Abschlussprüfung Sommer 2022
1201

1 Planen eines Softwareproduktes

Fachinformatiker
Fachinformatikerin
Anwendungsentwicklung (AO 2020)

Teil 2 der Abschlussprüfung Bearbeitungshinweise

Die Aufgaben 1 bis 4 beziehen sich auf die folgende Ausgangssituation:

Der Energieversorger Wind und Sonne AG möchte den Prozess zur Strom-Abrechnung weiter digitalisieren. Innerhalb dieses Projekts sollen mehrere Apps entwickelt werden. Dabei sollen Sie bei der Planung, Umsetzung und Einführung mitarbeiten und unterstützen.

4. Aufgabe (25 Punkte)

Um für die App einen Support bereitstellen zu können, soll ein Ticketsystem eingeführt werden. Der Energieversorger stellt daher das Ticketsystem auf einem Webserver zur Verfügung.

a) Erläutern Sie drei Vorteile und einen Nachteil beim Einsatz eines Ticketsystems. 12 Punkte

Vorteile eines Ticketsystems:

1. **Effiziente Verfolgung:** Strukturierte Erfassung und Verfolgung von Anfragen für eine effiziente Lösung.

2. **Ressourcenallokation:** Optimierte Zuweisung von Aufgaben und Ressourcen, um die Arbeitslast zu verteilen.

3. **Verbesserte Kommunikation:** Transparente Kundenbetreuung durch klare Kommunikation und Statusverfolgung.

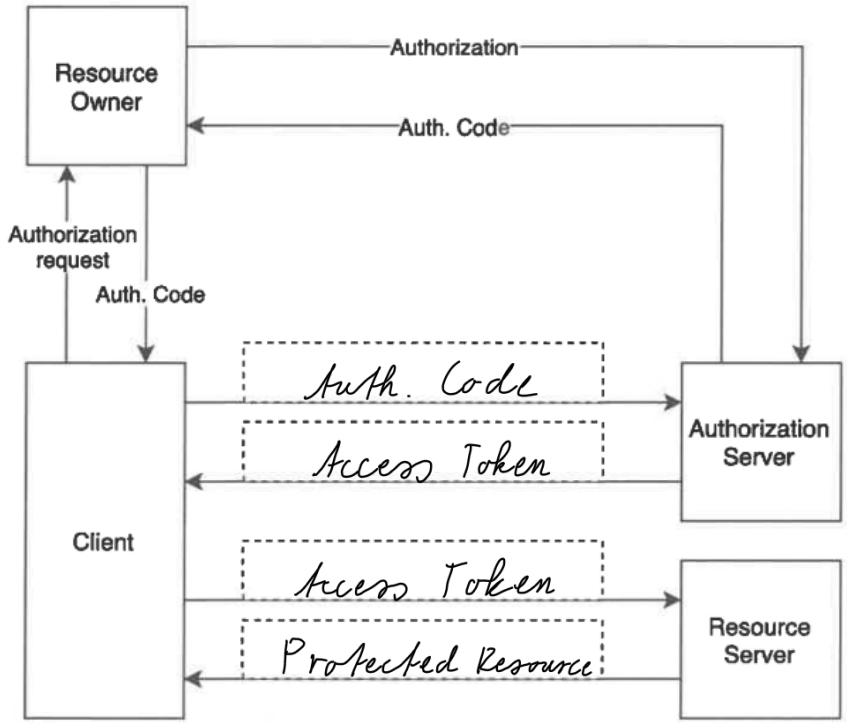
Nachteil eines Ticketsystems:

1. **Einführungskosten:** Initiale Kosten für Software, Schulungen und Anpassungen können für kleinere Organisationen eine Hürde darstellen.

b) Das Ticketsystem verwendet zum Login OAuth2. Dazu liegt Ihnen die nachfolgende Grafik vor, die den Autorisierungs-Prozess beschreibt.

Ordnen Sie die folgenden Begriffe den korrekten Positionen in der Grafik zu, damit der Prozess vollständig beschrieben ist:
- Access Token
- Protected Resource
- Auth. Code

Hinweis: Einer dieser Begriffe muss doppelt verwendet werden. 4 Punkte



Fortsetzung 4. Aufgabe →

Fortsetzung 4. Aufgabe

c) Um Datensicherheit und Datenschutz zu gewährleisten, soll der Webserver, auf dem das Ticketsystem installiert werden soll, mit einem Secure Sockets Layer (SSL)-Zertifikat gesichert werden.

Erläutern Sie drei Sicherheitsmechanismen, die durch den Einsatz von SSL-Zertifikaten erreicht werden. 9 Punkte

1. **Verschlüsselung:** SSL-Zertifikate verschlüsseln die Datenübertragung zwischen dem Webserver und dem Browser, schützen so vor Abfangen und Lesen durch Unbefugte.

2. **Authentifizierung:** SSL-Zertifikate ermöglichen die Überprüfung der Website-Identität, da sie von vertrauenswürdigen Certificate Authorities ausgestellt werden, was das Vertrauen der Benutzer stärkt und Phishing-Angriffe erschwert.

3. **Integrität:** Durch kryptografische Hash-Funktionen sichern SSL-Zertifikate die Integrität der übertragenen Daten, indem sie sicherstellen, dass die Informationen unverändert und authentisch beim Empfänger ankommen.

Kommunikation zwischen Client und Server ist Verschlüsselt.