Corona COVID 19

Notfallkonzept der

identity Trust Management AG

Version 1.5 vom 23.03.2020

Inhaltsverzeichnis

1 Dokumentenhistorie

Version	Stand	Autor/Bearbeiter	Änderung	Kommentar zur Änderung
0.9.1	03.03.2020	Jacobs Harald	Arbeitsversion	Initialversion
1.0	10.03.2020	Jacobs Harald	Initialversion	
1.1	16.03.2020	Jacobs Harald	Redaktionelle Überarbeitung	Überarbeitung/ Ergänzungen/Aktualisierung
1.2	16.03.2020	Johannes Meerloo		Freigabeversion
1.3	17.03.2020	Jacobs Harald	Änderung der Einstufung RKI	
1.4	18.03.2020	Jacobs Harald	Änderung der Lage bei Kurier- und Shop	Tägliche Aktualisierung
1.4	18.03.2020	Uwe Stelzig		Freigabeversion
1.5	23.03.2020	Jacobs Harald	Änderung der Lage; weitere Maßnahmen	Aktualisierung
1.5		Johannes Meerloo		Freigabeversion

Tabelle 1: Dokumentenhistorie

2 Einleitung

Allgemeiner Hinweis 23.03.2020:

Die jeweils weiteren Änderungen zur Vorversion, werden in der neuen Version in rot vermerkt (bessere Lesbarkeit)

Die identity Trust Management AG ist ein Identifikationsdienstleister, der seinen Kooperationspartnern im Bereich der Identitätsprüfung natürlicher und juristischer Personen Produktprozesse bietet, die präzise auf die Anforderungen ihrer Kooperationspartner abgestimmt werden.

Die Identitätsprüfung am Wohnort oder Arbeitsplatz der Endkunden der Kooperationspartner, in Shops, in einer Video-Konferenz, mittels der eID Funktion des neuen Personalausweises, im Verfahren identity Giro oder über einen bei der Verimi GmbH hinterlegten Identifizierungsdatensatz, gehört ebenso zum Service, wie gegebenenfalls das professionelle Vertragsmanagement, eine Unterschriftseinholung mittels eIDAS konformer elektronischer Signaturprozesse, die elektronische Bereitstellung der Identifikationsergebnisse und das aktive Ident-Management zur Unterstützung der Endkunden (prozessbegleitenden Kontakt- und Switch-Möglichkeiten).

Grundlage der Dienstleistungen der identity Trust Management AG, ist die gesetzeskonforme Identifizierung nach dem Geldwäschegesetz, dem De-Mail Gesetz mit seinen technischen Richtlinien, dem TKG und dem Vertrauensdienstegesetz/eIDAS.

Die Identifizierung erfolgt unter Hinzunahme technischer Hilfsmittel oder im persönlichen Kontakt zwischen natürlichen Personen.

Die weltweite Gesundheitssituation vor dem Hintergrund der Corona Pandemie erfordert eine darauf bezogene Betrachtung des Notfallkonzeptes der identity Trust Management AG.

Corona Pandemie - Aktuelle Lage:

Coronaviren können Menschen und Tiere infizieren. Sieben Vertreter dieser Gruppe verursachen beim Menschen Atemwegserkrankungen - von gewöhnlichen Erkältungen bis zu gefährlichen oder gar potenziell tödlich verlaufenden Krankheiten.

Das neue NCP-Coronavirus zeigt möglicherweise viele Tage lang keine Anzeichen einer Infektion und führt so zu unbekannten Übertragungswegen.

Die Gefährdung für die Gesundheit der Bevölkerung in Deutschland wird derzeit vom Robert Koch Institut nunmehr insgesamt als hoch (17.03.2020) eingeschätzt. Die Wahrscheinlichkeit für schwere Krankheitsverläufe nimmt mit zunehmendem Alter und bestehenden Vorerkrankungen zu. Die Belastung des Gesundheitswesens hängt maßgeblich von der regionalen Verbreitung der Infektion, den vorhandenen Kapazitäten und den eingeleiteten Gegenmaßnahmen (Isolierung, Quarantäne, soziale Distanzierung) ab und kann örtlich sehr hoch sein.

Diese Einschätzung kann sich kurzfristig durch neue Erkenntnisse ändern. Daher unterliegt dieses Notfallkonzept laufenden Betrachtung und soweit erforderlich täglichen Änderungen.

17.03.2020: Die Änderung von mittel auf hoch führt zu keinen Änderungen im Konzept, da die Maßnahmen bereits darauf abgestimmt waren.

18.03.2020: Die Bundesregierung hat mit den Ländern Leitlinien zum einheitlichen Vorgehen zur weiteren Beschränkung von sozialen Kontakten im öffentlichen Leben vereinbart. Der Lebensmitteleinzelhandel, Wochenmärkte und Lieferdienste, Apotheken, Drogerien, Banken, Tankstellen sowie der Großhandel bleiben davon unberührt. Bars, Clubs, Theater, Museen, Kinos, Zoos, Sporteinrichtungen und Spielplätze werden vorerst geschlossen. Darüber hinaus sind Zusammenkünfte in Vereinen, Sport- und Freizeiteinrichtungen sowie Zusammenkünfte in Kirchen, Moscheen, Synagogen und Zusammenkünfte anderer Glaubensgemeinschaften fürs Erste verboten. (https://www.bundesregierung.de/breg-de/themen/coronavirus/coronavirus-1725960)

Inzwischen sind in allen Bundesländern Infektionsfälle mit dem neuen Coronavirus (SARS-CoV-2) bestätigt worden. (https://www.rki.de/DE/Home/homepage_node.html)

Vor dem Hintergrund wachsender Zahlen erkrankter Menschen und den Empfehlungen der Bundesregierung soziale Kontakte weiter einzuschränken können die Shop und Kurier-Systeme nicht mehr im gewohnten Umfang durch uns verpflichtet werden, eine persönliche Face to Face Identifizierung durchzuführen.

Shop: Aufgrund von Krankheitszahlen bei Mitarbeitern oder Risikoabwägungen von Shop-Inhabern kommt es zu Schließungen einzelner regionaler Shops, bzw. zum Aussetzen des Services einer persönlichen Identitätsprüfung im vertraulichen Rahmen. Die Mindestanforderung an den vertraulichen Rahmen wiedersprechen den dringenden Empfehlungen des RKI auf einzuhaltenden Mindestabstand und persönlichen Kontakt. Entsprechend der Verantwortung für die Gesundheit, der in diesen Prozessen arbeitenden Menschen, haben wir mit heutigen Datum die Durchführung von Identitätsprüfungen in den Shops freigestellt und die vertraglichen Verpflichtungen hierzu ausgesetzt.

Wir setzen alles daran die Shop-Liste laufend zu aktualisieren. Dennoch erfordert die momentan dynamische Lage aus unserer Sicht einen Hinweis im Shop-Finder:

„Aufgrund der aktuellen Lage (Corona/ COVID 19) kann es leider vorkommen, dass der Shop, den Sie zum Zwecke einer Identifizierung besuchen möchten, geschlossen hat oder die Öffnungszeiten abweichen. Wenn es für Sie möglich ist, kontaktieren Sie bitte den Shop vorher telefonisch, um nähere Informationen zu den Öffnungszeiten und der Verfügbarkeit zu erhalten.
Wir arbeiten mit Hochdruck stetig daran, uns immer eine möglichst aktuelle Übersicht über die Lage zu verschaffen und den Shop Finder aktuell zu halten. Wir bitten Sie um Verständnis.“

Meldungen werden wir aktualisieren. Noch sind nur einzelne Shops betroffen.

Kurier: Leider kommt er auch bei unseren Kurier-Partnern krankheitsbedingt und aus Gründen von Quarantäne Anordnungen zu Einschränkungen bzw. Schließungen einzelner Zustell-Depots. Die weiterführende Leistungserbringung der persönlichen Identifizierung im pers. Umfeld des zu Identifizierenden ist gegenüber den verpflichteten Kurieren mit sofortiger Wirkung bundesweit ausgesetzt. Wir sehen keinen anderen Handlungsspielraum, um unserer Verantwortung für die Gesundheit und Sicherheit der Mitarbeiter gerecht zu werden.

Meldelinien halten uns weitestgehend auf dem Laufenden und wir versuchen jeweils zeitnah Termine abzusagen bzw. zu verlegen. Telefonkapazitäten dazu haben wir erhöht.

Noch sind nur einzelne Regionen betroffen. Wir aktualisieren hier laufend

22.03.2020: Die Bundeskanzlerin und die Regierungschefinnen und Regierungschefs der Bundesländer und des Freistaat Bayern fassen am 22. März 2020 folgenden Beschluss:

Die rasante Verbreitung des Coronavirus (SARS-CoV-2) in den vergangenen Tagen in Deutschland ist besorgniserregend.

