Verfahrensanweisung für die Anlage von HR Stammdaten im „Service Fremdkräfte verwalten“ im SAP HR bzw. MyPortal zur Vergabe von IT-Accounts für externe Mitarbeiter, konzerninterne Fremdeinsätze, Pseudonyme, Robot und Funktionsgruppen

Inhaltsverzeichnis

1. ALLGEMEINE HINWEISE

Durch die Deutsche Telekom AG werden jedem Mitarbeiter, jedem externen Mitarbeiter aber auch Funktions-/ Gruppen-Accounts und Robot-Accounts der Deutschen Telekom AG, deren Töchter und Beteiligungen, die durch Workplace Services betreut werden, digitale Zertifikate für Signatur, Verschlüsselung und Authentifizierung als Arbeitsmittel zur Verfügung gestellt.
Mit Anlegen eines Stammdatensatzes wird der dazugehörende IT-Account berechtigt Zertifikate mit diesen Daten zu beantragen und zu nutzen.
Da die Ausstellung und Nutzung der Zertifikate aus einer öffentlichen Zertifizierungsstelle (CA) erfolgt, ist die Einhaltung dieser Verfahrensanweisung zur Anlage von Stammdatensätzen sowie der hier genannten Nutzungsbedingungen und eine Zustimmung erforderlich.

Was ist ein Zertifikat?
Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften (Identität) von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten.
Die Ausstellung der Zertifikate innerhalb der Deutschen Telekom AG erfolgt durch eine offizielle Zertifizierungsstelle, die Certification Authority (CA).
Die Verwendung einer digitalen Signatur, bindet unter Nutzung des öffentlichen Schlüssels die Identität (z.B. Person, Gerät) an ein elektronisches Dokument, bzw. Email.

Bitte lesen Sie deshalb diese Verfahrensanweisung aufmerksam durch!
Legen Sie nur dann einen Stammdatensatz an, wenn Sie dieser Verfahrensanweisung und den Nutzungsbedingungen der Corporate PKI zustimmen.
Im Falle, dass Sie mit diesen Bedingungen nicht einverstanden sind, dürfen Sie keinen Stammdatensatz erstellen, der zur Beantragung, bzw. Ausstellung eins Zertifikats führt.

Hintergrund ist, dass sowohl für interne Mitarbeiter als auch externe -Mitarbeiter IT-Accounts mit einem Email-Postfach und myCard benötigt werden.

Ebenso werden für Testsysteme, Schulungen, Messerechner und Automaten IT-Accounts benötigt, die genauso funktionieren müssen wie die von den Mitarbeitern verwendeten persönlichen IT-Accounts mit Postfach und MyCard. Des Weiteren kann es erforderlich sein, dass für einen Mitarbeiter ein IT-Account angelegt werden muss, bei dem der Name von dem Namen der realen Person abweicht.

Die Verwaltung dieser Accounts und deren Inhalt unterliegen bestimmten Anforderungen, die in diesem Dokument beschreiben werden.

1.1. Risiken beim Falschangaben oder Bestätigung von nicht Richtigen Stammdaten im „Service Fremdkräfte verwalten“ im SAP HR bzw. MyPortal zur Vergabe von IT-Accounts

Hintergrund dieser Verfahrensanweisung ist, dass das Accountmanagement wie auch die zertifikatsausgebende Zertifizierungsstelle der Deutschen Telekom AG verschiedenen regulatorischen und gesetzlichen Anforderungen unterliegt. Von den Browser- und Betriebssystemherstellern werden Richtlinien verabschiedet, die für die Teilnahme an deren Rootprogramm verpflichtend sind.

Besondere Beachtung gilt zudem der Einhaltung der electronic IDentification, Authentication and trust Services (eIDAS) (deutsch: Verordnung über elektronische Identifizierung und Vertrauensdienste der Europäischen Union), deren Gesetz zur Durchführung dieser Verordnung und von Urheberrechten und Datenschutz. Des Weiteren sind die gesetzlichen Vorgaben und Anforderungen der Externen Wirtschaftsprüfer an das Accountmanagement einzuhalten.

Nach diesen Vorgaben muss:

- eine eindeutige Identifizierung des Antragsstellers und des Zertifikatsinhabers jederzeit möglich sein.
- bei natürlichen Personen der Vor- und Nachname mit dem Namen im amtlichen Ausweisdokument identisch sein und das Geburtsdatum und ggf. der Geburtsort als Unterscheidungsmerkmal wahrheitsgemäß angegeben werden.
- bei Abweichungen des Vor- oder Nachnamens einer natürlichen Person darf kein Stammdatensatz erstellt und es dürfen keine Zertifikate erstellt werden. Eine Ausnahme bilden hier Pseudonyme.
- bei Abweichungen des Vor- oder Nachnamens einer natürlichen Person vom amtlichen Ausweisdokument oder wenn das amtliche Ausweisdokument nicht geprüft werden kann um die Person zu identifizieren, muss die Person als Pseudonym klassifiziert und gekennzeichnet werden. Ein Pseudonym ist z.B. dann schon gegeben, wenn der korrekte Name um Namenszusätze oder andere Bezeichnungen erweitert wird. Es ist zudem immer die Identität der realen natürlichen Person zu prüfen und in den Stammdaten zu erfassen.
- bei Accounts, die nicht mit einer natürlichen Person identisch sind, ein Schlüsselverantwortlicher benannt sein, der die Verantwortung für die Nutzung des Accounts und der ausgestellten Zertifikate trägt. Dies ist im Konzern der DTAG immer der aktuelle Kostenstellenverantwortliche (KostV) für diesen Account.

Die Einhaltung aller Anforderungen werden im TrustCenter der DTAG einmal im Jahr durch einen unabhängigen externen Auditor nach den European Telecommunications Standards Institute (ETSI) Regularien ETSI 319411-1 und ETSI 319401 überprüft und ggf. bestätigt. Die Browser- und Betriebssystemhersteller verlangen jährlich die Ergebnisse der Überprüfung.

Sollte der Nachweis durch die Auditierung nicht erbracht werden, können die Hersteller das Root-Zertifikat der Deutschen Telekom AG aus deren Rootprogramm entfernen. Das hat massive Auswirkungen auf den Betrieb der Deutschen Telekom, des TrustCenters der DTAG und bestehenden Kunden und Services. Des Weiteren können gegen die Deutsche Telekom Strafzahlungen und Bußgelder in erheblichem Ausmaß verhängt werden.

Zusätzlich erfolgt einmal jährlich eine Überprüfung des Accountmanagements durch einen unabhängigen Wirtschaftsprüfer. Abweichungen von den Anforderungen der Wirtschaftsprüfer oder der gesetzlichen Vorgaben können zu einem Eintrag im jährlichen Rechenschaftsbericht der Deutschen Telekom AG und ebenfalls zu Strafzahlungen und Bußgelder in erheblichem Ausmaß führen.

