

7 PHASE BETRIEBSÜBERNAHME

7.1 MIGRATION DER DATENBANK

Die Daten des kompletten beA-Systems werden in einer Oracle-Datenbankinstanz in verschiedenen Schemata verwaltet. Die beA-Komponenten nutzen dazu ein oder mehrere Schemata zur Datenablage. Da die Schema bzw. Benutzernamen nicht unbedingt festgelegt sind, werden in der folgenden Tabelle die Komponenten benannt, deren zugehörige Schemata im Rahmen der Migration berücksichtigt werden müssen. Ggf. kann es sein, dass Komponenten bzw. Subkomponenten dasselbe Schema nutzen (z. B. SAFE BRAK Autent SA und SAFE-Connector). Die voreingetragenen Benutzernamen stammen aus der ATOS-Entwicklungsumgebung und dienen lediglich der Orientierung.

Komponente	Beschreibung	Benutzer	geschätzte zu erwartende Größe in PROD
beA-Anwendung	Das Schema enthält alle Daten der beA-Anwendung, wie Postfächer, Nachrichten, Rollen, Rechte, Konfigurationsdaten, etc.	BEA	7TB
SAFE BRAK (Autent)	Das Schema enthält den Identity Store der SAFE BRAK, d.h. alle Identitäten und deren	BEASAFE	1TB

Komponente	Beschreibung	Benutzer	geschätzte zu erwartende Größe in PROD
Attribute.			
SAFE BRAK (AutentSA)		SAFE_CONNECTOR	<<1TB
beA-Safe-Connector	Logdaten zu Datenimports	SAFE_CONNECTOR	<<1TB
Intermediär BRAK	Das Schema enthält die vom Intermediär BRAK empfangenen bzw. zu versendenden Nachrichten.	OSCISERVER_INT	2TB
OCSP-CRL-Relay	Vertraute Root Zertifikate, Certificate Revocation lists	RELAY_INT	<<1TB
GovSC-Kernsystem	Allgemeiner Keystore, Definitionen von Algorithmen, Operationen und Konsumenten und Vergabe der ID zur Referenzierung	GOV2SERVER_INT	<<1TB
FAL-Suche	View auf SAFE-BRAK Schema	BEAFAL	<<1TB
HSM	Das Schema enthält die Konfigurationsdaten der HSMs, wie IP Adressen, etc.		

Die dargestellten DB-Größen stellen den Ist-Stand zum Zeitpunkt der Erstellung des Transitionskonzeptes dar. Eine Erhöhung der Zahlen ist anzunehmen. Ende Januar war SAFE ca 500 GB, OSCI ca 5,5 TB und beA ca 3 TB groß. Zuwachs pro Monat etwas unter 1 TB. Auswirkung der Löschung von "alten" Nachrichten auf dem Intermediär noch nicht berücksichtigt.

Da der Datenumfang im Produktivsystem sehr groß ist, scheidet ein Export der Schemata per DB-Dump aus. In den Umgebungen STA und SPT könnten die Daten prinzipiell per Dump exportiert und importiert werden, jedoch soll das Migrationsvorgehen an der Datenübertragung für STA und SPT evaluiert und getestet werden. Daher wird das beschriebene Vorgehen für alle Umgebungen STA, SPT und PROD Anwendung finden. Weiterhin ist für die PROD-Umgebung ein Testlauf geplant, der insbesondere zur Abschätzung der benötigten Datentransferzeiten benötigt wird.

7.1.1 VORAUSSETZUNGEN

Es gibt Voraussetzungen, die vor einem Oracle-Datenabzug gegeben sein müssen

- Ablauf von Löschjobs, um unnötigen Datentransfer zu vermeiden. Die Jobs werden bis dahin auf allen Instanzen aktiv sein bzw eingerichtet sein.
- Entfernung von ATOS-spezifischen Daten, die außerhalb des ATOS-RZ nicht sichtbar sein dürfen.

