```
{
  "auditPath": [
    "GDyUoeC5rbK9drQYDmrWEgZBHnj4jW1wXjWb74h3ttnv",
    "72Yze51yrDBkbFgR5ZdUJiLB9QbP9JTw8tKJbacayVKG",
    "D52hsZf4iH4Kp4x4eEp18FicbPNdirG9TL2cvat1eKvL",
    "2fKw6teotaep8GDZyzBbdHUsUXwXh8nxGHUkPnLhjU8j"
  ],
  "ledgerSize": 10,
  "reqSignature": {
    "type": "ED25519",
    "values": [
      {
        "from": "4cU41vWW82ArfxJxHkzXPG",
        "value": "2iFCpuo137eX73kDCr4Ts8WHEyRNu1wJRDUkhivxARMUZMGRSAwefGPvwB9giggrBZnhRvUGHm5FojkaFmdz4bS8"
      }
    ]
  },
  "rootHash": "CLqaCCYRZv4cinYNYVmBowEeuPKaDQ3iyGno2eNSHCwa",
  "txn": {
    "data": {
      "alias": "Company",
      "dest": "JiVLsA5wxVnbHQ5s7pDN58",
      "role": "101",
      "verkey": "Af1wegtCKdqjjWqjdP89tkLGLhfM8oRoLWaHpn8wpRU8"
    },
    "metadata": {
      "digest": "442a28bd1b9947867fc65ec8ef62c2b21d465498224a729f322143bce3967351",
      "from": "4cU41vWW82ArfxJxHkzXPG",
      "payloadDigest": "15bab600e46d5119df83e75bb56469eb185baebcc5e1c6e597956ec4f83acf50",
      "reqId": 1612383608927929900
    },
    "protocolVersion": 2,
    "type": "1"
  },
  "txnMetadata": {
    "seqNo": 8,
    "txnId": "80f7aeea87d46e00d0516528924aa825658bb3c294b0c6ef4e5de4738455107d",
    "txnTime": 1612383611
  },
  "ver": "1"
}
```


Abbildung 2: Onboarding einer öffentlichen DID

Erstellen der Schemas und Credential Definitions (Onboarding der Arbeitgeber-Unternehmen II)

In einem nächsten Schritt (und vor Beginn des Pilotbetriebs) müssen von den Arbeitgeber-Unternehmen die von ihnen ausgegebenen VCs definiert werden. Hierzu wird zunächst ein grundlegendes Schema („Template“) auf der Indy-Blockchain erstellt, etwa von einem der Stewards. Dieses enthält die notwendigen Attribute, die die jeweiligen VCs beinhalten sollen. Das Schema für eine MasterID beinhaltet beispielsweise die in 4.1 benannten notwendigen Datenfelder für einen deutschen Personalausweis (Stadt, Familienname, Geburtsort, Geburtsname, Vorname, Geburtsdatum, Straße, Land, Ablaufdatum, akademischer Titel, PLZ). Die Definition des Schemas sowie der Public Key des definierenden Stewards werden auf der Blockchain gespeichert. Ein Beispiel für das Schema anhand der MasterID findet sich in folgender Abbildung: Neben den oben beschriebenen Metadaten findet sich in „txn“ die tatsächliche Form des Schemas, also dessen Name (im Falle der MasterID) sowie die Attribute, die in einer MasterID eingetragen sein müssen. Im Schema

befinden sich entsprechend ebenfalls wohl **keine personenbezogenen Daten**.


```
{
  "auditPath": [
    "GtBkPbR2wgGKuthxFj9SGZicEqXkEgYunRhD6CEGYrS3",
    "CWYPYX5TRgb3yGzVB7ztNgbxUjygjvPqwar9BqwAHMWE",
    "BnlHMUlFpTWZmd3JPMP4bCcCzTMUPlwcxVdQbHB5Q2Ha"
  ],
  "ledgerSize": 29,
  "reqSignature": {
    "type": "ED25519",
    "values": [
      {
        "from": "XwQCiUus8QubFNJPJD2mDi",
        "value": "Wqz2dzouY5GcgEpoJLqTqtULJSiauCnnvtAsPGXCof3eDwjWxoVZ7YL8N4VLAErlgX7hTsLT4JHzRVTUhknm75w"
      }
    ]
  },
  "rootHash": "FtFcEWvc9AZagBey6ApTKlWZm6zPjSuPczyEpABj7HCJ",
  "txn": {
    "data": {
      "data": {
        "attr_names": [
          "addressZipCode",
          "academicTitle",
          "dateOfExpiry",
          "firstName",
          "familyName",
          "birthName",
          "addressCountry",
          "dateOfBirth",
          "placeOfBirth",
          "addressStreet",
          "addressCity"
        ],
        "name": "masterID",
        "version": "1.0"
      }
    },
    "metadata": {
      "digest": "d8dc8812cb4b73b8d25b55607985f6ddb8195239b2c466fab72523e0e97343ed",
      "from": "XwQCiUus8QubFNJPJD2mDi",
      "payloadDigest": "2a03105bcac1874a2c4b4ec245698a50f6a740944042479a04d9f282b17fc66a",
      "reqId": 1612453082228177400
    },
    "protocolVersion": 2,
    "type": "101"
  },
  "txnMetadata": {
    "seqNo": 29,
    "txnId": "XwQCiUus8QubFNJPJD2mDi:2:masterID:1.0",
    "txnTime": 1612453084
  },
  "ver": "1"
}
```


Abbildung 3: Erstellen eines Schemas

Auf Basis der Schema-Definition wird dann von allen beteiligten Institutionen (Bundesdruckerei, Arbeitgeber-Unternehmen), die basierend auf einem Schema VCs erzeugen möchten, eine eigene, sogenannte “Credential Definition” erstellt. In dieser ist zusätzlich zu den im Schema, auf das sich die Credential Definition bezieht (referenziert durch die Blocknummer, in der das Schema definiert wurde), die DID (und damit auch der Public Key) des Credential-Definition-Erstellers aufgeführt. Zudem wird für jedes Attribut eine große Zufallszahl erzeugt, die beim späteren Nachweisen der Attribute durch die Nutzer*Innen und den Verifizierenden als Referenz benötigt wird (ein sogenannter Common Reference String, welcher oft für die eingesetzten Zero-Knowledge Proofs benötigt wird). Auch in der Credential Definition befinden sich damit keine personenbezogenen Daten. Ein Beispiel für eine solche Credential Definition für die MasterID, wie sie die Bundesdruckerei erzeugt hat, findet sich in folgender Abbildung.

```
{
  "auditPath": [
    "AzHyGe2gJk9LGdvXbGeVDZml91Sy7Ze7Yu4y3FExokzr",
    "GtBkPbR2wgGKuthxFj9SGZicEqXkEgYunRhD6CEGYrS3",
    "CWYPYX5TRgb3yGzVB7ztNgbxUjygjvPqwar9BqwAHMWE",
    "BnlHMU1FpTWZmd3JPMP4bCcCzTMUP1wcxVdQbHB5Q2Ha"
  ],
  "ledgerSize": 30,
  "reqSignature": {
    "type": "ED25519",
    "values": [
      {
        "from": "XwQCiUus8QubFNJPJD2mDi",
        "value": "mjxwU1PHBLG6juvbVK7NKfv2MzEXJvSTEB5v7UMadhSBMtyezy6z21UxXTydEWYxtvQ7reXWqAspik442darH4V"
      }
    ]
  },
  "rootHash": "BohGJuyZmkXe9eFrAMdyPYmGHMGgX25K1J3kkYMTXN7H",
  "txn": {
    "data": {
      "data": {
        "primary": {
          "n": "840562701292560653023914371181975694221465010621576986698298406870232182967194431122063474869240
          "r": {
            "academictitle": "709122764334594511067197538962319465440932227597742774530130410619446365528909439
            "addresscity": "183195248843622939514051116276911457245907552392897628015956823794966009539797491766
            "addresscountry": "74259298020794733366790695863265679665861303633192331680593270731230458688525360
            "addressstreet": "194688873743903851819928177017169767995716546189085280619551712609664083006799100
            "addresszipcode": "609235921525986719986803721589082876487289590470936718725936570951961274219021117
            "birthname": "83921694451814952392257612649580318004654503637753818942133039211769085238150667238333
            "dateofbirth": "215527628935379508348776796782682158690693530700849141419982020622312312679830120888
            "dateofexpiry": "486431228116713978427377547693790343782777860114060904297385991228395029124673869696
            "familyname": "24281378638226930237702961557758254320802215210214985815397310240895722385228963841919
            "firstname": "54839975713580572975368461654984373915044379141972464820695606284521877166644301294251
            "master_secret": "80607757739514350230881474712197839670748582925659312395526485502760606556322771616
            "placeofbirth": "29485677501955430067273136395296051250348293426649968861108289630043157296499195271
          },
          "rctxt": "61690737307749089343833056751708839404476328581060197188140804445044880600244346739276599566
          "s": "23929355862512609823567947618697184636388996650357719665881306933218792239395604504150647208640
          "z": "29209483474122572026593935178849298439966837500933761716515031578927325024258530764538868778569
        }
      },
      "ref": 29,
      "signature_type": "CL",
      "tag": "masterID Dev"
    },
    "metadata": {
      "digest": "117fc7af65cbbc74705fb82c5f8d58a73f9c2ffbe7c7a9afd1d2aadef6dfe3fd",
      "from": "XwQCiUus8QubFNJPJD2mDi",
      "payloadDigest": "0fed6da4ale6484a0ac80f596093af234528db1a63bce7ebe45d4f83a489fb55",
      "reqId": 1612453139691817200
    },
    "protocolVersion": 2,
    "type": "102"
  },
  "txnMetadata": {
    "seqNo": 30,
    "txnId": "XwQCiUus8QubFNJPJD2mDi:3:CL:29:masterID Dev",
    "txnTime": 1612453142
  },
  "ver": "1"
}
```


Abbildung 4: Erstellen einer Credential Definition

Falls keine Funktionalität zum Rückruf von einmal ausgestellten VCs benötigt würde, wäre hiermit das Onboarding eines Arbeitgeber-Unternehmens, welches VCs ausstellen möchte, bzw. der Bundesdruckerei beendet. Die Möglichkeit zum Rückruf von VCs ist jedoch sowohl für die Arbeitgeber-Unternehmen (bspw. aufgrund der Kündigung eines Mitarbeiters) als auch für Nutzer*Innen (bspw. im Falle des Verlusts des entsperrten Handys mit entsperrter Wallet-App) sinnvoll. Für den privatsphäre-schützenden Rückruf von VCs kommen bei SSI sogenannte kryptographische Akkumulatoren, die auf der Blockchain gespeichert werden, in Verbindung mit Zero-Knowledge Proofs zum Einsatz. Damit ist es möglich, dass der Besitzer eines VC einen Beweis erstellt, dass das eigene VC nicht widerrufen ist, ohne dass der Verifizierer dadurch Rückschlüsse auf

das VC selbst (etwa in Form einer Wiedererkennung desselben VCs oder Ermitteln von weiteren Informationen durch Nachfragen beim Aussteller) ziehen kann. Dazu erstellt der Aussteller gemeinsam mit der Credential Definition auch eine sogenannte Revocation Registry, in der zufällige Zahlen als Common Reference String erstellt werden sowie zusätzlich ein sogenanntes Tails-File, das öffentlich zugänglich sein muss. Das Tails-File besteht aus einer Liste von Zufallszahlen, die den zukünftig ausgestellten VCs zugeordnet werden (erste Zahl, erstes ausgestelltes VC, etc.). Das Tails-File hat eine Größe von ca. 256 Bytes je VC, also bei einer Revocation Registry, die bis zu 1000 VCs umfasst, also ca. 256 kB. Je größer das Tails-File, desto größer die von der Wallet herunterzuladende Datei, aber auch desto größer der Herdenschutz bei Revocation, da die Registry, auf die sich ein Proof of non-revocation bezieht, dann insgesamt mehr VCs umfasst. Ein Beispiel für eine Registrierung einer Revocation Registry findet sich in folgender Abbildung. Auch hier beziehen sich alle Informationen nur auf den Aussteller; entsprechend befinden sich **keine personenbezogenen Daten** auf der Blockchain.


```
{
  "auditPath": [
    "HjbYP5n3aRrpW7Bs6tFtzDRD4XnaucfUv5HyjKLkvgbJ",
    "6ojqSwScNRkDKayhzUUpviXiMxlobo8q79LQuXREWsc4",
    "DcQnUYbMAXJ5LbKam5D8Kg826652bnW7sJDK5Bn2ztJR",
    "H7rUb5Lg24zvKw8CzkF9Sr2CptowUWnr4AKo8Mc9QfY3",
    "CWYPYX5TRgb3yGzVB7ztNgbxUjygjvPqwar9BqwAHMWE"
  ],
  "ledgerSize": 24,
  "reqSignature": {
    "type": "ED25519",
    "values": [
      {
        "from": "JiVLsA5wxVnbHQ5s7pDN58",
        "value": "2SHxbdEwofkwmkxcyj5Brg6A5mBu2FCFLPD3TXkusXx7bcqqQGL9Wj6mKUoyER3yTwEXwM35ANyaZ74n2P4GpKFs"
      }
    ]
  },
  "rootHash": "4XvbH5NqVFluzxuAfZsTBnEz79rGlQxR9hPnwaiBKjtB",
  "txn": {
    "data": {
      "credDefId": "JiVLsA5wxVnbHQ5s7pDN58:3:CL:7:default3",
      "id": "JiVLsA5wxVnbHQ5s7pDN58:4:JiVLsA5wxVnbHQ5s7pDN58:3:CL:7:default3:CL_ACCUM:0e65905a-b77e-4897-a521-e1ed3a5d7783",
      "revocDefType": "CL_ACCUM",
      "tag": "0e65905a-b77e-4897-a521-e1ed3a5d7783",
      "value": {
        "issuanceType": "ISSUANCE_BY_DEFAULT",
        "maxCredNum": 1000,
        "publicKeys": {
          "accumKey": {
            "z": "1 03D9418C8110ADE3B70FB3448CB0F98110A488E76BD1C82DF4A68B8F54F97A76 1 008C05667D1CD2E3FC4DF53BB58C15172E90978BA9B85436B
          }
        },
        "tailsHash": "BQ1akyqLecHSjcKnmHhReTFDwrwJs3pLV9wZGP5pQpiJ",
        "tailsLocation": "http://192.168.178.38:6543/JiVLsA5wxVnbHQ5s7pDN58:4:JiVLsA5wxVnbHQ5s7pDN58:3:CL:7:default3:CL_ACCUM:0e65905a-b
      }
    },
    "metadata": {
      "digest": "5b2056993809fafe5e0f2e217e21cdd8851678cc109093461c68d9063fb26d54",
      "from": "JiVLsA5wxVnbHQ5s7pDN58",
      "payloadDigest": "b738b001bed04ef2e1b7c0cd47d8eb4876d9cfc7749cfe4ee1311cc5dfe231c4",
      "reqId": 1612433532851721000
    },
    "protocolVersion": 2,
    "type": "113"
  },
  "txnMetadata": {
    "seqNo": 16,
    "txnId": "JiVLsA5wxVnbHQ5s7pDN58:4:JiVLsA5wxVnbHQ5s7pDN58:3:CL:7:default3:CL_ACCUM:0e65905a-b77e-4897-a521-e1ed3a5d7783",
    "txnTime": 1612433533
  },
  "ver": "1"
}
```