1.2. Verantwortlichkeit für die Nutzung des Accounts und der ausgestellten Zertifikate

- Verantwortlich für die ordnungsgemäße Nutzung der genannten Accounts und der hierfür ausgestellten Zertifikate ist die natürliche Person auf dessen Namen das Zertifikat ausgestellt wurde.
- Bei Pseudonymen, Funktions- und Gruppenaccounts bzw. Robot-Accounts ist der KostV für das Arbeitsverhältnis, dem der Stammsatz bzw. Account zugeordnet ist, für die ordnungsgemäße Nutzung der Accounts und der hierfür ausgestellten Zertifikate verantwortlich.

Bei deliktischem Handeln oder Straffällen wird diese Person zur Verantwortung gezogen. Dies kann arbeitsrechtliche als auch strafrechtliche Konsequenzen zur Folge haben.

2. DEFINITION KATEGORISIERUNG:

ACHTUNG: IM RAHMEN VON REGULATORISCHEN VORGABEN WURDEN DIE KATEGORIEN ÜBERARBEITET. DIE KATEGORIE "TECHNISCHE PERSON" IST WEGGEFALLEN UND TEILT SICH IN MEHRERE KATEGORIEN AUF. TECHNISCHE PERSONEN KÖNNEN NICHT MEHR ANGELEGT WERDEN. AB SOFORT GELTEN DIE FOLGENDEN DEFINITIONEN FÜR DIE KATEGORIEN

1. External Workforce (Konzernextern):
   In der Kategorie "External Workforce" werden Fremdkräfte erfasst, welche über einen Bestellvorgang im Rahmen von Dienst- oder Werkverträgen als auch Leih- und Zeitarbeitsverträgen beauftragt wurden. Bei der Eingabe ist eine valide Bestellnummer erforderlich. Da es sich um eine natürliche Person handelt, muss der angegebene Vor- und Nachname exakt mit dem Namen im amtlichen Ausweisdokument übereinstimmen. Dies muss bei der Eingabe bestätigt werden.

2. Interner Fremdeinsatz (Konzernintern):
   In der Kategorie "Interner Fremdeinsatz" werden konzerninterne Mitarbeiter erfasst, die außerhalb ihres Betriebes tätig sind. Da es sich um eine natürliche Person handelt, muss der angegebene Vor- und Nachname, sowie das Geburtsdatum exakt mit den Angaben im amtlichen Ausweisdokument übereinstimmen. Dies muss bei der Eingabe bestätigt werden.

3. Pseudonym-Account:
   Ein Pseudonym ist eine natürliche Person, bei der der Vorname und oder Nachname vom Namen im amtlichen Ausweisdokument abweicht, bzw. bei dem der amtliche Ausweis nicht geprüft werden kann. Dies trifft bei Duplikate Accounts zu, welche i.d.R. konzerninterne Mitarbeiter internationaler Einheiten betrifft, die bereits einen Account (bspw. EMEA2) besitzen, aber noch einen zusätzlichen Duplikat-Account benötigen (bspw. EMEA1, um mit deutschen Applikationen arbeiten zu können). Bei der Eingabe wird dem Vornamen automatisch ein „PN-“ vorangestellt (PN-Vorname). Zusätzlich ist aber darauf zu achten, dass die Namenskonversion bei Duplikat Accounts eines internationalen Mitarbeiter wie folgt aufgebaut und einzugeben ist: „PN-DUP“+[Richtiger Vorname]+“-“+[2-stelliger ISO Country Code] : z. B. PN-DUPMaximilian-RO.

4. Funktions-Account:
   In der Kategorie „Funktions-Accounts“ werden keine natürlichen Personen erfasst. Diese Kategorie dient ausschließlich dafür einen Account für bestimmte Personengruppen zu generieren z. B. für Empfänge oder zur Nutzung von Messerechner, Schulungsrechner, Benutzer für Testsysteme, etc. Es muss immer ein Schlüsselverantwortlicher benannt sein. Aktuell ist dies der hinterlegte Kostenstellenverantwortliche. Bei der Eingabe wird dem Vornamen automatisch ein „GRP-“ vorangestellt (GRP-Vorname).

5. Robot-Account:
   In der Kategorie „Robot-Accounts“ werden keine natürlichen Personen oder Personengruppen erfasst. Diese Kategorie dient ausschließlich dafür Accounts zu generieren, die automatisiert von Roboter, bzw. Bots bedient werden. Es muss immer ein Schlüsselverantwortlicher benannt sein. Aktuell ist dies der hinterlegte Kostenstellenverantwortliche. Bei der Eingabe wird dem Vornamen automatisch ein „ROBOT-“ vorangestellt (ROBOT-Vorname).

6. Sales & Partner:
   In der Kategorie „Sales & Partner“ werden externe Mitarbeiter (natürliche Personen) von Partneragenturen und sonstigen Partnerfirmen, welche einen Telekom Benutzeraccount (inkl. external-Mailadresse) für die Herstellung der Arbeitsfähig benötigen. Bei diesen externen Mitarbeitern handelt es sich nicht über Fremdkräfte, die über einen Bestellvorgang (Dienst- oder Werkvertrag) beauftragt werden.
   Die Eingabe einer Bestellnummer ist hier nicht erforderlich. Da es sich um eine natürliche Person handelt, muss der angegebene Vor- und Nachname exakt mit dem Namen im amtlichen Ausweisdokument übereinstimmen. Dies muss bei der Eingabe bestätigt werden.

3. ANLAGE EINES STAMMDATENSATZ FÜR EXTERNE MITARBEITER (EXTERNAL WORKFORCE) IM SAP HR BZW. MYPORTAL

3.1. Prüfung der Daten

- Die Angaben im „Service Fremdkräfte verwalten“ sind auf Vollständigkeit und Korrektheit durch den Antragsteller zu prüfen. Name und Geburtsdatum bei natürlichen Personen müssen hierbei einem gültigen amtlichen Identitätsnachweis wie z.B. Personalausweis oder Reisepass entsprechen und sind ggf. auf Verlangen nachzuweisen.
- Stimmen die im System vorhandenen Daten nicht mit dem amtlichen Ausweis Dokument überein müssen die Daten angepasst werden, andernfalls darf der Externe Mitarbeiter nicht übernommen werden.
- Bitte beachten Sie Kapitel 10 „Handhabung Überprüfung der Ausweisdaten“

Checkbox

☐ Die angegebenen Persönlichen Daten sind mit den Daten im amtlichen Ausweis identisch.