Wir müssen alles dafür tun, um einen unkontrollierten Anstieg der Fallzahlen zu verhindern und unser Gesundheitssystem leistungsfähig zu halten. Dafür ist die Reduzierung von Kontakten entscheidend.

Bund und Länder verständigen sich auf eine Erweiterung der am 12. März beschlossenen Leitlinien zur Beschränkung sozialer Kontakte:

I. Die Bürgerinnen und Bürger werden angehalten, die Kontakte zu anderen Menschen außerhalb der Angehörigen des eigenen Hausstands auf ein absolut nötiges Minimum zu reduzieren.

II. In der Öffentlichkeit ist, wo immer möglich, zu anderen als den unter I. genannten Personen ein Mindestabstand von mindestens 1,5 m einzuhalten.

III. Der Aufenthalt im öffentlichen Raum ist nur alleine, mit einer weiteren nicht im Haushalt lebenden Person oder im Kreis der Angehörigen des eigenen Hausstands gestattet.

IV. Der Weg zur Arbeit, zur Notbetreuung, Einkäufe, Arztbesuche, Teilnahme an Sitzungen, erforderlichen Terminen und Prüfungen, Hilfe für andere oder individueller Sport und Bewegung an der frischen Luft sowie andere notwendige Tätigkeiten bleiben selbstverständlich weiter möglich.

V. Gruppen feiernder Menschen auf öffentlichen Plätzen, in Wohnungen sowie privaten Einrichtungen sind angesichts der ernsten Lage in unserem Land inakzeptabel. Verstöße gegen die Kontaktbeschränkungen sollen von den Ordnungsbehörden und der Polizei überwacht und bei Zuwiderhandlungen sanktioniert werden.

VI. Gastronomiebetriebe werden geschlossen. Davon ausgenommen ist die Lieferung und Abholung mitnahmefähiger Speisen für den Verzehr zu Hause.

VII. Dienstleistungsbetriebe im Bereich der Körperpflege wie Friseure, Kosmetikstudios, Massagepraxen, Tattoo-Studios und ähnliche Betriebe werden geschlossen, weil in diesem Bereich eine körperliche Nähe unabdingbar ist. Medizinisch notwendige Behandlungen bleiben weiter möglich.

VIII. In allen Betrieben und insbesondere solchen mit Publikumsverkehr ist es wichtig, die Hygienevorschriften einzuhalten und wirksame Schutzmaßnahmen für Mitarbeiter und Besucher umzusetzen.

IX. Diese Maßnahmen sollen eine Geltungsdauer von mindestens zwei Wochen haben.

22.03.2020: Robert Koch Institut: Die Gefährdung für die Gesundheit der Bevölkerung in Deutschland wird derzeit insgesamt als hoch eingeschätzt.

Die Einschätzung des RKI hat sich insoweit nicht geändert.

22.03.2020:

Leider wurde Kroatien um 06.24 Uhr von zwei Erdbeben der Stärke: 5,4 heimgesucht.

Betroffene Länder: Bosnien und Herzegowina, Kroatien, Ungarn, Slowenien und Österreich

Zagreb, Kroatien – war nur 9 km vom Epizentrum entfernt und die Standorte bei unserem Partner M.S.S. sind davon betroffen.

Sehen sie bitte die Maßnahmen und Risikobewertungen unter 8.

3 Zuständigkeiten und verantwortliche operative Rollen

3.1 Übersicht

Die Zuordnung von Aufgaben, Tätigkeiten und Zuständigkeiten zur Bereitstellung der Dienstleistungen im Rahmen des Ident-Managements erfolgt über definierte Rollen. Die Aufgabenverteilung auf Rollen und nicht auf dezidierte natürliche Personen erlaubt eine Notfallplanung auf Kapazitäten und nicht nur auf die einzelne natürliche Person.

3.2 Die operative Rollen-Struktur

Für die Bereitstellung der Ident-Dienstleistung sind operativ die folgenden Rollen relevant:

- Hub Erfassung
- Hub Prüfung
- Identifizierer
- Verwalter

3.3 Verwalter

Alle Personen die mit den übertragenen Datensätzen der Kooperationspartner der identity AG auch nur theoretisch in Kontakt kommen können, sind als Verwalter oder Identifizierer angelegt. Nur bei der identity AG angelegte und anschließend freigeschaltete Verwalter/Identifizierer können wirksam für Aufträge der identity AG und deren Kooperationspartner tätig werden. Jeder einzelne rückübertragene Datensatz, ist daher mit der von der identity AG nach Freischaltung vergebenen eindeutigen Verwalter/ Identifizierer-Nummer des Bearbeiters zu versehen. Dies geschieht automatisch.

Als Verwalter im engeren Sinne werden die Mitarbeiter bezeichnet, die verwaltende und schulende Funktionen übernehmen. Durch ihre Rolle als Verwalter dürfen sie andere Personen (insb. Identifizierer) intern identifizieren und schulen.

Zusätzlich zur Identifikation von Rolleninhabern übernehmen die Verwalter auch die Aufgaben der Schulung. Im Anschluss an die Schulungen kann der Verwalter die Identifikation der neuen Rolleninhaber durchführen und gleichzeitig die Fachkundenachweise der Identifizierer/ Verwalter bestätigen. Alle Unterlagen werden zentral zur Erfassung im Softwaresystem an das Digitalisierungszentrum der identity AG weitergeleitet.

Die Verwalter dienen in Alarmfällen und entsprechenden Eskalationsstufen sowohl dem Qualitätsmanagement als auch dem Sicherheitsbeauftragten der identity AG zur Abwendung von Gefahren und Sicherstellung der Qualität als Ansprechpartner.

Die Verwalter verantworten die Beibringung aller benötigten Dokumentationen zu den Video Identifizierern zur lückenlosen Dokumentation der Eignung und Fachkunde.

Die Video Verwalter liefern alle, vor der Freischaltung eines Identifizierers, benötigten Dokumentationen an das Digitalisierungszentrum der identity AG.

Verwalter sind ebenfalls, neben dem Identleiter, Ansprechpartner bei Reklamationen.

Verwalter sind zudem Ansprechpartner für Nachfragen des Qualitätsmanagements in Bezug auf Negativlisten noch nicht erledigter Aufträge.

3.4 Identifizierer

Der Identifizierer führt die Ident-Prozesse mit den zu identifizierenden Personen innerhalb der Video Konferenz durch.

Nur bei der identity AG angelegte und anschließend freigeschaltete Identifizierer können wirksam für Aufträge der identity AG und deren Kooperationspartner tätig werden.

Um für die identity AG tätig werden zu können, müssen alle Dokumente zur Person des Identifizierers vorliegen. Zunächst wird überprüft, ob dokumentiert ist, dass das polizeiliche Führungszeugnis des Bewerbers im Original vorgelegt wurde und den vereinbarten Mindestanforderungen entspricht. Ist dies der Fall, durchläuft der Bewerber zunächst die Schulungs- und Ausbildungsveranstaltungen unter der Beaufsichtigung der Schulungsbeauftragten oder der bereits bestehenden Verwalter. Auch eine e-Learning Verfahren ist möglich. Nach erfolgreichem Abschluss der vorgenannten Veranstaltungen, wird der Identifizierer im System der identity AG durch eine Freischaltung intern autorisiert. Er erhält seine eindeutige Identifizierer ID, die ihn zur Bearbeitung von Aufträgen berechtigt. Gegebenenfalls ist zusätzlich für bestimmte Kooperationspartner der identity AG eine weitere zusätzliche Freischaltung in deren Systemen notwendig.

