

B. Leistungsbeschreibung

Vorhaben: Support Spring LTS (26_ITD_013)

Inhaltsverzeichnis

1	Vertragspartner	1
2	Gegenstand der Beschaffung	1
3	Rahmenbedingungen	2
I.	Zeitplanungen	2
II.	Technische Rahmenbedingungen	2
III.	Organisatorische und räumliche Rahmenbedingungen	2
IV.	Mengengerüste	2
V.	Mitwirkungsleistungen / Beistellungen	3
VI.	Datenschutzrechtliche Rahmenbedingungen	3
VII.	Vorgaben zur Projektabwicklung	3
4	Anforderungsbeschreibung (Leistungsbeschreibung im engeren Sinn)	3
I.	Allgemeine Anforderungen	3
II.	Reaktionszeit.....	4
III.	Pakete.....	5

1 Vertragspartner

Der Deutsche Gesetzliche Unfallversicherung e.V. (im Folgenden Auftraggeber) ist der Spitzenverband der gewerblichen Berufsgenossenschaften und der Unfallversicherungsträger der öffentlichen Hand. Die neun gewerblichen Berufsgenossenschaften sind nach Branchen orientiert. Die Unfallversicherungsträger der öffentlichen Hand gliedern sich in 16 Unfallkassen, drei Gemeindeunfallversicherungsverbände, vier Feuerwehr-Unfallkassen sowie die Unfallversicherung Bund und Bahn.

Der Verband nimmt die gemeinsamen Interessen seiner Mitglieder wahr und fördert deren Aufgaben zum Wohl der Versicherten und Unternehmen. Er vertritt die gesetzliche Unfallversicherung gegenüber Politik, Bundes-, Landes-, europäischen und sonstigen nationalen und internationalen Institutionen sowie Sozialpartnern.

2 Gegenstand der Beschaffung

Gegenstand der Beschaffung ist die Long-Term-Support (im folgenden LTS) für das Spring Framework (<https://spring.io/projects/spring-framework>). Zur Leistung gehört eine Wartung des Codes, welche unaufgefordert erfolgt, wenn entsprechende Schwachstellen bekannt werden.

Vorhaben: Support Spring LTS (26_ITD_013), Version 1

Bei der Wartung geht es darum, alle existierenden und während der Vertragslaufzeit bekannt gewordenen Schwachstellen zu schießen und als Quellcode und kompilierte Artefakte auszuliefern. Siehe die Punkte 1, 5, 6, 14 und 15 in dem Kapitel 4.I.

Ergänzend gehören zur Beschaffung Beratungsleistungen, welche über E-Mail, Chat oder Telefon erfolgen und die erbrachte Leistung bei der Beseitigung von Schwachstellen vervollständigen.

3 Rahmenbedingungen

I. Zeitplanungen

Zu den durch LTS betreuten Anwendungen gehört eine breite Palette von hausinternen Anwendungen, insgesamt je nach Zählweise etwa 50 Stück unterschiedlicher Komplexität und Größe

II. Technische Rahmenbedingungen

Der Auftragsnehmer betreibt ein Maven-Repository und stellt darin die gewarteten Pakete dem Auftragnehmer zum Abruf bereit. Das Repository wird über das Internet erreichbar. Zugang zum Repository erfolgt mithilfe eines technischen Benutzers.

Ergänzende Information wird in Form einer durchsuchbaren Datenbank im Web bereitgestellt. Zugang zur Datenbank muss für alle Entwickler des Auftraggebers möglich sein.

III. Organisatorische und räumliche Rahmenbedingungen

Der Auftraggeber greift auf das Repository des Auftragnehmers von dem eigenen Maven-Server zu und verteilt die Pakete in dem geschlossenen Netzwerk der Unfallversicherung (a.k.a. CNUV). Interne Verteilung erfolgt mit oder ohne Autorisierung. Das Einhalten der Vertragsbedingungen erfolgt organisatorisch.

IV. Mengengerüste

Der Auftraggeber strebt eine entwicklerbasierte Lizenzierung an. Auftraggeber beschäftigt aktuell 50 Backend-Entwickler. Es werden nur menschliche Entwickler gezählt, welche den Java Code erzeugen oder warten. Automatische Build- und Deployment-Pipelines, sowie die KI-Agenten werden bei der Lizenzierung nicht berücksichtigt.

Die aktuelle Anzahl von Entwicklern (50) wird unter der Annahme ermittelt, dass alle geführten Spring-Anwendungen in den Support-Vertrag übergehen. Die Anzahl von Lizenzen kann zum Ablauf des Jahres verkleinert werden.

Als Entwickler werden alle Committer vom Java-Code in die GIT-Repositories der Projekte gezählt. Es werden nur GIT-Repос berücksichtigt, welche die im Rahmen des Support-Vertrages vorbereiteten Pakete importieren oder referenzieren.

Vorhaben: Support Spring LTS (26_ITD_013), Version 1

Es werden alle Entwickler gezählt, die im Laufe eines Kalendermonats commitet haben. Diese Prüfung wird mehrmals jährlich wiederholt, um die Konformität mit dem Vertrag sicherzustellen.

Auftraggeber behält sich eine kurzzeitige Überschreitung der vereinbarten Zahl vor, wenn ein Teamwechsel bei der Projektbetreuung durchgeführt wird.

Sollten über Maven-Repositories des Auftragnehmers Software-Produkte bereitgestellt werden, welche nicht unter den Wartungsvertrags fallen, haben sie keinen Einfluss auf die Berechnung. Im Zweifel ist es die Aufgabe des Auftragnehmers, den nicht gewünschten und nicht lizenzierten Zugang des Auftraggebers zu sperren.

Fertig gebaute Software-Produkte auf Basis von unter dem Wartungsvertrag stehenden Teilen des Spring Frameworks werden von den Mitgliederorganisationen des Dachverbandes DGUV installiert und betrieben. Der Wartungsvertrag muss es zulassen.

V. Mitwirkungsleistungen / Beistellungen

Auftragnehmer erbringt die Leistung und stellt die Erzeugnisse bereit, wie es in dem Kapitel "Technische Rahmenbedingungen" beschrieben ist.

Auftraggeber überprüft regelmäßig den Umfang der Nutzung, wie es in dem Kapitel "Mengenrüste" beschrieben ist.

VI. Datenschutzrechtliche Rahmenbedingungen

Die von Auftragnehmer gewartete Pakete beinhalten keine datenschutzrelevanten Daten. Leistung beinhalten Sollen in der Kommunikation im Rahmen des Vertrages datenschutzrelevante Daten verarbeitet werden (z.B. Namen der Mitarbeiter), gilt DSGVO.

VII. Vorgaben zur Projektabwicklung

Auftragsnehmer stellt unmittelbar nach dem Vertragsabschluss die notwendigen Zugänge bereit.

4 Anforderungsbeschreibung (Leistungsbeschreibung im engeren Sinn)

I. Allgemeine Anforderungen

Es gelten folgende Anforderungen:

1. Die bereitgestellten Pakete **müssen** kompilierte JARs, Quellcode und JavaDocs enthalten, in mindestens der für das Spring Framework üblichen Qualität.
2. Die Releases **müssen** auf der Webseite des Anbieters oder per Newsletter angekündigt werden und die Liste von Änderungen (Release Notes) erhalten.