3.2. Bestätigung

- Nach Überprüfung der Daten müssen Sie die Richtigkeit der Daten durch Aktivierung der entsprechenden Checkbox bestätigen.
- Wir weisen Sie darauf hin, dass Sie mit Eingabe oder Bestätigung der Stammdaten eine Identität bestätigen oder ausstellen. Diese Identitäten unterliegen rechtliche und gesetzliche Vorgaben sowie Zertifizierungsvorgaben nach eIDAS und ETSI.
- Derjenige, der den Stammdatensatz anlegt trägt nach bestem Wissen und Gewissen die Verantwortung dafür, dass die Stammdatenanlege unter Vermeidung der im Kapitel 1.1 beschriebenen Risiken, insbesondere der straf- und arbeitsrechtlichen Risiken erfolgt.
- Vorwerfbares bewusstes Fehlverhalten in diesem Zusammenhang wird im Rahmen der geltenden gesetzlichen und arbeitsrechtlichen Bestimmungen geahndet.

Checkboxen

☐ * Hiermit bestätige ich die Kenntnisnahme der Vorgaben für das Anlegen gemäß Verfahrensanweisung. Bei deliktischem Handeln oder Straffällen kann ich zur Verantwortung gezogen werden. Dies kann arbeitsrechtliche als auch strafrechtliche Konsequenzen zur Folge haben.
Die Verfahrensanweisungen finden Sie unter:
https://cpki.telekom.de/downloads/Verfahrensanweisung_Anlage_User_PN_Robot_Funktionsaccounts.pdf

☐ * Hiermit bestätige ich, dass die Identität oben genannten Person anhand eines gültigen amtlichen Ausweisdokumentes geprüft habe und die angegebenen Persönlichen Daten zur Person bzw. zur realen natürlichen Person, die sich hinter dem Pseudonym verbirgt, mit denen in dem amtlichen Ausweisdokument identisch sind.

4. ANLAGE EINES STAMMDATENSATZES FÜR MITARBEITER MIT EINEM INTERNEN FREMDEINSATZ IM SAP HR BZW. MYPORTAL

4.1. Eingabe und Prüfung der Daten

- Das Anlegen eines Stammdatensatzes für Mitarbeiter mit einem internen Fremdeinsatz im „Service Fremdkräfte verwalten“ ist auf Vollständigkeit und Korrektheit durch den Ersteller zu prüfen. Name und Geburtsdatum bei natürlichen Personen müssen hierbei einem gültigen amtlichen Identitätsnachweis wie z.B. Personalausweis oder Reisepass entsprechen und sind ggf. auf Verlangen nachzuweisen.
- Stimmen die im System vorhandenen Daten nicht mit dem amtlichen Ausweis Dokument überein müssen die Daten angepasst werden, andernfalls darf der Externe Mitarbeiter nicht übernommen werden.
- Bitte beachten Sie Kapitel 10 „Handhabung Überprüfung der Ausweisdaten“

Checkbox

☐ Die angegebenen Persönlichen Daten sind mit den Daten im amtlichen Ausweis identisch.

4.2. Bestätigung

- Nach Überprüfung der Daten müssen Sie die Richtigkeit der Daten durch Aktivierung der entsprechenden Checkbox bestätigen.
- Wir weisen Sie darauf hin, dass Sie mit Eingabe oder Bestätigung der Stammdaten eine Identität bestätigen oder ausstellen. Diese Identitäten unterliegen rechtliche und gesetzliche Vorgaben sowie Zertifizierungsvorgaben nach eIDAS und ETSI.
- Derjenige, der den Stammdatensatz anlegt trägt nach bestem Wissen und Gewissen die Verantwortung dafür, dass die Stammdatenanlege unter Vermeidung der im Kapitel 1.1 beschriebenen Risiken, insbesondere der straf- und arbeitsrechtlichen Risiken erfolgt.
- Vorwerfbares bewusstes Fehlverhalten in diesem Zusammenhang wird im Rahmen der geltenden gesetzlichen und arbeitsrechtlichen Bestimmungen geahndet.

Checkboxen

☐ * Hiermit bestätige ich die Kenntnisnahme der Vorgaben für das Anlegen gemäß Verfahrensanweisung. Bei deliktischem Handeln oder Straffällen kann ich zur Verantwortung gezogen werden. Dies kann arbeitsrechtliche als auch strafrechtliche Konsequenzen zur Folge haben.
Die Verfahrensanweisungen finden Sie unter:
https://cpki.telekom.de/downloads/Verfahrensanweisung_Anlage_User_PN_Robot_Funktionsaccounts.pdf

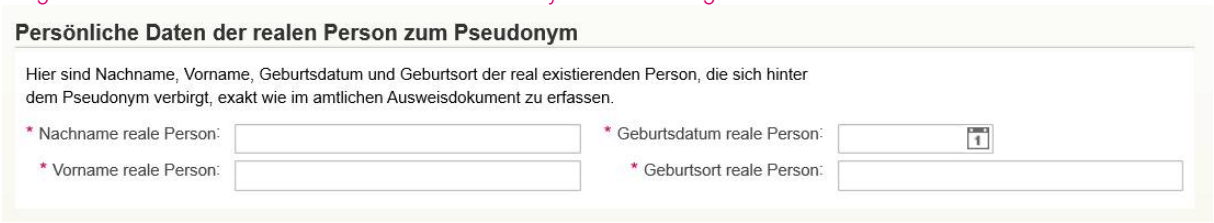
☐ * Hiermit bestätige ich, dass die Identität oben genannten Person anhand eines gültigen amtlichen Ausweisdokumentes geprüft habe und die angegebenen Persönlichen Daten zur Person bzw. zur realen natürlichen Person, die sich hinter dem Pseudonym verbirgt, mit denen in dem amtlichen Ausweisdokument identisch sind.