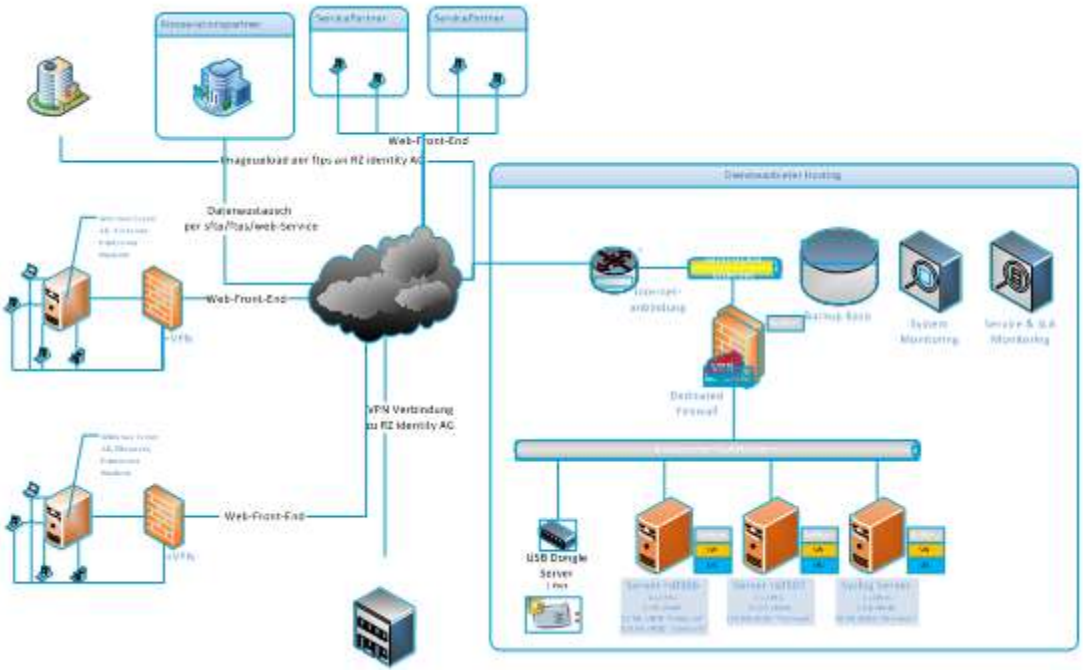
Die Rolle Identifizierer ist damit grundsätzlich generell nicht örtlich gebunden und kann je nach Verfahren Europa-weit besetzt werden.

4 Allgemeine IT Infrastruktur

Die IT-Infrastruktur der identity Trust Management AG ist entsprechend der webbasierenden Betriebssoftware „identity Portal“ maßgeblich in die Strukturbereiche Administration der Standorte und Betriebssoftware unterteilt. Die Infrastruktur ist der Untergliederung der Bereiche folgend, örtlich getrennt und unabhängig voneinander aufgebaut.

Während die Software und Datenbanken der Betriebssoftware auf Servern, in einem gesicherten Rechenzentrum eines Dienste-Anbieters – Hosting, installiert sind, werden die betriebsüblichen benötigten Datenbanken und Software auf Windows-Servern an den jeweiligen Unternehmensstandorten betrieben. Der Zugriff von den Standorten auf die Betriebssoftware und somit auf Auftragsdaten erfolgt über das Internet und sicheren Web-Front-End Zugängen.

4.1 Visio Darstellung der IT-Infrastruktur



Legende: SysMgmt – System Management

SW – Softwareinstallation

OS – OS-Installation

Die Zugriffsmöglichkeiten werden beschriftet dargestellt

Das Rechenzentrum der identity AG wird durch einen Dienste-Anbieter-Hosting betrieben

4.2 Technische und organisatorische Sicherheit der IT-Infrastruktur

Unternehmen, die personenbezogene Daten erheben, verarbeiten oder nutzen, müssen technische und organisatorische Maßnahmen treffen, um den Bestimmungen des DSGVO zu entsprechen.

Die identity Trust Management AG fühlt sich dem Ziel verpflichtet, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen und diese Daten unter Berücksichtigung höchster Sicherheit entsprechend den gesetzlichen Vorschriften zu verwalten.

Hohe Dokumenten- und Datensicherheit gewährleistet die identity AG durch eine physikalische Trennung der Server der administrativen Verwaltung der Betriebsstandorte und der Server auf denen die Betriebssoftware arbeitet, welche durch einen Dienste-Anbieter-Hosting betrieben werden.

Während das Rechenzentrum des Dienste-Anbieters-Hosting durch Hinterlegung von Sicherheitskonzepten, Notfallkonzepten, betrieblichen Datenschutzkonzepten, entsprechenden Zertifikaten und Verfügbarkeitsgarantien eine hohe Systemverfügbarkeit und Zuverlässigkeit garantiert, haben eventuelle Ausfälle der lokalen Serverstrukturen an den Standorten keine Auswirkungen auf die Funktionalität der unter beschriebenen zentralen Rollen und Funktionen.

Auf den Servern und Betriebssystemen an den Standorten der identity Trust Management AG werden keine Auftrags- oder Identprüfdaten verarbeitet. Somit ist sichergestellt, dass bei einem Angriff auf die Betriebssysteme der Standorte keine Gefahrenlage für die Betriebssoftware entstehen kann.

Nicht, durch den Hosting-Anbieter, erfolgreich abzuwehrende Angriffe auf die Server der Betriebssoftware der identity AG sind als äußerst unwahrscheinlich zu klassifizieren. Aber selbst wenn es gelingt den Kommunikationsserver (Linux) im Rechenzentrum des Dienste-Anbieters-Hosting zu attackieren, werden die eigentlichen, in einem geschlossenen Netzwerk mit dem Linux-Server kommunizierenden, Datenbankserver (Windows) vom Linux-Server getrennt und ein Zugriff auf die Auftrags- und Identprüfdaten verhindert. Eine solche Gefahrenlage wird wie unter beschrieben behandelt.

Die identity AG verfügt über lokale Kommunikationsnetzwerke an ihren Standorten. Diese Netzwerke laufen unabhängig von den Servern für das Auftrags-Verfolgungssystem und dienen ausdrücklich nicht der Erhebung und Speicherung personenbezogener Daten.

Sämtliche Daten der Auftragsverfolgung und damit die personenbezogenen Daten der Kooperationspartner werden im Rechenzentrum des Dienste Anbieter Hosting in einem geschlossenen Netzwerk, welches durch eine interne Firewall geschützt ist, über Webserver verarbeitet und auf, von den Webservern getrennten, Datenservern gelagert, die im Rechenzentrum des Dienste-Anbieter-Hosting vorgehalten werden. Die Datensicherung erfolgt über einen Backup-Server. Ein qualifizierter Zugriff auf diese Datenserver ist ausschließlich via VPN möglich, wobei jeder Zugriff mit einem Zeitstempel und Benutzerkennung auf einem Syslog Server protokolliert wird.

Der Syslog-Server ist über das Internet oder mittels VPN nicht zu erreichen. Er dient ausdrücklich nur der Protokollierung aller Zugriffsereignisse auf die IT-Infrastruktur der identity AG und wird vom Standartdienst Page-Management ausgeschlossen.

Der Einsatz eines Datenbankservers realisiert eine Speicherung und Dokumentation, die getrennt vom Webserver erfolgt.

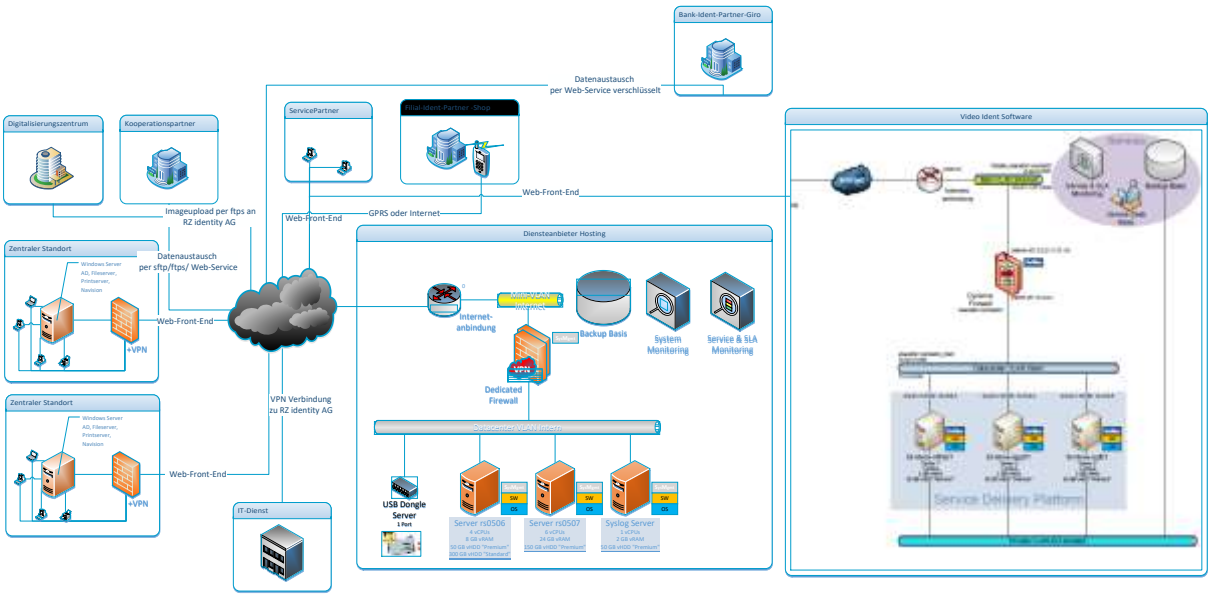
Die personenbezogenen Daten werden auf dedizierten Serversystemen der identity AG, beim externen Dienste-Anbieter-Hosting räumlich getrennt und abgeschlossen, verwaltet. Die Server stehen in einem, in höchstem Maße gesicherten, Rechenzentrum, physisch getrennt und verschlossen in gesicherten Räumen, deren Funktionen durch elektronische Türsicherungen, Zutrittskontrollsysteme, Videoüberwachung und Einbruchmeldeanlagen mit direkter Aufschaltung des Sicherheitsdienstes mehrfach gesichert und geschützt sind.

