

# SOFTWARELIZENZVERTRAG

zwischen

## **SPRIND GmbH**

Lagerhofstraße 4, 04103 Leipzig  
(im Folgenden: „Auftraggeber“)

und

[...]  
[...]

(im Folgenden: „Lizenzgeber“)

## **Präambel**

Die überarbeitete EU-Verordnung über elektronische Identifizierung, Authentifizierung und Vertrauensdienste (eIDAS-EU) erfordert den Aufbau eines sicheren und nutzerfreundlichen Ökosystems, dessen zentrales Instrument die Europäische Digitale Identitätswallet (European Digital Identity Wallet, „EUDI Wallet“) ist. In Deutschland erfolgt die Einführung der EUDI Wallet als Zugang zu einer vertrauenswürdigen, interoperablen und nicht-diskriminierenden digitalen Wallet als gemeinschaftliches Vorhaben des Bundesministeriums für Digitales und Staatliche Modernisierung („BMDS“) und der Bundesagentur für Sprunginnovationen („SPRIND“) im Rahmen eines offenen Architektur- und Konsultationsprozesses mit besonderem Fokus auf Sicherheit, Datenschutz, Nutzerfreundlichkeit und Innovation.

Vor diesem Hintergrund beabsichtigt der Auftraggeber die Beschaffung und Integration einer sog. Runtime Application Self Protection-Lösung für Wallet-Anwendungen auf iOS und Android (sowie ggf. zukünftig weiterer Betriebssysteme), um eine zusätzliche Sicherheitsschicht zur Laufzeit bereitzustellen, den Anwendungscode zu verschleiern sowie datenschutzkonforme Telemetrie zu unterstützen.

Die vorweggeschickt und nach Durchführung eines vorangegangenen öffentlichen Vergabeverfahrens, vereinbaren die Parteien was folgt:

## **1. Definitionen**

- 1.1 In diesem Vertrag bezeichnet der Begriff „SDK“ (Software Development Kit) die mobile RASP-Komponente für iOS und Android (sowie ggf. zukünftig weitere Betriebssysteme), die die funktionalen Anforderungen gem. Ziff. 5.1 sowie gem. der Leistungsbeschreibung erfüllt, unabhängig von der dabei konkret verwendeten Technologie.

- 1.2 Der Begriff „Backend“ bezeichnet eine etwaig gewünschte serverseitige Komponente, die auf der Infrastruktur des Auftraggebers zu betreiben ist.
- 1.3 Der Begriff „Telemetrie“ bezeichnet die in diesem Vertrag näher beschriebenen sicherheitsbezogenen Ereignisdaten einschließlich der Nachverfolgbarkeit der Richtlinienversion und der Protokollierung ausgelöster Sicherheitsregeln mit Maßnahmen und eindeutigen Identifikatoren.

## **2. Vertragsgegenstand; Geltungsreihenfolge**

- 2.1 Vertragsbestandteile und Rechtsgrundlagen – in der Reihenfolge ihrer Geltung – sind:
- die Leistungsbeschreibung sowie etwaige Antworten des Auftraggebers auf Bieterfragen;
  - die Bestimmungen dieser Vereinbarung;
  - die sonstigen dem Vergabeverfahren zugrundeliegenden (Vergabe-)Unterlagen;
  - das Angebot des Lizenzgebers mit den Anlagen, einschließlich des Preisblatts und des Konzeptes, welches Gegenstand der qualitativen Zuschlagskriterien war;
  - Verdingungsordnung für Leistungen, Teil B Allgemeine Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) – Fassung 2003 – Bekanntmachung vom 5.8.2003 (BAnz Nr. 178a);
  - die gesetzlichen Regelungen des Bürgerlichen Gesetzbuches (BGB).
- 2.2 Die Regelungen dieser Vereinbarung gelten ausschließlich. Abweichende, entgegenstehende oder ergänzende Regelungen und Allgemeine Geschäftsbedingungen des Lizenzgebers gelten nicht.
- 2.3 Sollte der Auftraggeber in seiner jetzigen Rechtsform nicht mehr fortbestehen, tritt – soweit gesetzlich zulässig – sein Rechtsnachfolger in sämtliche Rechte und Pflichten aus dieser Vereinbarung ein. Die jeweiligen Pflichten beider Parteien aus dieser Vereinbarung gelten unverändert fort. Ferner ist der Auftraggeber berechtigt, seine Rechte und Pflichten aus dieser Vereinbarung – nach angemessener Ankündigung gegenüber dem Lizenzgeber – auf eine im Rahmen der Ankündigung konkret zu benennende Tochter- oder Schwestergesellschaft zu übertragen. Die Rechte und Pflichten des Lizenzgebers gelten in diesem Fall gegenüber der benannten Gesellschaft unverändert fort.
- 2.4 Der Gegenstand dieses Vertrags ist die Lizenzierung und Bereitstellung einer mobilen Runtime Application Self-Protection („RASP“) Software-Komponente in Form eines SDK für iOS und Android (sowie ggf. zukünftig weiterer Betriebssysteme) und gegebenenfalls einer optionalen, ergänzenden Backend-Komponente, die auf einer vom Auftraggeber oder dessen benannten Unterauftragnehmern bereitgestellten und kontrollierten Infrastruktur betrieben

werden kann. Der Lizenzgeber erbringt insoweit die in der Leistungsbeschreibung genannten Leistungen.

- 2.5 Der Leistungsgegenstand kann im gegenseitigen Einvernehmen der Parteien um vergleichbare Leistungen ergänzt oder konkretisiert werden, die im Zusammenhang mit dem Leistungsgegenstand gem. Ziff. 2.4 und der Leistungsbeschreibung stehen, sofern diese Leistungen den ursprünglichen Leistungsgegenstand nicht wesentlich verändern.
- 2.6 Das SDK ist sowohl im Standalone-Betrieb ohne Backend als auch, wenn optional gewünscht, in Verbindung mit einer Backend-Komponente zu betreiben.
- 2.7 Es findet keine Übermittlung von Betriebs- oder Sicherheits-Telemetriedaten an vom Lizenzgeber betriebene oder kontrollierte Systeme statt, es sei denn, die Parteien treffen hierzu ausdrücklich eine abweichende schriftliche Vereinbarung.

### **3. Lizenzeinräumung**

- 3.1 Der Lizenzgeber räumt dem Auftraggeber ein nicht ausschließliches, unterlizenzierbares und übertragbares Recht ein, das SDK und, wenn vom Auftraggeber gewünscht, das Backend während der Laufzeit dieses Vertrags weltweit zu nutzen, zu vervielfältigen und in die Anwendungen des Auftraggebers zu integrieren, und zwar zum Zwecke des Betriebs und Schutzes der Wallet-Anwendungen des Auftraggebers im Kontext mit dem EUDI Wallet. Die vorstehende Lizenzeinräumung gilt unabhängig von der Anzahl der Nutzer sowie der Art und Anzahl der Wallet-Anwendungen des Auftraggebers.
- 3.2 Das Recht zur Vervielfältigung ist auf die für Installation, Betrieb, Laden, Anzeigen, Ablaufen, Übertragen und Speichern erforderlichen Kopien sowie auf erforderliche Sicherungskopien beschränkt. Das Recht zur Bearbeitung ist auf Maßnahmen beschränkt, die der Erhaltung oder Wiederherstellung der vertraglich vereinbarten Funktionalität dienen. Das Recht zur Dekompilierung wird ausschließlich im Rahmen und unter den Voraussetzungen der §§ 69e Abs. 1 und Abs. 2 UrhG gewährt.
- 3.3 Die Nutzung ist auf die EUDI Wallet Apps des Auftraggebers beschränkt; der Auftraggeber beabsichtigt, Quellcodes seiner Anwendungen zu veröffentlichen, wobei RASP-bezogene Aufrufe vor der Veröffentlichung aus dem öffentlich bereitgestellten Code entfernt werden.

### **4. Lieferung und Betrieb**

- 4.1 Der Lizenzgeber liefert das SDK mit der zugehörigen Dokumentation als eine „out-of-the-box“ Lösung für iOS und Android spätestens eine (1) Woche nach Zuschlagserteilung.
- 4.2 Sofern ein Backend gewünscht ist, gewährleistet der Lizenzgeber, dass diese Komponente auf der Infrastruktur des Auftraggebers oder seiner benannten Unterauftragnehmer betrieben werden kann; zugleich gewährleistet der Lizenzgeber, dass das SDK den Standalone-Betrieb

ohne Backend unterstützt. Die Abnahme erfolgt nach erfolgreicher Integrations- und Funktionsprüfung des SDK und, soweit einschlägig, des Backends gegen die in diesem Vertrag festgelegten Spezifikationen, und der Lizenzgeber verpflichtet sich, etwaige wesentliche Abweichungen innerhalb der in diesem Vertrag vereinbarten Reaktions- und Abhilfefristen zu beheben.

## **5. Funktionale Anforderungen**

### **5.1 Der Lizenzgeber sichert zu, dass das SDK**

- Laufzeitbedrohungen erkennt und angemessen darauf reagiert, indem es das Vorliegen von Hooking-Frameworks und aktiven Debugging-Versuchen erkennt und Manipulationen der Applikationslogik zur Laufzeit verhindert;
- die Veränderung oder Neu-Signierung von App-Paketen erkennt und die Integrität der verteilten Binärdateien verifiziert;
- die Änderung von Code und unautorisierte Änderungen erkennt und Mechanismen zur Laufzeit-Integritätsvalidierung bereitstellt;
- das Vorliegen gerooteter oder jailbreakter Geräte sowie Emulatoren und virtualisierte Umgebungen erkennt und kompromittierte oder risikobehaftete Gerätezustände identifiziert;
- die Obfuskation (Verschleierung) sensibler Logik einschließlich der RASP-Aufrufe unterstützt und mit gängigen Build-Tools kompatibel ist;
- mit der zugehörigen Dokumentation sowie einer aktuellen Software Bill of Materials (SBOM) als eine „out-of-the-box“ Lösung bereitgestellt wird.

### **5.2 Sofern ein Backend gewünscht ist: Der Lizenzgeber sichert zu, dass Sicherheitsrichtlinien dynamisch und zentral bereitgestellt werden, ohne dass App-Updates erforderlich sind, wobei nur vorab definierte Parameterbereiche (Guardrails) geändert werden, und dass die Richtlinienbereitstellung sicher und signiert erfolgt, um Manipulationen zu verhindern.**

### **5.3 Sofern ein Backend gewünscht ist: Der Lizenzgeber sichert ferner zu, dass die Telemetrie die jeweils angewandte Richtlinienversion je App-Instanz oder Sitzung ausweist und alle ausgelösten Sicherheitsregeln sowie die jeweils durchgesetzte Maßnahme einschließlich etwaiger App-Beendigungen mit Zeitpunkt, Grund und einer eindeutigen Sitzungs- oder Ereignis-ID berichtet, sodass eine Korrelation, eine betriebliche Auswertung und die Untersuchung von Fehlalarmen möglich sind.**

### **5.4 Sofern ein Backend gewünscht ist: Der Lizenzgeber verpflichtet sich zugleich, dass keine Telemetriedaten an vom Lizenzgeber betriebene oder kontrollierte Systeme übertragen werden und dass der Betrieb der Telemetrie auf der Infrastruktur des Auftraggebers erfolgt, sofern die Parteien nicht ausdrücklich etwas anderes schriftlich vereinbaren.**

- 5.5 Der Lizenzgeber verpflichtet sich, auf Anfrage – höchstens einmal pro Vertragsjahr und auf Kosten des Lizenzgebers – innerhalb angemessener Zeit belastbare Nachweise über Penetrationstests oder gleichwertige Sicherheitsüberprüfungen vorzulegen, die belegen, dass das SDK die vorstehenden funktionalen Anforderungen erfüllt und gegen Angriffe gehärtet ist, und den Umfang und die Dauer der Prüfungen zu dokumentieren.

## **6. Nicht-funktionale Anforderungen und Compliance**

- 6.1 Der Lizenzgeber erklärt, dass er und etwaige Subunternehmer über eine Zertifizierung nach ISO/IEC 27001 oder SOC2 Typ 2 oder eine gleichwertige Zertifizierung des Informationssicherheitsmanagements verfügen. Der Lizenzgeber ist verpflichtet, diese als Nachweis auf Anfrage vorzulegen und während der Vertragslaufzeit aufrecht zu erhalten bzw. gegenüber Subunternehmer darauf hinzuwirken, dass die entsprechenden Nachweise vorgelegt werden und aufrecht erhalten bleiben.
- 6.2 Ergänzend gilt: Der Einsatz von Subunternehmern, die nicht bereits im Angebot benannt und zugelassen wurden (insb. für Support oder Entwicklung), bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Alle Subunternehmer müssen zwingend denselben Sicherheitsstandards (ISO 27001/SOC2, DSGVO) unterliegen wie der Lizenzgeber selbst.
- 6.3 Der Auftraggeber betreibt ein ISO 27001-konformes Informationssicherheits-Management-system (ISMS). Es wird erwartet, dass der Auftragnehmer durch geeignete Maßnahmen diese Compliance aktiv unterstützt.
- 6.4 Dem Auftraggeber oder einem von ihm beauftragten, zur Verschwiegenheit verpflichteten Dritten wird das Recht eingeräumt, die Einhaltung der Sicherheitsanforderungen sowie die technischen und organisatorischen Maßnahmen des Lizenzgebers (inkl. Backend) nach vorheriger Ankündigung zu auditieren.
- 6.5 Der Lizenzgeber verpflichtet sich ungeachtet der Regelungen in Ziff. 7, sämtliche Kategorien der durch das SDK und gegebenenfalls das Backend verarbeiteten Daten offenzulegen und innerhalb der Umgebung des Auftraggebers die vollständige Unterstützung der DSGVO-Compliance sicherzustellen.
- 6.6 Der Lizenzgeber verpflichtet sich, die Einhaltung von Compliance-, Sicherheitsbewertungs- und Prüfprozessen durch geeignete Dokumentation und technische Informationen zu unterstützen, die für unabhängige Sicherheitsprüfungen oder Audits erforderlich sind.
- 6.7 Darüber hinaus räumt der Lizenzgeber dem Auftraggeber ausdrücklich das Recht ein, sämtlichen Programmcode, einschließlich iOS-, Android- oder anderer Betriebssystemanwendungen sowie aller integrierten RASP-Komponenten, in das „Bug-Bounty“-Programm des Auftraggebers einzubeziehen. Der Auftraggeber trägt die alleinige Verantwortung für die Verwaltung, das Management und die Durchführung des „Bug-Bounty“-Programms.

## **7. Datenschutz**

- 7.1 Der Lizenzgeber wird im Rahmen dieses Vertrags keine personenbezogenen Daten im Auftrag i.S.v. Art. 28 DSGVO verarbeiten.
- 7.2 Der Auftraggeber verpflichtet sich, dem Lizenzgeber keine personenbezogenen (Nutzer-)Daten zur Verfügung zu stellen und die Konfiguration von SDK, ggf. Backend und Telemetrie so auszugestalten, dass keine personenbezogenen Daten an den Lizenzgeber übermittelt werden und dass sämtliche Verarbeitungen ausschließlich innerhalb der vom Auftraggeber oder seinen benannten Unterauftragnehmern bereitgestellten Infrastruktur erfolgen.
- 7.3 Der Auftraggeber stellt sicher, dass etwaige für Support- oder Fehleranalysezwecke bereitgestellte Informationen vorab so anonymisiert oder anderweitig bereinigt werden, dass die Übermittlung personenbezogener Daten ausgeschlossen ist, und der Lizenzgeber erbringt seine Leistungen ohne die Verarbeitung personenbezogener Daten.
- 7.4 Die Parteien stellen klar, dass aufgrund der vorstehenden Regelungen kein Auftragsverarbeitungsverhältnis im Sinne der DSGVO zwischen ihnen begründet wird. Die Parteien bestätigen, dass die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen umgesetzt werden.

## **8. Betrieb und Support**

- 8.1 Der Lizenzgeber stellt eine durchgängige Entgegennahme von Sicherheitsvorfällen an sieben (7) Tagen in der Woche rund um die Uhr sicher, garantiert eine maximale Erstreaktionszeit von vier (4) Stunden und stellt Abhilfemaßnahmen oder Patches innerhalb von achtundvierzig (48) Stunden bereit, soweit dies technisch möglich ist.
- 8.2 Der Lizenzgeber stellt sicher, dass Sicherheitsupdates und die Behebung von Schwachstellen innerhalb von achtundvierzig (48) Stunden für kritische Schwachstellen und innerhalb von fünf (5) Geschäftstagen für Schwachstellen mit hoher Schwere erfolgen und benachrichtigt den Auftraggeber proaktiv über neu identifizierte Sicherheitsrisiken, die das SDK oder etwaige Backend-Komponenten betreffen.
- 8.3 Der Lizenzgeber gewährleistet die laufende Kompatibilität des SDK und etwaiger Backend-Komponenten mit neuen Hauptversionen der Betriebssysteme iOS und Android (und ggf. weiteren Betriebssystemen).
- 8.4 Der Lizenzgeber benennt einen dedizierten technischen Ansprechpartner und stellt strukturierte Eskalationsverfahren für sicherheitsrelevante Vorfälle bereit. Der Lizenzgeber sorgt für regelmäßige Wartungsversionen und die kontinuierliche Verbesserung der Erkennungsfähigkeiten, der Performance und der Stabilität.
- 8.5 Der Lizenzgeber verpflichtet sich, den Auftraggeber unverzüglich, spätestens jedoch innerhalb von vierundzwanzig (24) Stunden, über jegliche Informationssicherheitsvorfälle in seiner

eigenen Infrastruktur oder bei seinen Subunternehmern (Supply-Chain-Angriffe) zu informieren, die potenziell die bereitgestellten Services, den Quellcode oder Daten des Auftraggebers gefährden könnten.

## **9. Vergütung und Preisstruktur**

9.1 Die Parteien vereinbaren eine monatliche Pauschalvergütung, die sämtliche zur vollständigen Leistungserbringung gemäß Leistungsbeschreibung erforderlichen Komponenten umfasst.

9.2 Die Pauschalvergütung umfasst insbesondere:

- Integration
- Support
- Wartung
- Upgrades/Härtung
- eine unbegrenzte Anzahl von Geräten
- eine unbegrenzte Anzahl von Downloads
- alle angebotenen Funktionalitäten gemäß Leistungsbeschreibung

9.3 Alle Preise sind in EUR (netto) anzugeben und verstehen sich einschließlich sämtlicher anfallender Gebühren wie Transport, Reisen und sonstiger Kosten, die für eine vollständige Leistungserbringung und effektive Zusammenarbeit mit dem Auftraggeber erforderlich sind.

9.4 Die Vergütung für das SDK bestimmt sich als monatlicher Gesamtpreis je Device-Staffel gemäß Abschnitt A des Preisblatts „Runtime Application Self-Protection (RASP) – Preisblatt“; die monatlichen Gesamtkosten gelten pauschal je Device-Staffel. Das SDK-Nutzungsentgelt deckt iOS und Android (sowie zukünftig weitere Betriebssysteme) gleichermaßen ab, einschließlich aller in der Leistungsbeschreibung ausgewiesenen Funktionalitäten.

9.5 Maßgeblich für die Einstufung in die Device-Staffel ist die Zahl der auf Geräten installierten und vom RASP geschützten Apps auf Basis der jeweils verfügbaren Store-KPIs; eine Differenzierung nach aktiven/inaktiven Devices findet nicht statt; deinstallierte Geräte werden nicht gezählt. Für die Berechnung des anwendbaren und vom Auftraggeber zu zahlenden Monatspreises wird jeweils der Referenzwert zum Ende des Folgemonats zugrunde gelegt (letzter Tag, 23:59:59 Uhr), insbesondere anhand der Metriken „Active Device Installs“ (Google Play Store) bzw. „Opt-in Installations“ (Apple App Store).

9.6 Die Vergütung für das optionale Backend erfolgt als monatlicher Festpreis, unabhängig von der Zahl installierter Devices oder dem Transaktionsvolumen, gemäß Abschnitt B des

Preisblatts. Die optionalen Funktionalitäten werden im Preisblatt als „Kategorie 6 – Optionale Funktionalitäten“ gesondert ausgewiesen.

## **10. Laufzeit und Kündigung**

- 10.1 Dieser Vertrag wird initial bis einschließlich 31.12.2028 geschlossen. Die Vertragslaufzeit beginnt mit dem Abschluss des Vertrages.
- 10.2 Dem Auftraggeber steht das Recht zu, den Vertrag um maximal zwei (2) Mal um eine Laufzeit von jeweils zwölf (12) Monaten zu verlängern.
- 10.3 Der Vertrag gilt als beendet, wenn und soweit der Auftraggeber dem Lizenzgeber nicht drei (3) Monate vor Ende der Vertragslaufzeit mitteilt, den Vertrag zu verlängern und von der Verlängerungsoption Gebrauch zu machen. Im Falle dieser Mitteilung verlängert sich die Vertragslaufzeit gemäß Ziff. 10.2 um weitere zwölf (12) Monate; andernfalls endet der Vertrag zum nächstmöglichen Zeitpunkt.
- 10.4 Jede Partei kann den Vertrag während der Vertragslaufzeit nur aus wichtigem Grund kündigen, der vorliegt, wenn Tatsachen bestehen, aufgrund derer der kündigenden Partei unter Berücksichtigung aller Umstände des Einzelfalls und der Interessen beider Parteien die Fortsetzung des Vertragsverhältnisses nicht zugemutet werden kann. Ein wichtiger Grund liegt für die Auftraggeberin insbesondere vor, wenn
- ein Antrag auf Eröffnung des Insolvenzverfahrens oder eines vergleichbaren Verfahrens über das Vermögen des Lizenzgebers gestellt wird und dieser Antrag nicht innerhalb von sechs Wochen zurückgenommen wird oder ein vorläufiger Insolvenzverwalter bestellt oder die Eröffnung des Insolvenzverfahrens angeordnet oder die Eröffnung eines solchen Verfahrens mangels Masse abgelehnt wird;
  - der Lizenzgeber mitteilt, dass er nicht in der Lage sein wird, die Leistungen innerhalb der vereinbarten Fristen zu erbringen, es sei denn, der Lizenzgeber hat die Verzögerung nicht zu vertreten;
  - der Lizenzgeber wiederholt gegen eine der in dieser Vereinbarung oder ihren Anhängen festgelegten Verpflichtungen verstößt;
  - der Lizenzgeber die Verpflichtungen nach Ziff. 5 i.V.m. Ziff. 4 dieser Vereinbarung auch nach Ablauf einer angemessenen Frist zur Nachbesserung nicht erbringt;
  - das Finanzierungsverhältnis zwischen der Bundesrepublik Deutschland und der Auftraggeberin vorzeitig beendet wird oder nicht entsprechend den vertraglichen Bestimmungen der Finanzierungsvereinbarung zwischen der Bundesrepublik Deutschland und dem Auftraggeber fortgesetzt wird.



- 10.5 Wird das Vertragsverhältnis aus wichtigem Grund gekündigt, so kann der Auftragnehmer eine ihrer bisherigen Leistung entsprechende Teilvergütung verlangen.

## **11. Gewährleistung**

Der Lizenzgeber gewährleistet, dass die in diesem Vertrag beschriebenen funktionalen und nicht-funktionalen Anforderungen einschließlich der Erkennungsfunktionen, der Maßnahmen zum Code-Schutz, der dynamischen Richtlinienbereitstellung (sofern ein Backend gewünscht ist), der Telemetrie (sofern ein Backend gewünscht ist), der Support-Servicelevels und der Kompatibilitätspflege eingehalten werden, sowie dass einer vertragsgemäßen Nutzung der RASP-Softwarekomponente keine Rechte Dritter entgegenstehen und der Lizenzgeber verpflichtet sich, Abweichungen innerhalb der in diesem Vertrag (Ziff. 8) festgelegten Fristen zu beheben.

## **12. Haftung; Haftpflichtversicherung**

### **12.1 Der Lizenzgeber haftet unbeschränkt**

- bei Vorsatz oder grober Fahrlässigkeit,
- für die Verletzung von Leben, Leib oder Gesundheit,
- nach den Vorschriften (und im Umfang) des Produkthaftungsgesetzes,
- im Umfang einer vom Lizenzgeber zugesicherten Eigenschaft und/oder einer übernommenen Garantie sowie
- in sonstigen Fällen, in denen die Haftung gesetzlich zwingend vorgeschrieben ist.

### **12.2 Bei einfach fahrlässiger Verletzung einer Pflicht, die wesentlich für die Erreichung des Vertragszwecks ist (Kardinalpflicht), ist die Haftung des Lizenzgebers der Höhe nach begrenzt auf den Schaden, der nach der Art des hier in Rede stehenden Geschäfts vorhersehbar und typisch ist.**

### **12.3 Der Lizenzgeber weist nach Abschluss des Vertrags dem Auftraggeber nach, dass er über eine Versicherung verfügt, wie in den Vergabeunterlagen gefordert bzw. in der Eigenerklärung angegeben. Der Lizenzgeber wird diesen Versicherungsschutz bis zum Ende des Vertrags aufrechterhalten. Kommt der Lizenzgeber dieser Verpflichtung nicht nach, ist der Auftraggeber nach erfolgloser angemessener Fristsetzung zur Kündigung des Vertrags berechtigt, wenn ihr ein Festhalten am Vertrag nicht mehr zuzumuten ist. Weitergehende Ansprüche des Auftraggebers, insbesondere Schadensersatzansprüche, bleiben hiervon unberührt.**

### **13. Vertraulichkeit**

- 13.1 Die Parteien verpflichten sich, vertrauliche Informationen der anderen Partei strikt und unbedingt geheim zu halten und durch angemessene technische und organisatorische Vorkehrungen zu schützen. Diese Verpflichtung besteht nach Beendigung des Vertrags fort.
- 13.2 Von der vorstehenden Verpflichtung ausgenommen sind solche vertraulichen Informationen,
- die dem Empfänger bei Abschluss des Vertrags nachweislich bereits bekannt waren oder danach von dritter Seite bekannt werden, ohne dass dadurch eine Vertraulichkeitsvereinbarung, gesetzliche Vorschriften oder behördliche Anordnungen verletzt werden;
  - die bei Abschluss des Vertrags öffentlich bekannt sind oder danach öffentlich bekannt gemacht werden, soweit dies nicht auf einer Verletzung dieses Vertrags beruht;
  - die aufgrund gesetzlicher Verpflichtungen oder auf Anordnung eines Gerichtes oder einer Behörde offen gelegt werden müssen. Soweit zulässig und möglich wird der zur Offenlegung verpflichtete Empfänger die andere Partei vorab unterrichten und ihr Gelegenheit geben, gegen die Offenlegung vorzugehen.
- 13.3 Die Parteien werden nur solchen Beratern Zugang zu vertraulichen Informationen gewähren, die dem Berufsgeheimnis unterliegen oder denen zuvor den Geheimhaltungsverpflichtungen dieses Vertrags entsprechende Verpflichtungen auferlegt worden sind. Des Weiteren werden die Parteien nur denjenigen Mitarbeitern die vertraulichen Informationen offenlegen, die diese für die Durchführung dieses Vertrags kennen müssen, und diese Mitarbeiter auch für die Zeit nach ihrem Ausscheiden in arbeitsrechtlich zulässigem Umfang zur Geheimhaltung verpflichten.

### **14. Sprache, anwendbares Recht und Gerichtsstand**

- 14.1 Die deutsche Sprachfassung dieses Vertrages ist die rechtlich verbindliche Fassung. Im Falle von Widersprüchen gilt diese daher vorrangig; dies gilt nicht für die Leistungsbeschreibung und sonstige Vergabeunterlagen, die auch in englischer Sprache verbindlich bereitgestellt werden dürfen.
- 14.2 Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG).
- 14.3 Die Parteien vereinbaren, dass die Gerichte am Sitz des Lizenzgebers für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ausschließlich zuständig sind, soweit gesetzlich zulässig.

## 15. Schlussbestimmungen

- 15.1 Mit Vertragsende hat der Lizenzgeber unverzüglich und unaufgefordert sämtliche vom Auftraggeber erhaltenen Unterlagen, Hilfsmittel, Materialien oder Gegenstände herauszugeben, die ihm zum Zwecke der Vertragsausführung bestimmungsgemäß nicht dauerhaft überlassen wurden. Dies gilt auch für alle Kopien. Des Weiteren sind mit Vertragsende alle beim Lizenzgeber oder seinen Subunternehmern verbliebenen (auch aggregierten) Telemetrie-, Protokoll- und Support-Daten unwiderruflich zu löschen und dies dem Auftraggeber nachzuweisen. Der Auftraggeber ist berechtigt, an Stelle der Herausgabe ganz oder teilweise die sichere Löschung oder Vernichtung zu verlangen. Diese ist dem Auftraggeber auf Verlangen und nach seiner Wahl durch entsprechende Erklärung oder anderweitig nachzuweisen. Gesetzliche Aufbewahrungspflichten bleiben unberührt.
- 15.2 Änderungen und Ergänzungen dieses Vertrags bedürfen zu ihrer Wirksamkeit der Schriftform; dies gilt auch für die Änderung dieses Schriftformerfordernisses.
- 15.3 Sollten einzelne Bestimmungen dieses Vertrags ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so wird hierdurch die Wirksamkeit der übrigen Bestimmungen nicht berührt; an die Stelle der unwirksamen oder undurchführbaren Bestimmung tritt eine wirksame und durchführbare Regelung, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Parteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Nebenabreden bestehen nicht, und Anlagen sind nicht Bestandteil dieses Vertrags.

_____	_____	_____
(Ort)	(Datum)	(Unterschrift)

_____	_____	_____
(Ort)	(Datum)	(Unterschrift)

# SOFTWARE LICENCE AGREEMENT

between

**SPRIND GmbH**

Lagerhofstraße 4, 04103 Leipzig

(hereinafter: "Client")

and

[...]  
[...]

(hereinafter: "Licensor")

## Preamble

The revised EU Regulation on electronic identification, authentication and trust services (eIDAS-EU) requires the establishment of a secure and user-friendly ecosystem, the central instrument of which is the European Digital Identity Wallet ("EUDI Wallet"). In Germany, the introduction of the EUDI Wallet as access to a trustworthy, interoperable and non-discriminatory digital wallet is being implemented as a joint project of the Federal Ministry for Digital Affairs and State Modernisation ("BMDS") and the Federal Agency for Breakthrough Innovations ("SPRIND") as part of an open architecture and consultation process with a particular focus on security, data protection, user-friendliness and innovation.

Against this background, the Client intends to procure and integrate a so-called Runtime Application Self-Protection solution for wallet applications on iOS and Android (and, where applicable, other operating systems in the future) in order to provide an additional layer of security at runtime, obfuscate the application code and support data protection-compliant telemetry.

Having said that, and following the completion of a prior public procurement procedure, the Parties agree as follows:

## 1. Definitions

- 1.1 In this Agreement, the term "SDK" (Software Development Kit) refers to the mobile RASP component for iOS and Android (and, where applicable, other operating systems in the future) which fulfils the functional requirements set out in Clause 5.1 and in the specification of services, irrespective of the specific technology used.
- 1.2 The term "Backend" refers to any required server-side component to be operated on the Client's infrastructure.

- 1.3 The term “telemetry” refers to the security-related event data described in more detail in this Agreement, including the traceability of the policy version and the logging of triggered security rules with measures and unique identifiers.

## **2. Subject matter of the Agreement; order of precedence**

- 2.1 The components of the Agreement and legal bases – in order of precedence – are:
- the service description and any responses from the Client to tenderers’ queries;
  - the provisions of this Agreement;
  - the other (tender) documents underlying the procurement procedure;
  - the Licensor’s tender with its annexes, including the price list and the concept which formed the subject of the qualitative award criteria;
  - Contract Conditions for Services, Part B General Contract Conditions for the Performance of Services (VOL/B) – 2003 version – published on 5 August 2003 (BA<sup>nz</sup> No. 178a);
  - the statutory provisions of the German Civil Code (BGB).
- 2.2 The provisions of this Agreement shall apply exclusively. Any deviating, conflicting or supplementary provisions and general terms and conditions of the Licensor shall not apply.
- 2.3 Should the Client cease to exist in its current legal form, its legal successor shall – to the extent permitted by law – assume all rights and obligations under this Agreement. The respective obligations of both Parties under this Agreement shall continue unchanged. Furthermore, the Client is entitled to transfer its rights and obligations under this Agreement – following reasonable notice to the Licensor – to a subsidiary or sister company to be specifically named in the notice. In this case, the Licensor’s rights and obligations shall continue to apply unchanged vis-à-vis the named company.
- 2.4 The subject matter of this Agreement is the licensing and provision of a mobile Runtime Application Self-Protection (“RASP”) software component in the form of a SDK for iOS and Android (and, where applicable, other operating systems in the future) and, where applicable, an optional, supplementary backend component that can be operated on an infrastructure provided and controlled by the Client or its designated subcontractors. In this respect, the Licensor shall provide the services specified in the Service Description.
- 2.5 The scope of services may, by mutual agreement between the Parties, be supplemented or specified in more detail to include comparable services related to the scope of services as set out in clause 2.4 and the service description, provided that such services do not materially alter the original scope of services.

- 2.6 The SDK is to be operated both in standalone mode without a backend and, if optionally desired, in conjunction with a backend component.
- 2.7 No operational or security telemetry data shall be transmitted to systems operated or controlled by the Licensor, unless the parties expressly agree otherwise in writing.

### **3. Grant of Licence**

- 3.1 The Licensor grants the Client a non-exclusive, sub-licensable and transferable right to use, reproduce and integrate the SDK and, if desired by the Client, the backend into the Client's applications worldwide during the term of this Agreement, for the purpose of operating and protecting the Client's wallet applications in the context of the EUDI Wallet. The above license grant applies irrespective of the number of users and the type and number of the Client's wallet applications.
- 3.2 The right to reproduce is limited to the copies necessary for installation, operation, loading, display, execution, transmission and storage, as well as to necessary backup copies. The right to modify is limited to measures serving to maintain or restore the contractually agreed functionality. The right to decompile is granted exclusively within the scope and subject to the conditions of Sections 69e(1) and (2) of the German Copyright Act (UrhG).
- 3.3 Use is limited to the Client's EUDI Wallet Apps; the Client intends to publish the source code of its applications, whereby RASP-related calls will be removed from the publicly available code prior to publication.

### **4. Delivery and Operation**

- 4.1 The Licensor shall deliver the SDK with the accompanying documentation as an 'out-of-the-box' solution for iOS and Android no later than one (1) week after the Agreement is awarded.
- 4.2 If a backend is required, the Licensor warrants that this component can be operated on the Client's infrastructure or that of its designated subcontractors; at the same time, the Licensor warrants that the SDK supports standalone operation without a backend. Acceptance shall take place following successful integration and functional testing of the SDK and, where applicable, the backend against the specifications set out in this Agreement, and the Licensor undertakes to rectify any material deviations within the response and rectification periods agreed in this Agreement.

### **5. Functional requirements**

- 5.1 The Licensor warrants that the SDK
- detects runtime threats and responds appropriately by identifying the presence of hooking frameworks and active debugging attempts, and preventing manipulation of the application logic at runtime;

- detects the modification or re-signing of app packages and verifies the integrity of the distributed binary files;
- detects code modification and unauthorized changes and provides mechanisms for runtime integrity validation;
- detects the presence of rooted or jailbroken devices, as well as emulators and virtualized environments, and identifies compromised or high-risk device states;
- supports the obfuscation of sensitive logic, including RASP calls, and is compatible with common build tools;
- is provided as an 'out-of-the-box' solution, complete with accompanying documentation and a current Software Bill of Materials (SBOM).

5.2 If a backend is required: The licensor warrants that security policies are deployed dynamically and centrally without the need for app updates, whereby only predefined parameter ranges (guardrails) are modified, and that policy deployment is secure and signed to prevent tampering.

5.3 If a backend is required: The Licensor further warrants that the telemetry identifies the applicable policy version for each app instance or session and reports all triggered security rules as well as the respective enforcement action, including any app terminations, with the time, reason and a unique session or event ID, so that correlation, operational analysis and the investigation of false alarms are possible.

5.4 If a backend is required: The Licensor also undertakes that no telemetry data shall be transmitted to systems operated or controlled by the Licensor and that the operation of the telemetry shall take place on the Client's infrastructure, unless the parties expressly agree otherwise in writing.

5.5 The Licensor undertakes, upon request – no more than once per contract year and at the Licensor's expense – to provide, within a reasonable period of time, reliable evidence of penetration tests or equivalent security audits demonstrating that the SDK meets the above functional requirements and is hardened against attacks, and to document the scope and duration of the tests.

## **6. Non-functional requirements and compliance**

6.1 The Licensor declares that it and any subcontractors hold ISO/IEC 27001 or SOC2 Type 2 certification, or an equivalent information security management certification. The Licensor is obliged to provide evidence of this upon request and to maintain it throughout the term of the contract, or to ensure that subcontractors provide and maintain the relevant evidence.

6.2 In addition: The use of subcontractors not already named and approved in the quotation (in particular for support or development) requires the prior written consent of the Client. All

subcontractors must be subject to the same security standards (ISO 27001/SOC2, GDPR) as the Licensor itself.

- 6.3 The Client operates an ISO 27001-compliant Information Security Management System (ISMS). The Licensor is expected to actively support this compliance through appropriate measures.
- 6.4 The Client or a third party appointed by the Client and bound by a duty of confidentiality is granted the right to audit the Licensor's compliance with security requirements and its technical and organizational measures (including the backend) following prior notice.
- 6.5 Notwithstanding the provisions of Clause 7, the Licensor undertakes to disclose all categories of data processed by the SDK and, where applicable, the backend, and to ensure full support for GDPR compliance within the Client's environment.
- 6.6 The Licensor undertakes to support compliance, security assessment and testing processes by providing appropriate documentation and technical information required for independent security tests or audits.
- 6.7 Furthermore, the Licensor expressly grants the Client the right to include all programme code, including iOS, Android or other operating system applications as well as all integrated RASP components, in the Client's 'Bug Bounty' programme. The Client bears sole responsibility for the administration, management and implementation of the 'Bug Bounty' programme.

## **7. Data Protection**

- 7.1 The Licensor shall not process any personal data on behalf of the Client within the meaning of Article 28 of the GDPR under this Agreement.
- 7.2 The Client undertakes not to provide the Licensor with any personal (user) data and to configure the SDK, backend and telemetry in such a way that no personal data is transmitted to the Licensor and that all processing takes place exclusively within the infrastructure provided by the Client or its designated subcontractors.
- 7.3 The Client shall ensure that any information provided for support or fault analysis purposes is anonymised or otherwise processed in advance in such a way that the transmission of personal data is excluded, and the Licensor shall provide its services without processing personal data.
- 7.4 The parties clarify that, on the basis of the above provisions, no data processing relationship within the meaning of the GDPR is established between them. The parties confirm that the principles of data protection by design and by default are implemented.



## **8. Operation and Support**

- 8.1 The Licensor ensures the continuous receipt of security incidents twenty-four (24) hours a day, seven (7) days a week, guarantees a maximum initial response time of four (4) hours, and provides remedial measures or patches within forty-eight (48) hours, insofar as this is technically possible.
- 8.2 The Licensor shall ensure that security updates and the rectification of vulnerabilities are carried out within forty-eight (48) hours for critical vulnerabilities and within five (5) business days for high-severity vulnerabilities, and shall proactively notify the Client of newly identified security risks affecting the SDK or any backend components.
- 8.3 The Licensor shall ensure the ongoing compatibility of the SDK and any backend components with new major versions of the iOS and Android operating systems.
- 8.4 The Licensor shall appoint a dedicated technical contact person and provide structured escalation procedures for security-related incidents. The Licensor shall ensure regular maintenance releases and the continuous improvement of detection capabilities, performance and stability.
- 8.5 The Licensor undertakes to inform the Client immediately, and at the latest within twenty-four (24) hours, of any information security incidents within its own infrastructure or at its subcontractors (supply chain attacks) that could potentially compromise the services provided, the source code or the Client's data.

## **9. Remuneration and pricing structure**

- 9.1 The parties agree on a monthly flat-rate fee which covers all components necessary for the full provision of services in accordance with the service description.
- 9.2 The flat-rate remuneration includes, in particular:
  - Integration
  - Support
  - Maintenance
  - Upgrades/Hardening
  - an unlimited number of devices
  - an unlimited number of downloads
  - all features offered as per the service specification

- 9.3 All prices must be quoted in EUR (net) and include all applicable charges such as transport, travel and other costs necessary for the full provision of services and effective cooperation with the client.
- 9.4 The fee for the SDK is determined as a total monthly price per device tier in accordance with Section A of the 'Runtime Application Self-Protection (RASP) – Price List'; the total monthly costs apply as a flat rate per device tier. The SDK usage fee covers iOS and Android (as well as other operating systems in the future) equally, including all functionalities specified in the service description.
- 9.5 The number of apps installed on devices and protected by RASP, based on the relevant store KPIs, is decisive for classification into the device tier; no distinction is made between active and inactive devices; uninstalled devices are not counted. The applicable monthly price to be paid by the Client is calculated on the basis of the reference value at the end of the following month (last day, 23:59:59), in particular using the metrics "Active Device Installs" (Google Play Store) or "Opt-in Installations" (Apple App Store).
- 9.6 The fee for the optional backend is a fixed monthly price, regardless of the number of installed devices or the transaction volume, in accordance with Section B of the price list. The optional functionalities are listed separately in the price list as "Category 6 – Optional Functionalities".

## **10. Term and Termination**

- 10.1 This Agreement is initially concluded until 31 December 2028. The contract term commences upon conclusion of the Agreement.
- 10.2 The Client shall be entitled to extend the Agreement a maximum of two (2) times, each time for a term of twelve (12) months.
- 10.3 The Agreement shall be deemed terminated if and to the extent that the Client does not notify the Licensor three (3) months prior to the end of the contract term of its intention to extend the Agreement and to exercise the extension option. In the event of such notification, the contract term shall be extended by a further twelve (12) months in accordance with Clause 10.2; otherwise, the Agreement shall terminate at the next possible date.
- 10.4 Either party may terminate the Agreement during the term of the Agreement only for good cause, which exists where there are facts on the basis of which, taking into account all the circumstances of the individual case and the interests of both parties, the terminating party cannot reasonably be expected to continue the contractual relationship. Good cause shall be deemed to exist for the Client in particular if
- an application is made to open insolvency proceedings or comparable proceedings in respect of the Licensor's assets and this application is not withdrawn within six weeks, or a provisional insolvency administrator is appointed, or the opening of insolvency

proceedings is ordered, or the opening of such proceedings is refused due to lack of assets;

- the Licensor notifies that it will not be able to perform the services within the agreed time limits, unless the Licensor is not responsible for the delay;
- the Licensor repeatedly breaches any of the obligations set out in this Agreement or its annexes;
- the Licensor fails to fulfil the obligations under Clause 5 in conjunction with Clause 4 of this Agreement even after the expiry of a reasonable period for rectification;
- the financing relationship between the Federal Republic of Germany and the Client is terminated prematurely or is not continued in accordance with the contractual provisions of the financing agreement between the Federal Republic of Germany and the Client.

10.5 If the contractual relationship is terminated for good cause, the Licensor may demand partial remuneration commensurate with the services rendered to date.

## **11. Warranty**

The Licensor warrants that the functional and non-functional requirements described in this Agreement, including the recognition functions, the code protection measures, the dynamic policy provision (where a backend is required), telemetry (provided a backend is required), support service levels and compatibility maintenance, are met, and that no third-party rights preclude the contractual use of the RASP software component; the Licensor undertakes to rectify any deviations within the time limits specified in this Agreement (Clause 8).

## **12. Liability; Liability Insurance**

12.1 The Licensor shall be liable without limitation

- in cases of willful misconduct or gross negligence,
- for injury to life, limb or health,
- in accordance with the provisions (and to the extent) of the Product Liability Act,
- to the extent of a quality warranted by the Licensor and/or a guarantee assumed by the Licensor, and
- in other cases where liability is mandatory under law.

12.2 In the event of a breach of duty due to simple negligence, where such duty is essential to the fulfilment of the purpose of the Agreement (cardinal duty), the Licensor's liability shall be

limited in amount to the damage that is foreseeable and typical for the type of transaction in question.

- 12.3 Upon conclusion of the contract, the Licensor shall provide the Client with evidence that it holds insurance as required in the tender documents or as stated in the self-declaration. The Licensor shall maintain this insurance cover until the end of the contract. If the Licensor fails to fulfil this obligation, the Client shall be entitled to terminate the Agreement after setting a reasonable deadline which has expired without result, if it can no longer be reasonably expected to continue with the contract. Any further claims by the Client, in particular claims for damages, shall remain unaffected by this.

### **13. Confidentiality**

- 13.1 The parties undertake to keep the other party's confidential information strictly and unconditionally secret and to protect it by means of appropriate technical and organizational measures. This obligation shall continue after the termination of the contract.

- 13.2 Excluded from the above obligation is any confidential information

- which the recipient can prove was already known to them at the time of conclusion of the Agreement or which subsequently becomes known from a third party without thereby breaching a confidentiality agreement, statutory provisions or official orders;
- which is publicly known at the time of conclusion of the Agreement or is subsequently made public, provided this is not due to a breach of this contract;
- which must be disclosed due to legal obligations or by order of a court or public authority. To the extent permissible and possible, the recipient obliged to disclose shall inform the other party in advance and give it the opportunity to take action against the disclosure.

- 13.3 The Parties shall only grant access to confidential information to such advisers who are bound by professional secrecy or who have previously been subject to obligations corresponding to the confidentiality obligations of this contract. Furthermore, the parties shall only disclose the confidential information to those employees who need to know it for the performance of this Agreement, and shall also oblige such employees to maintain confidentiality for the period following their departure to the extent permitted under employment law.

### **14. Language, applicable law and jurisdiction**

- 14.1 The German language version of this Agreement is the legally binding version. In the event of any inconsistencies, this version shall therefore take precedence; this does not apply to the service description and other tender documents, which may also be provided in English in a binding form.

14.2 This Agreement is governed by the laws of the Federal Republic of Germany, to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG).

14.3 The parties agree that the courts at the Licensor's registered office shall have exclusive jurisdiction over all disputes arising out of or in connection with this Agreement, to the extent permitted by law.

## 15. Final Provisions

15.1 Upon termination of the Agreement, the Licensor shall immediately and without being asked return all documents, aids, materials or items received from the Client which were not permanently provided to it for the purpose of performing the Agreement in accordance with their intended use. This also applies to all copies. Furthermore, upon termination of the Agreement, all telemetry, log and support data (including aggregated data) remaining with the Licensor or its subcontractors must be irrevocably deleted, and proof of this must be provided to the Client. The Client is entitled to demand the secure deletion or destruction of such data, in whole or in part, in lieu of its return. Proof of this must be provided to the Client on request and, at the Client's discretion ( ), by means of a corresponding declaration or otherwise. Statutory retention obligations remain unaffected.

15.2 Amendments and additions to this Agreement must be in writing to be valid; this also applies to any amendment to this requirement for written form.

15.3 Should individual provisions of this Agreement be or become wholly or partially invalid or unenforceable, this shall not affect the validity of the remaining provisions; the invalid or unenforceable provision shall be replaced by a valid and enforceable provision whose effects come closest to the economic objective which the parties sought to achieve with the invalid or unenforceable provision. There are no ancillary agreements, and annexes do not form part of this Agreement.

_____	_____	_____
(Place)	(Date)	(Signature)

_____	_____	_____
(Place)	(Date)	(Signature)