5. ANLAGE EINES STAMMDATENSATZES FÜR PSEUDONYMACCOUNTS IM SAP HR BZW. MYPORTAL

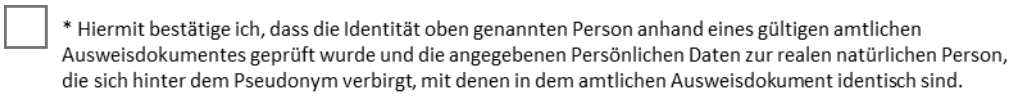
5.1. Eingabe und Prüfung der Daten

- Weicht der Vor- oder/und Nachname einer natürlichen Person vom amtlichen Identitätsnachweis ab, ist der Stammdatensatz als Pseudonym zu anzulegen.
- Hierbei wird vom System dem Vornamen immer ein PN- vorangestellt um den entsprechenden IT-Account und das Zertifikat als Pseudonym zu kennzeichnen. Diese Kennzeichnung darf nicht gelöscht oder verändert werden.
- Die Pseudonymbezeichnung (nach dem vorangestellten PN-), d.h. der Vor- und Nachname kann freigewählt werden. Jedoch ist die Pseudonymbezeichnung so zu wählen, dass ausgeschlossen ist, dass Namen Berechtigungen suggerieren (wie z.B. Telekom CA), die der Zertifikatsinhaber nicht besitzt. Des Weiteren dürfen keine politischen Parolen, anstößige Namen verwendet werden oder Namen die Markenrechte verletzen könnten. Das TrustCenter der DTAG behält sich vor, die Vergabe eines Pseudonyms abzulehnen. Die Ablehnung bedarf keiner Begründung.
- Die Angaben zur realen natürlichen Person, die sich hinter dem Pseudonym verbirgt, sind zu erfassen und auf Vollständigkeit und Korrektheit durch den Antragsteller zu prüfen. Der Vor- und Nachname, das Geburtsdatum und der Geburtsort der natürlichen Person müssen hierbei dem gültigen amtlichen Identitätsnachweis wie z.B. Personalausweis oder Reisepass entsprechen.
- Das Anlegen eines Stammdatensatzes für Pseudonyme im „Service Fremdkräfte verwalten“ ist auf Vollständigkeit und Korrektheit durch den Ersteller zu prüfen.
- Bitte beachten Sie Kapitel 10 „Handhabung Überprüfung der Ausweisdaten“
- Bei nicht Übereinstimmung darf der Stammdatensatz nicht angelegt werden.

Eingabefelder zur realen Person hinter der Pseudonymbezeichnung



Checkbox



5.2. Bestätigung

- Nach Überprüfung der Daten müssen Sie die Richtigkeit der Daten durch Aktivierung der entsprechenden Checkbox bestätigen.
- Derjenige, der den Stammdatensatz anlegt trägt nach bestem Wissen und Gewissen die Verantwortung dafür, dass die Stammdatenanlege unter Vermeidung der im Kapitel 1.1 beschriebenen Risiken, insbesondere der straf- und arbeitsrechtlichen Risiken erfolgt.
- Vorwerfbares bewusstes Fehlverhalten in diesem Zusammenhang wird im Rahmen der geltenden gesetzlichen und arbeitsrechtlichen Bestimmungen geahndet.

Checkboxen

☐ * Hiermit bestätige ich die Kenntnisnahme der Vorgaben für das Anlegen gemäß Verfahrensanweisung. Bei deliktischem Handeln oder Straffällen kann ich zur Verantwortung gezogen werden. Dies kann arbeitsrechtliche als auch strafrechtliche Konsequenzen zur Folge haben.
Die Verfahrensanweisungen finden Sie unter:
https://cpki.telekom.de/downloads/Verfahrensanweisung_Anlage_User_PN_Robot_Funktionsaccounts.pdf

☐ * Hiermit bestätige ich, dass die Identität oben genannten Person anhand eines gültigen amtlichen Ausweisdokumentes geprüft habe und die angegebenen Persönlichen Daten zur Person bzw. zur realen natürlichen Person, die sich hinter dem Pseudonym verbirgt, mit denen in dem amtlichen Ausweisdokument identisch sind.

6. ANLAGE EINES STAMMDATENSATZES FÜR FUNKTIONSACCOUNTS IM SAP HR BZW. MYPORTAL

6.1. Eingabe und Prüfung der Daten

- Wird ein Account benötigt, der nicht einer natürlichen Person zugeordnet werden kann und von einer Personengruppe verwendet wird, so ist ein Funktionsaccount anzulegen. Dies können zum Beispiel Accounts für Empfänge, Schulungsrechner, Messerechner oder Testsysteme sein, die durch mehrere Personen verwendet werden.
- Hierbei wird vom System dem Vornamen immer ein GRP- vorangestellt um den entsprechenden IT-Account und das Zertifikat als Gruppen, bzw. Funktionsaccount zu kennzeichnen. Diese Kennzeichnung darf nicht gelöscht oder verändert werden.
- Die Funktions- bzw. Gruppenbezeichnungen (nach dem vorangestellten GRP-), d.h. der Vor- und Nachname kann freigewählt werden, jedoch ist die Funktions- bzw. Gruppenbezeichnungen so zu wählen, dass ausgeschlossen ist, dass Namen Berechtigungen suggerieren (wie z.B. Telekom CA), die der Zertifikatsinhaber nicht besitzt. Des Weiteren dürfen keine politischen Parolen, anstößige Namen verwendet werden oder Namen die Markenrechte verletzen könnten.
  Das TrustCenter der DTAG behält sich vor, die Vergabe einer Funktions- bzw. Gruppenbezeichnungen abzulehnen. Die Ablehnung bedarf keiner Begründung.
- Das Anlegen eines Stammdatensatzes für einen Funktions- bzw. Gruppen-Account im „Service Fremdkräfte verwalten“ ist auf Vollständigkeit und Korrektheit durch den Ersteller zu prüfen.

6.2. Bestätigung

- Nach Überprüfung der Daten müssen Sie die Richtigkeit der Daten durch Aktivierung der entsprechenden Checkbox bestätigen.
- Wir weisen Sie darauf hin, dass Sie mit Eingabe oder Bestätigung der Stammdaten eine Identität bestätigen oder ausstellen. Diese Identitäten unterliegen rechtliche und gesetzliche Vorgaben sowie Zertifizierungsvorgaben nach eIDAS und ETSI.
- Derjenige, der den Stammdatensatz anlegt trägt nach bestem Wissen und Gewissen die Verantwortung dafür, dass die Stammdatenanlege unter Vermeidung der im Kapitel 1.1 beschriebenen Risiken, insbesondere der straf- und arbeitsrechtlichen Risiken erfolgt.
- Vorwerfbares bewusstes Fehlverhalten in diesem Zusammenhang wird im Rahmen der geltenden gesetzlichen und arbeitsrechtlichen Bestimmungen geahndet.

