Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

INTERN

Ausnahmeantrag SSZ-Policy

Titel:	**Migration ARAMIS von DMZ in die SSZ / Portöffnung BV-Netz nach SSZ**
Dokumentidentifikation:	**SSZ-Beschluss Nr. SUR-1604-001**
Datum:	**06.12.2018**
Version:	**V 2.3**
Antragssteller:	**Trachsler Tobias, IM SBFI**
Klassifizierung:	**Intern**

Status:

in Arbeit	Antrag	genehmigt
☐	☐	X

Änderungskontrolle, Prüfung, Genehmigung			
Version	Datum	Beschreibung	Name
V 1.0	18.05.2015	Antrag stellen	Diane Kalek-Fischer
V 1.1	11.06.2015	Anpassung Skizze und MAC Auftrag	Diane Kalek-Fischer
V 1.2	18.06.2015	Anpassung MAC Antrag	Diane Kalek-Fischer
V 2.0	08.04.2016	Verlängerung Ausnahmenantrag	Christian Brunner
V 2.1	06.03.2017	Anpassung MAC Antrag	Marco Dal Farra
V2.2	06.12.2018	Erneute Verlängerung beantragt	Tobias Trachsler IM SBFI
V2.3 Genehmigung:	25.11.2020	Ausnahmenantrag mit Vorbehalt bis am 31.12.2022 genehmigt, sow eit folgende Massnahmen umgesetzt w erden: . **alle Datenbankverbindungen müssen transportverschlüsselt sein – Umsetzungstermin bis 31.12.2020** . **siehe Punkt 6**	Signaturerklärung: mit Vorbehalt bis am 31.12.2022 genehmigt, siehe Massnahmen Digital signiert von Meleskevicius Mantas SN1AAG 2020-11-25 (mit Zeitstempel)

1 Ausgangslage

Veranlassung gem. Mail vom 09.03.2015
Das „Informationssystem ARAMIS über die Forschung und Entwicklung (F+E) des Bundes“ ist seit 1997 in Betrieb. Das Informationssystem funktioniert als eine einfache Datenbankanwendung, in welcher alle Forschungsvorhaben der Bundesverwaltung als einzelne oder miteinander verknüpfte Projekte abgebildet werden – diese Projekte enthalten dabei neben Grundinformationen wie Titel und Laufzeit auch beschreibende Angaben wie Projektziele oder Abschlussberichte sowie Vertragsdaten. Namentlich letztere dienen dem Bundesamt für Statistik und dem Staatssekretariat für Bildung und Forschung als Grundlage für statistische und weitere Auswertungen. Seit 2004 ist ARAMIS als ein Pfeiler in die Qualitätssicherung in der Ressortforschung des Bundes eingebunden, indem das bereits in ARAMIS bestehende Reporting über die Ressortforschung in den Richtlinien über die Qualitätssicherung stärker verankert wurde. ARAMIS ist über Internet unter der Adresse https://www.aramis.admin.ch/ zugänglich; öffentlich konsultiert werden kann dabei jedoch nur eine Teilmenge der Informationen. Seit 2005 werden in ARAMIS auch alle Wirksamkeitsüberprüfungen/ Evaluationen der Bundesverwaltung erfasst

Die Anwendung ARAMIS .NET des Kunden SBFI steht heute in der DMZ und muss im Rahmen des Lifecycle-Managements (MS Server 2003 auf MS Server 2012) im FaMig Projekt migriert werden. Mitarbeitende des SBFI greifen zum Teil direkt auf die Datenbank zu. Dabei werden die folgenden Werkzeuge verwendet:

- Access (ODBC)
- SQL Server Management Studio Express (SQLNet)
- Java Anwendung (JDBC)

Nebst der Server-Migration sind die drei folgenden Punkte zu regeln:

1. Nutzung von eIAM anstatt der lokalen Benutzer- und Berechtigungsverwaltung
2. Migration in die SSZ
3. Oben genannte direkten DB-Zugriffe die eine SSZ-Policy Verletzung darstellen.

2 Antrag

Auf der FW sind für ARAMIS PROD und ABNA bis Ende 2018 die Ports für SFTP und ODBC geöffnet. Diese Portöffnungen sind um zwei Jahre (bis 31.03.2020) zu verlängern, da es für folgende Arbeiten keine Ersatztechnologien gibt:
- SFTP: Konsultation der Log-Files
- ODBC: Statistikerstellung zu Handen BFS und Bundesrat

3 Risiken

keine

4 Risikominimierende Massnahmen

keine

5 Konsequenzen bei Nicht-Bewilligung

Das ARAMIS-Tagesgeschäft sowie die Statistikerstellung zu Handen BFS und Bundesrat können nicht durchgeführt werden.

6 Wichtige Information

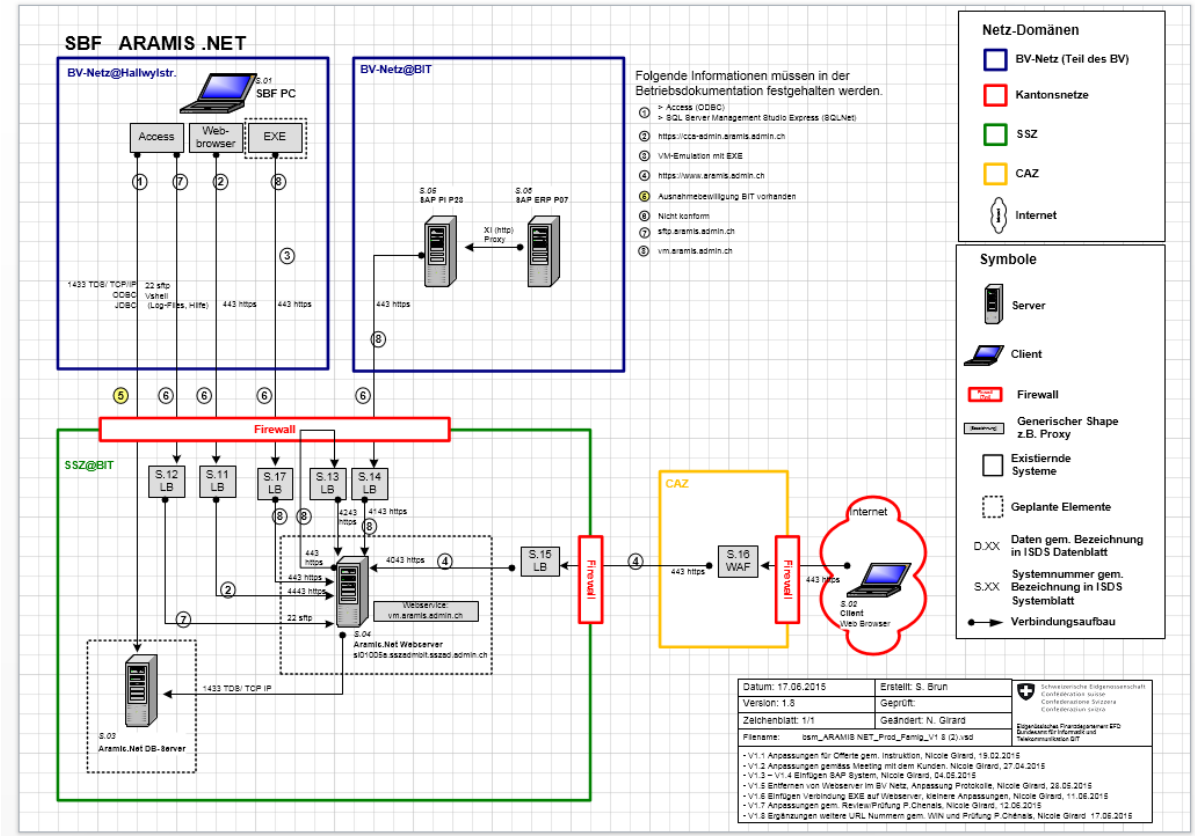
Nach Ablauf der Frist, ist der Antragssteller verantwortlich für eine Bestätigung an SI-SUR-SEC, dass die Ausnahme nicht mehr benötigt wird und diese zurückgebaut wurde.

7 Informationsfluss

LE-seitig: IM Kunde -> ISBO BIT

8 Beilagen

→ Architekturskizze V 1.8



– Die Architektur für ARAMIS PROD und ABNA ist identisch, die Portöffnungen werden für PROD und ABNA benötigt.

Kommunikationsmatrix zur ArchitekturskizzeV1.8

Entspricht Architekturskizze Version 1.8

Kommunikationsmatrix (Produktion)		Destination												
	System	8.01	8.05	8.08	8.03	8.04	8.11	8.12	8.13	8.14	8.16	8.17	8.18	8.02
von \ auf	Basisdienste (DNS, NTP, Virenschutz, Backup, Patch usw.)	SBF PC	SAP PI P23	SAP ERP P07	DB-Server	Webserver	Loadbalancer	Loadbalancer	Loadbalancer	Loadbalancer	Loadbalancer	Loadbalancer	WAF	Client
System	Basisdienste (DNS, NTP, Virensohutz, Baokup, Patoh usw.)													
Source 8.01	SBF PC				TDS, TCP/IP: 1433		https: 443	sftp: 22				https: 443		
8.05	SAP PI P23									https: 443				
8.08	SAP ERP P07		XI (http) Proxy											
8.03	DB-Server													
8.04	Webserver				TDS, TCP/IP: 1433				https: 443					
8.11	Loadbalancer					https: 4443								
8.12	Loadbalancer					sftp: 22								
8.13	Loadbalancer					https: 4243								
8.14	Loadbalancer					https: 4143								
8.16	Loadbalancer					https: 4043								
8.17	Loadbalancer					https: 443								
8.18	WAF										https: 443			
8.02	Client												https: 443	

Legende

- BV-Netz
- SSZ
- DMZ
- CAZ
- Partnernetze
- Internet

Für Netzwerk-Fragen und insbesondere Firewall-Fragen müssen die entsprechenden Engineers möglichst früh beigezogen werden.