Abbildung 5: Erstellung einer Revocation Registry

Ausstellen der MasterID:

Voraussetzung für das Ausstellen der MasterID ist die aktivierte eID-Funktion des Personalausweises, die zugehörige PIN und eine auf dem Smartphone installierte Wallet-App. Beim Ausstellen der MasterID sorgt die Bundesdruckere nach Prüfung der Daten dafür, dass die richtigen Daten im MasterID Credential ausgestellt werden und dass sie von Verifiern geprüft werden kann. Es wird Vertrauen in die Korrektheit der Daten durch Verwendung der eID gewährleistet. Anschließend werden die Sicherungsmaßnahmen des SSI-

Ökosystems genutzt. Genau wie bei anderen Vorgängen im Indy Ökosystem sind die öffentlichen Schlüssel im Ledger. Es ist Vertrauen in den Aussteller notwendig. Auf einem separaten Kanal wird die Authentizität des Issuers zu den Verifiern transportiert. Im Projekt werden die vertrauenswürdigen Beteiligten bekannt gegeben. Derzeit haben nur Projektbeteiligte Schreibzugriff auf das Netzwerk. Für die Vertrauenskette sind die Prüfung der „mittleren Teile“ durch die Partner notwendig. Eine Anforderung des BSI könnte sein, dass sichergestellt werden muss, dass das MasterID Credential in eine sichere Wallet ausgestellt werden darf. Die Vertrauenskette für die Korrektheit der Daten aus der MasterID (und ebenso der CompanyID) ist direkt vom Zertifikat (bzw. dem Beweis, dass eine gültige Signatur des Issuers, also der Bundesdruckerei bzw. des Unternehmens vorliegt) auf die Blockchain, auf der die Zertifikatsdefinition inklusive des öffentlichen Schlüssels (public keys) der Bundesdruckerei abliegt. Der Link zu dieser Zertifikatsdefinition liegt lokal auf einem geschützten Server des Unternehmens. Daher kann die Vertrauenskette nur unterbrochen sein, wenn

- Der private Schlüssel der Bundesdruckerei in die falschen Hände gelangt ODER
- Das Unternehmen einen falschen Link zur Blockchain (also der NodeIPs und Public Keys) erhält UND der Link zur Zertifikatsdefinition auf der Blockchain falsch ist ODER
- Mindestens zwei (1/3 bei aktuell 5) Knoten im Blockchain-Netzwerk sind kompromittiert.

Analog für die (hinsichtlich Korrektheit weniger essentiellen) Zertifikate der Unternehmen. Der Prozess zur Erstellung des MasterID VC kann von den Nutzer*Innen dann vollständig an dem Endgerät durchlaufen werden. Bei der Ausstellung der MasterID wurde der initiale QR Code entfernt. Der Nutzer kann nur mit einem Session-spezifischen Button die Wallet öffnen. So wird ein „shoulder surfing“ verhindert. Bei der anvisierten Variante der Ausstellung der MasterID mit integriertem AusweisApp2-SDK bietet sich eine enge Kopplung des Identifizierungsvorgangs (eID) und der Ausstellung der MasterID. So werden unnötige Context-Switches verhindert. Die MasterID wird in der Wallet persistiert, über die auch die Connection-Anfrage gestellt wird. Aufgrund einer Ende-zu-Ende Verschlüsselung der Kommunikation und auch der Übertragung des Zertifikats können die personenbezogenen Daten nur auf demselben Gerät / in derselben Wallet entschlüsselt und gelesen werden. Ein absichtliches Kopieren des Zertifikats des Nutzers kann aber nicht vermieden werden. In der erstellten MasterID ist neben den Werten der im Schema definierten Attribute unter anderem auch ein Verweis auf die Credential Definition hinterlegt, auf der das VC basiert. In der Revocation Registry wird der Akkumulator durch das Ausstellen des Credentials selbst zunächst nicht aktualisiert. Nur der Rückruf von VCs wird durch den Aussteller in die Revocation Registry eingetragen. Ein Rückruf kann dabei nur durch den Aussteller selbst, also in diesem Fall die Bundesdruckerei, stattfinden, da nur sie die entsprechenden Schreibrechte in der von ihr erstellten Revocation Registry auf der Blockchain besitzt. Verlangt werden kann der Rückruf etwa durch die Bundesdruckerei oder eine andere Behörde, wenn sich herausstellt, dass das Ausstellen der MasterID fälschlich geschah, oder durch die Nutzer*in mit Hilfe des Personalausweises und dessen Sperr-Code. Der Vorgang ist folglich zweigeteilt: a) Es erfolgt eine Authentifizierung des Nutzers, damit nur er/sie selbst seine/ihre Master ID zurückrufen kann. Hierzu dient

entweder das Sperrkennwort, das als Hash ausschließlich intern im Sperrdienst für die MasterID vorgehalten wird. Andernfalls kann sich der/die Nutzerin mittels Personalausweis authentifizieren und der Sperrdienst macht eine Zuordnung mittels Hash der RestrictedID (dienst- und kartenspezifisches Kennzeichen/Pseudonym). Damit verknüpft sind Sperrinformationen für das konkret ausgegebene MasterID Credential. Bei einer Sperranfrage wird erneut mittels Hash über das Sperrkennwort bzw. die RestrictedID eine Zuordnung hergestellt. Der Hash wird ausschließlich intern vom MasterID-Issuer zur Nutzerauthentifizierung verwendet, ist also niemals nach außen sichtbar und wird auch nicht zur operativen „Durchsetzung“ der Sperrung verwendet. Das SSI-Ökosystem bringt dann bereits Standardmethoden für den Rückruf mit (Tails Files, Revocation Registry, Kryptografischer Akkumulator). Nach erfolgreicher Zuordnung wird über die Standardverfahren von Hyperledger Indy (Tails Files und Sperrindex) die Sperrung vorgenommen. Dabei spielt der Hash keinerlei Rolle mehr, wird also insbesondere in keiner Form veröffentlicht oder auf den Ledger geschrieben.. Eine solche, unten beispielhaft abgebildete, Transaktion enthält die Revocation-ID des zurückgerufenen Credentials (hier: 5). Zu jedem Zeitpunkt enthält die auf der Blockchain liegende Revocation Registry die IDs aller zurückgerufenen VCs. Entscheidend ist jedoch, dass das Vorzeigen der VCs selbst gegenüber einem Verifier (wie einem Hotel) keine Informationen über die dem VC zugrunde liegende Revocation-ID beinhaltet und daher der Stand des Akkumulators selbst wohl kein personenbezogenes Datum darstellt, solange die Nutzer*Innen nicht die Inhalte ihrer Credentials mit Hilfsmitteln aus der Wallet-App auslesen und an Dritte preisgeben (die Revocation ID ist selbst für die Nutzer*Innen in der Wallet-App nicht direkt ersichtlich).

```
{
  "auditPath": [
    "CMKw3c5y9c6CXNo7QJ7gloAxMtMRy8SKaDTEqvFkYRkh",
    "cAFRCxpHMh2BtJhuFJvNENZuueUmRWfxmulwMthMssm",
    "CHKJL7BAhu6D5tDbpK7QEEA3sh6anc6H66t8gb3NpUlk",
    "AS7mfXemxEDVcXFwHaVy6LY1PWBCgve63pvTnUWr62su",
    "7NmonaDvjy2WZpjVBWJsGzklgxkHr2Mc5U8Zn8Q5iYie",
    "5UxVWkjJ9bYP1Qcd4subh2XjEzYMeMcq9uFTpPxL4rnP",
    "GuC6LojD4yx7JSAaruNsJYKrPB4XyioSLr3PK8oe9maD"
  ],
  "ledgerSize": 639,
  "reqSignature": {
    "type": "ED25519",
    "values": [
      {
        "from": "5NMPyTTsWzvLNfBNnDt8g8",
        "value": "4SHFJN17TuytqF8LVu9aagKATFpPMQew2bEdHaKXuMBpTgVyXxbQGFVdutZxlVT8tUaj2WjsuZ6emuP5GtKkq4JP"
      }
    ]
  },
  "rootHash": "HhGzpaTyQooBtKjNiEm3utyoKtEKFVWTgLhtwVqmlJfM",
  "txn": {
    "data": {
      "revocDefType": "CL_ACCUM",
      "revocRegDefId": "5NMPyTTsWzvLNfBNnDt8g8:4:5NMPyTTsWzvLNfBNnDt8g8:3:CL:7:Arbeitgeberbescheinigung:CL_ACCUM:28e738c3-a0d5-45b7-b6d8-e4561b0
      "value": {
        "accum": "21 135C9FB239D11C2307E27D4DFB9B035BF1282D158B3458BF10C804685372D0584 21 145D143E605804164DDB80E8599E715F0C67A1467E3AE463CA135I
        "prevAccum": "21 11EA8BE4770BA6C752B6AF9A39B689EBACF9804AABF861218EEC38555CEA33F19 21 128B269581BCA7C5CD929901B2689F8B262B65F10DF52849B8
        "revoked": [
          5
        ]
      }
    },
    "metadata": {
      "digest": "df68e8e02aa64a14a0b486ecc3ff7bc10f9d55511f382f33cc6754546be06854",
      "from": "5NMPyTTsWzvLNfBNnDt8g8",
      "payloadDigest": "ddd699423a22a5cd893111f97f9c22d7aa74423dfc02c19dafld3434f82efa91",
      "reqId": 1615822577038986000
    },
    "protocolVersion": 2,
    "type": "114"
  },
  "txnMetadata": {
    "seqNo": 639,
    "txnId": "5:5NMPyTTsWzvLNfBNnDt8g8:4:5NMPyTTsWzvLNfBNnDt8g8:3:CL:7:Arbeitgeberbescheinigung:CL_ACCUM:28e738c3-a0d5-45b7-b6d8-e4561b03085c",
    "txnTime": 1615822577
  },
  "ver": "1"
}
```


Abbildung 6: Revocation eines VCs

Ausstellen der CompanyID:

Hierfür wird zunächst wie für das Ausstellen der MasterID eine ende-zu-ende-verschlüsselte Verbindung zwischen Nutzer*Innen und dem Cloud-Agent des entsprechenden Arbeitgeber-Unternehmens hergestellt. Dazu können Nutzer*Innen etwa einen QR-Code scannen, den sie per E-Mail zugeschickt bekommen oder vor Ort aus dem FrontEnd abscannen, etwa während eines Termins mit der Personalabteilung. Sobald die Verbindung aufgebaut wurde, stellt das Arbeitgeber-Unternehmen den Nutzer*Innen das VC aus. Der Prozess des Ausstellens (und auch der Revocation) läuft damit analog zum Ausstellen der MasterID. Das im Tails-Server zum Download verfügbare öffentliche Tails-File wird von der Wallet-App gemeinsam mit dem VC gespeichert und für die spätere Erstellung des Proofs of Non-Revocation benötigt. Das Tails-File selbst muss für die Wallet-App nur beim Ausstell-Prozess über das Internet erreichbar sein, um es einmalig herunterzuladen. Danach ist die Verfügbarkeit des Tails-Servers für einen erfolgreichen Verifizierungsprozess inklusive eines Proofs of Non-Revocation für Nutzer*Innen, die bereits ein VC von diesem Aussteller haben, nicht mehr erforderlich.

Dabei ist wichtig, dass in den Komponenten Company-Controller und Company-MongoDB vor und während des Ausstellprozesses personenbezogene Daten verarbeitet werden und auch möglicherweise personenbeziehbare Daten gespeichert werden: Vor dem Ausstellprozess wird ein Arbeitnehmer mit einer (ihm bereits im Bestehenden IT-System zugeordneten) eindeutigen ID sowie den für das Befüllen der

CompanyID nötigen Daten (wie etwa dem Namen des Arbeitnehmers) in der MongoDB abgespeichert. Nach dem Ausstellen der CompanyID wird dann statt der ausgestellten, personenbezogenen Attribute ein Eintrag in die MongoDB geschrieben, der die eindeutige ID des Arbeitnehmers sowie die Revocation-ID des VCs und die ID der Revocation Registry enthält. Zusätzlich enthält der Company-Agent nach dem Ausstellen einer CompanyID Informationen zur Verbindung zur Wallet des Arbeitnehmers (etwa die Verbindungs-ID und Metadaten wie der Zeitpunkt der Verbindungserstellung), die ebenfalls personenbezogene Daten enthalten kann (etwa der Namen der Wallet-App, z.B. hier “esatus Wallet”) in Verbindung mit der Arbeitnehmer-ID. Im Zusammenspiel mit den Daten im bestehenden System des Unternehmens (Zuordnung Arbeitnehmerdaten – Arbeitnehmer-ID) sind diese Daten als personenbezogen einzustufen. Das Abfragen dieser Daten aus dem Agent ist über einen API-Key abgesichert. Die Daten im Agent (Zuordnung Arbeitnehmer-ID – Verbindungs-ID und Metadaten) sowie in der MongoDB isoliert betrachtet (Zuordnung Arbeitnehmer-ID – Revocation-ID) sind jedoch unproblematisch. Das Vorhalten dieser Daten ist notwendig, um die CompanyID eines bestimmten Arbeitnehmers zu widerrufen (Zuordnung Arbeitnehmer-ID – Revocation- ID) und über die bestehende sichere Verbindung zur Wallet-App eines Arbeitnehmers diesem eine neue, aktualisierte CompanyID auszustellen (Zuordnung Arbeitnehmer-ID – Verbindungs-ID).