Checkbox

☐ * Hiermit bestätige ich die Kenntnisname der Vorgaben für das Anlegen von Externen Mitarbeitern.
Bei deliktischem Handeln oder Straffällen kann ich zur Verantwortung gezogen werden. Dies kann arbeitsrechtliche als auch strafrechtliche Konsequenzen zur Folge haben.
Die Verfahrensanweisung finden Sie unter:
s://cpki.telekom.de/downloads/Verfahrensanweisung_Anlage_User_PN_Robot_Funktionsaccounts.pdf

7. ANLAGE EINES STAMMDATENSATZES FÜR ROBOTER-ACCOUNTS IM SAP HR BZW. MYPORTAL

7.1. Eingabe und Prüfung der Daten

- Wird ein Account benötigt, der und von einem Roboter verwendet wird, so ist ein Robot-Account anzulegen.
- Hierbei wird vom System dem Vornamen immer ein Robot- vorangestellt um den entsprechenden IT-Account und das Zertifikat als Gruppen, bzw. Funktionsaccount zu kennzeichnen. Diese Kennzeichnung darf nicht gelöscht oder verändert werden.
- Die Bezeichnungen des Robot-Accounts (nach dem vorangestellten Robot-), d.h. der Vor- und Nachname kann freigewählt werden, jedoch ist die Bezeichnungen des Robot-Accounts so zu wählen, dass ausgeschlossen ist, dass Namen Berechtigungen suggerieren (wie z.B. Telekom CA), die der Zertifikatsinhaber nicht besitzt. Des Weiteren dürfen keine politischen Parolen, anstößige Namen verwendet werden oder Namen die Markenrechte verletzen könnten.
  Das TrustCenter der DTAG behält sich vor, die Vergabe einer Funktions- bzw. Gruppenbezeichnungen abzulehnen. Die Ablehnung bedarf keiner Begründung.
- Das Anlegen eines Stammdatensatzes für einen Funktions- bzw. Gruppen-Account im „Service Fremdkräfte verwalten“ ist auf Vollständigkeit und Korrektheit durch den Ersteller zu prüfen.

7.2. Bestätigung

Nach Überprüfung der Daten müssen Sie die Richtigkeit der Daten durch Aktivierung der entsprechenden Checkbox bestätigen.
Wir weisen Sie darauf hin, dass Sie mit Eingabe oder Bestätigung der Stammdaten eine Identität bestätigen oder ausstellen. Diese Identitäten unterliegen rechtliche und gesetzliche Vorgaben sowie Zertifizierungsvorgaben nach eIDAS und ETSI.
Derjenige, der den Stammdatensatz anlegt trägt nach bestem Wissen und Gewissen die Verantwortung dafür, dass die Stammdatenanlege unter Vermeidung der im Kapitel 1.1 beschriebenen Risiken, insbesondere der straf- und arbeitsrechtlichen Risiken erfolgt.
Vorwerfbares bewusstes Fehlverhalten in diesem Zusammenhang wird im Rahmen der geltenden gesetzlichen und arbeitsrechtlichen Bestimmungen geahndet.

Checkbox

☐ * Hiermit bestätige ich die Kenntnisname der Vorgaben für das Anlegen von Externen Mitarbeitern.
Bei deliktischem Handeln oder Straffällen kann ich zur Verantwortung gezogen werden. Dies kann arbeitsrechtliche als auch strafrechtliche Konsequenzen zur Folge haben.
Die Verfahrensanweisung finden Sie unter:
https://cpki.telekom.de/downloads/Verfahrensanweisung_Anlage_User_PN_Robot_Funktionsaccounts.pdf

8. ANLAGE EINES STAMMDATENSATZES FÜR SALES & PARTNER-ACCOUNTS IM SAP HR BZW. MYPORTAL

8.1. Eingabe und Prüfung der Daten

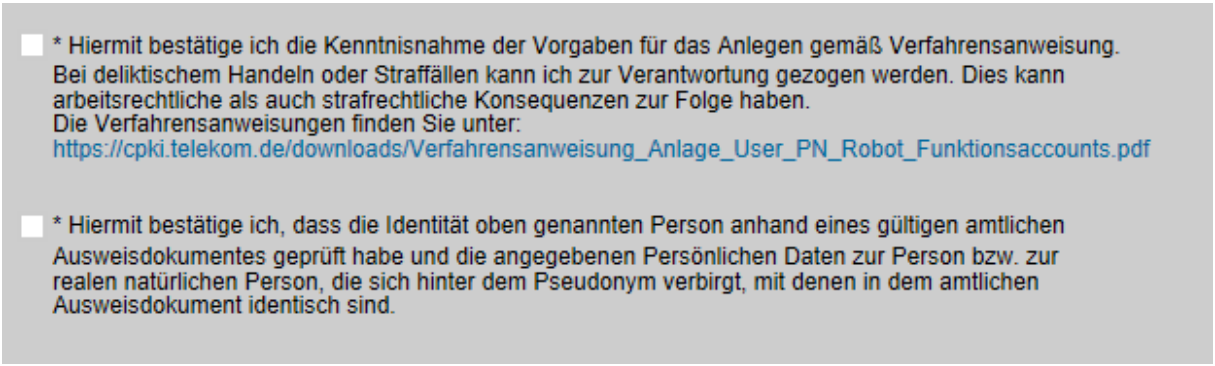
- Die Angaben im „Service Fremdkräfte verwalten“ sind auf Vollständigkeit und Korrektheit durch den Antragsteller zu prüfen. Name und Geburtsdatum bei natürlichen Personen müssen hierbei einem gültigen amtlichen Identitätsnachweis wie z.B. Personalausweis oder Reisepass entsprechen und sind ggf. auf Verlangen nachzuweisen.
- Stimmen die im System vorhandenen Daten nicht mit dem amtlichen Ausweis Dokument überein müssen die Daten angepasst werden, andernfalls darf der Externe Mitarbeiter nicht übernommen werden.
- Bitte beachten Sie Kapitel 10 „Handhabung Überprüfung der Ausweisdaten“

Checkbox

8.2. Bestätigung

- Nach Überprüfung der Daten müssen Sie die Richtigkeit der Daten durch Aktivierung der entsprechenden Checkbox bestätigen.
- Wir weisen Sie darauf hin, dass Sie mit Eingabe oder Bestätigung der Stammdaten eine Identität bestätigen oder ausstellen. Diese Identitäten unterliegen rechtliche und gesetzliche Vorgaben sowie Zertifizierungsvorgaben nach eIDAS und ETSI.
- Derjenige, der den Stammdatensatz anlegt trägt nach bestem Wissen und Gewissen die Verantwortung dafür, dass die Stammdatenanlege unter Vermeidung der im Kapitel 1.1 beschriebenen Risiken, insbesondere der straf- und arbeitsrechtlichen Risiken erfolgt.
- Vorwerfbares bewusstes Fehlverhalten in diesem Zusammenhang wird im Rahmen der geltenden gesetzlichen und arbeitsrechtlichen Bestimmungen geahndet.