Die Sicherheit und Authentizität der Datensätze ist durch die geschilderte IT-Infrastruktur, den räumlichen Sicherungssystemen und den Zugriffsprotokollen in hohem Maße gesichert.

Gesichert ist der Zutritt unter anderem durch strenge dokumentierte Zutrittsregelungen. Externe Personen haben zu diesen mehrfach gesicherten Räumlichkeiten keinen Zutritt.

Die rein technischen Komponenten müssen unter den Gesichtspunkt der Corona Pandemie nicht neu betrachtet werden. Notwendige Administratoren Verantwortungen und erforderlicher Support sind im Rahmen definierter Rechte verteilt und so mehrfach besetzt.

4.3 Erweiterte IT-Infrastruktur bei identity Video



Die eigentliche Identitätsüberprüfung im identity Video Verfahren kann abgebildet werden durch eine eigen entwickelte Software der Identity Trust Management AG oder durch die Einbindung der Software eines identity Video Partners, die die gleichen inhaltlichen wie sicherheitstechnischen Kriterien, wie in diesem Dokument geschildert, erfüllen müssen

Im Falle der Nutzung einer eigenen identity Video Software, wird diese in die bestehende IT-Infrastruktur der identity AG integriert. Zusätzlich notwendige Server und/oder Speicherkapazitäten, werden in die bestehende Infrastruktur integriert.

Die Kommunikation einer eigenen identity Video Software mit dem „identity Portal“ erfolgt dann über gesicherte Webservice-Schnittstellen.

Das identity Video Callcenter-Modul, wird als Webbrowser-Anwendung programmiert und kommuniziert mit der jeweiligen App-Technik, die sich der Empfänger vorab ausgewählt und via Download installiert hat.

Die Software realisiert eine webbasierte Nutzung nach dem Grundsatzprinzip der Applikationsnutzung via Internet. Die Programmierung der Software kommt als Windows-App, Android – und/oder iOS-App für Endkunden zum Einsatz. Die Programmierung ist dynamisch gehalten und bedeutet, dass logische Anwendungssequenzen, Layout, Hinweistexte usw. Kooperationspartner-Variabel gestaltet werden können. Die Applikation fragt via Webservice an dieser Stelle die dynamischen Anwendungen ab.

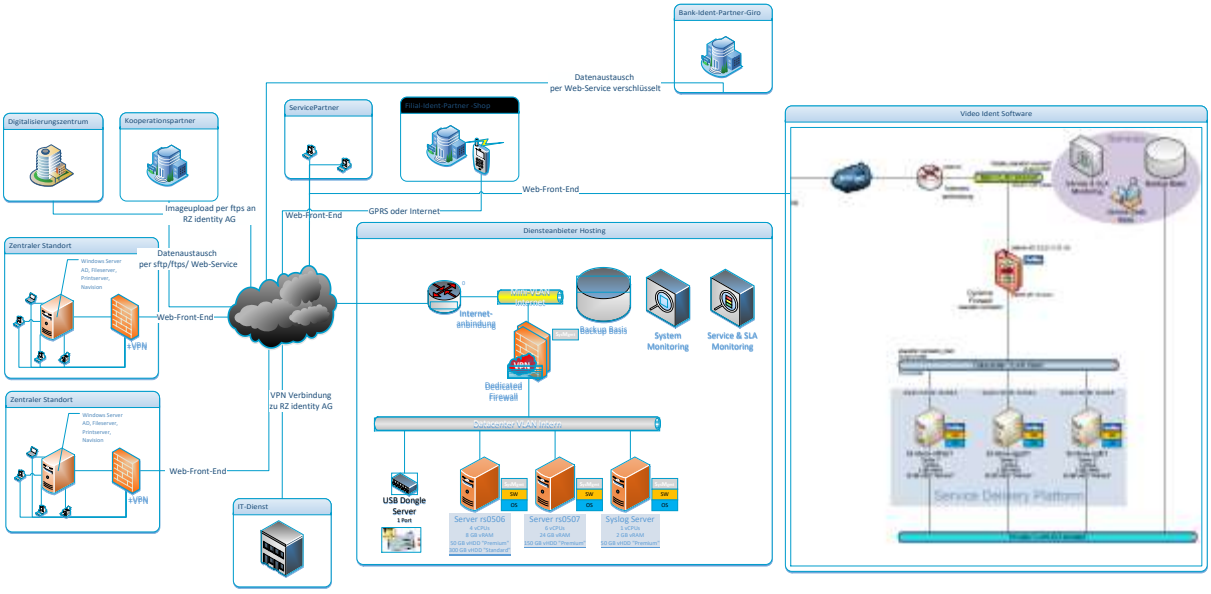
Alle Daten laufen vom Backend-System der identity Trust Management AG durchgängig und bi-direktional ausschließlich verschlüsselt über geschützte Verbindungen und Server zum jeweiligen identity Video Partner und wieder zurück und sind somit von außen nicht physisch greifbar.

Die IT-Systeme eines jeweiligen identity Video Partners werden bei einem zertifizierten Rechenzentrum in Deutschland gehostet. Der Web-App-Server ist getrennt vom Infrastruktur-Server eingerichtet, über welchen die Administration der Systeme gesteuert wird.

Dieser IT - Aufbau ermöglicht es der identity Trust Management AG Callcenter-Kapazitäten weltweit und vor allem in ganz Europa aufzubauen.

Damit kann unabhängig von der gesundheitlichen Konstitution einzelner Identifizierer oder regionaler Identifizierer-Gruppen, der Service jederzeit und skalierbar überregional dargestellt werden. Mithin ist hier die personelle Abhängigkeit nicht auf bestimmte Länder oder Regionen beschränkt und lokale, den Arbeitsablauf einschränkende Phänomene (Sperrzonen; Quarantäne) können ausgeglichen werden.

4.4 Erweiterte IT-Infrastruktur bei identity Giro



Die Datensätze der Auftraggeber oder Kooperationspartner der identity AG werden via SSL-Verbindung an das Rechenzentrum des Dienste-Anbieters-Hosting der identity AG übertragen und dort separiert von Daten anderer Kunden verarbeitet.

Die Speicherung von Nachweisdateien erfolgt dann in der bestehenden IT-Infrastruktur der identity AG im Nachweismanagement.

Die eigentliche Identitätsüberprüfung im identity Giro Verfahren wird abgebildet durch eine Schnittstellenbildung zu den gebundenen Geldinstituten oder durch die Einbindung der Software und Schnittstellen eines Bank-Ident-Partners.

Die Kommunikation zum Bank-Ident-Partner oder Geldinstitut mit dem „identity Portal“ erfolgt über SSL: TLS 1.2 gesicherte Webservice-Schnittstellen (z.B. SOAP, JSON, REST, XML).

Der Bank-Ident-Partner oder das Geldinstitut erhalten von der identity AG keinen zu prüfenden Datensatz des Empfängers. In der IT-Infrastruktur eines jeweilig eingesetzten Bank-Ident-Partners werden daher keine der vom Auftraggeber übertragenen personenbezogenen Daten verarbeitet, vorgehalten oder gespeichert.

Der Bank-Ident-Partner unterhält Schnittstellen zu seinen verbundenen Geldinstituten oder zum technischen Dienstleister der Geldinstitute.

Die Schnittstellen zum Bank-Ident-Partner sind nur über eine HTTPS Verbindung, die über ein SSL Zertifikat abgesichert sind, erreichbar. Alle Daten sind durch einen Hash, z.B. einen HMAC-MD 5 Hash, gegen Manipulation gesichert. Das Passwort für die Generierung des Hash Wertes wird nicht übermittelt.