Hotel Check-in (Request Proof)

Den Hotel Check-in können Nutzer*Innen im Anschluss digital mit den erhaltenen VCs (MasterID und CompanyID) erledigen. Mit Hilfe der Wallet-App wird an der Rezeption ein QR-Code aus der Wallet gescanned, woraufhin diese (über https) eine Anfrage an den Hotel-Controller schickt. Der Hotel-Controller legt den Vorgang in der MongoDB an und erstellt mit Hilfe des zugeordneten Agents einen sogenannten Proof Request. Dieser Request beinhaltet den Endpoint sowie Public Key des Agents (für die spätere Kommunikation von Wallet-App zu Agent), eine Liste der nachzuweisenden Attribute aus MasterID und CompanyID sowie weitere Informationen (etwa der Zeitraum, in dem Non-Revocation nachgewiesen werden muss). Dabei wird auch die Einschränkung, dass die MasterID einer bestimmten Credential Definition entsprechen muss (also von der Bundesdruckerei entsprechend deren Public Key auf dem Ledger signiert ist) und dass die CompanyID von einem der Unternehmen auf dem Indy-Ledger nach dem CompanyID-Schema erstellt wurde. Die Korrektheitsgarantie der Angaben aus der MasterID ist damit stärker als die der CompanyID, da es bereits genügt, wenn einer der Stewards ein neues Unternehmen zum Ledger hinzufügt, damit dieses eine Credential Definition für eine eigene CompanyID ausstellen könnte, die von den Hotels akzeptiert wird. Dies ist aber im vorliegenden Projekt beabsichtigt, da die Informationen zum Unternehmen nur eine Hilfestellung zur Rechnungsstellung sind und keinen gesetzlich vorgegebenen Zweck (Identitätsprüfung für den Beherbergungsmeldeschein) erfüllen. Die Sicherheitsgarantien für Angaben aus der CompanyID müssen somit nicht so hoch sein, wie die für Daten aus der MasterID. Über einen Redirect wird der Proof Request dann zurück an die Wallet-App gegeben, wo die Wallet-App den Proof Request verarbeitet. Die Wallet-App erstellt dabei eine sogenannte Verifiable Presentation als Antwort auf den Proof

Request. Diese Antwort enthält die geforderten Attribute aus MasterID und CompanyID, einen Beweis, dass diese jeweils tatsächlich aus einem VC, das die Bundesdruckerei bzw. eines der Arbeitgeber-Unternehmen signiert haben, sowie einen Beweis, dass das jeweilige VC bis kürzlich nicht zurückgerufen war. Im Gegensatz zu herkömmlichen Zertifikaten (wie bspw. JSON-Web oder X.509) muss dabei das VC nicht komplett vorgezeigt werden, um die Herkunft der angegebenen Werte darin mit Hilfe der Signatur zu beweisen (dieses Verfahren zum Nachweis, dass die Signatur vorliegt, wird als Zero-Knowledge Proof bezeichnet und ist durch das Camenisch-Lysyanskaya-Signaturverfahren implementiert). Dadurch können nicht benötigte Attribute, korrelierende Informationen wie der Wert der Signatur auf dem VC, und die (in Kombination mit den Informationen zum Akkumulator in der Blockchain) datenschutzrelevante Revocation-ID zurückbehalten werden. Sobald die Antwort beim Agent über eine ende-zu-ende-verschlüsselte Verbindung von der Wallet-App eingeht, prüft dieser den Beweis auf Korrektheit und benachrichtigt über einen Webhook den Hotel-Controller. Dieser fragt anschließend die im Beweis enthaltenen Daten aus dem Hotel-Agent ab und löscht im Hotel-Agent alle Informationen, die im Zuge des Nachweisprozesses entstanden sind. Danach übermittelt der Hotel-Controller die aus MasterID und CompanyID abgefragten Daten an das Hotel-Backend, damit der Check-in-Vorgang über das bestehende System abgeschlossen werden kann. Anschließend werden auch die zu dem Vorgang gehörigen Daten in der zum Hotel-Controller gehörigen MongoDB gelöscht. Nach diesem Vorgang beinhalten damit sowohl der Hotel-Agent als auch die MongoDB genau dieselben Daten wie zuvor, sodass dort keine personenbezogenen Daten mehr vorliegen.

3.3 Risikobetrachtung anhand der Prozesskette

Nachfolgend wird eine Risikobetrachtung des Check-in-Prozesses beim Hotel vorgenommen. Hierzu wird vor allem die MasterID betrachtet, da die Meldebescheinigung vom Hotel mit Hilfe der Daten aus der MasterID erstellt wird. Durch das Bereitstellen der Credential-Definition in der Hotel-Controller-Komponente wird festgelegt, welche Spezifikation das MasterID-Credential hat. Mit Hilfe der eID-Funktion des Personalausweises und der entsprechenden digitalen Signatur kann die Bundesdruckerei über die bestehende Vertrauenskette mit sehr hohem Level of Assurance sicherstellen, dass die von der Wallet-App übermittelten Daten korrekt sind. Mit diesen Daten stellt dann die Bundesdruckerei das MasterID VC aus und sendet es, ebenfalls digital signiert, an die Wallet-App. Damit ist über bisherige Vertrauensketten sichergestellt, dass die MasterID nur die tatsächlichen Daten vom Personalausweis enthält. Über die im Pilotprojekt bekannte Credential Definition der MasterID (die den Public Key der Bundesdruckerei enthält) kann die Authentizität der Daten im VC nun von Dritten mit Hilfe der Credential Definition überprüft werden. Somit können die Hotels beim Check-in überprüfen, dass die Daten im MasterID Credential mit den Daten aus dem zugehörigen Personalausweis übereinstimmen. Im Rahmen des Hotel Check-ins werden dabei die Daten aus dem MasterID-Credential über eine ende-zu-ende-verschlüsselte Verbindung vorgezeigt, wobei die Gültigkeit der digitalen Signatur und Non-Revocation mit Hilfe eines kryptographischen Zero-Knowledge-

Proofs belegt und vom Hotel mit Hilfe der lokal hinterlegten Credential Definition ID und den dazu auf der Blockchain gehörigen Credential Definition und Revocation Registry überprüft werden. Sobald die Daten beim Check-in im Hotel überprüft wurden, werden diese im Hotel-Backend gespeichert. Danach verläuft der Check-In-Prozess im Hotel unabhängig von der Identifikationsmethode, insbesondere das Erstellen der Meldebescheinigung aus dem bestehenden Backendsystem des Hotels.

Der Prozess des Prüfens der Informationen aus der eID und das entsprechende Ausstellen des MasterID VCs durch die Bundesdruckerei genügt aufgrund der Erfahrungen der Bundesdruckerei und der Integration des Services in die bestehenden Kompetenzen der Bundesdruckerei hohen Sicherheitsanforderungen; dabei wird eine bestehende kryptographische Vertrauenskette (eID) auf eine neue Vertrauenskette (Credential Definition der MasterID in der Blockchain und Signatur durch die Bundesdruckerei) übertragen. Die Wallet-App selbst kann keine gültige Änderung des VCs erstellen, da sie den privaten Schlüssel der Bundesdruckerei nicht kennt. Als Herausforderung und schwächstes Glied in der beschriebenen Vertrauenskette kann das Referenzieren der korrekten Credential Defintion durch den Hotel-Controller festgestellt werden. Nur wenn diese korrekt angegeben wird, können die übergebenen Werte aus dem MasterID Credential korrekt überprüft werden (In der analogen Welt würde das einer Schulung, wie ein echter Personalausweis aussieht, entsprechen). Beim Starten der Hotel-Controller Komponente ist daher zu beachten, dass die korrekte Credential Definition für die MasterID in Form einer Umgebungsvariable übergeben wird. Diese Herausforderung lässt sich gut durch organisatorische Maßnahmen, wie Schulungen und spezielle Trainings lösen. Eine rein technische Lösung ist hierfür aktuell nicht vorgesehen, auch wenn langfristig auch hier zertifikatsbasierte Ansätze oder ein Verlängern der Vertrauenskette direkt in die Blockchain denkbar sind.

3.4 Datenfelder

Die folgenden Daten werden verarbeitet:

Abbildung 7: Datenfelder

3.5 Informationsverb., Netzplan und Kommunikationsverbindungen

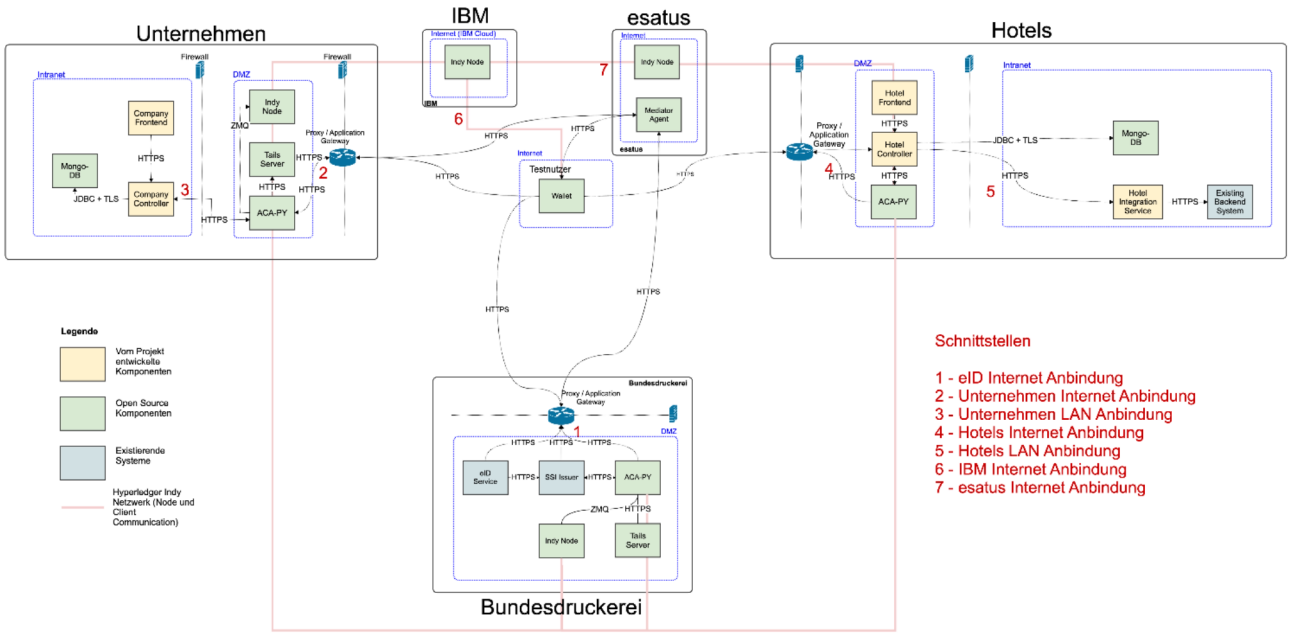

Abbildung 8: Gesamtüberblick

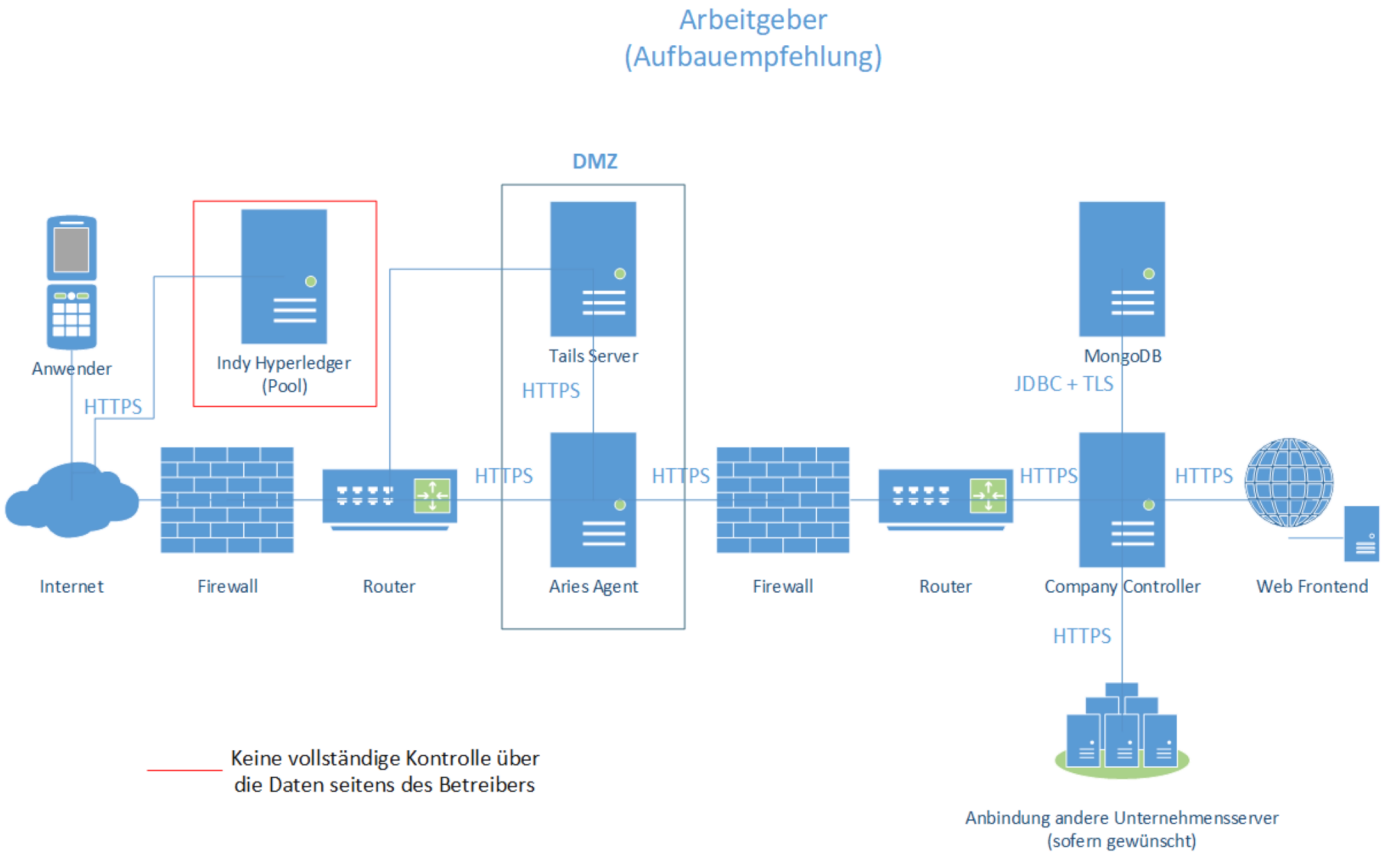

Abbildung 9: Netzplan Arbeitgeber

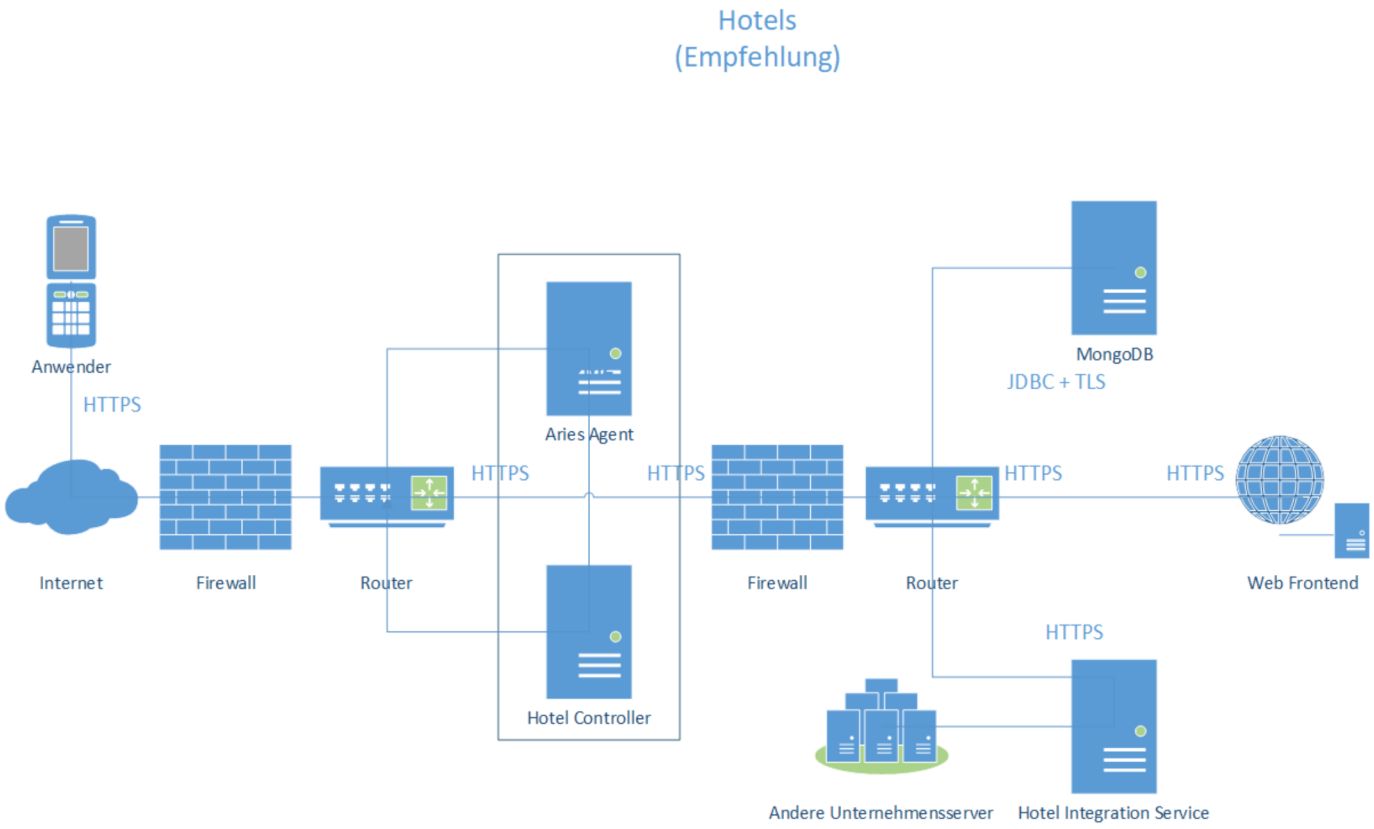

Abbildung 10: Netzplan Hotels

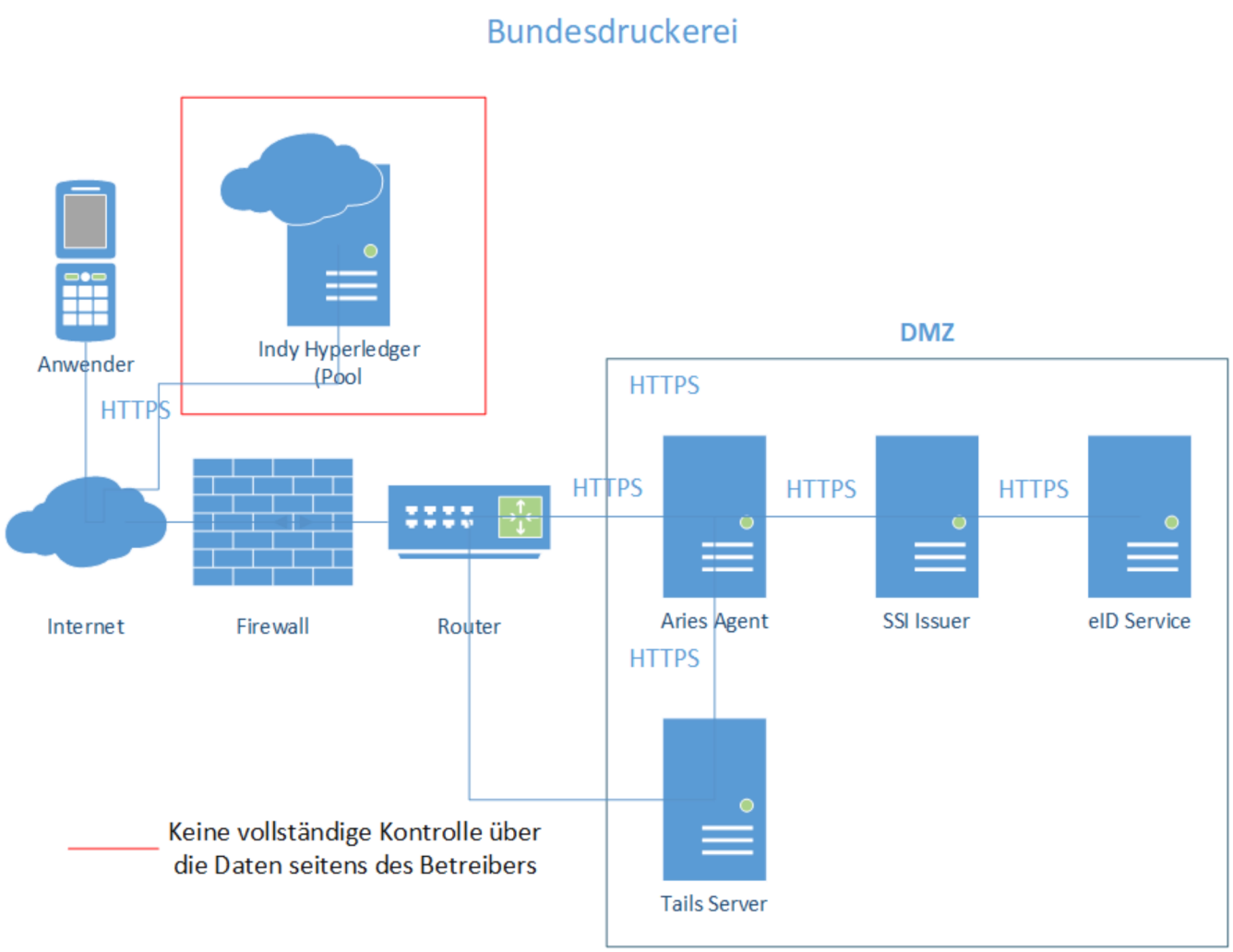

Abbildung 11: Bundesdruckerei

3.6 Wesentliche IT-Anwendungen und IT-Systeme

Die Komponenten des Gesamtsystems laufen derzeit in Kubernetes Clustern bzw. werden als virtuelle Maschine betrieben. Die verschiedenen Komponenten werden auf Ubuntu (Linux) Servern installiert und konfiguriert.

Durch die teilnehmenden Hotels werden jeweils ein oder mehrere Komponenten für SSI-Interaktionen betrieben (Aries Agent/s für Interaktionen, die zudem eine Wallet-App beinhalten, Tails-Server zur Speicherung und Bereitstellung von Tails-Files) sowie verschiedene Backend-Komponenten (Hotel-Controller zur Koordination, MongoDB zur Datenspeicherung, Integration Service zur Backendintegration, Frontend). Die Arbeitgeber-Unternehmen betreiben jeweils die entsprechenden Komponenten ohne Integration in ihr Backend. Die Endnutzer*innen der Anwendung nutzen eine Smartphone-App für SSI-Interaktionen, die esatus Wallet. Seitens der Bundesdruckerei wird neben einem eID-Service zur Erstellung von MasterID Credentials ein weiterer Aries Agent betrieben, um die Credentials auszustellen. Zudem betreiben die DB und BWI (Arbeitgeberunternehmen), die Bundesdruckerei, esatus sowie IBM einen Knoten des unternehmensübergreifenden Indy Blockchain-Netzwerkes.

Auf den Mobilgeräten (iOS und Android) der Testnutzer*Innen kommt die von esatus entwickelte ID-Wallet App zum Einsatz.

Übersicht:

Komponente	**Technologie**	**Zweck**
Server Basis	Ubuntu Server, Docker	Hostsystem der Infrastruktur für alle untenstehenden Komponenten
Company-Controller	Java, Spring Boot	Koordinierung des Ausstellvorgangs des Company-Credentials
Hotel-Controller	Java, Spring Boot	Koordinierung des Verifizierungsvorgangs beim Check-in
Hotels Integration Service	REST Interface	Übermittlung der aus MasterID und CompanyID beim Verifizierungsvorgang

		bestätigten Daten für das Hotel-Backend
Web-Frontend Company	Angular	Benutzeroberfläche für Angestellte im Arbeitgeber-Unternehmen für die Ausstellung von CompanyIDs an die Arbeitnehmer*Innen der Arbeitgeber-Unternehmen
Web-Frontend Hotel	Angular	Benutzeroberfläche für Angestellte im Hotel, um den Check-in an ihrem Schalter zu koordinieren
Hyperledger Indy Netzwerk	Hyperledger Indy	Infrastruktur zum Speichern und öffentlichen Auslesen von Schemas, Credential Definitions und Revocation Registries
Tails-Server	bcgov / indy-tails-server	Infrastruktur zum Download der Tails-Files durch die Wallet-Apps beim Ausstell-Vorgang von VCs durch Arbeitgeber-Unternehmen und Bundesdruckerei
Aries Agent (ACA-PY)	Python	Client-Funktionen für die Blockchain, Kommunikation mit den Wallets der Nutzer*Innen, Ausstellen (Arbeitgeber-Unternehmen, Bundesdruckerei) und Prüfen (Hotels) von VCs

Mobiltelefon	esatus SSI Wallet	Speichern von kryptographischen Schlüsseln und VCs, Kommunikation mit den Agents und dem Hotel-Controller auf Seite der Nutzer*Innen Die App ist über eine PIN, gespeichert im gesicherten Speicher des Smartphones (sowohl iOS (Secure Enclave) als auch Android (Secure storage)), geschützt. Diese PIN entsperrt die App und gewährt anschließend den Zugriff auf weitere Elemente des sicheren Speichers. Bei der Generierung des Wallet wird der „master key“ mittels der Indy-SDK Methode „indy_generate_wallet_key“ erzeugt. Die „key derivation method“ des Wallet kann angepasst werden und ist per default „ARAGON2I_MOD“; Die für den Nutzer optionale biometrische Überprüfung erfolgt durch die von den Systemen bereitgestellten Funktionen, heißt die App selbst verwaltet keine biometrischen Daten.

eID Service	Bereits BSI-Konformität[1]	Prüfen der auf dem Personalausweis aktivierten eID durch die Bundesdruckerei
SSI Issuer	Bereits BSI-Konformität	Ausstellen eines MasterID VCs auf Basis der aus der eID stammenden, verifizierten Daten durch die Bundesdruckerei

Tabelle 4: IT Systeme und Anwendungen

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03130/tr-03130.html

4 SCHUTZBEDARFSFESTSTELLUNG

4.1 Datenklassen

Die folgenden Datenklassen wurden definiert. Der Schutzbedarf wird an Hand der Definitionen des BSI Standards 100-2 in Stufen normal, hoch und sehr hoch bewertet.

Datenklasse	**Enthaltene Daten**	**Schutzbedarf Integrität**	**Schutzbedarf Verfügbarkeit**	**Schutzbedarf Vertraulichkeit**
Credential Templates				
MasterID (Master ID)	• Stadt • Familienname • Geburtsort • Geburtsname • Vorname • Geburtsdatum • Straße • Land, • Ablaufdatum • akademischer Titel • PLZ	hoch	normal	hoch
Arbeitgeber-Credential (Corporate ID)	• Vorname • Nachname • Firma Name • Firma Land • Firma Straße • Firma PLZ • Firma Stadt	normal	normal	normal
Bisherige Daten im Rahmen des Check-Ins				
Daten Hotelsystem	• Vorname • Nachname • Straße	normal	normal	hoch

	• PLZ • Stadt • Land • Geburtsdatum • Firma Name • Abteilung • Firma Straße • Firma PLZ • Firma Stadt			
Rechnung	• Vorname • Nachname • Firma Name • Abteilung • Firma Straße • Firma PLZ	normal	normal	hoch
Meldeschein	• Vorname • Nachname • Straße • Hausnummer, • PLZ • Stadt • Land • Geburtsdatum Weitere Daten, die nicht dem SSI Verfahren entstammen: • Staatsangehörigkeiten • Zahl Mitreisende Angehörige • Zahl Mitreisende • Name Zahlungsdienstleister • Zahlungstoken • Datum Ankunft	hoch	hoch	hoch

	• Datum Abreise • Beherbergungsstätte Name • Beherbergungsstätte Anschrift • Seriennummer Pass (optional) • Ortsteil • Alternative Adressangabe • Staatsangehörigkeit Mitreisender			
Öffentliche Daten (auf der Blockchain bzw. dem Tails-Server)				
Corporate ID Schema	• Name • Version • eine Liste mit Attributsnamen	normal	normal	normal
Corporate ID Credential Definition	• Schema ID (das DID eines Credential Schemas) • Issuer DID (die DID eines Schema Credential Ausstellers)	hoch	normal	normal
Revocation Registry	• ID (Registry ID) • revocDefType (Registry Typ) • tag (einzigartige beschreibende ID der Registry), credDefId (Credential Definition ID), • issuanceType: (Default oder OnDemand) • maxCredNum (maximale Anzahl der Credentials, die die Registry bedienen kann) • tailsHash (Hash der Tails)	hoch	normal	normal