Checkboxen

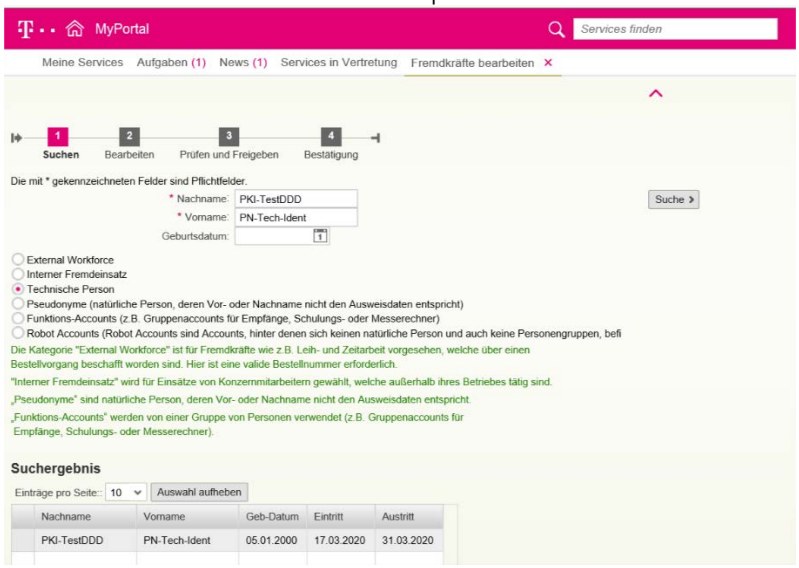


9. VERLÄNGERUNG UND ÄNDERUNG VON BISHERIGEN TECHNISCHEN PERSONEN

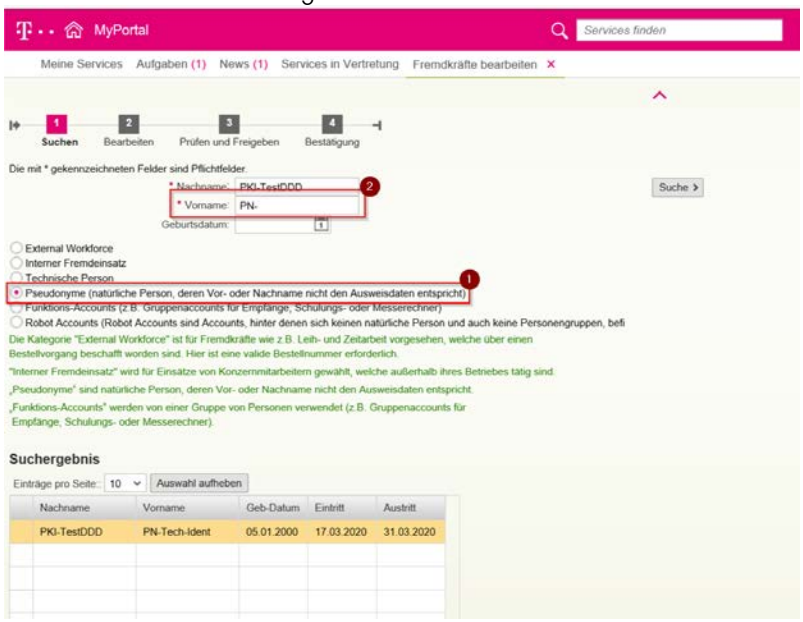
Eine Verlängerung von bisherigen Technischen Personen ist nur mit einer Neukategorisierung möglich. Es ist deshalb im Falle einer Verlängerung eine Neu-Kategorisierung erforderlich.

Des Weiteren ist im Rahmen der Zertifikatserneuerung ebenfalls eine Neu-Kategorisierung erforderlich.

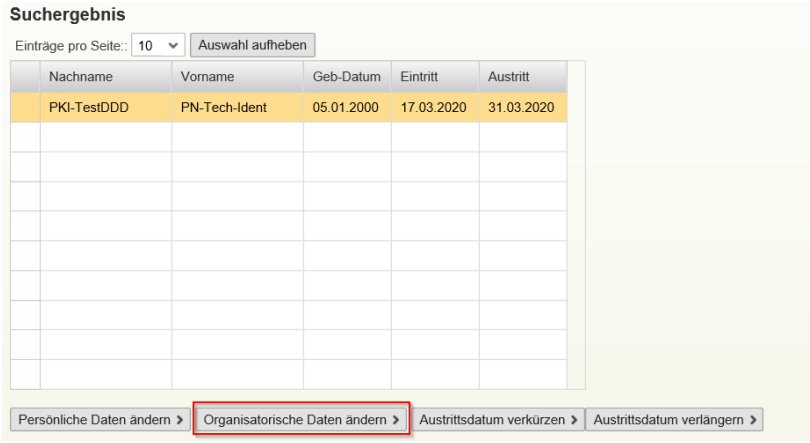
Hierzu rufen Sie bitte über MyPortal „Fremdkräfte bearbeiten“ auf, wählen Sie die Kategorie technische Person aus und suchen über die entsprechenden Suchfelder den zu verlängernden Stammdatensatz.



Bitte wählen Sie die Person aus und ändern Sie nun die Kategorie von Technische Person auf eine der anderen Kategorien. Die Klassifizierung der entsprechenden Kategorie finden Sie in Kapitel 2.
Dadurch wird im Feld Vorname, je das Kategorie, ein Präfix vorgestellt (PN-, GRP-, ROBOT-) und Sie müssen den Vornamen ergänzen.



Danach klicken Sie auf „Organisatorische Daten“ ändern.



Beispiel 1: Pseudonym Account
Bisheriger Vorname: PN-DUPHans-HU,
Bisheriger Nachname: Mustermann

Nach Auswahl der Kategorie „Pseudonym“ wird der bisherige Vorname gelöscht, im Feld Vornamen steht nur das nichtänderbare Präfix für Pseudonyme:
PN-
Ergänzen Sie nun wieder den Vornamen PN- **DUPHans-HU**
Der Nachname bleibt unverändert.

Beispiel 2: Robot Account
Bisheriger Vorname: PN-Hans
Bisheriger Nachname: RobotAMustermann

Nach Auswahl der Kategorie „Robot“ wird der bisherige Vorname gelöscht, im Feld Vornamen steht nur das nichtänderbare Präfix für Roboter:
Robot-
Ergänzen Sie nun wieder den Vornamen Robot-**Hans**
Die Bezeichnung für Roboter darf kein PN- mehr enthalten.

Beispiel 3: Funktions Account
Bisheriger Vorname: PN-Zentrale-Bonn
Bisheriger Nachname: Empfang Bonn

Nach Auswahl der Kategorie „Funktion-Account“ wird der bisherige Vorname gelöscht, im Feld Vornamen steht nur das nichtänderbare Präfix für Funktions-Accounts:
GRP-
Ergänzen Sie nun wieder den Vornamen GRP-Zentrale-Bonn
Die Bezeichnung für Funktions-Accounts darf kein PN- mehr enthalten.