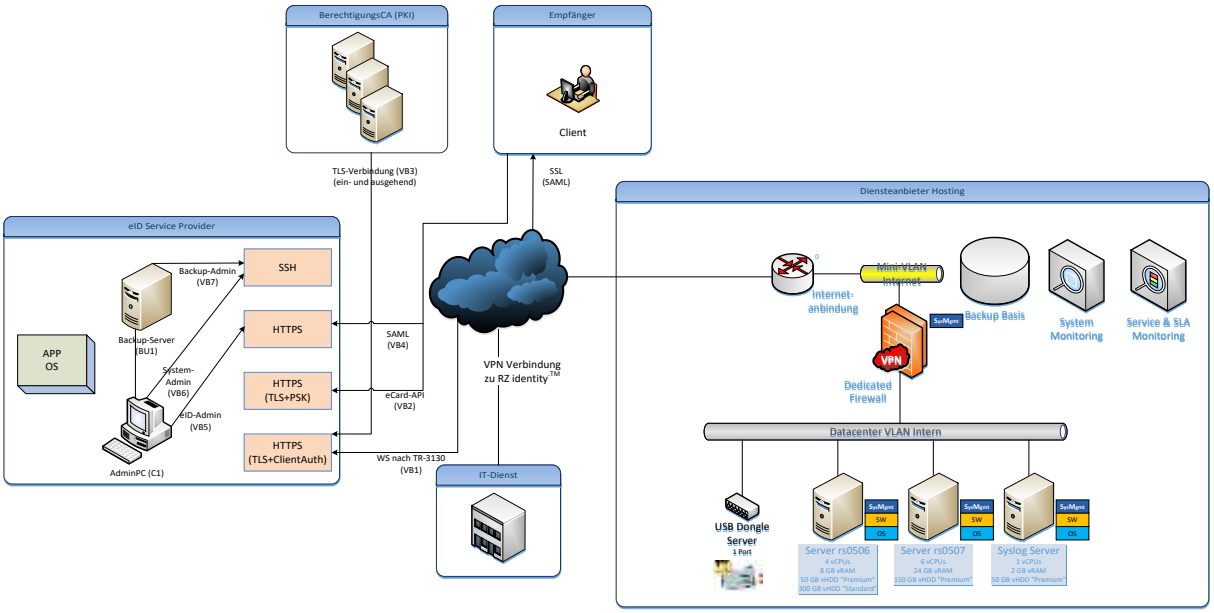
Darüber gelangt der Empfänger in das ihm vertraute Online-Banking Portal seines Geldinstitutes und wird aufgefordert seine Zugangsdaten, Benutzername/ Passwort einzugeben.

Die Kommunikation zwischen dem Empfänger und seinem online Banking erfolgt im Browser per SSL z.B. typischer Weise über ein EV-Zertifikat. In seinem online Banking gibt er den Datensatz zweckbezogen zur Identifikation frei und Bestätigt die per TAN.

Dieser IT-Aufbau ermöglicht es der identity Trust Management AG unabhängig von natürlichen Personen zu agieren.

Damit kann unabhängig von der gesundheitlichen Konstitution einzelner Identifizierer oder regionaler Identifizierer-Gruppen der Service überregional dargestellt werden. Mithin ist hier eine personelle Abhängigkeit in diesem Verfahren nicht vorhanden und das identity Giro Verfahren kann unabhängig von Einschränkungen der Bewegungsfreiheit (Quarantäne) oder Erkrankungen einzelner Personen zur Verfügung gestellt werden.

4.5 Erweitere IT-Infrastruktur bei identity eID



Die eigentliche Identitätsüberprüfung im identity eID Verfahren, kann durch einen eID Server der identity Trust Management AG oder durch die Einbindung eines eID-Service-Providers, die die gleichen inhaltlichen wie sicherheitstechnischen Kriterien erfüllen müssen, abgebildet werden.

Ein eingebundener eID-Service-Provider (Governikus) sichert die Kommunikation mit dem Personalausweis-Client des Empfängers sowie den Bezug aktueller Berechtigungszertifikate und Sperrlisten. Er übermittelt nach erfolgreicher Authentisierung des Personalausweisinhabers die aus dem Ausweis-Chip gelesenen Daten an den anfragenden Diensteanbieter. Er kommuniziert mit der identity AG über eine abgesicherte Verbindung (WS nach TR 03130).

In der IT-Infrastruktur eines jeweilig eingesetzten identity eID-Service-Providers, werden keine personenbezogenen Daten außerhalb des Zeitraumes der Identitätsprüfung verarbeitet, vorgehalten oder gespeichert. Alle Daten vom Kooperationspartner zur identity AG und umgekehrt, laufen vom Backend-System der identity Trust Management AG durchgängig und bi-direktional ausschließlich verschlüsselt über geschützte Verbindungen und Server und sind somit von außen nicht physisch greifbar.

Die Sicherheit und Authentizität der Datensätze sind durch die bereits auf ihre Sicherheit hin bestätigte IT-Infrastruktur der identity Trust Management AG in höchstem Maße gesichert.

Beteiligte in diesem Szenario sind:

- der Bürger mittels Client-Software (z. B. AutentClient_PA oder AusweisApp 2) und geeigneten Kartenlesegeräten;
- der Diensteanbieter
- der eID-Service-Provider als Anbieter der Dienstleistung „eID-Service“ durch den Betrieb eines oder mehrerer eID-Server einschließlich der unterliegenden Komponenten, wie
- Hardware-Sicherheitsmodul,
- Verbindung zur PKI des Beschaffungsamtes,
- MySQL-Server,
- Administrations-Client zur Wartung des Systems.

Der eID-Service-Provider kann für den Betrieb des eID Servers ein externes Rechenzentrum zum Betrieb der Systeme nutzen. Erforderlich dazu ist ein Rechenzentrum in Deutschland, welches nach DIN ISO 27001 auf der Basis von IT-Grundschutz zertifiziert ist und damit die zuvor geschilderten Anforderungen an die Sicherheit der IT-Infrastruktur erfüllt.

Die Server sind in einem, in höchstem Maße gesicherten, Rechenzentrum in gesicherten Räumen, deren Funktionen durch elektronische Türsicherungen, Zutrittskontrollsysteme, Videoüberwachung und Einbruchmeldeanlagen gesichert und geschützt sind zu betreiben. Das Rechenzentrum befindet sich in einem eigenen Sicherheitsbereich in dem die Bewachung z.B. über eine Alarmanlage auch außerhalb der Betriebsstunden gesichert ist.

Der Zutritt zum Gebäude ist durch ein zweistufiges Sicherheitsschließsystem ausreichend gesichert und die Zutrittsberechtigungen sind schriftlich in einer Sicherheitsrichtlinie dokumentiert.

Besuche werden dokumentiert. Besucher dürfen nur mit Administratoren die Sicherheitsbereiche betreten.

Die Verfügbarkeit ist gesichert durch entsprechende Brandschutzmaßnamen, Maßnahmen zur Sicherung der Stromversorgung, Notfallplanungen und Datensicherungsmaßnahmen.

Damit kann unabhängig von der gesundheitlichen Konstitution einzelner Identifizierer oder regionaler Identifizierer-Gruppen der Service überregional dargestellt werden. Mithin ist hier eine personelle Abhängigkeit in diesem Verfahren nicht vorhanden und das identity eID Verfahren kann weitestgehend unabhängig von Einschränkungen der Bewegungsfreiheit (Quarantäne) oder Erkrankungen einzelner Personen zur Verfügung gestellt werden.

4.6 Identifikation über einen bei der Verimi GmbH hinterlegten Identifizierungsdatensatz

Im Rahmen der Identifizierungslösung der Verimi GmbH wird die Verimi GmbH mit Zustimmung des jeweiligen Auftraggebers in den Identifizierungsprozess für den Auftraggeber in der Form eingebunden, so dass ein Kunde des Auftraggebers die Möglichkeit erhält, sich durch Übermittlung eines bei der Verimi GmbH hinterlegten Identitätsdatensatz durch die Verimi GmbH an den Auftraggeber zu identifizieren, sofern der hinterlegte Identitätsdatensatz der vom Auftraggeber beim Auftragnehmer angefragten Identifizierung entspricht.

Die eigentliche Identitätsüberprüfung in diesem Verfahren wird durch eine Schnittstellenbildung zu Verimi mit Einbindung der Software und Schnittstellen der Verimi abgebildet. Die Kommunikation zu Verimi und mit dem „identity Portal“ erfolgt über SSL: mind. TLS 1.2 gesicherte Webservice-Schnittstellen.

Damit kann unabhängig von der gesundheitlichen Konstitution einzelner Identifizierer oder regionaler Identifizierer-Gruppen der Service überregional dargestellt werden. Mithin ist hier eine personelle Abhängigkeit in diesem Verfahren nicht vorhanden und das identity Giro Verfahren kann weitestgehend unabhängig von Einschränkungen der Bewegungsfreiheit (Quarantäne) oder Erkrankungen einzelner Personen zur Verfügung gestellt werden.