	• tailsLocation (Ort des Tail Files) • publicKeys (ursa formatierte Public Keys) • ver (Version des Revocation Registry Definition json) • revoc_reg_entry_json (Revocation Registry Eintrag der den initialen Status der Revocation Registry beinhaltet) • prevAccum (vorheriger Accumulator Wert) • accum (derzeitiger Accumulator Wert) • issued (ein Array von ausgestellten Indizes) • revoked (Array von revoked Indizes)			
Tails-File	• Liste mit randomisierten Zahlen (aktuell: 1.000)	normal	normal	normal
SSI-Daten im Rahmen der Ausstellung der CompanyID				
Employee	• Id (einzigartige ID des Angestellten) • firstName • familyName • companyName • companySubject • companyAddressStreet • companyAddressZipCode • companyAddressCity	normal	normal	normal

Connection Invitation	• recipientKeys (öffentliche Schlüssel, die mit der Einladung verbunden sind, der private Schlüssel befindet sich beim Einladenden / Ersteller der Verbindungs-Einladung) • @type (Typ der didcomm Nachricht) • imageUrl (URL der Grafik die das einladende Unternehmen repräsentiert) • @id (einzigartige ID der Verbindungseinladung) • Label (label für das einladende Unternehmen) • serviceEndpoint (Host Name oder IP-Addresse des company-agents)	normal	normal	normal
Connection	Accept (kontrolliert die automatische Annahme von Verbindungen, ist hier auf „auto“ gesetzt) • alias (ein Label für die Verbindung, im Projekt wir hier die „employee id“ genutzt) • connection_id (einzigartige ID der Verbindung) • created_at (Zeitstempel des Aufbaus der Verbindung) • initiator (definiert wer die Verbindung aufgebaut hat, hier immer „self“)	normal	normal	normal

	• invitation_key (der Empfänger Key der Einladung die zum Verbindungsaufbau führte) • invitation_mode (kontrolliert wie oft die Verbindungseinladung genutzt werden kann, hier immer auf „once“ (einmal) gesetzt) • my_did (die DID des DID Dokuments welches mit der lokalen Seite der Verbindung zusammen hängt) • state (Status der Verbindung wie sie im Aries DID Exchange Protocol definiert ist) • their_did (die DID des DID Dokuments welches mit der Remote Seite der Verbindung zusammen hängt) • their_label (ein Label dass die einladende Partei definiert, hier bspw. auf „esatus Wallet“ gesetzt) • updated_at (Zeitstempel des letzten Updates)			
Credential Exchange Record Issue Credential	Der „credential exchange record“ ist ein temporärer Eintrag, der erstellt wird, wenn einem Angestellten ein Credential angeboten wird.	hoch	normal	hoch

	Akzeptiert dieser das Credential, so wird der Eintrag gelöscht.			
Issued Credential	• cred_rev_id (die Credential Revocation ID) • rev_reg_id (die ID der Credential Revocation Registry) • employee_id (die ID des Angestellten dem das Credential zugeordnet ist)	normal	normal	normal
SSI-Daten im Rahmen des Check-ins beim Hotel				
PresentProofUrl	• hotel_id (die ID des Hotels) • desk_id (die ID der Rezeptionsschalters) • ip_address (die IP-Adresse des hotel-controllers)	normal	normal	normal
Proof Request	• @type (der Typ der didcomm Nachricht) • @id (einzigartige ID dieser Bestätigungsanfrage) • request_presentation_attach (Information darüber welche Datenfelder von welchem Credential in der Bestätigungsantwort erwartet werden) • recipientKeys (öffentlicher Schlüssel des Hotel Agents, dieser hat den damit verbunden Privaten Schlüssel, was erlaubt, dass eine verschlüsselte connection-less	normal	normal	normal

	Bestätigungsanfrage an den Hotel Agent geschickt wird) • routingKeys (öffentliche Schlüssel aller mit dem Routing oder der Mediation in Zusammenhang stehenden Agenten die eine Nachricht im Laufe einer Bestätigungsanfrage durchlaufen hat) • serviceEndpoint (IP Adresse oder Host Name des hotel-agents)			
Presentation Exchange Record	Der „presentation exchange record“ ist ein temporärer Eintrag, der erstellt wird, wenn eine Bestätigung (proof) angefragt wird. Der Eintrag wird gelöscht, sobald die Bestätigung gesendet wurde.	hoch	normal	hoch
Proof Presentation	• @type (Typ der didcomm Nachricht) • @id (einzigartige ID der didcomm Nachricht) • request_presentation_attach (die „Payload” der Bestätigungsanfrage, inklusive aller angeforderten Datenfelder der Corporate und Master ID)	hoch	normal	hoch
Checkin Credential	• Id (einzigartige ID des Eintrags) • hotel_id (ID des Hotels)	hoch	normal	hoch

	• desk_id (ID des Rezeptionsschalters) • scan_date (Zeitstempel des QR Code Scans) • send_date (Zeitstempel wann die Präsentation der Bestätigung (proof) empfangen wurde) • pres_ex_id (identifiziert den proof mit dem entsprechenden Check-In Vorgang), • masterId (enthält alle Datenfelder der Master ID) • corporateId (enthält alle Datenfelder der Corporate ID)			

Tabelle 5: Datenklassen

4.2 Verarbeitete Daten je Komponente, Schutzbedarfsermittlung

In diesem Abschnitt wurden die Datenklassen den Komponenten zugeordnet, sowie deren Schutzbedarf hinsichtlich Integrität, Verfügbarkeit und Vertraulichkeit bewertet.

Komponente	**Verarbeitete Daten**	**Schutzbedarf Integrität**	**Schutzbedarf Verfügbarkeit**	**Schutzbedarf Vertraulichkeit**
Blockchain-Knoten (Indy Node)	*Speicherung:* DIDs der Nodes, Bundesdruckerei, Arbeitgeber, Corporate ID Schema, Corporate ID Credential Definitions, Revokation Registries	hoch	hoch	normal
Aries Agent (ACA-PY) Unternehmen	*Erstellung, Zwischenverarbeitung, Durchleitung:* Arbeitgeber-Credential, Corporate ID Schema, Corporate ID Credential Definition, Revocation Registry, Tails File, Connection Invitation, Connection, Credential Exchange Record, Corporate ID, Issued Credential	hoch	normal	hoch
Aries Agent (ACA-PY) Hotels	*Erstellung, Zwischenverarbeitung, Durchleitung:* Arbeitgeber-Credential, MasterID, Proof Request, Presentation Exchange Record, Proof Presentation	hoch	normal	hoch
Tails Server	*Speicherung:* Tails Files	gering	normal	normal
Company-Controller	*Zwischenverarbeitung, Durchleitung:* Arbeitgeber-Credential, Employee,	normal	normal	normal

	Connection Invitation, Issued Credential			
Hotel-Controller	*Zwischenverarbeitung, Durchleitung:* MasterID, CompanyID, CheckIn Credential, Proof Request	hoch	normal	hoch
Web-Frontend Company	*Verarbeitung:* Einwilligung zur Teilnahme am Piloten, Mitarbeiter Firmendetails, Ausstellung Arbeitgeber-Credential, Proof Request, Proof Presentation	normal	normal	normal
MongoDB Company	*Speicherung:* Einwilligung zur Teilnahme am Piloten, Arbeitgeber-Credential	normal	normal	normal
Web-Frontend Hotel	*Anzeige:* kombinierte Details Arbeitgeber-Credential, MasterID, Meldebescheinigung, CheckIn Credential	hoch	normal	hoch
MongoDB Hotel	*Speicherung:* kombinierte Details Arbeitgeber-Credential, MasterID, Meldebescheinigung	hoch	normal	hoch
Hotels Integration Service	*Durchleitung:* Check-in Credential	hoch	normal	hoch
ID-Wallet App (signierte Daten)	*Verarbeitung, Speicherung:* MasterID, Arbeitgeber-Credential, DID Document, Tails File, Connection Invitation, Connection, Credential Exchange Record, Corporate ID, Proof	normal	normal	hoch

	RequestPresentation Exchange Record			

Tabelle 6: Schutzbedarf Daten je Komponente

Die Abbildung *Gesamtüberblick Schnittstellen* enthält eine Auflistung der wesentlichen Verbindungen. Nachstehend werden diese Verbindungen beschrieben.

Verbindung	Beschreibung
eID Ausstellung	Der Anwender initiiert die Ausstellung seiner MasterID via AusweisApp2. Die App baut eine Verbindung zum eID-Service der Bundesdruckerei auf, nach Verifizierung [tbd] baut dieser eine Verbindung zum SSI-Issuer auf zwecks Ausstellung der Master ID. Der SSI-Issuer baut eine Verbindung zur AusweisApp2 zwecks Übermittlung der signierten MasterID auf. Die Wallet erstellt ein Schlüsselpaar mit privater DID und speichert die MasterID ab. Die Kommunikation läuft über das Internet (Kommunikation Wallet mit Blockchain-Knoten, Tails-Server und Company-Agent) sowie das LAN der Bundesdruckerei, innerhalb der DMZ. Die Verbindung zwischen dem Mobiltelefon und der Bundesdruckerei ist bidirektional, die Verbindung wird nach Ausstellung der MasterID getrennt.
Ausstellung Arbeitgeber-Credential	Schnittstellen: S2, S3 und gegebenenfalls S6 Nach Erhalt einer E-Mail initiieren die Testnutzer*Innen (Mitarbeiter*Innen) die Ausstellung des Arbeitgeber Credentials mittels eines QR Code Scans. Nachfolgend baut das Mobiltelefon eine Verbindung zum Unternehmensnetzwerk auf und lädt das Credential herunter, dieses wird dann zusammen mit der dazugehörigen DID in der Wallet gespeichert.

	Besitzt ein Unternehmen keinen eigenen Hyperledger Indy Node, so wird seitens der Unternehmens Aries Agents noch eine Verbindung zu zwei Hyperledger Indy Node aufgebaut, um die DID auch dort zwecks späterer Verifizierung der Authentizität zu speichern. Die Kommunikation läuft hier über das Internet, sowie das LAN des Unternehmens. Die Verbindung Mobiltelefon – Unternehmensnetzwerk verlässt die DMZ nicht. Der Aries Agent baut intern noch eine Verbindung zum Company Controller auf, der sich im Intranet des Unternehmens befindet. Die Verbindung zwischen Mobiltelefon und Unternehmensnetzwerk ist bidirektional, endet jedoch nach Übertragung des Credentials. Die eventuell aufgebaute Verbindung zu einem Hyperledger Node ist ebenfalls bidirektional, wird aber nach Übertragung der DID ebenfalls beendet.
Hotel Check-In	Beim Hotel Check-in wird die Übermittlung der Daten des Anwenders an das Hotel nach dem Einscannen eines QR Codes ausgelöst. Während dieses Prozesses übermittelt der Anwender die Daten, sowie die zuvor erstellten DIDs über seine Wallet. Der Hotel Controller empfängt die Daten und verifiziert die DIDs mittels Abfrage auf einem Hyperledger Node. Im Anschluss werden die verifizierten Daten im Property Management System des Hotels gespeichert sowie zur Speicherung des Meldescheindaten gemäß den gesetzlichen Anforderungen genutzt. Die Kommunikation läuft hier über das Internet, sowie das LAN des Hotels. Die Verbindung Mobiltelefon – Hotelnetzwerk verlässt die DMZ

	nicht. Der Aries Agent baut intern noch eine Verbindung zum Hotel Controller auf, der sich im Intranet des Unternehmens befindet. Die Verbindung des Mobiltelefons zum Hotelnetzwerk ist bidirektional, wird jedoch nach Übertragung der Daten beendet. Die Verbindung des Hotel Aries Agents zu einem Hyperledger Node ist ebenfalls bidirektional, wird aber nach Verifizierung der DIDs ebenfalls beendet.
Hyperledger Nodes Synchronisierung	Jeder Blockchain-Knoten repliziert neue Ledger-Einträge mit den anderen Blockchain-Knoten.Die Verbindungen sind bidirektional. Die Node-Betreiber haben keinen vollständigen Einfluss auf die Daten, die in das Ledger geschrieben werden. Die Kommunikation findet hier über das Internet statt.

Tabelle 7: Kommunikationsverbindungen

5 MODELLIERUNG NACH IT-GRUNDSCHUTZ

Zur Ergänzung der Sicherheitskonzepte der Organisationen, die Teile der neuen Infrastruktur betreiben werden, werden diejenigen Anforderungen des Grundschutzes identifiziert, denen ggf. neue, spezifische Maßnahmen gegenübergestellt werden müssen.

5.1 Auswahl der relevanten IT-Grundschutz-Bausteine

Im Rahmen dieses Sicherheitskonzepts werden folgende Bausteine betrachtet:

Sicherheitsmanagement
ISMS.1 Sicherheitsmanagement

Betrieb
OPS.2.1 Outsourcing für Kunden
OPS.2.2 Cloud-Nutzung
OPS.3.1 Outsourcing für Dienstleister

Konzeption und Vorgehensweise
CON.2 Datenschutz
CON.3 Datensicherungskonzept

Anwendungen
APP.1.4 Mobile Anwendung (Apps)
APP.3.1 Webanwendungen
APP.3.2 Webserver
APP.4.3 Relationale Datenbanksysteme
APP.5.2 Microsoft Exchange und Outlook
APP.5.3 Allgemeiner E-Mail-Client und -Server
APP.6 Allgemeine Software
APP.7 Entwicklung von Individualsoftware

IT-Systeme
SYS.1.1 Allgemeiner Server
SYS.1.2.2 Windows Server 2012
SYS.1.3 Server unter Linux und Unix
SYS.1.5 Virtualisierung
SYS.1.6 Kubernetes (CD)
SYS.3.2.1 Allgemeine Smartphones und Tablets
SYS.3.2.2 Mobile Device Management (MDM)
SYS.3.2.3 iOS (for Enterprise)
SYS.3.2.4 Android
SYS.3.3 Mobiltelefon

Netze und Kommunikation
NET.3.1 Router und Switches
NET.3.2 Firewall
NET.3.3 VPN

Die folgenden Bausteine werden **nicht** betrachtet, da sie entweder keinen Bezug zum Projekt haben, beziehungsweise davon ausgegangen wird, dass die Anforderungen der Bausteine bereits ausreichend durch geeignete Maßnahmen erfüllt werden:

Organisation und Personal
ORP.1 Organisation
ORP.2 Personal
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
ORP.4 Identitäts- und Berechtigungsmanagement
ORP.5 Compliance Management (Anforderungsmanagement)

Konzeption und Vorgehensweise
CON.1 Kryptokonzept
CON.2 Datenschutz
CON.3 Datensicherungskonzept
CON.6 Löschen und Vernichten
CON.7 Informationssicherheit auf Auslandsreisen
CON.8 Software-Entwicklung
CON.9 Informationsaustausch
CON.10 Entwicklung von Webanwendungen