Beispiel 4: Zu verlängernder Accounts für External Workforces oder interner Fremdeinsatz
Bisheriger Vorname: Max

Bisheriger Nachname: Mustermann

Nach Auswahl der Kategorie „External Workforces“ oder „interner Fremdeinsatz“ steht im Feld Vor- bzw. Nachnamen die gleichen Namen wie vorher, der Vornamen wird nicht gelöscht:
Es muss nur eine Änderung/Korrektur der Namen erfolgen, wenn bei der durchzuführenden Identifikation (siehe Kapitel 10) der externen Fremdkraft eine Abweichung des Eingetragenen Namens zu dem amtlichen Ausweisdokument festgestellt wird.
„External Workforces“ oder „interner Fremdeinsatz“ dürfen keine Bezeichnungen enthalten, die nicht im amtlichen Ausweisdokument stehen.

10. HANDHABUNG ÜBERPRÜFUNG DER AUSWEISDATEN

Die Prüfung der Ausweisdaten muss beifolgenden Kategorien erfolgen

- Externer Mitarbeiter
- Pseudonyme
- Mitarbeiter mit einem internen Fremdeinsatz
- Sales & Partner

Es sind nur Amtliche Ausweisdokumente wie Personalausweis, Reisepass oder Aufenthaltstitel zulässig. In Staaten, in denen kein Personalausweis oder Reisepass üblich ist, wie z.B. den USA kann statt eines Personalausweises oder Reisepasses auch die State ID der US-Bundesstaaten oder ein amtlicher Führerschein verwendet werden. In Indien ist statt eines Passes auch die Aadhaar-Karte zulässig.

10.1. Ersterfassung bei dem Anlegen eines Stammdatensatzes

Die Ausweisdaten müssen vor dem Anlegen des Stammdatensatzes durch die eingebende Person geprüft werden.
Werden die Daten in einem anderen Tool, wie z.B. ZEUS vorerfasst sind die Ausweisdaten dort bei der Erfassung zu prüfen und zu bestätigen.
Bei Namen, die nicht in Lateinischer Schrift vorliegen, ist der Name aus dem maschinenlesbaren Teil des Ausweises zu erfassen (siehe dazu auch die FAQ).

Die Ausweisdaten können wie folgt verifiziert werden

- Persönliche Vorlage des Ausweises
- Sichtprüfung per Video
- Per Mail oder Fax (Nicht relevante Daten können geschwärzt werden, es muss jedoch immer eine Identifikation anhand des Lichtbildes zu der Person erfolgen, z.B. mittels Videochat)
- Bei Leih- und Zeitarbeitskräften entfällt die Ausweisüberprüfung durch Einzelbestätigung der Ausweisprüfung durch den Verleiher (Arbeitnehmerüberlassungsvertrag).
  Der Arbeitnehmerüberlassungsvertrag ist der Bestellbestätigung als PDF Dokument beigefügt, anhand dieser Bestätigung kann die erfolgte Identifikation bestätigt werden.

Relevante Daten, die geprüft werden müssen:

- Nachname
- Vorname
- Geburtstag
- Gültigkeit des Ausweises anhand des Gültigkeitsdatums des Ausweisdokumentes (dieses muss jedoch nicht erfasst werden), der Ausweis darf zudem nicht entwertet sein.
- Sichtprüfung des Lichtbildes zur Person

Alle anderen Informationen sind nicht relevant und müssen nicht geprüft werden. Bei Bedarf können Ausweiskopien entsprechend geschwärzt sein. Die Ausweiskopie ist nach der Überprüfung der Daten zu sicher zu vernichten.

Beispiel Deutschland:

Beispiel Ungarn:

Beispiel Österreich:

10.2. Personen bei denen keine Ausweisüberprüfung durchgeführt werden kann

Bei natürlichen Personen, bei denen keine Ausweisüberprüfung erfolgen kann, dürfen nicht als „external Workforce“, interner Fremdeinsatz, Pseudonyme oder Sales & Partner erfasst werden.

Accounts für Partner Firmen, bei denen keine natürlichen Personen explizit benannt werden und deshalb keine Ausweisüberprüfung durchgeführt werden kann, sind als Funktionsaccounts anzulegen.
Hierbei ist zu beachten, dass der KostV als Schlüsselverantwortlicher gilt und die volle Verantwortung für den Gebrauch und Missbrauch der Accounts und der Zertifikate trägt. Auf Maßgabe der internen Sicherheit der Telekom Security ist von den Nutzern ein Logbuch anzulegen und ordnungsgemäß die Nutzung (Wer hat wann, was mit dem Account bzw. den Zertifikaten gemacht) zu dokumentieren. Auf Verlangen ist das Logbuch jeder Zeit vorzulegen.

10.3. Verlängerung:

Sollte es sich um eine Verlängerung handeln, ist eine Überprüfung notwendig, sollte die Überprüfung der Ausweisdaten bei der Erstanlage nicht erfolgt sein.
Eine Überprüfung bei Verlängerungen ist notwendig sobald sich Änderungen ergeben.

10.4. Austritt

Bei einem Austritt müssen keine Ausweisdaten überprüft werden.

11. WEITERFÜHRENDE REGELUNGEN UND DOKUMENTE

Eine Ausführliche Anleitung zur Anlage von HR Stammdaten im „Service Fremdkräfte verwalten“ im SAP HR bzw. MyPortal finden Sie YAM unter:
https://yam.telekom.de/groups/external-workforce-deployment/pages/stammdatenpflege

Des Weiteren gelten die Nutzungsbedingungen der Corporate-PKI der DTAG (Nutzungsbedingungen – LINK) und die Konzernrichtlinien zur Sicherheit (Konzernrichtlinien IT-/NT-Sicherheit).

Darüber hinaus gilt weiterhin die KBV IT APS 4.0 Anlage 11 „MyCard/cPKI” Version 2.1 (KBV IT APS 4.0 - LINK) und alle weiteren Regeln und Gesetze.

Der PKI-Service „cPKI“ stellt Zertifikate für unterschiedliches Verwendungszwecke (Mail, VPN, Server, usw.) aus, basierend auf dem Standard X.509v3. Abhängig von der Nutzung verwendet die „cPKI“ unterschiedliche Zwischenzertifizierungsstellen (Intermediat CA), die hierarchisch einer öffentlichen oder internen Stammzertifizierungsstelle (Root-CA) untersteht.

Die Prozesse werden durch unabhängige Dritte einer regelmäßigen jährlichen Prüfung (ETSI EN 319 411-1) unterzogen. Zertifizierungsgegenstand sind alle Prozesse, die zur Beantragung, Ausstellung, Sperrung und Erneuerung von Endteilnehmer-Zertifikaten in Verbindung mit einer öffentlichen Zertifizierungsstelle (secure email CA und secure email CA E02) dienen.
T-Systems führt zusätzlich in regelmäßigen Abständen selbstaufsichtsmaßnahmen (Quality Assessment Self Audits) und Stichproben der Datenqualität durch.

