auf Ausweis nicht vorhanden). Nur bei Identifikation in der Filiale: Falls der Filialmitarbeiter bei Ausweisdokumenten ohne Adresse trotzdem eine Adresse erfasst, ist diese im Filialdatensatz mit einem zusätzlichen Sternchen am Ende markiert: * Selbstauskunft – bei Verwendung eines deutschen Reisepasses oder eines vorläufigen deutschen Reisepasses; ** ggf. erfragt – bei ausländischem Reisepass oder ausländischer Identitätskarte
Plz		
Ort		

Feldname	Wertebereich / Beispiel	Beschreibung
Ausweisart	<p><u>Wertebereich Filial-Datensatz (Basic)</u></p> <ul style="list-style-type: none"> • "Personalausweis" • "Identitätskarte (Personalausweis Ausland)" • "Reisepass" • "Reisepass (Inland)" • "Reisepass (Ausland)" • Aufenthaltstitel (Ausweisersatz)" • "Vorläufig ausgestellt Personalausweis" • "Vorläufig ausgestellt Reisepass" • "Reiseausweis für Staatenlose (Übereinkommen von 1954)" • "Reiseausweis für Flüchtlinge (Übereinkommen von 1951)" • "Reiseausweis für Ausländer (Abkommen von 1946)" • "Dienstpass" • "Diplomatenpass" • "Ministerialpass" • "Ministerial- oder Diplomatenpass" <p><u>Wertebereich Video-Datensatz</u></p> <ul style="list-style-type: none"> • "Personalausweis" • "Reisepass" • "Aufenthaltstitel (Ausweisersatz)" • "Vorläufiger Personalausweis" • "Vorläufiger Reisepass" 	Ausweisart entsprechend des gelieferten Datensatzes aus dem jeweiligen Verfahren

Feldname	Wertebereich / Beispiel	Beschreibung
	<ul style="list-style-type: none"> "Reiseausweis für Staatenlose (Übereinkommen von 1954)" "Reiseausweis für Flüchtlinge (Übereinkommen von 1951)" "Reiseausweis für Ausländer (Abkommen von 1946)" "Dienstpass" "Diplomatenpass" "Ministerialpass" "Ministerial- oder Diplomatenpass" <p><u>Wertebereich Foto-Datensatz</u> wie Video</p> <p><u>Wertebereich eID-Datensatz</u></p> <ul style="list-style-type: none"> "Personalausweis" "Aufenthaltstitel" "eID-Karte für Unionsbürger und EWR-Staatsangehörige" 	
Ausweisnummer		Nicht bei eID
Geburtsdatum	dd.mm.yyyy	
Geburtsort		Nur bei GWG
Staatsangehörigkeit		Nicht bei TKG
Ausstellungsbehörde		Behörde, die den Ausweis ausgestellt hat (teilweise inklusive Ausstellungsort). Nur bei GWG und TKG Nicht bei eID
Ausstellungsort		Nur bei GWG Nicht bei eID
Ausstellungsdatum	dd.mm.yyyy	Nur bei GWG und TKG Nicht bei eID
Dienste und kartenspezifische Kennzeichen		Nur bei eID Ein dienste- und kartenspezifisches Kennzeichen (DKK) ist eine Zeichenfolge, die im Speicher- und Verarbeitungsmedium des Personalausweises berechnet wird. Es dient der eindeutigen elektronischen Wiedererkennung eines Personalausweises durch den Diensteanbieter, für den es errechnet wurde, ohne dass weitere personenbezogene Daten übermittelt werden müssen (Definition nach PAuswG-Personalausweisgesetz // Quelle: http://www.gesetze-im-internet.de/pauswg/_2.html).
Sonstige Merkmale		

Feldname	Wertebereich / Beispiel	Beschreibung
Merkmale_filiale	<ul style="list-style-type: none"> • LEER = Keine Daten aus ZORA (Filial-Daten) erhalten • 1 = Filial-Daten erhalten 	Gibt an, ob Daten aus dem Filialsystem im Postident-System eingegangen sind
Merkmale_scandienstleister	<ul style="list-style-type: none"> • LEER 	Scanservice steht nicht mehr bereit, daher immer leer
Merkmal_eID	<ul style="list-style-type: none"> • LEER = keine Identifikation über eID durchgeführt • 0 = Identifikation über eID (Versuch); keine Daten über eID-Schnittstelle erhalten • 1 = Identifikation über eID durchgeführt; Daten über eID-Schnittstelle erhalten 	<p>Gibt an, ob eine Identifikation mittels Online-Ausweisfunktion (eID) durchgeführt wurde und ob Daten übernommen wurden.</p> <p>Einsetzbar für die eID sind:</p> <ul style="list-style-type: none"> • deutscher Personalausweis • eAT (elektronischer Aufenthaltstitel) • eID-Karte für Unionsbürger und EWR-Staatsangehörige (eID-Karte UB)
Merkmale_Datenabgleich	<ul style="list-style-type: none"> • LEER = Kein Abgleich durchgeführt. • 0 = Abgleich ohne Ergebnis • 1 = Nachsendeauftrag Inland bekannt • 2 = Nachsendeauftrag Ausland bekannt • 4 = Soll verstorben sein • 8 = Postalisch unzustellbar 	<p>Ergebnis Abgleich mit DPAG Adressdatenbanken</p> <p>Bei Kombinationen wird die Summe der Werte geliefert.</p>
Merkmale_einwohnermeldeamt	<ul style="list-style-type: none"> • LEER = kein Abgleich durchgeführt • 0 = Abgleich ohne Ergebnis • 1 = Ohne Abweichung getroffen • 2 = Auf abweichender Inlandsadresse gemeldet • 4 = Auf abweichender Auslandsadresse gemeldet • 8 = Abgemeldet • 16 = ohne festen Wohnsitz/ Meldeverhältnis nicht eindeutig • 32 = Auskunftssperre • 64 = Verstorben 	<p>OBSOLET - derzeit ungenutzt</p> <p>Ergebnis Adressabgleich Einwohnermeldeamt</p>