Betrieb
OPS.1.1.2 Ordnungsgemäße IT-Administration
OPS.1.1.3 Patch- und Änderungsmanagement
OPS.1.1.4 Schutz vor Schadprogrammen
OPS.1.1.5 Protokollierung
OPS.1.1.6 Software-Tests und -Freigaben
OPS.1.2.2 Archivierung
OPS.1.2.4 Telearbeit
OPS.1.2.5 Fernwartung
OPS.2.1 Outsourcing für Kunden
OPS.2.2 Cloud-Nutzung
OPS.3.1 Outsourcing für Dienstleister

Detektion und Reaktion
DER.1 Detektion von sicherheitsrelevanten Ereignissen
DER.2.1 Behandlung von Sicherheitsvorfällen
DER.2.2 Vorsorge für die IT-Forensik
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
DER.3.1 Audits und Revisionen
DER.3.2 Revision auf Basis des Leitfadens IS-Revision
DER.4 Notfallmanagement

Anwendungen
APP.1.1 Office-Produkte
APP.1.2 Web-Browser
APP.2.1 Allgemeiner Verzeichnisdienst
APP.2.2 Active Directory
APP.2.3 OpenLDAP
APP.3.3 Fileserver
APP.3.4 Samba
APP.3.6 DNS-Server

APP.4.2 SAP-ERP-System
APP.4.6 SAP ABAP-Programmierung

IT-Systeme
SYS.1.7 IBM Z-System
SYS.1.8 Speicherlösungen
SYS.2.1 Allgemeiner Client
SYS.2.2.2 Clients unter Windows 8.1
SYS.2.2.3 Clients unter Windows 10
SYS.2.3 Clients unter Linux und Unix
SYS.2.4 Clients unter macOS
SYS.3.1 Laptops
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
SYS.4.3 Eingebettete Systeme
SYS.4.4 Allgemeines IoT-Gerät
SYS.4.5 Wechseldatenträger

Industrielle IT
IND.1 Prozessleit- und Automatisierungstechnik
IND.2.1 Allgemeine ICS-Komponente
IND.2.2 Speicherprogrammierbare Steuerung (SPS)
IND.2.3 Sensoren und Aktoren
IND.2.4 Maschine
IND.2.7 Safety Instrumented Systems

Netze und Kommunikation
NET.1.1 Netzarchitektur und -design
NET.1.2 Netzmanagement
NET.2.1 WLAN-Betrieb
NET.2.2 WLAN-Nutzung
NET.4.1 TK-Anlagen
NET.4.2 VoIP
NET.4.3 Faxgeräte und Faxserver

Infrastruktur
INF.1 Allgemeines Gebäude
INF.2 Rechenzentrum sowie Serverraum
INF.5 Raum sowie Schrank für technische Infrastruktur
INF.6 Datenträgerarchiv
INF.7 Büroarbeitsplatz
INF.8 Häuslicher Arbeitsplatz
INF.9 Mobiler Arbeitsplatz
INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum
INF.11 Allgemeines Fahrzeug
INF.12 Verkabelung

6 ANFORDERUNGEN - EMPFEHLUNGEN

Die folgenden Anforderungen sollten von allen beteiligten Unternehmen besonders und gesondert nochmals auf ihren Erfüllungsgrad überprüft werden.

6.1 Sicherheitsmanagement

ISMS.1 Sicherheitsmanagement

ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen (B)

Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert werden. Die Sicherheitsmaßnahmen SOLLTEN regelmäßig aktualisiert werden.

(alle SSI Komponenten)

ISMS.1.A10 Erstellung eines Sicherheitskonzepts (S)

Für den festgelegten Geltungsbereich (Informationsverbund) SOLLTE ein angemessenes Sicherheitskonzept als das zentrale Dokument im Sicherheitsprozess erstellt werden. Es SOLLTE entschieden werden, ob das Sicherheitskonzept aus einem oder aus mehreren Teilkonzepten bestehen soll, die sukzessive erstellt werden, um zunächst in ausgewählten Bereichen das erforderliche Sicherheitsniveau herzustellen.

Im Sicherheitskonzept MÜSSEN aus den Sicherheitszielen der Institution, dem identifizierten Schutzbedarf und der Risikobewertung konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet werden. Sicherheitsprozess und Sicherheitskonzept MÜSSEN die individuell geltenden Vorschriften und Regelungen berücksichtigen.

Die im Sicherheitskonzept vorgesehenen Maßnahmen MÜSSEN zeitnah in die Praxis umgesetzt werden. Dies MUSS geplant und die Umsetzung MUSS kontrolliert werden.

(alle SSI Komponenten)

ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien (H)

Neben den allgemeinen SOLLTE es auch zielgruppenorientierte Sicherheitsrichtlinien geben, die jeweils bedarfsgerecht die relevanten Sicherheitsthemen abbilden.

(alle SSI Komponenten)

6.2 Betrieb

OPS.2.1 Outsourcing für Kunden

OPS.2.1.A2 Rechtzeitige Beteiligung der Personalvertretung [Zentrale Verwaltung](S)

Die Personalvertretung SOLLTE rechtzeitig über ein Outsourcing-Vorhaben informiert werden. Die Personalvertretung SOLLTE schon in der Angebotsphase beteiligt werden. Je nach Outsourcing- Vorhaben SOLLTEN die gesetzlichen Mitwirkungsrechte beachtet werden.

(Relevanz: MongoDB – Arbeitgeber)

OPS.2.1.A3 Auswahl eines geeigneten Outsourcing-Dienstleisters (S)

Für die Auswahl des Outsourcing-Dienstleisters SOLLTE ein Anforderungsprofil mit den Sicherheitsanforderungen an das Outsourcing-Vorhaben erstellt werden. Außerdem SOLLTEN Bewertungskriterien für den Outsourcing-Dienstleister und dessen Personal vorliegen. Diese SOLLTEN auf dem Anforderungsprofil basieren.

(Relevanz: jegliche Komponente, jedoch im Besonderen bei Komponenten, die Personendaten verarbeiten, im Hinblick auf Datenschutz und den Ort der Speicherung, MongoDB, Controller, Aries Agent)

OPS.2.1.A6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben[Fachverantwortliche] (S)

Der Outsourcing-Kunde SOLLTE für jedes Outsourcing-Vorhaben ein Sicherheitskonzept basierend aufden zugehörigen Sicherheitsanforderungen erstellen. Ebenso SOLLTE jeder Outsourcing-Dienstleister ein individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben vorlegen. Beide Sicherheitskonzepte SOLLTEN miteinander abgestimmt werden. Das Sicherheitskonzept des Outsourcing-Dienstleisters und dessen Umsetzung SOLLTEN zu einem gesamten Sicherheitskonzept zusammengeführt werden. Der Outsourcing-Kunde oder unabhängige Dritte SOLLTEN regelmäßig überprüfen, ob das Sicherheitskonzept wirkt.

(Relevanz: betrifft jegliche Komponente, die abgegeben werden soll)

OPS.2.1.A11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (S)

Es SOLLTE ein Betriebskonzept für das Outsourcing-Vorhaben erstellt werden, das auch die Sicherheitsaspekte berücksichtigt. Die Sicherheitskonzepte der Outsourcing-Partner SOLLTEN regelmäßig daraufhin überprüft werden, ob sie aktuell und zueinander konsistent sind. Der Status der vereinbarten

Sicherheitsmaßnahmen SOLLTE regelmäßig kontrolliert werden. Zwischen den Outsourcing-Partnern SOLLTE regelmäßig kommuniziert werden. Vorschläge zu Änderungen und Verbesserungen SOLLTEN regelmäßig besprochen und abgestimmt werden.

Die Outsourcing-Partner SOLLTEN regelmäßig gemeinsame Übungen und Tests durchführen, um das Sicherheitsniveau aufrechtzuerhalten. Informationen über Sicherheitsrisiken und wie damit umgegangen wird, SOLLTEN regelmäßig zwischen den Outsourcing-Partnern ausgetauscht werden. Es SOLLTE ein Prozess festgelegt werden, der den Informationsfluss bei Sicherheitsvorfällen sicherstellt, welche die jeweiligen Vertragspartner betreffen.

(Relevanz: betrifft den Betrieb jeder abgegebenen Komponente)

OPS.2.1.A16 Sicherheitsüberprüfung von Mitarbeitern (H)

Mit externen Outsourcing-Dienstleistern SOLLTE vertraglich vereinbart werden, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird. Dazu SOLLTEN gemeinsam Kriterien festgelegt werden.

(Relevanz: bei Betrieb von Komponenten, die personenbezogene Daten verarbeiten, wie MongoDB, Controller, Aries Agent)

OPS.2.2 Cloud-Nutzung

OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung [Fachverantwortliche, Institutionsleitung, Datenschutzbeauftragter] (B)

Eine Strategie für die Cloud-Nutzung MUSS erstellt werden. Darin MÜSSEN Ziele, Chancen und Risiken definiert werden, die die Institution mit der Cloud-Nutzung verbindet. Zudem MÜSSEN die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen untersucht werden, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung MÜSSEN in einer Machbarkeitsstudie dokumentiert werden.

Es MUSS festgelegt werden, welche Dienste in welchem Bereitstellungsmodell zukünftig von einem Cloud-Diensteanbieter bezogen werden sollen. Zudem MUSS sichergestellt werden, dass bereits in der Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden.

Für den geplanten Cloud-Dienst SOLLTE eine grobe individuelle Sicherheitsanalyse durchgeführt werden. Diese SOLLTE wiederholt werden, wenn sich technische und organisatorische Rahmenbedingungen

wesentlich verändern. Für größere Cloud-Projekte SOLLTE zudem eine Roadmap erarbeitet werden, die festlegt, wann und wie ein Cloud-Dienst eingeführt wird.

(Relevanz: alle SSI Komponenten)

OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung[Fachverantwortliche] (B)

Auf Basis der Strategie für die Cloud-Nutzung MUSS eine Sicherheitsrichtlinie für die Cloud-Nutzung erstellt werden. Sie MUSS konkrete Sicherheitsvorgaben beinhalten, mit denen sich Cloud-Dienste innerhalb der Institution umsetzen lassen. Außerdem MÜSSEN darin spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter sowie das festgelegte Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert werden. Wenn Cloud-Dienste internationaler Anbieter genutzt werden, MÜSSEN die speziellen länderspezifischen Anforderungen und gesetzlichen Bestimmungen berücksichtigt werden.

(Relevanz: alle SSI Komponenten)

OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung (S)

Auf Grundlage der identifizierten Sicherheitsanforderungen (siehe OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) SOLLTE durch den Cloud-Kunden ein Sicherheitskonzept für die Nutzung von Cloud-Diensten erstellt werden.

(Relevanz: alle SSI Komponenten, Erweiterung bestehender Sicherheitskonzepte)

OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters [Institutionsleitung](S)

Basierend auf der Service-Definition für den Cloud-Dienst SOLLTE durch den Cloud-Kunden ein detailliertes Anforderungsprofil für einen Cloud-Diensteanbieter erstellt werden. Eine Leistungsbeschreibung und ein Lastenheft SOLLTEN erstellt werden. Für die Bewertung eines Cloud-Diensteanbieters SOLLTEN auch ergänzende Informationsquellen herangezogen werden. Ebenso SOLLTEN verfügbare Service-Beschreibungen des Cloud-Diensteanbieters sorgfältig geprüft und hinterfragt werden.

(Relevanz: bei Betrieb von Komponenten, die personenbezogene Daten verarbeiten, wie MongoDB, Controller, Aries Agent)

OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb (S)

Alle für die eingesetzten Cloud-Dienste erstellten Dokumentationen und Richtlinien SOLLTEN durch den Cloud-Kunden regelmäßig aktualisiert werden. Der Cloud-Kunde SOLLTE außerdem periodisch kontrollieren, ob der Cloud-Diensteanbieter die vertraglich zugesicherten Leistungen erbringt. Auch

SOLLTEN sich der Cloud-Diensteanbieter und der Cloud-Kunde nach Möglichkeit regelmäßig abstimmen. Ebenso SOLLTE geplant und geübt werden, wie auf Systemausfälle zu reagieren ist.

(Relevanz: alle SSI Komponenten)

OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung (S)

Der Cloud-Kunde SOLLTE sich vom Cloud-Diensteanbieter regelmäßig nachweisen lassen, dass die vereinbarten Sicherheitsanforderungen erfüllt sind. Der Nachweis SOLLTE auf einem international anerkannten Regelwerk basieren (z. B. IT-Grundschutz, ISO/IEC 27001, Anforderungskatalog Cloud Computing (C5), Cloud Controls Matrix der Cloud Security Alliance). Der Cloud-Kunde SOLLTE prüfen, ob der Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst.

Nutzt ein Cloud-Diensteanbieter Subunternehmer, um die Cloud-Dienste zu erbringen, SOLLTE er dem Cloud-Kunden regelmäßig nachweisen, dass diese die notwendigen Audits durchführen.

(Relevanz: alles SSI Komponenten)

OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung (H)

Wenn Daten durch einen Cloud-Diensteanbieter verschlüsselt werden, SOLLTE vertraglich geregelt werden, welche Verschlüsselungsmechanismen und welche Schlüssellängen eingesetzt werden dürfen. Wenn eigene Verschlüsselungsmechanismen genutzt werden, SOLLTE ein geeignetes Schlüsselmanagement sichergestellt sein. Bei der Verschlüsselung SOLLTEN die eventuellen Besonderheiten des gewählten Cloud-Service-Modells berücksichtigt werden.

(Relevanz: alle SSI Komponenten, auch eine Prüfung hinsichtlich einer Störung der Komponenten)

OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern [Personalabteilung] (H)

Mit externen Cloud-Diensteanbietern SOLLTE vertraglich vereinbart werden, dass in geeigneter Weise überprüft wird, ob das eingesetzte Personal qualifiziert und vertrauenswürdig ist. Dazu SOLLTEN gemeinsam Kriterien festgelegt werden.