Weiterführende Informationen zur Corporate Public Key Infrastructure der Deutschen Telekom AG finden Sie unter:
https://corporate-pki.telekom.de

12. FAQ

Frage:

Auf welcher datenschutzrechtlichen Grundlage ist der Versand von Kopien amtlicher Ausweise zulässig (diese Frage wurde im Zuge einer Identitätsprüfung an uns herangetragen)?

Antwort:

Die Identitätsprüfung erfolgt auf Basis der Vorgaben zur Identitätsfeststellung zur Ausstellung von fortgeschrittenen Zertifikaten (ETSI und eIDAS), sowie auf den Anforderungen externer Wirtschaftsprüfer für das Accountmanagement.

Frage:

Ist zwingend ein Videochat vorgeschrieben oder reicht auch die Vorlage des amtlichen Ausweisdokuments?

Antwort:

Es muss eine eindeutige Identifizierung anhand eines amtlichen Lichtbildausweises erfolgen.
Dies kann entweder durch die persönliche Überprüfung Vorort oder per Video Chat erfolgen.
Eine Zusendung einer Ausweiskopie mittels Fax oder Mail ist zulässig, jedoch entbindet dies nicht der Identifizierung anhand eines amtlichen Lichtbildausweises, entweder mittels Face to Face oder Videochat.

Frage:

In der Anleitung wird darauf verwiesen, dass derjenige der den Datensatz anlegt bei Missbrauch haftbar gemacht werden kann. Ist die Prüfung und Haftbarkeit auf eine im Prozess vorgelagerte Person übertragbar, wenn diese per Unterschrift die Identitätsprüfung wie in der Verfahrensanweisung beschrieben bestätigt? Denn diese Personen sind schon im Kontakt mit den beauftragten Firmen und ggf. auch der Fremdkraft. Wir würden hierzu das beigefügte Onboarding Formblatt, das in unserm Bereich genutzt wird, entsprechend erweitern.

Antwort:

Eine Auslagerung der Identitätsfeststellung an einen externen Arbeitgeber, z.B. bei Leih- und Zeitkräften dem Verleiher nur möglich, wenn es einen entsprechenden Vertrag, bzw. eine Erweiterung des Rahmenvertrages mit dem externen Arbeitgeber, bzw. Verleiher zur Identitätsfeststellung gibt, in dem explizit festgehalten wurde,

- dass die Identität ordnungsgemäß anhand eines gültigen amtlichen Ausweisdokumentes geprüft wurde,
- die weitergegeben Daten 1:1 identisch mit den Ausweisweis daten sind
- eine Identifizierung der mittels Sichtprüfung (Person ist mit der Person auf dem Ausweis identisch) erfolgt ist
- die Prüfung für jede Identität bei Lieferung der Daten bestätigt wird.
- eine Dokumentation der Bestätigung erfolgt und auf Verlangen vorgezeigt werden kann. Eine Aufbewahrungsfrist von 8 Jahren nach Beendigung des Beschäftigungsverhältnisses die der DTAG ist erforderlich.

Frage:

Muss bei internen Fremdeinsätzen eine erneute Identitätsprüfung erfolgen, auch wenn dies beim Hauptanstellungsverhältnis bei einem ausländischen Telekomunternehmen bereits erfolgt ist?

Antwort:

Da wir nicht wissen, bei welchem Tochterunternehmen eine Identitätsprüfung erfolgt ist und dies in den Systemen leider nicht dokumentiert ist, ist eine Identitätsprüfung und ggf. eine Korrektur der Bestandsdaten erforderlich.

Frage:

Können Sie uns mitteilen bei welchen Unternehmen des Telekomkonzerns schon eine Identitätsprüfung erfolgt ist, durchgeführt wird und weiterhin durchgeführt werden wird, um ggf. den Bearbeitungsprozess zu verkürzen.

Antwort:

Da wir nicht wissen, bei welchem Tochterunternehmen eine Identitätsprüfung erfolgt ist und dies in den Systemen leider nicht dokumentiert ist, ist eine Identitätsprüfung und ggf. eine Korrektur der Bestandsdaten erforderlich.

Frage:

Wie ist hinsichtlich der Schreibweise des Namens zu verfahren, bis jetzt wurde in den meisten Fällen nur der Rufname der Personen bei der Datensatzanlage berücksichtigt. Falls der volle Name zum Tragen kommen muss, wie wird diese Änderung in die Folgesysteme überführt? Es sollte zu keiner Arbeitsbeeinträchtigung bei den Fremdkräften kommen, da hier dem Unternehmen ein wirtschaftlicher Schaden zugefügt werden kann, wenn die ext. Kraft nicht mehr arbeitsfähig ist.

Antwort:

Es sind immer die vollständigen Namen aus dem amtlichen Ausweis zu übernehmen. Der Rufname genügt leider nicht. In wieweit die Probleme in Folgesysteme verursacht können wir leider nicht sagen. Der Wirtschaftliche Schaden die sich aus einer Änderung/Anpassung des Vornamens ergeben, sind wesentlich geringer als der Wirtschaftliche Schaden, der sich aus falsch aufgestellten Identitäten ergibt.

Frage:

Was ist bei Namen zu beachten, die nicht den Konventionen der üblichen Schreibweise entsprechen, die z.B. mit diakritischen Zeichen im Namen, wie á, cs, dz, dzs, é, gy, í, ly, ny, ó, ö, ő, sz, ty, ú, ü, ű geschrieben werden. SAP löst zwar die Buchstaben entsprechend auf, aber verschiedene Folgesysteme haben diese Schriftzeichen nicht und setzen zum Beispiel den Email-Account mit Fehlern um (die unbekannten Schriftzeichen werden in seltsame Sonderzeichen umgesetzt).

Antwort:

Die cPKI kann alle Lateinische Schriftzeichen inklusive diakritischen Zeichen im Namen verarbeiten. Sollte Ihr es Probleme in Folgesysteme (cIAM, MyIT) geben, kann in diesem Fall die internationale Schreibweise des Namens aus dem maschinenleserlichen Teil des Ausweises eingetragen werden.

Beispiel ungarischer Personalausweis:

Frage:

Was ist bei Namen zu beachten, die nicht der lateinischen Schrift entsprechen, z.B. kyrillische Schriftzeichen Zeichen im Namen.

Antwort:

Die internationale Schreibweise ist Latein, daher sind die Namen in Lateinischer Schrift zu erfassen, in diesem Fall muss die internationale Schreibweise des Namens aus dem maschinenleserlichen Teil des Ausweises eingetragen werden.

Beispiel russischer Pass: