Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

Abteilung Zürich

Studiengang Informatik der ZHAW am Standort Zürich

Aufgabenstellung Semesterarbeit

Thema:	**Entwicklung eines Software-Moduls zur Verifikation von Einmal-passwörtern**
Studierende(r):	A. Muster, InformatikstudentIn im Bachelorstudiengang Informatik
Betreuungsperson:	Giovanni Serafini, Dozent für Angewandte Kryptografie
Ausgangslage: (inkl. Randbedingungen)	Die Firma XXX AG hat im vergangenen Jahr eine Authentifizierungs-Lösung entwickelt, die dann eingesetzt werden kann, wenn eine starke Authentifizierung der Benutzer erforderlich ist. Die Applikation bietet heute bereits die Prüfung von zwei (und mehr) Merkmalen an, um Benutzer zu authentifizieren. Die starke Authentifizierung basiert dabei auf zwei Schritten: Zuerst werden Benutzername und Passwort geprüft. In einem zweiten Schritt wird dem Benutzer ein serverseitig generiertes Einmalpasswort (One Time Password, OTP) per SMS zugestellt, das er zusätzlich bestätigen muss. Erst wenn dieses erfolgreich geprüft wurde, gilt der Benutzer als authentifiziert und erhält Zugang zum gewünschten System. Die Firma XXX AG möchte die bestehende Authentifizierungs-Lösung nun um ein weiteres Modul zur Prüfung von OTPs erweitern. Dabei sollen die OTPs offline auf den Smartphones der Benutzer generiert werden. Der Versand über SMS entfiele somit. Die Implementierung soll gemäss den Standards der „Initiative for Open Authentication“ (OATH) erfolgen. Das Investment-Compliance-Modul (IC-Modul) ist der Hauptanwender der Business Rule-Engine. Im IC-Modul können die Fondsverwalter die gesetzlichen und vertraglichen Richtlinien für ihre Investments prüfen. Diese Richtlinien wurden über Business Rules formuliert und werden täglich geprüft. Bei dieser Investment-Compliance-Prüfung treten Performance-Probleme auf, die auf die Laufzeit der Ausführung von einigen Business Rules zurückzuführen sind. Eine Analyse der Business-Rules-Entwicklungsabteilung hat ergeben, dass essich um ein konzeptionelles Problem handelt, da mit den vorhandenen Sprachkonstrukten der Rule-Engine diese Regeln nicht effizient definiert werden können.
Ziel der Arbeit: (inkl. Abgrenzungen)	Das Ziel der Semesterarbeit besteht in der Konzeption und der Entwicklung eines Java-basierten Software-Prototyps zur Verifikation von OTPs, die offline auf dem Smartphone des Benutzers generiert werden. Innerhalb einer Testumgebung soll der neue Authentisierungsvorgang funktional verifiziert werden. Zudem sollen theoretische Grundlagen zur Authentifizierung über OTPs untersucht und zusammengestellt werden.

Aufgabenstellung:

Im Rahmen dieser Semesterarbeit werden von der Studentin bzw. vom Studenten folgende Aufgaben durchgeführt:

1. Studie der heute verbreiteten Verfahren zur Generierung/Verifizierung von OTPs.
2. Durchführen einer Analyse über Stärken, Schwächen und Einsatzmöglichkeiten der einzelnen Verfahren.
3. Durchführen einer Anforderungsanalyse für den Software-Prototyp.
4. Auswahl eines Verfahrens zur Implementierung.
5. Konzeption und Spezifikation eines Software-Prototyps, der die ermittelten Anforderungen erfüllt.
6. Implementieren des Software-Prototyps.
7. Verifikation des Software-Prototyps in der Testumgebung und Protokollieren der Ergebnisse.
8. Präsentation des Software-Prototyps.

Erwartete Resultate:
nen (je Teilaufgabe)

Im Rahmen dieser Semesterarbeit werden folgende Resultate für die einzel-Teilaufgaben erwartet:

1. Detaillierte Beschreibung der heute verbreiteten Verfahren zur Generierung/Verifizierung von OTPs.
2. Analyse über Stärken, Schwächen und Einsatzmöglichkeiten der einzelnen Verfahren.
3. Anforderungsanalyse des Software-Prototyps.
4. Dokumentierte Auswahlkriterien für das gewählte Verfahren.
5. Beschreibung der Spezifikation des Software-Prototyps.
6. Lauffähiger Software-Prototyp (kompilierte Form).
7. Dokumentierte Testfälle.
8. Vorbereitete Demonstrationsumgebung.

Geplante Termine:

Kick-Off-Meeting
Design-Review
Abschlusspräsentation

Anmerkung zum Zweck des Dokuments:

Es dient als erstes Arbeitspapier/erste Anleitung für die Absprache des Themas der Aufgabenstellung mit der Betreuungsperson – anschliessend erfolgt die Erfassung und jeweilige Anpassung der Aufgabenstellung direkt in EBS!