Feldname	Wertebereich / Beispiel	Beschreibung
Gesamtscorewert_schufa a (Feldname im CSV: Gesamttreffergüte Schufa)	<ul style="list-style-type: none"> • LEER = Kein Abgleich mit Schufa durchgeführt • 0 = keine Übereinstimmung getroffen • 1-100 = Güte der Übereinstimmung 	OBSOLET - derzeit ungenutzt Ergebnis Identitätscheck Schufa
Merkmale_kontotransaktion	<ul style="list-style-type: none"> • LEER = Keine Kontotransaktion angestoßen • 0 = keine Ergebnisse • 1: Land der Kontoverbindung ist in der Whitelist (z.B. sichere Drittstaaten enthalten) • 2: Nachname und Vorname des Kontoinhabers entsprechen den Identifikationsdaten • 4: Konto des Kunden ist der Schufa bekannt • 8: Kontonummerncheck wurde von Schufa durchgeführt • 16: Konto ist ein deutsches Konto 	OBSOLET - derzeit ungenutzt Ergebnis Kontotransaktion und Kontonummerncheck bei Schufa
Merkmale_e_postbrief	<ul style="list-style-type: none"> • LEER = kein Abgleich mit E-Postbrief durchgeführt • 0 = Abgleich mit E-Postbrief durchgeführt (Versuch); keine Daten erhalten • 1 = Abgleich mit E-Postbrief erfolgreich; Daten aus E-Postbrief übernommen 	OBSOLET - derzeit ungenutzt Ergebnis Abgleich E-Postbrief
Merkmale Video (Feld nur in CSV)	siehe Feld Substatus	siehe Feld Substatus

5.2.3 Liste der weiteren Ergebnisdateien

Neben der Ergebnisdatendatei können abhängig vom genutzten Verfahren und Ihrer POSTIDENT-Konfiguration weitere Dateien in einer Lieferung enthalten sein.

Die folgende Liste gibt die Dateinamen dieser Dateien für CSV an.

i Die weiteren Dateien werden nur im Datenformat JSON komplett referenziert, nicht in dem älteren Datenformat CSV. Die Dateien können bei CSV jedoch durch die Namenskonvention (Vorgangsnummer am Beginn des Dateinamens) zugeordnet werden.

Basic Identifikationen:

- <Vorgangsnummer>_result_basic.pdf (Ergebnis-PDF mit Daten und Bildern)
- <Vorgangsnummer>_resultdata_basic.pdf (Ergebnis-PDF nur Daten)
- <Vorgangsnummer>_resultimages_basic.pdf (Ergebnis-PDF nur Bilder)
- <Vorgangsnummer>_<abrechnungsnr>_<referenznr>_<lfidnr 1>.jpg (Ausweisbild 1)
- <Vorgangsnummer>_<abrechnungsnr>_<referenznr>_<lfidnr 2>.jpg (Ausweisbild 2)
- <Vorgangsnummer>_usersignature.jpg (Unterschrift von Signpad)

Video Identifikationen:

- <Vorgangsnummer>_result_video.pdf (Ergebnis-PDF mit Daten und Bildern)
- <Vorgangsnummer>_resultdata_video.pdf (Ergebnis-PDF nur Daten)
- <Vorgangsnummer>_resultimages_video.pdf (Ergebnis-PDF nur Bilder)
- <Vorgangsnummer>_ausweisgesichtsfoto.jpg (Portraitfoto)
- <Vorgangsnummer>_ausweisvorderseite.jpg (Ausweisbild 1)
- <Vorgangsnummer>_ausweisrueckseite.jpg (Ausweisbild 2)
- <Vorgangsnummer>_idsignature.jpg (Unterschrift aus Ausweis)

eID Identifikationen:

- <Vorgangsnummer>_result_eid.pdf (Ergebnis-PDF nur Daten) // Hinweis: eID enthält keine Bilder
- <Vorgangsnummer>_resultdata_eid.pdf (Ergebnis-PDF nur Daten)

Foto Identifikationen:

Für Foto gibt es derzeit keine Zusatzdateien.

AutoID Identifikationen:

- <Vorgangsnummer>_result_autoid.pdf (Ergebnis-PDF nur Daten) // Hinweis: AutoID enthält keine Bilder
- <Vorgangsnummer>_resultdata_autoid.pdf (Ergebnis-PDF nur Daten)

Alle Verfahren:

Zusätzlich Signaturdateien mit Suffix ".sig" für alle o.g. Dateien, falls die Dateisignierung in Ihrer POSTIDENT-Konfiguration aktiviert ist.