4.7 identity autoID Verfahren

Gegenstand des identity autoID Verfahrens ist eine weitestgehend automatisierte Prüfung dahingehend, ob eine bestimmte natürliche Person ein zulässiges und gültiges Ausweisdokument vorgelegt hat. Dazu werden Bilder vom Ausweisdokument, sowie von der Person (Selfies) erfasst und an das Backend weitergeleitet. Dort findet ein Abgleich zwischen initialen Daten und den erfassten Daten, sowie ein Gesichtsabgleich zwischen Dokument und Selfie statt. Darüber hinaus findet eine Liveness Detection statt. Die Prüfung im Backend kann manuell oder automatisiert erfolgen. Ist das Ergebnis der identity autoID Prüfung nicht eindeutig positiv, erfolgt die Überleitung des Nutzers in das Video Verfahren und die Verbindung zum Video Agenten wird aufgebaut. In der Video Konferenz werden Ausweisdokument und die Zuordnung zur natürlichen Person erneut geprüft. Hier gelten die Erwägungen zu 4.3.

Damit kann unabhängig von der gesundheitlichen Konstitution einzelner Identifizierer oder regionaler Identifizierer-Gruppen der Service überregional dargestellt werden. Mithin ist hier eine personelle Abhängigkeit in diesem Verfahren nicht vorhanden und das identity autoID Verfahren kann weitestgehend unabhängig von Einschränkungen der Bewegungsfreiheit (Quarantäne) oder Erkrankungen einzelner Personen zur Verfügung gestellt werden.

5 Zertifikate

Das Rechenzentrum ist jeweils DIN ISO 27001 zertifiziert.

Die ISO 27001 ist die international führende Norm für Informationssicherheits-Managementsysteme. Sie gilt für privatwirtschaftliche und öffentliche Unternehmen sowie gemeinnützige Organisationen und definiert die Forderungen für die Einführung, Umsetzung, Überwachung und Verbesserung eines Informationssicherheits-Managementsystems (ISMS). Die ISO 27001 bietet einen systematischen und strukturierten Ansatz, der vertrauliche Daten schützt, die Integrität der betrieblichen Daten sicherstellt und die Verfügbarkeit der IT-Systeme im Unternehmen erhöht.

Das Rechenzentrum ist Tier 3 zertifiziert.

Qualitätsstufe 3 - Tier 3 Rechenzentren verwenden redundante Komponenten sowie mehrfache, aktive und passive, Versorgungswege. Das System wird dadurch fehlertolerant und eine Wartung ist auch während des Betriebs möglich. Single Points of Failure kommen auch in Qualitätsstufe 3 - Tier 3 Rechenzentren vor. Rechenzentren der Qualitätsstufe 3 - Tier 3 erhöhen ihre Ausfallsicherheit zudem durch mehrere Brandabschnitte. Insgesamt erreicht ein Rechenzentrum in Qualitätsstufe 3 bei einer Ausfallzeit von 1,6 Stunden **jährlich eine Verfügbarkeit von 99,98 Prozent**.

6 Zwischen-Fazit für die online Verfahren

Dieser IT- Aufbau ermöglicht es der identity Trust Management AG, Callcenter-Kapazitäten weltweit und vor allem in ganz Europa aufzubauen und vorzuhalten, die die Produktivität des identity Video Verfahrens sichern. **identity autoID, identity Giro und das identity eID** Verfahren bestehen aus der Kombination technischer Komponenten und können daher personalunabhängig betrieben werden.

Zurzeit bestehende Video Callcenter-Kapazitäten:

	M.S.S. Vertriebsgesellschaft mbH & CO.KG Manteuffelstr. 74 12103 Berlin	Callcenter- Dienstleistungen im Video Ident; 2 Callcenter in Kroatien
	Younixq Identity AG Tentschertstr. 7 1230 Wien	Callcenter- Dienstleistungen im Video Ident; Callcenter in Österreich
	Te-No GmbH Siemensstraße 6 71101 Schönaich	Callcenter- Dienstleistungen im Video Ident; Callcenter in Griechenland
	CHO-TIME GmbH Berliner Platz 12 41061 Mönchengladbach	Callcenter- Dienstleistungen im Video Ident in Deutschland
	CMF Consulting G7, 22 68159 Mannheim	Callcenter- Dienstleistungen im Video Ident in Deutschland
	S-Markt & Mehrwert GmbH & Co. KG Grenzstraße 21 06112 Halle	Callcenter- Dienstleistungen im Video Ident in Deutschland
	identity Trust Management AG Lierenfelder Str. 51 40231 Düsseldorf	Callcenter- Dienstleistungen im Video Ident in Deutschland
	TELLCONNECT SERVICE SOLUTIONS S.R.L. Bulevardul VICTORIEI Nr. 42 550024 Sibiu	Callcenter- Dienstleistungen im Video Ident in Rumänien
	Online Office Service s.r.l. Str. Szemler Ferenc. Nr 4 500331 Brasov	Callcenter- Dienstleistungen im Video Ident in Rumänien
	MSS Hermes Iletisim Bahcelievler mah. G.M.K Blv., 32421 Yenisehir Mersin	Callcenter- Dienstleistungen im Video Ident

Video CC stehen auch in der Türkei zur Verfügung und auf Abruf bereit. Hierzu müssen EU Model Clauses für eine Herstellung europäischen Datenschutzniveaus gezeichnet werden. Damit kann unabhängig von der gesundheitlichen Konstitution einzelner Identifizierer oder regionaler Identifizierer-Gruppen der Service überregional dargestellt werden. Mithin ist hier die personelle Abhängigkeit nicht auf bestimmte Länder oder Regionen beschränkt und lokale, den Arbeitsablauf einschränkende Phänomene (Sperrzonen; Quarantäne) können ausgeglichen werden.

7 Offline Verfahren identity Kurier und identity Shop

identity Shop

In dem Verfahren identity Shop arbeitet die identity Trust Management AG mit vertraglich gebundenen Filial-Ident-Partnern oder unmittelbar mit Shop-Betreibern zusammen.

Im Verfahren identity Shop wird dem Endkunden die Möglichkeit zur Wahl von Ort und Zeit der Identitätsprüfung im Rahmen der Örtlichkeiten und Öffnungszeiten der Shops gelassen. Im identity Shop Verfahren, sprechen wir von einem passiven Vorhalten der Identitätsprüfleistung in autorisierten Shops.

Im identity Shop Verfahren wird der Ort der Identitätsprüfung durch die Auswahl der autorisierten Shops begrenzt und muss im Rahmen der jeweiligen Öffnungszeiten des Shops erfolgen.

identity Kurier

Das Identifizierungs-System der identity Trust Management AG für das identity Kurier Verfahren, besteht aus regional aktiven Kurierunternehmen (Service Partner), die durch eine bundesweit einheitliche und genormte Betriebssoftware (identity Portal) sowie einem Transportlogistiksystem (intern oder extern) vernetzt sind und im Auftrag der identity Trust Management AG die Durchführung der Identitätsprüfungen leisten.

8 Risikobetrachtung

Die zwischen der identity AG und seinen Kooperationspartnern vertraglich vereinbarten Prozesse, sind für die **online Verfahren** im Hinblick auf die Nichtverfügbarkeit einzelner Räumlichkeiten und Personal nicht als sicherheitskritisch einzustufen.

Unabhängig von der gesundheitlichen Konstitution einzelner Identifizierer oder regionaler Identifizierer-Gruppen kann der Service überregional dargestellt werden. Mithin ist hier die personelle Abhängigkeit nicht auf bestimmte Länder oder Regionen beschränkt und lokale, den Arbeitsablauf einschränkende Phänomene (Sperrzonen; Quarantäne) können ausgeglichen werden.

Die identity AG verfügt über eigene und externe Callcenter von Video Ident Partnern. Der Wegfall einzelner Räumlichkeiten oder von Personal in einzelnen Callcentern, kann jederzeit kurzfristig, in Tagesfrist, durch andere Callcenter Einheiten aufgefangen werden.

identity Giro, identity eID. Identity autoID und das Verfahren **über Verimi** laufen weitestgehend unabhängig von Personalkapazitäten.

Der identity Legal Service wird im Wesentlichen in eigenen Callcentern mit eigenen Mitarbeitern abgebildet. Die Software ist jedoch Standort unabhängig einsetzbar.

