

#### 4. Aufgabe (25 Punkte)

Korrekturrand

- a) Um Daten zwischen der Client-Anwendung und dem Server nicht unverschlüsselt zu übertragen, wird vom Projektleiter vorgeschlagen, diese mit dem Lizenzschlüssel der Software zu verschlüsseln.

aa) Beschreiben Sie das oben dargestellte Verschlüsselungsverfahren.

2 Punkte

Beim oben genannten Verfahren handelt es sich um eine Symmetrische Verschlüsselung, da beide den gleichen Schlüssel für ver- und entschlüsseln nehmen. Nachteil dabei ist, dass der Austausch des Schlüssels nicht sicher ist.

- ab) Beschreiben Sie ein alternatives Verschlüsselungsverfahren mit jeweils einem Vor- und Nachteil, welches die zuvor genannten Probleme löst.

6 Punkte

Asymmetrisches Verschlüsselungsverfahren, bei dem Jeder Nutzer einen Privaten und Öffentlichen Schlüssel besitzt. Der öffentliche Schlüssel kann ohne Bedenken an das Gegenüber gegeben werden. Das Gegenüber benutzt diesen öffentlichen Schlüssel zum Verschlüsseln, dieses Verschlüsselte kann nur durch den geheimen privaten Schlüssel entschlüsselt werden.

Sicherer eine Verschlüsselte Kommunikation aufzubauen, jedoch ist diese Kommunikation viel langsamer, da das ver- und entschlüsseln länger dauert.

- b) Bei Ihrem Test der Client-Anwendung bekommen Sie beim Start die Meldung „Das Programm stammt aus einer nicht vertrauenswürdigen Quelle. Wollen Sie dieses Programm trotzdem öffnen?“

ba) Beschreiben Sie, was diese Meldung bedeutet.

2 Punkte

Das Programm wurde beim Kompilieren nicht signiert.

- bb) Beschreiben Sie, wie Sie das Problem durch eine Änderung in den Kompilierungs-Einstellungen beheben können. 2 Punkte

Um das Problem zu beheben, müssen beim Kompilieren die Dateien signiert werden. Das hierfür verwendete Zertifikat wird üblicherweise vom Hersteller des Betriebssystems ausgestellt.

c) Die Geschäftsführung Ihres Unternehmens beauftragt Sie, sich über Möglichkeiten zur Qualitätssicherung von Software zu informieren und Vorschläge zu unterbreiten.

Korrekturrand

ca) Bei Ihrer Recherche finden Sie die ISO Normen 9126 und 25010, welche Qualitätsmerkmale von Softwareanwendungen beschreiben. Zwei der darin beschriebenen Merkmale sind „Effizienz“ und „Änderbarkeit“.

Beschreiben Sie, was unter diesen beiden Qualitätsmerkmalen zu verstehen ist.

4 Punkte

Effizienz:

Die erwartete Ausgabe des Programms soll mit möglichst wenig Rechenleistung erreicht werden. Je effizienter die Software arbeitet, umso größer ist die Bandbreite möglicher Hardwareunterstützung (bezogen auf Hardware Ressourcen).

Änderbarkeit:

Änderbarkeit ist die Möglichkeit, die Software durch individuelle Programmierung zu verändern. Je strukturierter eine Software aufgebaut ist, umso einfacher ist die spätere Änderbarkeit.

cb) Aus Ihrem Projektteam kommt der Vorschlag, zur Qualitätssicherung ausschließlich automatische Code-Reviews und Unit-Tests einzusetzen.

Nehmen Sie Stellung zu diesem Vorschlag und begründen Sie fachlich Ihren Standpunkt.

5 Punkte

d) Sie schlagen Ihrem Projektteam vor, zusätzlich für jeden Release einen Black-Box- und White-Box-Test durchzuführen.

Beschreiben Sie diese beiden Testarten.

4 Punkte

Black-box-test:

Funktionstest, erfordert keine Kenntnis über die innere Funktion der Software. Dieser Test wird von Anwendern durchgeführt, welche an der Entwicklung nicht beteiligt waren.

White-box -Test:

Setzt Kenntnisse über inneren Aufbau und der Funktion der Software voraus. Wird von Entwicklerteam durchgeführt.

## PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

- ☐ 1 Sie hätte kürzer sein können.
- ☐ 2 Sie war angemessen.
- ☐ 3 Sie hätte länger sein müssen.