(Relevanz: Aries Agent, Controller, MongoDB)

OPS.3.1 Outsourcing für Dienstleister

OPS.3.1.A3 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben (S)

Der Outsourcing-Dienstleister SOLLTE für seine Dienstleistungen ein Sicherheitskonzept besitzen. Für individuelle Outsourcing-Vorhaben SOLLTE er außerdem spezifische Sicherheitskonzepte erstellen, dieauf den

Sicherheitsanforderungen des Outsourcing-Kunden basieren. Zwischen Outsourcing-Dienstleister und Outsourcing-Kunden SOLLTEN gemeinsame Sicherheitsziele erarbeitet werden. Es SOLLTE außerdem eine gemeinsame Klassifikation für alle schutzbedürftigen Informationen erstellt werden. Es SOLLTE regelmäßig überprüft werden, ob das Sicherheitskonzept auch umgesetzt wird.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A7 Erstellung eines Mandantentrennungskonzeptes durch denOutsourcing-Dienstleister (S)

Durch ein geeignetes Mandantentrennungskonzept SOLLTE sichergestellt werden, dass Anwendungs-und Datenkontexte verschiedener Outsourcing-Kunden sauber getrennt sind. Das Mandantentrennungskonzept SOLLTE durch den Outsourcing-Dienstleister erstellt und dem Outsourcing-Kunden zur Verfügung gestellt werden. Das Mandantentrennungskonzept SOLLTE für den Schutzbedarf des Outsourcing-Kunden angemessene Sicherheit bieten. Die benötigten Mechanismen zur Mandantentrennung beim Outsourcing-Dienstleister SOLLTEN ausreichend umgesetzt sein.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A10 Planung und Aufrechterhaltung der Informationssicherheit imlaufenden Outsourcing-Betrieb (S)

Die Sicherheitskonzepte der Outsourcing-Partner SOLLTEN regelmäßig daraufhin überprüft werden,ob sie noch aktuell und zueinander konsistent sind. Der Status der vereinbarten Sicherheitsmaßnahmen SOLLTE regelmäßig kontrolliert werden. Die Outsourcing-Partner SOLLTEN angemessen kooperieren. Hierüber hinaus SOLLTEN sie sich regelmäßig zu Änderungen und Verbesserungen abstimmen.

Die Outsourcing-Partner SOLLTEN regelmäßig gemeinsame Übungen und Tests durchführen. Informationen über Sicherheitsrisiken und wie damit umgegangen wird SOLLTEN regelmäßig zwischen den Outsourcing-Partnern ausgetauscht werden. Es SOLLTE ein Prozess festgelegt werden, der den Informationsfluss bei Sicherheitsvorfällen sicherstellt, welche die jeweiligen Vertragspartner betreffen.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A11 Zutritts-, Zugangs- und Zugriffskontrolle [Zentrale Verwaltung] (S)

Zutritts-, Zugangs- und Zugriffsberechtigungen SOLLTEN geregelt sein, sowohl für das Personal des Outsourcing-Dienstleisters als auch für die Mitarbeiter der Outsourcing-Kunden. Es SOLLTE ebenfalls geregelt sein, welche Berechtigungen Auditoren und andere Prüfer erhalten. Es SOLLTEN immer nur so iele Rechte vergeben werden, wie für die Wahrnehmung einer Aufgabe nötig ist. Es SOLLTE ein geregeltes Verfahren für die Vergabe, die Verwaltung und den Entzug von Berechtigungen geben.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A16 Sicherheitsüberprüfung von Mitarbeitern [Personalabteilung] (H)

Die Vertrauenswürdigkeit von neuen Mitarbeitern und externem Personal beim Outsourcing-Dienstleister SOLLTE durch geeignete Nachweise überprüft werden. Hierzu SOLLTEN gemeinsam mitdem Outsourcing-Kunden vertraglich Kriterien vereinbart werden.

(Relevanz: alle SSI Komponenten)

6.3 Konzeption und Vorgehensweise

CON.2 Datenschutz

CON.2.A1 Umsetzung Standard-Datenschutzmodell (B)

Die gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG und LDSG) MÜSSEN eingehalten werden. Wird die SDM-Methodik nicht berücksichtigt, die Maßnahmen also nicht auf der Basis der Gewährleistungsziele systematisiert und mit dem Referenzmaßnahmen-Katalog des SDM abgeglichen, SOLLTE dies begründet und dokumentiert werden.

(Relevanz: Aries Agent, Controller, MongoDB)

CON.3 Datensicherungskonzept

CON.3.A1 Erhebung der Einflussfaktoren für Datensicherungen[Fachverantwortliche, IT-Betrieb] (B)

Der IT-Betrieb MUSS für jedes IT-System und darauf ausgeführten Anwendungen die Rahmenbedingungen für die Datensicherung erheben. Dazu MUSS der IT-Betrieb die Fachverantwortlichen für die Anwendungen und die Zuständigen für die jeweiligen IT-Systeme befragen. Der IT-Betrieb MUSS mindestens die nachfolgenden Rahmenbedingungen berücksichtigen:

- Speichervolumen,
- Änderungsvolumen,
- Änderungszeitpunkte,
- Verfügbarkeitsanforderungen,
- Integritätsbedarf sowie
- rechtliche Anforderungen.

Die Ergebnisse MÜSSEN nachvollziehbar und auf geeignete Weise festgehalten werden. NeueAnforderungen MÜSSEN zeitnah berücksichtigt werden.

(Relevanz: alle SSI Komponenten)

CON.3.A6 Entwicklung eines Datensicherungskonzepts [Fachverantwortliche, IT-Betrieb] (S)

Der IT-Betrieb SOLLTE ein Datensicherungskonzept auf Basis des Minimaldatensicherungskonzepts erstellen. Dieses SOLLTE mindestens die nachfolgenden Punkte umfassen:

- Definitionen zu wesentlichen Aspekten der Datensicherung (z. B. zu differenzierende Datenarten),
- Gefährdungslage,
- Einflussfaktoren je IT-Systeme,
- Datensicherungsplan je IT-Systeme sowie
- relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point Objective (RPO) je IT-System.

Der IT-Betrieb SOLLTE das Datensicherungskonzept mit den jeweiligen Fachverantwortlichen derbetreffenden Anwendungen abstimmen.

Die Mitarbeiter SOLLTEN über den Teil des Datensicherungskonzepts unterrichtet werden, der sie betrifft. Regelmäßig SOLLTE kontrolliert werden, ob das Datensicherungskonzept korrekt umgesetztwird.

CON.3.A13 Einsatz kryptografischer Verfahren bei der Datensicherung [IT-Betrieb](H)

Um die Vertraulichkeit und Integrität der gesicherten Daten zu gewährleisten, SOLLTE der IT-Betrieb alle Datensicherungen verschlüsseln. Es SOLLTE sichergestellt werden, dass sich die verschlüsselten Daten auch nach längerer Zeit wieder einspielen lassen. Verwendete kryptografische Schlüssel SOLLTEN mit einer getrennten Datensicherung geschützt werden.

(Relevanz: alle SSI Komponenten)

6.4 Anwendungen

APP.1.4 Mobile Anwendung (Apps)

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

APP.3.1 Webanwendungen

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

APP.3.2 Webserver

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

APP.4.3 Relationale Datenbanksysteme

Der gesamte Baustein sollte seitens der Projektentwickler analog betrachtet werden.

APP.5.2 Microsoft Exchange und Outlook

Dieser Baustein ist nur zu betrachten bei Einsatz der betreffenden Software.

(Relevanz: Versand der QR Codes, Möglichkeit der Löschung, Fälschung, etc.)

APP.5.2.A3 Berechtigungsmanagement und Zugriffsrechte (B)

Zusätzlich zum allgemeinen Berechtigungskonzept MUSS die Institution ein Berichtigungskonzept fürdie Systeme der Exchange-Infrastruktur erstellen, geeignet dokumentieren und anwenden.

Der IT-Betrieb MUSS serverseitige Benutzerprofile für einen rechnerunabhängigen Zugriff der Benutzer*Innen auf Exchange-Daten verwenden. Er MUSS die Standard-NTFS-Berechtigungen für das Exchange-Verzeichnis so anpassen, dass nur autorisierte Administratoren und Systemkonten auf die Daten in diesem Verzeichnis zugreifen können.

(Relevanz: siehe oben)

APP.5.2.A9 Sichere Konfiguration von Exchange-Servern (S)

Der IT-Betrieb SOLLTE Exchange-Server entsprechend der Vorgaben aus der Sicherheitsrichtlinie installieren und konfigurieren. Konnektoren SOLLTEN sicher konfiguriert werden. Der IT-Betrieb SOLLTE die Protokollierung des Exchange-Systems aktivieren. Für vorhandene benutzerspezifischeAnpassungen SOLLTE ein entsprechendes Konzept erstellt werden.

Bei der Verwendung von funktionalen Erweiterungen SOLLTE sichergestellt sein, dass die definierten Anforderungen an die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit weiterhin erfüllt sind.

(Relevanz: siehe oben)

APP.5.2.A11 Absicherung der Kommunikation zwischen Exchange-Systemen (S)

Der IT-Betrieb SOLLTE nachvollziehbar entscheiden, mit welchen Schutzmechanismen die Kommunikation zwischen Exchange-Systemen abgesichert wird. Insbesondere SOLLTE der IT-Betrieb festlegen, wie die Kommunikation zu folgenden Schnittstellen abgesichert wird:

- Administrationsschnittstellen,
- Client-Server-Kommunikation,
- vorhandene Web-based-Distributed-Authoring-and-Versioning-(WebDAV)-Schnittstellen,
- Server-Server-Kommunikation und
- Public-Key-Infrastruktur, auf der die E-Mail-Verschlüsselung von Outlook basiert.

(Relevanz: siehe oben)

APP.5.3 Allgemeiner E-Mail-Client und -Server

APP.5.3.A2 Sicherer Betrieb von E-Mail-Servern (B)

Der IT-Betrieb MUSS Schutzmechanismen gegen Denial-of-Service (DoS)-Attacken ergreifen. Für den E-Mail-Empfang sowie den Zugriff von E-Mail-Clients über öffentliche Datennetze MÜSSEN E-Mail-Server eine sichere Transportverschlüsselung anbieten. Versenden E-Mails-Server von sich aus E-Mails, SOLLTEN sie dafür ebenfalls eine sichere Transportverschlüsselung nutzen.

Die Institution MUSS alle erlaubten E-Mail-Protokolle und Dienste festlegen. Außerdem MUSS der IT-Betrieb den E-Mail-Server so einstellen, dass er nicht als Spam-Relay missbraucht werden kann.

Werden Nachrichten auf einem E-Mail-Server gespeichert, MUSS der IT-Betrieb eine geeignete Größenbeschränkung für das serverseitige Postfach einrichten und dokumentieren.

APP.5.3.A6 Festlegung einer Sicherheitsrichtlinie für E-Mail (S)

Die Institution SOLLTE eine Sicherheitsrichtlinie für die Nutzung von E-Mails erstellen und regelmäßig aktualisieren. Die Institution SOLLTE alle Benutzer*Innen und Administrator*Innen über neue oder veränderte Sicherheitsvorgaben für E-Mail-Anwendungen informieren. Die E-Mail-Sicherheitsrichtlinie SOLLTE konform zu den geltenden übergeordneten Sicherheitsrichtlinien der Institution sein. Die Institution SOLLTE prüfen, ob die Sicherheitsrichtlinie korrekt angewendet wird.

Die E-Mail-Sicherheitsrichtlinie für Benutzer*Innen SOLLTE vorgeben,

- wie sich die Kommunikation absichern lässt,

- welche Benutzerzugriffsrechte es gibt,
- wie E-Mails auf gefälschte Absender überprüft werden,
- wie sich übermittelte Informationen absichern lassen,
- wie die Integrität von E-Mails überprüft werden soll,
- welche offenen E-Mail-Verteiler verwendet werden dürfen,
- ob E-Mails privat genutzt werden dürfen,
- wie mit E-Mails und Postfächern ausscheidender Mitarbeiter umgegangen werden soll,
- ob und wie Webmail-Dienste genutzt werden dürfen,
- wer für Gruppenpostfächer zuständig ist,
- wie mit Datei-Anhängen umgegangen werden soll und
- wie E-Mails im HTML-Format vom Benutzer*Innen behandelt werden sollen.

Die E-Mail-Sicherheitsrichtlinie SOLLTE ergänzend für Administratoren die Einstellungsoptionen der E-Mail-Anwendungen beinhalten, außerdem die Vorgaben für mögliche Zugriffe von anderen Servern auf einen E-Mail-Server. Auch Angaben zu berechtigten Zugriffspunkten, von denen aus auf einen E- Mail-Server zugegriffen werden darf, SOLLTEN in der Richtlinie enthalten sein.

Die E-Mail-Sicherheitsrichtlinie SOLLTE den Umgang mit Newsgroups und Mailinglisten regeln.

(Relevanz: Versand der QR Codes, Möglichkeit der Löschung, Fälschung, etc.)

APP.5.3.A9 Erweiterte Sicherheitsmaßnahmen auf dem E-Mail-Server (S)

Die E-Mail-Server einer Institution SOLLTEN eingehende E-Mails mittels des Sender Policy Frameworks (SPF) und mit Hilfe von Domain Keys überprüfen. Die Institution SOLLTE selbst Domain Keys und SPF einsetzen, um von ihr versendete E-Mails zu authentisieren.

Wird SPF verwendet, SOLLTE eindeutig vorgegeben werden, wie mit E-Mails verfahren werden soll. Der Softfail-Parameter („~“) SOLLTE nur zu Testzwecken verwendet werden.

Die Institution SOLLTE Domain-based Message Authentication, Reporting and Conformance (DMARC) nutzen, um festzulegen, wie von ihr versendete E-Mails durch den empfangenden E-Mail-Server überprüft

werden sollen. DMARC-Reporte SOLLTEN regelmäßig ausgewertet werden. Die Institution SOLLTE festlegen, ob DMARC-Reporte über empfangene E-Mails an andere Institutionen versendet werden.

Die Institution SOLLTE die E-Mail-Kommunikation über DANE und MTA-STS absichern.

(Relevanz: Versand der QR Codes, Möglichkeit der Löschung, Fälschung, etc.)

APP.6 Allgemeine Software

Der gesamte Baustein sollte seitens jedes Projektteilnehmers betrachtet werden.

APP.7 Entwicklung von Individualsoftware

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

6.5 IT-Systeme

SYS.1.1 Allgemeiner Server

SYS.1.1.A2 Benutzerauthentifizierung an Servern (B)

Für die Anmeldung von Benutzern und Diensten am Server MÜSSEN Authentisierungsverfahren eingesetzt werden, die dem Schutzbedarf der Server angemessen sind. Dies SOLLTE in besonderem Maße für administrative Zugänge berücksichtigt werden. Soweit möglich, SOLLTE dabei auf zentrale, netzbasierte Authentisierungsdienste zurückgegriffen werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A10 Protokollierung (B)

Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden, dazu gehören mindestens:

- Systemstarts und Reboots,
- erfolgreiche und erfolglose Anmeldungen am System (Betriebssystem und Anwendungssoftware),
- fehlgeschlagene Berechtigungsprüfungen,
- blockierte Datenströme (Verstöße gegen ACLs oder Firewallregeln),
- Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen,
- sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von

Kapazitätsgrenzen) sowie

- Warnmeldungen von Sicherheitssystemen (z. B. Virenschutz).