Für die verantwortlichen Rollen stehen mehrere ausgebildete Identifizierer/Prüfer zur Verfügung, so dass unerwartete Ausfälle jederzeit aufgefangen werden können.

identity Legal kann auch bei einem vorbereiteten und vertraglich gebundenen externen Callcenter durchgeführt werden. Bei einem Ausfall der Räumlichkeiten der identity AG, ist ein Wechsel und die Durchführung der Aufträge jederzeit möglich.

Ausfälle einzelner Identifizierer (Video) oder Störungen in einzelnen Verfahren, können so in der Gesamtstruktur (Video CC in anderen Ländern) aufgefangen werden.

Für das identity Video Verfahren kämen wir nur dann an Grenzen, wenn im unwahrscheinlichen Fall in einzelnen EU-Ländern Sperrzonen, Quarantäne oder sonstige Maßnahmen getroffen werden, die persönliche Arbeitsfreiheit einschränken.

Die Situation in den offline Verfahren:

Sowohl die Shops als auch die vertraglichen gebundenen Kuriere sind bundesweit verteilt. Beim Ausfall einzelner Shops oder Kuriere kann jederzeit auf andere Shops oder Kuriere zurückgegriffen werden.

Kurier können gebietsübergreifend eingesetzt werden. Der Endkunde kann den Shop frei wählen und gegebenenfalls eine längere Anreise in Kauf nehmen.

Diese offline Verfahren sind allerdings Verfahrensimmanent auf den persönlichen Kontakt zum Endkunden angewiesen.

Einschränkungen können hier entstehen durch Sperrzonen oder dann, wenn Quarantäne oder sonstige die persönliche Arbeitsfreiheit einschränkende Maßnahmen, getroffen werden.

Die Leistungserbringung in den Verfahren Kurier und Shop ist mit Wirkung des 18.03.2020 nicht mehr sichergestellt und alle Identifizierer wurden vorübergehend von der Verpflichtung zu Durchführung der Identifizierung befreit. Die Leistungserbringung erfolgt bundesweit sporadisch und selbstentschieden durch die Kurier- oder Shop-Unternehmer. Wir gehen davon aus, dass die Services solange beeinträchtigt werden, wie der allgemeine Pandemie-Gefährdungsstatus „hoch“ für das Bundesgebiet aktiv sein wird.

Getroffene Maßnahmen

In unserer Verwaltung in Düsseldorf sind wir seit dem 28. Februar 2020 im Notfallmodus unterwegs.

Seit dem 11. März 2020 haben wir die Maßnahmen deutlich ausgeweitet.

Alle „Head of `Department“, sowie die Kolleginnen/Kollegen aus der Entwicklung und IT arbeiten im Home-Office. Die durchgängige Erreichbarkeit ist hierbei jederzeit sichergestellt (Handy/Laptop). Auch alle operativen Abteilungen arbeiten von zu Hause. Am Standort in Düsseldorf ist aktuell nur die Buchhaltung besetzt, sowie in einem davon getrennten Gebäudeabschnitt die Düsseldorfer Video-Agenten.

Die Video Agenten wurden in zulässiger Ausnutzung der gesamten räumlichen Kapazität weitmöglichst auseinandergesetzt.

Diese Maßnahmen zielen darauf ab, alle Entscheidungsträger und soweit wie möglich auch sämtliche Mitarbeiterinnen/Mitarbeiter in häuslicher Quarantäne zu isolieren.

Allen iTM-Mitarbeitern wurde empfohlen bis auf Weiteres öffentliche Veranstaltungen zu meiden. Darüber hinaus wurden Hygiene-Hinweise gegeben, sowie Vorgaben, was zu tun ist, wenn es zu gesundheitlichen Veränderungen kommt bzw. Symptome auftreten.

Hier wurden auf die Meldepflichten besonderen Wert gelegt. Zudem wurden Links zum Gesundheitsministerium zur Verfügung gestellt.

Jeden Morgen werden aktuelle Statusmeldungen bei allen Mitarbeiterinnen/Mitarbeitern eingeholt.

Sämtliche Reisetätigkeiten wurden bis zur erneuten Freigabe durch den Vorstand eingestellt.

Geplante Reisen erfolgen nur noch im Fall einer besonderen Dringlichkeit und müssen vom Vorstand genehmigt werden. Neue Reisen werden nicht geplant.

Diese zuvor genannten Maßnahmen gelten auch für unsere externe Callcenter-Struktur. Sämtliche Informationen, die wir an unsere Mitarbeiterinnen/Mitarbeiter gegeben haben, wurden auch dort platziert.

Aktuell erhalten wir auch von dort jeden Morgen einen aktuellen Statusbericht. Auf plötzliche Agentenausfälle kann an jedem Standort kurzfristig reagiert werden. Es stehen ausreichende Ersatzkapazitäten bereit. Sollte der unwahrscheinliche Fall auftreten, dass ein oder zwei Callcenter komplett ausfallen, kann der Auftragseingang ohne größere Probleme in der restlichen Struktur bearbeitet werden. Alle Nachunternehmer der identity Trust Management AG wurden im Sinne des Notfallplans schriftlich verpflichtet und werden bei Aktualisierungen mit einbezogen. Schriftliche Verpflichtungserklärungen aller Nachunternehmer der identity Trust Management AG liegen vor.

23.03.2020:

Die Leistungserbringung in den Verfahren Kurier und Shop hat sich über das Wochenende weiter verunsichert.

Bereits seit dem 18.03.2020 wurden alle Identifizierer vorübergehend von der vertraglichen Verpflichtung zu Durchführung der persönlichen Identifizierung befreit. Soweit die Depots und Shops weiter freiwillig tätig waren war dies weiterhin möglich.

Vor dem Hintergrund der Ausgangs- und Tätigkeitsbeschränkungen vom Wochenende durch die Bundesregierung ist eine gewisse Unsicherheit entstanden:

Nach unserer Kenntnis und der unseres Filial Ident Partners dürfen DHL Shops/ Postbank im Wesentlichen weiter öffnen. Auch bei unserem Filial Ident Partner DPD sind die Shops weiter geöffnet, die sich in geöffneten Geschäften befinden, wie Lebensmittelversorgung, Kioske etc.

Grundsätzlich sehen wir und der DPD eine Benachteiligung gegenüber den privaten Paketdienstleistern (DPD, GLS, Hermes, etc.) und diese versuchen gerade denselben Status zu erhalten wie DHL, damit auch die weiteren Shops geöffnet bleiben dürfen.

Hier ist die Lage noch nicht abschließend geklärt. Aktuell bieten die identity-Shops die Identifikation auf freiwilliger Basis ab. Einige der Shops haben die Leistungserbringung eingestellt. Wir bemühen uns den Shop Finder in Abstimmung mit den Shops zu aktualisieren, was leider nicht vollständig gelingt. Dadurch bedingt kann es zu Störungen kommen.

Dies betrifft auch die Kurierdienste, die in Teilen weiter aktiv sind. Dies berücksichtigen wir bei der Terminvergabe.

Online Verfahren: Giro, eID und autoID funktionieren weiter uneingeschränkt. Wir empfehlen dringend die Zulassung dieser Verfahren zu prüfen. Die identity TM AG hat hierfür notwendige Vertragsergänzungen vorbereitet, die abgefordert werden können. Bitte nehmen Sie hierzu Kontakt zu Ihrem verantwortlichen Key-Account Manager auf.

Unser eID Service Provider, die Governikus, hat heute mitgeteilt:

„Unterdessen waren wir bei Governikus nicht untätig und haben unsererseits umfangreiche Maßnahmen ergriffen, um unseren Anteil zur Reduzierung von Übertragungsrisiken beizutragen.

- Wir halten uns an die vom Robert-Koch-Institut empfohlenen Maßnahmen.
- Bis auf wenige Ausnahmen arbeiten seit vergangener Woche alle unsere Mitarbeiter*innen aus dem Homeoffice. Aufgrund unserer bereits vor der Krise etablierten sicheren IT-Infrastruktur und dem Einsatz unserer hausinternen Systemadministratoren und -experten haben wir hier keine Einschränkungen in unserer Leistungsfähigkeit. Zusätzliche Arbeitsmittel in Form von Hardware bis hin zu Bildschirmen und Bürostühlen stellen wir unseren Mitarbeiter*innen für die Arbeit im Homeoffice bereit. Unsere ohnehin schon sehr flexible Vertrauensarbeitszeit und weiterführende Maßnahmen hinsichtlich der Kinderbetreuung für Eltern oder Betreuung von Angehörigen sind ebenfalls von Vorteil in der Krise.
- Sämtliche Meetings – sowohl intern als auch extern – haben wir auf Videokonferenzen umgestellt.

Sie können sich auf den gewohnten Service des Governikus-Teams verlassen. Wir sind auch in der Krise an Ihrer Seite und wie gewohnt für Sie erreichbar! Gemeinsam werden wir hoffentlich so unbeschadet wie möglich auch diese unvorhergesehenen Herausforderungen bestehen.“

Video Ident Verfahren:

In Anbetracht und Erwartung weiterer nationaler Einschränkungen, erweitern wir bereits seit einiger Zeit unsere Video CC Struktur:

Die Video CC in **Rumänien** sind eingerichtet und live verfügbar. Die Schulungen laufen weiter kontinuierlich und die verfügbaren Agentenzahlen steigen.

Weiter haben wir unsere Verträge zu bereits geschulten und im erfahrenen Video CC in der **Türkei und Bosnien** reaktiviert. Einzelne Kunden hatten auf eigenen Wunsch darauf schon in Vorjahren zugegriffen und die Video CC sind wieder im Einsatz, dort wo das regulatorisch möglich und vom Kunden die EU Model Clauses zur Herstellung des DSGVO Datenschutzniveaus gezeichnet wurden.

Die Leistungsfähigkeit im Video Ident Verfahren ist bislang **nicht** eingeschränkt. Wir können berichten, dass alle Mitarbeiter in den CC von Corona Fällen bislang verschont geblieben sind.

Einschränkungen im öffentlichen Nahverkehr haben in Griechenland zu erheblichen Einschränkungen geführt. Die Video CC arbeiten aber zurzeit mit geringfügigen Einschränkungen weiter. Diese beschränken sich vorwiegend auf die An- und Abreise.

In den anderen Ländern funktioniert, auch bei geringeren Stundentakten die Anreise der Identifizierer zur Arbeit, vermehrt auf privaten Wegen, KFZ, Fahrrad/Moped und Sonstiges. Auf die geänderten Fahrzeiten des öffentlichen Nahverkehrs sind wir den Mitarbeitern entgegengekommen und planen mit entsprechenden Gleitzeiten.

Erweitere Nachunternehmerliste Video Callcenter-.Möglichkeiten:

Nach jeweiliger Zeichnung der EU Model Clauses durch unsere Kunden können wir auch die Video CC in der Türkei und Bosnien einsetzen:

	M.S.S. Vertriebsgesellschaft mbH & CO.KG Manteuffelstr. 74 12103 Berlin	Callcenter- Dienstleistungen im Video Ident; 2 Callcenter
	Younixq Identity AG Tentschertstr. 7 1230 Wien	Callcenter- Dienstleistungen im Video Ident; Callcenter in Österreich
	Te-No GmbH Siemensstraße 6 71101 Schönaich	Callcenter- Dienstleistungen im Video Ident; Callcenter in Griechenland
	CHO-TIME GmbH Berliner Platz 12 41061 Mönchengladbach	Callcenter- Dienstleistungen im Video Ident in Deutschland
	CMF Consulting G7, 22 68159 Mannheim	Callcenter- Dienstleistungen im Video Ident in Deutschland
	S-Markt & Mehrwert GmbH & Co. KG Grenzstraße 21 06112 Halle	Callcenter- Dienstleistungen im Video Ident in Deutschland

	identity Trust Management AG Lierenfelder Str. 51 40231 Düsseldorf	Callcenter- Dienstleistungen im Video Ident in Deutschland
	TELLCONNECT SERVICE SOLUTIONS S.R.L. Bulevardul VICTORIEI Nr. 42 550024 Sibiu	Callcenter- Dienstleistungen im Video Ident in Rumänien
	Online Office Service s.r.l. Str. Szemler Ferenc. Nr 4 500331 Brasov	Callcenter- Dienstleistungen im Video Ident in Rumänien
	DE Line drusto za trgovini usluge d.o.o. Hamdije Kresevljakovica 40, 71000 Sarajevo Bosnien-Herzegowina	Callcenter- Dienstleistungen im Video Ident
	DM Solution Fenix d.o.o. Petra Preradovica 27, 78000 Banja Luka Bosnien-Herzegowina	Callcenter- Dienstleistungen im Video Ident
	MSS Hermes Iletisim Bahcelievler mah. G.M.K Blv., 32421 Yenisehir Mersin	Callcenter- Dienstleistungen im Video Ident

Mit Bezug auf das Erdbeben in Zagreb und die davon betroffenen Callcenter der M.S.S., gab es leichte zeitliche Verzögerungen mit geringfügig längeren Wartezeiten in der Warteschleife. Das konnte aber schnell durch die Verlagerung zwischen den CC, dort wo das vertraglich möglich war, im Gesamtsystem aufgefangen werden.

Wir empfehlen Ihnen vorsorglich den EU-Model Closes beizutreten und den Einsatz der Non-EU Callcenter zuzustimmen.

Verwaltung:

Vor dem Hintergrund der durch die Bundesregierung am 22.03.2020 verschärften Verhaltens-Regeln, haben wir unsere Mitarbeiter entsprechend angewiesen:

- Im Office- Betrieb ist der Mindestabstand von 1,50 m einzurichten und einzuhalten. Dies gilt auch für notwendige persönliche Kontakte!
- Den Callcenter Bereich dürfen ab sofort nur noch die dort arbeitenden Mitarbeiter und Mitarbeiterinnen betreten (über die Regularien hinaus wird der Zutritt von Aufsichtspersonal und IT soweit wie möglich reduziert)
- Der Verwaltungstrakt darf durch die Callcenter-Mitarbeiter und Mitarbeiterinnen nicht mehr betreten werden. Benötigte Materialien werden ohne gleichzeitige Anwesenheit über die Verbindungstür getauscht.
- Dritte erhalten keinen Zutritt mehr in unsere Räumlichkeiten- der Ident Shop-Betrieb am Empfang wurde mit sofortiger Wirkung eingestellt. Eine Benachrichtigung wurde an der Eingangstür platziert.
- Mitarbeiter im Home-Office, die einen Besuch im Büro planen, melden diesen beim Vorstand an, mit Grund und Dauer, der Vorstand behält sich vor, über Besuche im Einzelfall zu entscheiden.
- Persönliche Termine mit Dritten sind untersagt!

Alle anderen Anweisungen bleiben aktiv und gelten weiterführend ohne zeitliche Beschränkung.

9 Wiederanlauf nach Havarien

Die einzelnen Komponenten der Infrastruktur sind über den gesamten Prozess der Services der identity Trust Management AG **redundant** ausgelegt. Fällt eine Komponente aus, übernimmt eine andere deren Aufgabe und der betroffene Bereich wird vom identity System getrennt. Ist der havarierte Bereich wieder verfügbar, kann dieser nach der Wiederherstellung und Testphase seiner Zuverlässigkeit wieder aufgeschaltet werden. Beide Verfahren finden in enger Abstimmung zwischen dem IT-Dienst der identity AG, den betroffenen Partnern und dem Management statt. Ggf. werden in Einzelfällen direkt betroffene Kunden am Prozess beteiligt, wenn deren Zuarbeit für den Wiederanlauf benötigt werden.

Die einzelnen Bereiche im Rechenzentrum, welche zur Erbringung der Leistung der identity AG als kritische und zentrale Bereiche eingestuft werden, verfügen gem. ISO 27001 über abgestimmte Notfall- und Wiederanlaufkonzepte (durch die jeweils geforderten Mindestanforderung an regelmäßig erneuerte Zertifizierungen nachgewiesen DIN ISO 27001). Diese Konzepte und Dokumentationen können gegebenenfalls im Rahmen einer Auditierung, aufgrund der sicherheitsrelevanten Informationen, vor Ort eingesehen werden.

Einzelne Personen oder IT Infrastrukturbestandteile gehören ebenfalls aufgrund von Vertreterregelungen oder redundanter Auslegung nicht zu kritischen Bestandteilen der Services der identity AG, für die Erbringung der Leistungen der identity AG werden neben dem Rechenzentrum und den Callcentern keine speziellen IT Systeme benötigt. Daher hat ein Ausfall außerhalb dieser Infrastrukturen keine Auswirkung auf den Gesamtprozess.

Alle vertraglich gebundenen Dienstleister und externen Dienste zur Erbringung einzelner Teilprozesse der identity Services stehen ebenfalls hochverfügbar bereit. Dies bezieht sich im Besonderen auf die Systeme der Trust Service Provider im Bereich der QES oder anderer, nachgelagerter Dienstleistungen im Rahmen der Identifizierungen. Fällt dennoch einer der Dienste aus, ist der Service der identity Trust Management AG für diesen Teilbereich nicht verfügbar, bis der nachgelagerte Dienst wieder zur Verfügung steht bzw. die Ersatzkapazität, wie zuvor geschildert, in Anspruch genommen werden kann und aktiviert ist.