Vorhaben: Support Spring LTS (26_ITD_013), Version 1

3. Die Release Notes in Form von textuellen Ankündigungen (vorherige Punkt) oder einer durchsuchbaren Online-Datenbank (nächste Punkt) **müssen** die Liste von behobenen Schwachstellen enthalten.
4. Die Schwachstellen **sollen** in einer für die Entwickler verfügbaren und durchsuchbaren Online-Datenbank stehen mit der Angabe des Releases, wo die Schwachstelle behoben wurde.
5. Die Verteilung von Paketen **muss** über ein Maven-Server erfolgen. Der Server wird über das Internet an die Infrastruktur des Auftragsgeber angeschlossen.
6. Maven Repository inklusive verwendete Authentifizierung **muss** mit Sonatype Nexus und JFrog Artifactory kompatibel sein.
7. Die Wartung **muss** für jeden Major-Release (5.x, 6.x etc.) für mindestens 5 Jahre nach dem Auslaufen des Open-Source-Supports (OSS) gelten.
8. Die Wartung **soll** für jeden Major-Release (5.x, 6.x etc.) für mindestens 10 Jahre nach dem Auslaufen des Open-Source-Supports (OSS) gelten.
9. Die Wartung **soll** für jeden Minor-Release (5.3, 6.0, 6.1 etc.) für mindestens 5 Jahre nach dem Auslaufen des OSS-Supports gelten.
10. Versionierung von Paketen **muss** so erfolgen, dass gängige Werkzeuge für die Analyse der Abhängigkeit (z.B. OWASP Dependency Track) das neue Paket zu den entsprechenden Open Source Versionen zuordnen können. Ein unter Wartung stehende Paket darf an der Stelle nicht als völlig neue Komponente gesehen werden.
11. Die betreuten Pakete **sollen** einem externen Audit unterliegen.
12. Der Preis **darf** höchstens linear steigen. Z.B., wenn 50 Entwickler 10000€ kosten, kosten 55 Entwickler nicht mehr als 11000€ (es ist eine **muss**-Anforderung).
13. Der Preis **soll** im Bereich von mindestens -30% mindestens linear sinken. Z.B., wenn 50 Entwickler 10000€ kosten, kosten 45 Entwickler nicht mehr als 9000€.
14. Die Schwachstellen **müssen** mit National Vulnerability Database (NVD) abgeglichen werden.
15. Die Schwachstellen **sollen** mit GitHub Advisories (GHSA) abgeglichen werden.

Die Schwachstelle gilt als geschlossen (gefixt), wenn sie nach dem in NVD oder GHSA beschriebenen Angriffsvektor nicht mehr ausnutzbar ist.

Es kann vorkommen, dass es aufgrund eines konzeptionellen Problems des Spring Frameworks nicht möglich sein, eine Schwachstelle zu schließen. Das gilt z.B., wenn die Funktionalität des Frameworks dadurch wesentlich eingeschränkt wird. In diesem Fall gilt die Leistung als erbracht, wenn es beschrieben wird, welche Elemente welchen Einschränkungen unterliegen.

II. Reaktionszeit

Reaktionszeit auf die bestehenden und bekannt gewordenen Schwachstellen wird wie folgt vereinbart.

	Support Anfragen	Critical und High		Medium	
		Workaround	Fix	Workaround	Fix
soll	48 Stunden	48 Stunden	1 Woche	1 Woche	1 Monat

Vorhaben: Support Spring LTS (26_ITD_013), Version 1

muss	1 Woche	1 Woche	1 Monat		
-------------	---------	---------	---------	--	--

Bei den Angaben in Stunden sind Sonntage und gesetzliche Feiertage Tage ausgenommen.
Jede Tabellenzelle gilt als separate Anforderung.

III. Pakete

Folgende Pakete **müssen** vom Support abgedeckt werden.

- Kernkomponente: spring-core, spring-beans, spring-context, spring-aop
- Hilfskomponente: spring-expression
- Web: spring-web, spring-webmvc
- Security: spring-security-core, spring-security-web, spring-security-config, spring-security-oauth2-client
- Datenzugriff: spring-jdbc, spring-orm, spring-data-jpa, spring-tx
- Boot: spring-boot, spring-boot-autoconfigure, spring-boot-starter, spring-boot-starter-web, spring-boot-starter-security, spring-boot-starter-data-jpa, spring-boot-starter-jdbc, spring-boot-starter-validation, spring-boot-starter-actuator, spring-boot-starter-logging

Weitere Pakete **sollen** abgedeckt werden:

- Messaging: Spring AMQP, Spring JMS
- Secrets: Spring Vault
- Search: Spring Data Elasticsearch
- Directory: Spring LDAP
- Caching: Spring Data Redis, Spring Cache
- Testing: Unit-Testing, Integration-Testing (z.B. JDBC-Testing), API-Testing, Web-/E2E-Testing, Kontext- und Konfigurationstesting

Die Fixes müssen für den letzten OSS Release in 5. und 6. Reiher des Spring-Frameworks verfügbar sein, sofern die entsprechende Version von der Sicherheitslücke betroffen ist. Die Fixes sind im Dokument H. Preis- und Bewertungsblatt hinterlegt und stellen eine Mindestanforderung/ Ausschlusskriterien dar.

Jedes Listenelement gilt als separate Anforderung.