(Relevanz: alle SSI Komponenten)

SYS.1.1.A11 Festlegung einer Sicherheitsrichtlinie für Server (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an Server in einer separaten Sicherheitsrichtlinie konkretisiert werden. Diese Richtlinie SOLLTE allen Administratoren und anderen Personen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A12 Planung des Server-Einsatzes (S)

Jedes Server-System SOLLTE geeignet geplant werden. Dabei SOLLTEN mindestens folgende Punkte berücksichtigt werden:

- Auswahl der Hardwareplattform, des Betriebssystems und der Anwendungssoftware,
- Dimensionierung der Hardware (Leistung, Speicher, Bandbreite etc.),
- Art und Anzahl der Kommunikationsschnittstellen,
- Leistungsaufnahme, Wärmelast, Platzbedarf und Bauform,
- Realisierung administrativer Zugänge (siehe SYS.1.1.A5 *Schutz der Administrationsschnittstellen*),
- Zugriffe von Benutzern,
- Realisierung der Protokollierung (siehe SYS.1.1.A10 *Protokollierung*),
- Realisierung der Systemaktualisierung (siehe SYS.1.1.A7 *Updates und Patches für Betriebssystem und Anwendungen*) sowie
- Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS etc.).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A16 Sichere Grundkonfiguration von Servern (S)

Die Grundeinstellungen von Servern SOLLTEN überprüft und falls erforderlich entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Erst nachdem die Installation und die Konfiguration abgeschlossen sind, SOLLTE der Server mit dem Internet verbunden werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A19 Einrichtung lokaler Paketfilter (S)

Vorhandene lokale Paketfilter SOLLTEN über ein Regelwerk so ausgestaltet werden, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle bzw. Ports und Schnittstellen beschränkt wird. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen SOLLTE kryptografisch abgesichert sein.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A24 Sicherheitsprüfungen für Server (S)

Server SOLLTEN regelmäßigen Sicherheitstests unterzogen werden, die überprüfen, ob alle Sicherheitsvorgaben eingehalten werden und ggf. vorhandene Schwachstellen identifizieren. Diese Sicherheitsprüfungen SOLLTEN insbesondere auf Servern mit externen Schnittstellen durchgeführt werden. Um mittelbare Angriffe über infizierte Systeme im eigenen Netz zu vermeiden, SOLLTEN jedoch auch interne Server in festgelegten Zyklen entsprechend überprüft werden. Es SOLLTE geprüft werden, ob die Sicherheitsprüfungen automatisiert, z. B. mittels geeigneter Skripte, realisiert werden können.

Je nach installierter Komponente sollten auch die Anforderungen bei erhöhtem Schutzbedarf betrachtet werden.

(Relevanz: alle SSI Komponenten)

SYS.1.2.2 Windows Server 2016 (CD)

Dieser Baustein ist nur zu betrachten bei Einsatz von Hyper-V für den Betrieb von Docker Images, dann jedoch vollständig.

(Relevanz: alle SSI Komponenten)

SYS.1.3 Server unter Linux und Unix

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

(Relevanz: alle SSI Komponenten)

SYS.1.5 Virtualisierung

Der gesamte Baustein sollte seitens der Projektentwickler und Testteilnehmer betrachtet werden.

(Relevanz: alle SSI Komponenten)

SYS.1.6 Kubernetes (CD)

Der gesamte Baustein sollte seitens der Projektentwickler, aber auch der Testteilnehmer bei Nutzung von Kubernetes betrachtet werden.

(Relevanz: alle SSI Komponenten)

SYS.3.2.1 Allgemeine Smartphones und Tablets

Der gesamte Baustein sollte (nochmals) betrachtet werden bei Einsatz von betrieblichen Smartphones oder Tablets für den Testbetrieb.

(Relevanz: ID-Wallet)

SYS.3.2.2 Mobile Device Management (MDM)

Bei Einsatz dienstlicher Geräte in Verbindung mit MDM sollten die Anforderungen bei erhöhtem Schutzbedarf geprüft werden.

(Relevanz: ID-Wallet)

SYS.3.2.3 iOS (for Enterprise)

Bei Einsatz dienstlicher Geräte mit iOS sollten insbesondere die Anforderungen bei erhöhtem Schutzbedarf geprüft werden.

(Relevanz: ID-Wallet)

SYS.3.2.4 Android

Bei Einsatz dienstlicher Geräte mit Android sollten insbesondere die Anforderungen bei erhöhtem Schutzbedarf geprüft werden.

(Relevanz: ID-Wallet)

SYS.3.3 Mobiltelefon

Auch hier sollten bei Einsatz von dienstlichen Geräten insbesondere die Anforderungen bei erhöhtem Schutzbedarf geprüft werden.

(Relevanz: ID-Wallet)

6.6 Netze und Kommunikation

NET.3.1 Router und Switches

NET.3.1.A9 Betriebsdokumentationen (B)

Die wichtigsten betrieblichen Aufgaben eines Routers oder Switches MÜSSEN geeignet dokumentiert werden. Es SOLLTEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden. Die Dokumentation SOLLTE vor unbefugten Zugriffen geschützt werden.

(Relevanz: alle SSI Komponenten)

NET.3.1.A10 Erstellung einer Sicherheitsrichtlinie (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Sicherheitsrichtlinie erstellt werden. In der Sicherheitsrichtlinie SOLLTEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Router und Switches sicher betrieben werden können. Die Richtlinie SOLLTE allen Administratoren bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den festgelegten Anforderungen abgewichen, SOLLTE dasmit dem ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse SOLLTEN geeignet dokumentiert werden.

(Relevanz: alle SSI Komponenten, bestehende Sicherheitskonzepte)

NET.3.1.A12 Erstellung einer Konfigurations-Checkliste für Router und Switches (S)

Es SOLLTE eine Konfigurations-Checkliste erstellt werden, anhand derer die wichtigsten sicherheitsrelevanten Einstellungen auf Routern und Switches geprüft werden können. Da die sichere Konfiguration stark vom Einsatzzweck abhängt, SOLLTEN die unterschiedlichen Anforderungen der Geräte in der Konfigurations-Checkliste berücksichtigt werden.

(Relevanz: alle SSI Komponenten)

NET.3.1.A21 Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur (S)

Router und Switches SOLLTEN an ein zentrales Identitäts- und Berechtigungsmanagement angebunden werden (siehe ORP.4 *Identitäts- und Berechtigungsmanagement)*.

(Relevanz: alle SSI Komponenten)

NET.3.1.A23 Revision und Penetrationstests (S)

Router und Switches SOLLTEN regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Auch SOLLTEN regelmäßig Revisionen durchgeführt werden. Dabei SOLLTE unter anderem geprüft werden, ob der Ist-Zustand der festgelegten sicheren Grundkonfiguration entspricht. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden.

Abweichungen SOLLTE nachgegangen werden.

Sowie sämtliche Anforderungen bei Installation und Betrieb von Komponenten mit erhöhtem Schutzbedarf.

(Relevanz: alle SSI Komponenten)

NET.3.2 Firewall

NET.3.2.A1 Erstellung einer Sicherheitsrichtlinie (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie erstellt werden. In dieser MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Firewalls sicher betrieben werden können. Die Richtlinie MUSS allen im Bereich Firewalls zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

(Relevanz: alle SSI Komponenten, Erweiterung bestehender Sicherheitsrichtlinien)

NET.3.2.A2 Festlegen der Firewall-Regeln (B)

Die gesamte Kommunikation zwischen den beteiligten Netzen MUSS über die Firewall geleitet werden. Es MUSS sichergestellt sein, dass von außen keine unerlaubten Verbindungen in das geschützte Netz aufgebaut werden können. Ebenso DÜRFEN KEINE unerlaubten Verbindungen aus dem geschützten Netz heraus aufgebaut werden.

Für die Firewall MÜSSEN eindeutige Regeln definiert werden, die festlegen, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen

MÜSSEN durch die Firewall unterbunden werden (Whitelist-Ansatz). Die Kommunikationsbeziehungen mit angeschlossenen Dienst-Servern, die über die Firewall geführt werden, MÜSSEN in den Regeln berücksichtigt sein.

Es MÜSSEN Verantwortliche benannt werden, die Filterregeln entwerfen, umsetzen und testen. Zudem MUSS geklärt werden, wer Filterregeln verändern darf. Die getroffenen Entscheidungen sowie die relevanten Informationen und Entscheidungsgründe MÜSSEN dokumentiert werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A3 Einrichten geeigneter Filterregeln am Paketfilter (B)

Basierend auf den Firewall-Regeln aus NET.3.2.A2 *Festlegen der Firewall-Regeln* MÜSSEN geeignete Filterregeln für den Paketfilter definiert und eingerichtet werden.

Ein Paketfilter MUSS so eingestellt sein, dass er alle ungültigen TCP-Flag-Kombinationen verwirft. Grundsätzlich MUSS immer zustandsbehaftet gefiltert werden. Auch für die verbindungslosen Protokolle UDP und ICMP MÜSSEN zustandsbehaftete Filterregeln konfiguriert werden. Die Firewall MUSS die Protokolle ICMP und ICMPv6 restriktiv filtern.

(Relevanz: alle SSI Komponenten)

NET.3.2.A4 Sichere Konfiguration der Firewall (B)

Bevor eine Firewall eingesetzt wird, MUSS sie sicher konfiguriert werden. Alle Konfigurationsänderungen MÜSSEN nachvollziehbar dokumentiert sein. Die Integrität der Konfigurationsdateien MUSS geeignet geschützt werden. Bevor Zugangspasswörter abgespeichert werden, MÜSSEN sie mithilfe eines zeitgemäßen kryptografischen Verfahrens abgesichert werden (siehe CON.1 *Kryptokonzept*). Eine Firewall MUSS so konfiguriert sein, dass ausschließlich zwingend erforderliche Dienste verfügbar sind. Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin erfüllt sein. Auch MUSS begründet und dokumentiertwerden, warum solche Erweiterungen eingesetzt werden. Nicht benötigte (Auskunfts-)Dienste sowie nicht benötigte funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden.

Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen bestmöglich verborgen werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A14 Betriebsdokumentationen (B)

Die betrieblichen Aufgaben einer Firewall MÜSSEN nachvollziehbar dokumentiert werden. Es MÜSSEN alle Konfigurationsänderungen sowie sicherheitsrelevanten Aufgaben dokumentiert werden, insbesondere Änderungen an den Systemdiensten und dem Regelwerk der Firewall. Die Dokumentation MUSS vor unbefugten Zugriffen geschützt werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A16 Aufbau einer „P-A-P"-Struktur (S)

Eine „Paketfilter – Application-Level-Gateway – Paketfilter" (P-A-P)-Struktur SOLLTE eingesetzt werden. Sie MUSS aus mehreren Komponenten mit jeweils dafür geeigneter Hard- und Softwarebestehen. Für die wichtigsten verwendeten Protokolle SOLLTEN Sicherheitsproxies auf Anwendungsschicht vorhanden sein. Für andere Dienste SOLLTEN zumindest generische Sicherheitsproxies für TCP und UDP genutzt werden. Die Sicherheitsproxies SOLLTEN zudem innerhalb einer abgesicherten Laufzeitumgebung des Betriebssystems ablaufen.

(Relevanz: alle SSI Komponenten)

NET.3.2.A23 Systemüberwachung und -Auswertung (S)

Firewalls SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Es SOLLTE ständig überwacht werden, ob die Firewall selbst sowie die darauf betriebenen Dienste korrekt funktionieren. Bei Fehlern oder wenn Grenzwerte überschritten werden SOLLTE das Betriebspersonal alarmiert werden. Zudem SOLLTEN automatische Alarmmeldungen generiert werden, die bei festgelegten Ereignissen ausgelöst werden. Protokolldaten oder Statusmeldungen SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A24 Revision und Penetrationstests (S)

Die Firewall-Struktur SOLLTE regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Es SOLLTEN regelmäßige Penetrationstests und Revisionen durchgeführt werden.

Sowie sämtliche Anforderungen bei Installation und Betrieb von Komponenten mit erhöhtem Schutzbedarf.

(Relevanz: alle SSI Komponenten)

NET.3.3 VPN

NET.3.3.A1 Planung des VPN-Einsatzes (B)

Die Einführung eines VPN von Unternehmen MUSS sorgfältig geplant werden. Dabei MÜSSEN die Verantwortlichkeiten für den VPN-Betrieb festgelegt werden. Es MÜSSEN für das VPN zudem Benutzergruppen und deren Berechtigungen geplant werden. Ebenso MUSS definiert werden, wie erteilte, geänderte oder entzogene Zugriffsberechtigungen zu dokumentieren sind. Damit wäre eine Austellung einer CompanyID nur im virtuellen privaten Netzwerk möglich, in welchem das mobile Telefon des AN eine VPN Verbindung ins Unternehmensnetz aufbaut.

(Relevanz: alle SSI Komponenten)

NET.3.3.A4 Sichere Konfiguration eines VPN (B)

Für alle VPN-Komponenten MUSS eine sichere Konfiguration festgelegt werden. Diese SOLLTE geeignet dokumentiert werden. Auch MUSS der zuständige Administrator regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

(Relevanz: alle SSI Komponenten)

NET.3.3.A6 Durchführung einer VPN-Anforderungsanalyse (S)

Eine Anforderungsanalyse SOLLTE durchgeführt werden, um für das jeweilige VPN die Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigten Hard- und Software- Komponenten ableiten zu können. In der Anforderungsanalyse SOLLTEN folgende Punkte betrachtet werden:

- Geschäftsprozesse beziehungsweise Fachaufgaben,
- Zugriffswege,
- Identifikations- und Authentisierungsverfahren,
- Benutzer*Innen und deren Berechtigungnen
- Zuständigkeiten, sowie
- Meldewege.

NET.3.3.A12 Benutzer- und Zugriffsverwaltung bei Fernzugriff-VPNs (S)

Für Fernzugriff-VPNs SOLLTE eine zentrale und konsistente Benutzer- und Zugriffsverwaltung gewährleistet werden.

(Relevanz: alle SSI-Komponenten)

7 RISIKOANALYSE

Eine abschließende Risikoanalyse, die die Maßnahmen des Betreibers erfasst, muss nach der Umsetzung und dem Aufsetzen der Komponenten bei den Betreibern erfolgen.