

# Leistungsbeschreibung

## IT Security Consulting Services für EUDI-Wallet

### Table of Contents

<b>WER IST DIE SPRIND?</b> .....	<b>1</b>
<b>1. EINLEITUNG</b> .....	<b>1</b>
<b>2. BESONDERHEITEN DES PROJEKTKONTEXTES</b> .....	<b>2</b>
<b>3. LEISTUNGSBAUSTEINE</b> .....	<b>3</b>
3.1 SICHERE SYSTEMENTWICKLUNG FÜR MOBILE IDENTITÄTEN .....	3
3.2 COMPLIANCE ZU EIDAS 2.0 UND NATIONALE EIDAS-UMSETZUNG .....	4
3.3 NUTZBARKEIT FÜR SICHERE MOBILE IDENTITÄTEN .....	4
3.4 SONSTIGE IT SECURITY BEZOGENE ZUKUNFTSTHEMEN .....	5
<b>4. LIEFEROBJEKTE</b> .....	<b>5</b>
<b>5. ZUSAMMENARBEIT &amp; GOVERNANCE</b> .....	<b>6</b>
5.1 OPERATIVE ZUSAMMENARBEIT IM PROJEKT .....	6
5.2 INFORMATIONSSICHERHEIT & ISO 27001 KONFORMITÄT .....	7
5.3 AUDITIERUNGSRECHT (RIGHT TO AUDIT) .....	7
5.4 MELDEPFLICHTEN BEI SICHERHEITSVORFÄLLEN (INCIDENT MANAGEMENT SLAs) .....	8
5.5 VERTRAGSBEENDIGUNG / EXIT-STRATEGIE .....	8
<b>6. DATENSCHUTZ &amp; COMPLIANCE</b> .....	<b>8</b>

### Wer ist die SPRIND?

SPRIND, die Bundesagentur für Sprunginnovationen, ist eine Gesellschaft des Bundes und hat die Aufgabe, bahnbrechende Innovationen zu identifizieren, zu finanzieren und zu skalieren. Inspiriert von der amerikanischen DARPA ist ihr Hauptziel, agile und proaktive Unterstützung zu leisten, um Innovationen hervorzubringen, die unser Leben verändern.

### 1. Einleitung

Die EU Digital Identity Wallet (EUDIW) ist eine Initiative der Europäischen Kommission, die EU-Bürger:innen, -Einwohner:innen und -Unternehmen einen digitalen Ausweis und eine persönliche digitale Briefftasche (sog. EUDI Wallet) zur Verfügung stellen wird. Damit können europäische Bürger:innen, Einwohner:innen und Unternehmen sicher und einfach ihre Identität nachweisen,

wenn sie auf digitale Dienste zugreifen. Die Wallet-App wird es den Nutzer:innen ermöglichen, digitale Dokumente und Nachweise sicher zu erhalten, zu speichern und weiterzugeben sowie Dokumente elektronisch zu unterzeichnen bzw. mit einem Siegel zu versehen. So soll es z.B. möglich sein, die für die Eröffnung eines neuen Bankkontos, die Immatrikulation an einer Universität im Ausland oder die Bewerbung um einen Arbeitsplatz erforderlichen Dokumente bereitzustellen. Die Privatsphäre muss dabei stets gewahrt bleiben; die betroffene Person muss kontrollieren können, welche Daten weitergegeben werden und wer Zugang zu ihnen hat.

Die europäische Verordnung über die digitale Identität (EUDI) ermöglicht die digitale Transformation des öffentlichen Sektors und sorgt dafür, dass mehr Dienstleistungen digital zugänglich sind, auch grenzüberschreitend. Für Unternehmen wird es einfacher sein, Online-Dienste in ganz Europa anzubieten, da die EUDI Wallet eine sichere Authentifizierung bedeutet und jedem potenziellen Kunden bzw. jeder potenziellen Kundin in der EU zur Verfügung steht. Jeder Mitgliedstaat bietet mindestens eine Version der EUDI Wallet an, die nach denselben gemeinsamen Spezifikationen aufgebaut ist.

Die Bundesagentur für Sprunginnovationen - SPRIND GmbH (SPRIND) führt im Auftrag des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) das Projekt „EUDI Wallet Infrastruktur“ aus und entwickelt im Rahmen dieser Beauftragung die nationale EUDI Wallet für Deutschland sowie das Ökosystem.

Als Gegenstand dieser Vergabe sind Unterstützungsleistungen in den Bereichen Informationssicherheit sowie Usability Testing in Form einer Rahmenvereinbarung mit Einzelaufträgen ausgeschrieben. Die zu erbringenden Leistungen erfordern fundiertes Expertenwissen in beiden Bereichen und werden bedarfsgerecht und ohne Mindestabnahme von den relevanten Projektteams des Auftraggebers (AG) in Auftrag gegeben. Der Auftragnehmer (AN) erbringt **Beratungs-, Analyse-, Konzeptionierungs- und Unterstützungsleistungen** entlang des gesamten Entwicklungs- und Einführungszyklus der App und ihres Ökosystems, inklusive Dokumentation, Behördenkommunikation, Nutzer:innen-Interaktion und Qualitätssicherung.

Anmerkung: Im Verlaufe des ausgeschriebenen Projektes, wird der Auftraggeber von der SPRIND GmbH in eine frisch gegründete Tochter- oder Schwestergesellschaft übergehen. Die weitere Zusammenarbeit soll dabei uneingeschränkt weitergehen.

## 2. Besonderheiten des Projektkontextes

Die im Rahmen dieser Ausschreibung beschriebenen Leistungen erfordern ein hohes Maß an fachlicher Expertise im Bereich digitaler Identitäten, mobiler eID-Lösungen und der Umsetzung der eIDAS-Verordnung in Deutschland. Aufgrund der besonderen regulatorischen, technischen und organisatorischen Anforderungen legt der AG besonderen Wert auf praktische Projekterfahrung in vergleichbaren Vorhaben. Die nachfolgend beschriebenen Anforderungen an Referenzen und Mitarbeiterprofile dienen dem Nachweis dieser projektspezifischen Erfahrung.

Der Auftragnehmer hat sämtliche im Rahmen dieser Ausschreibung und der beschriebenen Leistungsbausteine geforderten Methoden, Verfahren und Fachkenntnisse durch geeignete Referenzen bzw. Referenzprojekte in den eingereichten Mitarbeiterprofilen nachzuweisen. Die Referenzen müssen einen unmittelbaren Bezug zu digitalen Identitätslösungen, EUDI-Wallets, eID-Systemen oder vergleichbaren Vorhaben im Kontext der eIDAS-Verordnung aufweisen.

Nachweise aus anderen fachlichen, regulatorischen oder branchenspezifischen Kontexten werden im Rahmen dieser Ausschreibung grundsätzlich nicht als gleichwertig angesehen und bei der Bewertung nicht berücksichtigt.

## 3. Leistungsbausteine

Der AG hat Leistungsbausteine definiert, in denen der AN bei der Konzeption, Entwicklung, Absicherung und kontinuierlichen Weiterentwicklung digitaler Identitätslösungen im Kontext der EUDI-Wallet unterstützen sollen. Der Schwerpunkt liegt auf der sicherheits- und datenschutzgerechten Gestaltung der technischen Architektur, der Erfüllung regulatorischer und normativer Anforderungen sowie der Förderung von Nutzbarkeit und Akzeptanz. Die Leistungen können sowohl strategische und konzeptionelle Tätigkeiten als auch die operative Begleitung von Entwicklungs-, Bewertungs- und Zertifizierungsprozessen umfassen.

### 3.1 Sichere Systementwicklung für mobile Identitäten

#### 3.1.1 Fortlaufende Risikoanalyse und Sicherheitskonzept

- Durchführung und Moderation einer entwicklungsbegleitenden Risikoanalyse der System- und Sicherheitsarchitektur (App & Ökosystem).
- Ableitung, Bewertung und Priorisierung von Maßnahmen zur Erreichung der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit, Datenschutz) in Form eines Sicherheitskonzepts.
- Pflege der Risikoanalyse und des Sicherheitskonzepts als lebende Dokumente (Versionierung, Änderungsmanagement) sowie bei Bedarf Anpassung an formelle Vorgaben, z.B. Security Targets oder Technische Richtlinien.

#### 3.1.2 Technischer Entwurf für die Architektur des Schwachstellenmanagement

- Unterstützung beim Entwurf einer technischen Zielarchitektur für das Schwachstellenmanagement auf mobilen Endgeräten (Android/iOS), inkl. Quellen-/Feed-Integration, Risikobewertung, Remediation-Prozessen und SLA-Definitionen.
- Integration in Sicherheitskonzept, Betriebsprozesse und Monitoring-/Telemetry-Landschaft.

#### 3.1.3 Dokumentation der Sicherheitsarchitektur und der kryptografischen Methoden

- Strukturierung und kontinuierliche Weiterentwicklung des Architekturkonzeptes (Funktional/Nicht-Funktional, Komponenten, Schnittstellen, Datenflüsse).
- Ausarbeitung der Sicherheitsarchitektur sowie Bewertung und Beschreibung der kryptographischen Verfahren (Algorithmen, Protokolle, Schlüsselmanagement, HSM/TEE/ eSE-Nutzung, Zertifikats-/Trust-Modelle).

#### 3.1.4 Begleitung der Entwicklung der technischen EUDI-Wallet Architektur hinsichtlich Umsetzung und Bewertung von Optionen

- Begleitung der Refinement- und Design-Phasen des Entwicklungsteams.
- Bewertung und Empfehlung von Umsetzungsoptionen (Build-/Runtime-Security, Hardening, Secure Storage, Secure Channel, Trusted UI, Anti-Tamper, Jailbreak/Root-Detection).

- Unterstützung bei der Umsetzung sicherheitstechnischer Funktionen wie Key Attestation, App Attestation, Plattform/Device Attestations und Remote Integrity Checking.

## 3.2 Compliance zu eIDAS 2.0 und nationale eIDAS-Umsetzung

### 3.2.1 Fortlaufende Konformitätsanalyse der Architektur

- Abgleich der Ziel- und Ist-Architektur gegen die Anforderungen der TR-03107-1.
- Erstellung einer Konformitätsmatrix inkl. Evidenzen, GAP-Analyse und Maßnahmenplan, sowie kontinuierliche Anpassung.
- Vorbereitung der Bewertung durch das BSI, via Unterstützung bei z.B. der Erstellung von Unterlagen, Anfertigung von Nachweisen oder Testkonzepten sowie bei der Zusammenarbeit mit dem beauftragten Prüflabor.

### 3.2.2 Begleitung und Unterstützung beim Austausch mit sicherheits- und datenschutzrelevanten Stakeholdern

- BSI (TR-03189, Schwachstellenmanagement), BFD und DSB (Datenschutzrisiken)
- Strukturierte Begleitung des Austauschs mit BSI (TR-03107-1, Mobile-Vulnerability-Management, BSZ bzw. EUCC Zertifizierung), mit BfDI und dem behördlichen DSB (Datenschutzrisiken, DSFA-Anforderungen).
- Erstellung von Entscheidungs- und Freigabeunterlagen, Teilnahme an Reviews/Workshops.

### 3.2.3 Begleitung von Bewertungs- und Zertifizierungsprozessen

- Begleitung von Bewertungs- und Zertifizierungsprozessen (z.B. BSI BSZ, FITCEM, EUCC) einschließlich Dokumentation für Evaluierung- und Zertifizierungsprozesse wie z.B. Security Targets
- Unterstützung bei der Abstimmung von Security Targets (ST) für z.B. WSCA/WSCD bzw. App oder anderen Komponenten

## 3.3 Nutzbarkeit für sichere mobile Identitäten

### 3.3.1 Durchführung von qualitativen und quantitative Nutzer- und Akzeptanzstudien

- Einbringung der bisherigen Erkenntnisse aus vorangegangenen Projekten im Kontext digitaler Identitäten und Wallet.
- Expertenreview und Validierung der erstellten Wireframes und finalen Screendesigns nach relevanten ISO-Normen und Standards hinsichtlich Verständlichkeit, Nutzungsbereitschaft und Nutzervertrauen.
- Vorbereitung, Durchführung und iterative Evaluierung der Wireframes und finalen Screens mittels Nutzerstudien.

### 3.3.2 Analyse von Barrierefreiheit in den Endnutzeranwendungen

- Expertenreview und Validierung der Barrierefreiheit für die Plattformen iOS und Android.
- Vorbereitung, Durchführung und Evaluierung der Barrierefreiheit mittels Nutzerstudien für die Plattformen iOS und Android.

### 3.4 Sonstige IT Security bezogene Zukunftsthemen

Über die beschriebenen Leistungsbausteine hinaus kann der Auftraggeber den Auftragnehmer bei Bedarf mit der Erbringung weiterer Beratungs- und Unterstützungsleistungen im Bereich der Informationssicherheit beauftragen. Voraussetzung hierfür ist, dass der Auftragnehmer über die erforderliche fachliche Expertise verfügt und die angefragten Leistungen mit geeignetem Personal erbringen kann. Die nachfolgenden Themenfelder stellen mögliche Einsatzbereiche dar und sind nicht abschließend.

Der Auftraggeber kann den Auftragnehmer zur Unterstützung des im Aufbau befindlichen Security Operations Centre (SOC) anfragen, um bei der Reaktion auf und der Eindämmung von Cybersicherheitsvorfällen und -ereignissen, auch kurzfristig, sowie bei der Ausarbeitung einer Strategie zur Schadensbegrenzung unterstützend tätig zu werden.

Der Auftragnehmer kann den Auftraggeber bei der Analyse, Bewertung und Einführung moderner Sicherheits-, Datenschutz- und Kryptografietechnologien unterstützen. Dies umfasst insbesondere Konzepte und Architekturen auf Basis von Differential Privacy, Zero-Knowledge-Verfahren und Zero-Trust-Architekturen sowie deren Integration in bestehende Sicherheitskonzepte und Systemarchitekturen. Darüber hinaus können Leistungen die Analyse und Bewertung kryptografischer Verfahren, die Einführung quantencomputerresistenter Kryptografie und Maßnahmen zur Kryptoagilität sowie die Konzeption, Bewertung und Absicherung von Machine-Learning-Verfahren mit besonderem Fokus auf Informationssicherheit, Datenschutz und den Schutz sensibler Daten umfassen.

## 4. Lieferobjekte

Der Auftraggeber kann im Rahmen der jeweiligen Leistungsbausteine die Erstellung und Übergabe von Arbeitsergebnissen verlangen. Die konkreten Liefergegenstände richten sich nach der jeweiligen Aufgabenstellung und können insbesondere, jedoch nicht abschließend, folgende Artefakte umfassen:

- Risikoanalyseberichte sowie fortlaufend aktualisierte Sicherheitskonzepte,
- Konformitätsanalyse zur Technischen Richtlinie TR-03107-1 einschließlich GAP-Analyse und Maßnahmenplan,
- Architektur- und Kryptodokumentationen einschließlich Datenfluss- und Sequenzdiagrammen,
- Zielbilder für das Vulnerability Management mobiler Anwendungen sowie zugehörige Betriebs- und SLA-Konzepte,
- technische Design Reviews, Attestation-Guides und Hardening-Guidelines,
- Protokolle, Ergebnisdokumentationen und weitere Unterlagen aus Abstimmungen mit Behörden und sonstigen Stakeholdern,
- Erstellung von Sicherheitsprofilen (Security Targets) und weiteren zugehörigen Dokumenten oder fachkundige Beratung bei deren Erstellung.

Die Dokumentation der Aufgabenstellung, die Festlegung von Qualitäts- und Abnahmekriterien sowie die Übergabe der Liefergegenstände erfolgen grundsätzlich über das vom Auftraggeber bereitgestellte Ticketsystem (z. B. Jira). Bei Bedarf kann der Auftraggeber darüber hinaus Handover-Workshops sowie ergänzende Dokumentationen verlangen, die über die eigentlichen

Liefergegenstände hinausgehen. Diese sind im Wissensmanagementsystem des Auftraggebers oder in einem vom Auftraggeber vorgegebenen alternativen Werkzeug bereitzustellen.

## 5. Zusammenarbeit & Governance

### 5.1 Operative Zusammenarbeit im Projekt

Der Auftraggeber arbeitet in einem agilen Projektrahmen mit zweiwöchigen Sprints, in dem festgelegte Prozesse den inhaltlichen Austausch von der Arbeitsplanung bis zur Abnahme von Arbeitspaketen strukturieren. Der Auftragnehmer ist verpflichtet, sich in diesen Arbeitsrhythmus einzufügen und bedarfsgerecht an den zugehörigen Terminen und Prozessschritten — einschließlich Sprint Refinement, Planning, Review und gegebenenfalls weiteren Regelformaten — aktiv teilzunehmen. Die Erfassung, Beschreibung und Nachverfolgung von Arbeitspaketen (= Einzelaufträgen) sowie die Dokumentation von Arbeitsfortschritten erfolgen, wenn nicht anders vereinbart, über das Ticket-System der Auftraggeberin. Der Auftragnehmer ist gehalten, dieses System vollständig und zeitnah zu nutzen und den aktuellen Bearbeitungsstand seiner Aufgaben darin kontinuierlich zu aktualisieren.

Der Auftraggeber strebt darüber hinaus eine effiziente und bedarfsorientierte Zusammenarbeit mit dem Auftragnehmer an. Daher und zur Verbesserung der Planbarkeit hat der Auftraggeber ein Mindestmaß an Kooperationsformaten definiert. Bei Bedarf können die Parteien vereinbaren, diese Liste zu ergänzen:

- **(Regelmäßige) Abstimmung:** Die Auftraggeberin kann Abstimmungsgespräche zwischen dem Auftragnehmer bzw. der Auftragnehmerin und dem Product Owner (PO) der Auftraggeberin und/ oder weiteren Teammitgliedern verlangen, um den Status quo und wesentliche Probleme zu bewerten und Auswirkungen auf den Zeitplan zu besprechen. Die Abstimmung erfolgt bedarfsgerecht und remote auf Basis einer Videokonferenz-Einladung der Auftraggeberin.
- **Beratungssitzungen:** Mitglieder des EUDI-Wallet Projektes der Auftraggeberin sind berechtigt, sich an den Auftragnehmer zu wenden und Beratungssitzungen zu jeder Gelegenheit zu vereinbaren, sofern keine Budgetbeschränkungen bestehen. Beratungssitzungen finden remote auf Basis einer Videokonferenz-Einladung der Auftraggeberin statt.
- **Workshops vor Ort:** Die Auftraggeberin veranstaltet Workshops in Form von internen Team-Tagen, aber auch externe Workshops im Zusammenhang mit Sicherheitsbewertungen, zu denen die Teilnahme des Auftragnehmers bzw. der Auftragnehmerin gewünscht sein kann. Die Auftraggeberin informiert rechtzeitig über anstehende Workshops vor Ort, sofern die Teilnahme des Auftragnehmers bzw. der Auftragnehmerin erforderlich ist.

Darüber hinaus bilden die nachfolgend aufgeführten Grundsätze die verbindliche Basis der Zusammenarbeit zwischen Auftraggeber und Auftragnehmer. Sie dienen der gemeinsamen Steuerung der Leistungserbringung und schaffen einen verlässlichen Rahmen:

- **Verfügbarkeit:** Es wird erwartet, dass der Auftragnehmer bzw. die Auftragnehmerin jeweils für jeden Folgemonat auf Stundenbasis verfügbar ist, wobei der Umfang im Voraus mit dem Auftraggeber abgestimmt wird. Als Ausgangspunkt vereinbaren Auftraggeberin und Auftragnehmer:in in einem Kick-off-Meeting, das die Zusammenarbeit einleitet, einen Rahmen. Es wird erwartet, dass die Arbeitszeiten jederzeit transparent sind.



- **Zeiterfassung:** Es wird erwartet, dass der Auftragnehmer bzw. die Auftragnehmerin seine Arbeitszeiten erfasst und der monatlichen Rechnung eine Stundenaufstellung beifügt.
- **Budgetierung:** Um den budgetierten Betrag nicht zu überschreiten, müssen sich der Auftragnehmer bzw. die Auftragnehmerin regelmäßig mit der zuständigen Ansprechperson der Auftraggeberin über das verbleibende Budget abstimmen. Abgerechnete Arbeitsstunden, die über den budgetierten Betrag hinausgehen, werden nicht vergütet.
- **Sprache:** Für das Vergabeverfahren ist deutsch die maßgebliche Sprache. Im Projekt, sowie im Austausch mit den externen Stakeholdern, wird vom Auftragnehmer ein Austausch in englischer und deutscher Sprache erwartet.