7.1.2 PRINZIPIELLES VORGEHEN ZUM DATENABZUG

Ein leerer wesroc-Server wird bei Atos mit Betriebssystem und Oracle installiert und als Standby-DB zur aktuellen DB aufgebaut. Zum Stichtag wird er dann abgebaut und ins RZ der wesroc transportiert. Bei wesroc wird die DB dann als DUPLICATE per RMAN aufgebaut.

Vorteile

- Direkter Datenaustausch zwischen zwei Oracle-Instanzen.
- Transport kann direkt nach Produktionsstop bei Atos erfolgen
- Man transportiert eine funktionsfähige DB

Nachteile

- Ein (wesroc-)Server muss in das ATOS-Netz integriert werden
- Erfordert Konfigurationsanpassung an der Atos DB (für Redo-Transport)

7.1.3 ABLAUF DER DATENÜBERNAHME AUS ORACLE

Die Datenübernahme für die unterschiedlichen Umgebungen STA, SPT und PROD erfolgt prinzipiell identisch, unterscheidet sich jedoch in kleineren Punkten. Daher werden an dieser Stelle zwei Ablaufpläne, einer für die Datenübernahme STA sowie ein Plan für die Übernahme der SPT und PROD dargestellt. Die Ablaufpläne werden hier mit relativen Zeitangaben dargestellt. Die konkreten Meilensteine finden sich im Projektplan.

7.1.3.1 ABLAUF DATENÜBERNAHME FÜR STA

Vorbereitung

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Serverlieferung	Der Datenübertragungsserver wird von Rockenstein mindestens drei Wochen vor Datenübernahme nach Fürth an das AToS-RZ geschickt.	Rockenstein	>3 Wochen vor Datenübernahme	Würzburg, Fürth	<2 Tage
RZ-Integration des Datenübertragungsserver	Der Datenübertragungsserver wird in das RZ der AToS hardware- und netzwerktechnisch integriert, so dass es mit der Oracle-DB der entsprechenden Umgebung (STA	AToS	>2 Wochen vor Datenübernahme	Fürth	1 Tag

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
	oder SPT) kommunizieren kann.				
Bereitstellung USB-Stick mit Oracle TDE-Wallet	Der aktuelle TDE-Schlüssel von STA bzw. SPT muss auf einem USB-Stick zur Verfügung stehen und am Datenübertragungsserver installiert werden.	AToS	>2 Wochen vor Datenübernahme	Fürth	< 1 Tag
Installation OS und Oracle DBMS	Auf dem Datenübertragungsserver wird OS und Oracle installiert. Die Oracle-DB nutzt dabei den TDE-Wallet auf dem USB-Stick.	AToS	>2 Wochen vor Datenübernahme	Fürth	1 Tag
Standby-Integration über Data-Guard	Auf dem Datenübertragungsserver wird eine physical Standby Datenbank erstellt und über Data-Guard mit der Datenbank von STA bzw. SPT verbunden. Die Datenreplikation (Redo Transport) kann asynchron erfolgen (Maxim Performance Mode des Data Guard), um den produktiven Betrieb nicht zu behindern. Auf den Umgebungen STA und SPT sollte wegen des jeweils geringen Datenvolumens hier	AToS	Start > 1 Woche vor Datenübernahme	Fürth	1 Tag

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
	jedoch keine Probleme auftreten.				
Bereitstellung IP-Adresse und Logindaten	AToS stellt wesroc die für die Datenübertragungsserver verwendete IP-Adresse und Logindaten bereit.	AToS	>2 Wochen vor Datenübernahme	Fürth	< 1 Tag
Bereitstellung des TDE-Schlüssels	Das Wallet mit den TDE-Schlüsseln wird der BRAK über einen sicheren Übertragungsweg vom SDM zur Verfügung gestellt. Die BRAK übergibt das Wallet dem SDM der Westernacher Solutions.	AToS, BRAK, WPS	mind. 2 Wochen vor Datenübernahme	Fürth	< 1 Tag
Installation des TDE-Schlüssels	Die Westernacher installiert das Wallet auf der vorbereiteten Oracle-Installation und hält es pro Umgebung auf USB-Stick für den späteren Datenübertragungsserver bereit.	WPS	mind. 1 Woche vor Datenübernahme	Berlin	< 1Tag

Datenübertragung

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Stoppen der Standby-DB	Der Data-Guard wird angehalten und die Standby-DB auf dem Datenübertragungsserver wird gestoppt.	AToS	Tag 1: Start der Datenübernahme	Fürth	1h

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Ausbau des Servers	Ausbau des Datenübertragungsservers im AToS-RZ zum Transport nach Würzburg	AToS	Tag 1	Fürth	1 Tag
Vernichtung des USB-Sticks mit dem TDE-Wallet	Der USB-Stick mit dem TDE-Wallet wird von Datenübertragungsserver abgezogen und vernichtet.	AToS	Tag 1	Fürth	< 1h
Transport	Der Datenübertragungsserver wird nach Würzburg transportiert.	Rockenstein	Tag 2	Fürth, Würzburg	2h
Installation USB-Stick mit TDE-Wallet	Der von wesroc vorbereitete USB-Stick mit dem TDE-Wallet wird am Datenübertragungsserver angebracht.	Rockenstein	Tag 2	Würzburg	<1h
RZ-Integration des Datenübertragungsserver	Der Datenübertragungsserver wird in das RZ der Rockenstein hardware- und netzwerktechnisch integriert, so dass es mit der Oracle-DB der entsprechenden Umgebung (STA oder SPT) kommunizieren kann.	Rockenstein	Tag 2	Würzburg	4h
Hochfahren der Oracle-DB	Die Oracle-DB auf dem Datenübertragungsserver wird testweise hochgefahren.	WPS	Tag 2	Würzburg, Berlin	< 1h
Erstellen eines Backups der DB	Die DB auf dem Datenübertragungsserver wird per RMAN	WPS	Tag 2	Berlin	< 1h

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
	gesichert, um ein späteres erneutes Einspielen des Standes der STA zu ermöglichen.				
Duplikation der DB	Der Datenübertragungsserver wird als Primär-DB rekonfiguriert (Data Guard Failover), anschließend die Data Guard Konfiguration entfernt und dann ein (rman) DUPLICATE der transportierten DB auf das Cluster bei wesroc durchgeführt.	WPS	Tag 2	Berlin	< 1h
Deaktivierung Datenübertragungsserver	Nach erfolgreicher Duplikation wird die DB des Datenübertragungsserver auf den Zustand nach Übertragung restored.	WPS	Tag 3	Berlin	2h
Einspielen spezifischer Konfigurationsdaten	Die Datenbank wird mit umgebungsspezifischen Konfigurationsdaten (z. B. eigene Zertifikate) befüllt.	WPS	Tag 3	Berlin	4h
Anbindung der Applikationsschicht	Die verschiedenen Anwendungskomponenten werden an die DB angebunden.	WPS	Tag 3	Berlin	1h
Transitionstests	Das System wird anhand der im Transitionstestplan beschriebenen Tests	WPS	Tag 4	Berlin	8h

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
--------	--------------	------	-------	-----	----------------

geprüft.

Betriebsübergang

Der Betriebsübergang der unterschiedlichen Umgebungen erfolgt nicht zwingend zum gleichen Termin. Im Gegenteil ist es eher wahrscheinlich, dass der Betriebsübergang der STA deutlich vor dem der anderen Umgebungen erfolgt. Da der Datenbestand der STA nicht zwingend aktuell sein muss, wird der Datenbestand lediglich auf den "Lieferstand" zurückgesetzt.

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Stoppen der Umgebung	Die Umgebung d. h. Zugänge, Applikationsebene und schließlich DB werden angehalten bzw. gesperrt. Die Umgebung steht anschließend für eine Nutzung nicht mehr zur Verfügung.	AToS	Tag 1: Start des Betriebsübergangs	Fürt	4h
Zurückspielen des Datenstandes	Zurückspielen des Datenstandes bei Datenübertragung mit Hilfe des Datenübertragungservers auf der entsprechenden Umgebung durch Westernacher.	WPS	Tag 1	Berlin	4h
Einspielen spezifischer Konfigurationsdateien	Die Datenbank wird mit umgebungsspezifischen Konfigurationsdaten (z. B. eigene Zertifikate) befüllt.	WPS	Tag 2	Berlin	4h
Anbindung der Applikationsschichten	Die verschiedenen Anwendungskomponenten werden an die DB angebunden.	WPS	Tag 2	Berlin	1h
Transitionstests	Das System wird anhand der im Transitionstestplan beschriebenen Tests geprüft.	WPS	Tag 3	Berlin	8h

Nachbereitung

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Abbau der Umgebung bei AToS	Die Umgebung kann bei AToS abgebaut werden.	AToS	nach Betriebsübergang	Fürth	?
Abbau des Datenübertragungservers	Abbau des Datenübertragungservers nach erfolgreicher Datenübertragung	Rockenstein	nach Betriebsübergang	Würzburg	4h

7.1.3.2 ABLAUF DATENÜBERNAHME FÜR PROD UND SPT

Vorbereitung

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Serverlieferung	Der Datenübertragungsserver wird von Rockenstein mindestens drei Wochen vor Datenübernahme nach Fürth an das AToS-RZ geschickt.	Rockenstein	>3 Wochen vor Datenübernahme	Würzburg, Fürth	<2 Tage
RZ-Integration des Datenübertragungservers	Der Datenübertragungsserver wird in das RZ der AToS hardware- und netzwerktechnisch integriert, so dass es mit der Oracle-DB der entsprechenden Umgebung (PROD) kommunizieren kann.	AToS	>2 Wochen vor Datenübernahme	Fürth	1 Tag
Bereitstellung USB-Stick mit Oracle	Der aktuelle TDE-Schlüssel von PROD muss auf	AToS	>2 Wochen vor Datenübernahme	Fürth	< 1 Tag

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
TDE-Wallet	einem USB-Stick zur Verfügung stehen und am Datenübertragungsserver installiert werden.		hme		
Installation OS und Oracle DBMS	Auf dem Datenübertragungsserver wird OS und Oracle installiert. Die Oracle-DB nutzt dabei den TDE-Wallet auf dem USB-Stick.	AToS	>2 Wochen vor Datenübernahme	Fürth	1 Tag
Standby-Integration über Data-Guard	Auf dem Datenübertragungsserver wird eine physical Standby Datenbank erstellt und über Data-Guard mit der Datenbank von PROD verbunden. Die Datenreplikation (Redo Transport) kann asynchron erfolgen (Maxim Performance Mode des Data Guard), um den produktiven Betrieb nicht zu behindern. Die Dauer der folgenden Schritte wird jeweils protokolliert, um eine möglichst genaue Zeitplanung für den späteren Produktivgang zu ermöglichen: • DUPLICATE zum Aufbau der Standby	AToS	Start > 1 Woche vor Datenübernahme	Fürth	1 Tag

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
	Dauer, bis die Standby die initialen Transport- und Apply-Lags abgebaut hat				
Replikation der Daten	Die Daten werden durch den Data-Guard in der Standby-DB synchron gehalten.	AToS	Start > 1 Woche vor Datenübernahme	Fürth	1 Woche
Bereitstellung IP-Adresse und Logindaten	AToS stellt wesroc die für die Datenübertragungsserver verwendete IP-Adresse sowie die benötigten Logindaten bereit.	AToS	>2 Wochen vor Datenübernahme	Fürth	< 1 Tag
Bereitstellung des TDE-Schlüssels	Das Wallet mit den TDE-Schlüsseln wird der BRAK über einen sicheren Übertragungsweg vom SDM zur Verfügung gestellt. Die BRAK übergibt das Wallet dem SDM der Westernacher Solutions.	AToS, BRAK, WPS	mind. 2 Wochen vor Datenübernahme	Fürth	< 1 Tag
Installation des TDE-Schlüssels	Die Westernacher installiert das Wallet auf der vorbereiteten Oracle-Installation und hält es pro Umgebung auf USB-Stick für den späteren Datenübertragungsserver bereit.	WPS	mind. 1 Woche vor Datenübernahme	Berlin	< 1 Tag

Test-Datenübertragung

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Start der Zeitmessung	Die Dauer der folgenden Schritte wird jeweils protokolliert, um eine möglichst genaue Zeitplanung für den späteren Produktivgang zu ermöglichen.	AToS, Rockenst ein, WPS			
Stoppen der Slave-DB	Der Data-Guard wird angehalten und die Slave-DB auf dem Datenübertragungs server gestoppt.	AToS	Tag 1: Start der Datenübertragung	Fürth	1h
Ausbau des Servers	Ausbau des Datenübertragungs servers im AToS-RZ zum Transport nach Würzburg	AToS	Tag 1	Fürth	1 Tag
Vernichtung des USB-Sticks mit dem TDE-Wallet	Der USB-Stick mit dem TDE-Wallet wird von Datenübertragungs server abgezogen und vernichtet.	AToS	Tag 1	Fürth	< 1h
Transport	Der Datenübertragungs server wird nach Würzburg transportiert.	Rockenst ein	Tag 2	Fürth, Würzburg	2h
Installation USB-Stick mit TDE-Wallet	Der von wesroc vorbereitete USB-Stick mit dem TDE-Wallet wird am Datenübertragungs server angebracht.	Rockenst ein	Tag 2	Würzburg	<1h
RZ-Integration des Datenübertragungs server	Der Datenübertragungs server wird in das RZ der Rockenstein hardware- und	Rockenst ein	Tag 2	Würzburg	4h

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
	netzwerktechnisch integriert, so dass es mit der Oracle-DB der entsprechenden Umgebung (PROD) kommunizieren kann.				
Hochfahren der Oracle-DB	Die Oracle-DB auf dem Datenübertragungsserver wird testweise hochgefahren.	WPS	Tag 2	Würzburg, Berlin	< 1h
Duplikation der DB	Der Datenübertragungsserver wird als Primär-DB rekonfiguriert (Data Guard Failover), anschließend die Data Guard Konfiguration entfernt und dann ein (rman) DUPLICATE der transportierten DB auf das Cluster bei wesroc durchgeführt.	WPS	Tag 2	Berlin	6h
Einspielen spezifischer Konfigurationsdaten	Die Datenbank wird mit umgebungsspezifischen Konfigurationsdaten (z. B. eigene Zertifikate) befüllt.	WPS	Tag 3	Berlin	4h
Anbindung der Applikationsschicht	Die verschiedenen Anwendungskomponenten werden an die DB angebunden.	WPS	Tag 3	Berlin	1h
Transitionstests	Das System wird anhand der im Transitionstestplan beschriebenen Tests	WPS	Tag 4	Berlin	8h

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
	geprüft.				
Bereinigen des Datenübertragungsservers	Der Datenübertragungsserver wird bereinigt (Löschen aller RAID-Konfigurationen und Überschreiben der Betriebssystem-Festplatten), ausgebaut und zum endgültigen Betriebsübergang nach Fürth gesendet.	Rockenst ein	Tag 5	Würzburg	8h
Serverlieferung	Der Datenübertragungsserver wird von Rockenstein nach Fürth an das AToS-RZ geschickt.	Rockenst ein	Tag 6	Würzburg, Fürth	<2 Tage
RZ-Integration des Datenübertragungsserver	Der Datenübertragungsserver wird in das RZ der AToS hardware- und netzwerktechnisch integriert, so dass es mit der Oracle-DB der entsprechenden Umgebung (PROD) kommunizieren kann.	AToS	Tag 8	Fürth	1 Tag
Bereitstellung USB-Stick mit Oracle TDE-Wallet	Der aktuelle TDE-Schlüssel von PROD muss auf einem USB-Stick zur Verfügung stehen und am Datenübertragungsserver installiert werden.	AToS	Tag 8	Fürth	< 1 Tag
Installation OS und	Auf dem Datenübertragungss	AToS	Tag 9	Fürth	1 Tag

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Oracle DBMS	erver wird OS und Oracle installiert. Die Oracle-DB nutzt dabei den TDE-Wallet auf dem USB-Stick.				
Standby-Integration über Data-Guard	Auf dem Datenübertragungsserver wird eine physical Standby Datenbank erstellt und über Data-Guard mit der Datenbank von PROD verbunden. Die Datenreplikation (Redo Transport) kann asynchron erfolgen (Maxim Performance Mode des Data Guard), um den produktiven Betrieb nicht zu behindern.	AToS	Tag 10	Fürth	1 Tag
Replikation der Daten	Die Daten werden durch den Data-Guard in der Standby DB synchron gehalten. Die Dauer für den Abbau von Gaps ist aus dem Testlauf nun bekannt.	AToS	Tag 10	Fürth	1 Woche
Bereitstellung IP-Adresse und Logindaten	AToS stellt wesroc die für die Datenübertragungsserver verwendete IP-Adresse sowie die benötigten Logindaten bereit.	AToS	Tag 10	Fürth	< 1 Tag

Betriebsübergang

Der Betriebsübergang der PROD- bzw. SPT-Umgebung erfolgt weitestgehend analog zum Testlauf:

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Stoppen der Umgebung	Die Umgebung d. h. Zugänge, Applikationsebene und schließlich DB werden angehalten bzw. gesperrt. Die Umgebung steht anschließend für eine Nutzung nicht mehr zur Verfügung.	AToS	Tag 1: Start des Betriebsübergangs	Fürth	4h
Ausbau des Servers	Ausbau des Datenübertragungsservers im AToS-RZ zum Transport nach Würzburg	AToS	Tag 1	Fürth	1 Tag
Vernichtung des USB-Sticks mit dem TDE-Wallet	Der USB-Stick mit dem TDE-Wallet wird von Datenübertragungsserver abgezogen und vernichtet.	AToS	Tag 1	Fürth	< 1h
Transport	Der Datenübertragungsserver wird nach Würzburg transportiert.	Rockenst ein	Tag 1	Fürth, Würzburg	2h
Installation USB-Stick mit TDE-Wallet	Der von wesroc vorbereitete USB-Stick mit dem TDE-Wallet wird am Datenübertragungsserver angebracht.	Rockenst ein	Tag 1	Würzburg	<1h
RZ-Integration des Datenübertragungsserver	Der Datenübertragungsserver wird in das RZ der Rockenstein hardware- und netzwerktechnisch integriert, so dass es mit der Oracle-DB der entsprechenden Umgebung (PROD) kommunizieren	Rockenst ein	Tag 1	Würzburg	4h

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
	kann.				
Hochfahren der Oracle-DB	Die Oracle-DB auf dem Datenübertragungsserver wird testweise hochgefahren.	WPS	Tag 1	Würzburg, Berlin	< 1h
Duplikation der DB	Der Datenübertragungsserver wird als Primär-DB rekonfiguriert (Data Guard Failover), anschließend die Data Guard Konfiguration entfernt und dann ein (rman) DUPLICATE der transportierten DB auf das Cluster bei wesroc durchgeführt.	WPS	Tag 1	Berlin	6h
Rollenwechsel	Nach erfolgreicher Replikation wird die eigentliche DB der Umgebung zum Master. Die DB des Datenübertragungsservers wird nicht zum Slave. Sie wird abgekoppelt.	WPS	Tag 2	Berlin	2h
Einspielen spezifischer Konfigurationsdaten	Die Datenbank wird mit umgebungsspezifischen Konfigurationsdaten (z. B. eigene Zertifikate) befüllt.	WPS	Tag 2	Berlin	4h
Anbindung der Applikationsschicht	Die verschiedenen Anwendungskomponenten werden an die DB angebunden.	WPS	Tag 2	Berlin	1h
Transitionstests	Das System wird	WPS	Tag 2/3	Berlin	8h

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
--------	--------------	------	-------	-----	----------------

anhand der im Transitionstestplan beschriebenen Tests geprüft.

Nachbereitung

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
--------	--------------	------	-------	-----	----------------

Abbau der Umgebung bei AToS	Die Umgebung kann bei AToS abgebaut werden.	AToS	nach Betriebsübergang	Fürth	?
-----------------------------	---	------	-----------------------	-------	---

Abbau des Datenübertragungsservers	Abbau des Datenübertragungsservers nach erfolgreicher Datenübertragung	Rockenstein	nach Betriebsübergang	Würzburg	4h
------------------------------------	--	-------------	-----------------------	----------	----

7.3 MIGRATION DER HSMS

7.3.1 PRINZIPIELLES VORGEHEN

In der aktuellen Betriebsumgebung werden fünf HSMs eingesetzt, eines für STA und SPT, vier für PROD. Zu jedem dieser HSMs werden Leihgeräte bereitgestellt, die mit den bestehenden Geräten synchronisiert werden. Zum Abgleich der HSMs mit den Leihgeräten sind folgende Schritte durchzuführen:

- Einbringen von Zertifikaten auf den Leih-HSMs
- Asymmetrisches Cloning

Zumindest für den ersten Schritt ist die Anwesenheit der Schlüsselerantwortlichen erforderlich. Dieser Schritt kann, muss aber nicht im RZ des aktuellen Betreibers stattfinden (ggf. nur für einen der vier HSM für PROD).

Zum asymmetrischen Clonen müssen die Leihgeräte im RZ des aktuellen Betreibers integriert werden, um über die HSM Maintenance integriert zu werden.

7.3.2 ABLAUF DER HSM-MIGRATION

Vorbereitung

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
ASM Lieferung 1	Lieferung von 2 ASM (1x Prod, 1x Staging) zu AtoS, Fürth	Worldline, AToS	KW10	Fürth	
Integration der Lieferung 1 ins RZ	Die ASM werden soweit in die jeweiligen Umgebungen (PROD und STA) integriert, dass die JSS Maintenance mit diesen für das spätere Cloning Verbindung aufnehmen kann.	AToS	KW10	Fürth	4h
Vorbereitung der ASMs Lieferung 1	Die KeyAdmin installieren via JSS Maintenance • auf dem Prod ASM das (Prod) CertImport-Template für das ACLCA Zertifikat (siehe Setup-Dokument Schritt	AToS	KW10/11	Fürth	1h

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
	2.2.1) auf dem Staging ASM das (Staging) CertImport-Template für das ACLCA Zertifikat Falls nicht mehr vorhanden, können beide Dateien von Worldline zur Verfügung gestellt werden.				
ASM Lieferung 2	Lieferung von 3 ASM (3x Prod) an WesRoc, Würzburg	Worldline, Rockenstein	KW10	Würzburg	
Integration Lieferung 2 ins RZ	1 ASM wird im RZ 1 installiert, 2 ASM werden im RZ 2 installiert. Die ASM werden soweit in die Prod-Umgebung integriert, dass eine JSS Maintenance mit diesen für das spätere Cloning Verbindung aufnehmen kann.	Rockenstein	KW10	Würzburg	4h
Vorbereitung der ASMs Lieferung 2	Die KeyAdmin installieren via JSS Maintenance auf allen 3 Prod ASM das (Prod) CertImport-Template für das ACLCA Zertifikat (siehe Setup-Dokument Schritt 2.2.1).	WPS	KW10/11	Würzburg/Berlin	3h

Synchronisation der Leihgeräte

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Anreise	Anreise der BRAK und der Key Custodians zum AtoS RZ Fürth	BRAK	Tag 1, bis 12 Uhr	Fürth	
Erzeugung CSRs	Zugang zum den ASM • Staging ASM: Durchführen Schritte 3-5, 8-10 gemäß Setup-Dokument • Prod ASM: Durchführen Schritte 3-5, 8-10 gemäß Setup-Dokument	BRAK, AToS, Worldline	Tag 1, 12 Uhr	Fürth	2*45 min
Signieren des Zertifikats	Staging ASM • Auslesen des CSR für das Staging System (siehe Setup-Dokument Schritt 2.2.10) • Für Staging wird die BNotK nicht benötigt, dafür wurde mit OpenSSL eine „eigene“ CA aufgesetzt. Die Schlüssel und Scripte kann ich Ihnen zukommen lassen (siehe Setup-Dokument Schritt 4.3). • Installation des Staging ASM Zertifikates und Cloning in dieses ASM Prod ASM • Auslesen des CSR und Versand an die BNotK (siehe Setup-Dokument Schritt 2.2.10) • Warten auf die Antwort der BNotK • Installation des Prod ASM Zertifikates und Cloning in dieses ASM	Worldline, AToS, BRAK	Tag 1, 13-15 Uhr	Fürth	2h
Übermittlung der Zertifikate	Übermitteln der Zertifikate von Prod und Staging ASM an WestRoc für Tag 2.	AToS, Worldline	Tag 1, 15:30 Uhr	Fürth	< 1h
Weiterreise	Weiterreise der BRAK nach Würzburg	BRAK, Wordline	Tag 1, 16 Uhr		

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Abbau ASMs	Abbau beider ASM und Vorbereitung des Transports nach Würzburg.	AToS	Tag 1, 16 Uhr	Fürth	1h

Installation der Leihgeräte

Aktion	Beschreibung	Wer?	Wann?	Wo?	Geplante Dauer
Transport	Transport beider ASM (Prod und Staging) von Fürth nach Würzburg RZ1 durch einen Sicherheitstransport	Rockenstein	Tag 2, 8-10 Uhr	Fürth	2h
Integration im RZ	Nach Erhalt der ASM werden die ASMs in den jeweiligen Umgebungen installiert. Anschließend erfolgt die Verbindungsaufnahme mit den jeweiligen JSS Maintenance Installationen.	Rockenstein, WPS	Tag 2, 10-14 Uhr	Würzburg	4h
Erzeugung CSRs	RZ 2 - Zugang 2 Prod ASM - Durchführen Schritte 3-5, 8-10 gemäss Setup-Dokument - 60min RZ 1 - Zugang 1 Prod ASM - Durchführen Schritte 3-5, 8-10 gemäss Setup-Dokument - 30min	Rockenstein, WPS, BRAK, Worldline	Tag 2, 9-11 Uhr	Würzburg	2h
Signieren der Zertifikate	3x Auslesen des CSR und Versand an die BNotK (siehe Setup-Dokument Schritt 2.2.10) – 45min - Warten auf die Antwort der BNotK - Installation der Prod ASM Zertifikate und	Rockenstein, WPS, BRAK, Worldline	Tag 2, 10-12 Uhr	Würzburg	3h
Cloning	Cloning in des PROD-ASM von AToS	Rockenstein, WPS, BRAK,	Tag 2, 13 Uhr	Würzburg	45 min

Aktion	Beschreibung	Wer?	Wann? Wo?	Geplante Dauer
		Worldline		
Installation Zertifikate	Installation der beiden Zertifikate, die von AToS bereitgestellt worden sind. Dieser Schritt kann parallel zu den ersten Schritten erfolgen.	WPS, Worldline	Tag 2, Würzburg 9 Uhr	1h
Setup Key Labels	Setup der JSS Key Labels zur Vorbereitung des Clonings. Dieser Schritt kann parallel zu den ersten Schritten erfolgen.	WPS, Worldline	Tag 2, Würzburg 10 Uhr	2h