Der Auftragnehmer legt zu Beginn der Zusammenarbeit einen Single-Point-of-Contact (SPOC) fest, der dem Auftraggeber für die Abstimmung und Steuerung administrativer Themen zur Verfügung steht. Der Auftraggeber präferiert darüber hinaus ein schlankes Team auf Seiten des Auftragnehmers, um Abstimmungsbedarfe zu reduzieren. Die Durchführung von ausgewählten Aufgaben durch weitere Teammitglieder im Backoffice des Auftragnehmers sind möglich. Die individuellen Referenzen und Tagessätze für alle im Projekt eingesetzten Teammitglieder des Auftragnehmers müssen angegeben werden, Details siehe Anlagen.

Die Bieterangabe im Preisblatt hat alle erforderlichen Kosten (Reise-, Personal-, Sach-, Nebenkosten) über die gesamte Vertragslaufzeit zu enthalten. Reisekosten werden nicht erstattet. Die anzugebenden Tagessätze gelten für die gesamte Vertragslaufzeit für alle Beschäftigten der Bieterin oder des Bieters. Dabei wird zwischen Arbeiten in den oben genannten Leistungsbausteinen unterschieden. Für die in 3.4 Sonstige IT Security bezogene Zukunftsthemen genannten Themenbereiche wird der Tagessatz des Leistungsbausteine „Sichere Systementwicklung für mobile Identitäten“ zugrundegelegt.

## 5.2 Informationssicherheit & ISO 27001 Konformität

- Der Auftraggeber (SPRIND / zukünftiger Tochter- oder Schwestergesellschaft) unterhält ein Information Security Management System (ISMS) nach ISO/IEC 27001. Der Auftragnehmer verpflichtet sich, den Auftraggeber bei der Aufrechterhaltung der Konformität aktiv zu unterstützen und eigene Geschäftsprozesse so zu gestalten, dass sie nicht im Widerspruch zu dieser Norm stehen.
- Der Auftragnehmer muss eine ISO 27001 oder vergleichbare Zertifizierungen (z.B. SOC 2) besitzen und die entsprechenden Zertifikate sowie Management Summaries von Überwachungsaudits dem Auftraggeber unaufgefordert jährlich bereitstellen.

## 5.3 Auditierungsrecht (Right to Audit)

- Der Auftraggeber ist berechtigt, die Einhaltung vertraglicher und sicherheitsrelevanter Vorgaben beim Auftragnehmer durch eigene Audits oder durch vom Auftraggeber beauftragte Dritte zu überprüfen.
- Der Auftragnehmer verpflichtet sich, auf Anfrage des Auftraggebers regelmäßig (mindestens jährlich) detaillierte Performance- und Compliance-Reports (inklusive Nachweisen zur Informationssicherheit) zur Verfügung zu stellen.

## 5.4 Meldepflichten bei Sicherheitsvorfällen (Incident Management SLAs)

- Der Auftragnehmer ist verpflichtet, jegliche Sicherheitsvorfälle (Security Incidents), die direkte oder indirekte Auswirkungen auf die Vertraulichkeit, Integrität oder Verfügbarkeit der Dienstleistungen, Daten oder Infrastruktur des Auftraggebers haben könnten, unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden dem Auftraggeber zu melden.
- Der Auftragnehmer kooperiert vollumfänglich und transparent mit dem Auftraggeber bei der Untersuchung, Eindämmung und Behebung des Vorfalles.

## 5.5 Vertragsbeendigung / Exit-Strategie

- Der Auftraggeber behält sich das Recht zur außerordentlichen Kündigung vor, wenn der Auftragnehmer Performance-Ziele wiederholt verfehlt, gegen wesentliche Vertrags- oder Sicherheitsbedingungen (inklusive DSGVO) verstößt oder ein andauerndes Risiko für die Informationssicherheit des Auftraggebers darstellt.

# 6. Datenschutz & Compliance

Der Auftragnehmer hat bei der gesamten Leistungserbringung die Prinzipien von Privacy by Design und Privacy by Default zu berücksichtigen und aktiv in seine Arbeitsergebnisse einzubetten. Datenschutzerfordernungen sind demnach nicht nachgelagert, sondern von Beginn an als integraler Bestandteil der jeweiligen Lösung zu konzipieren.