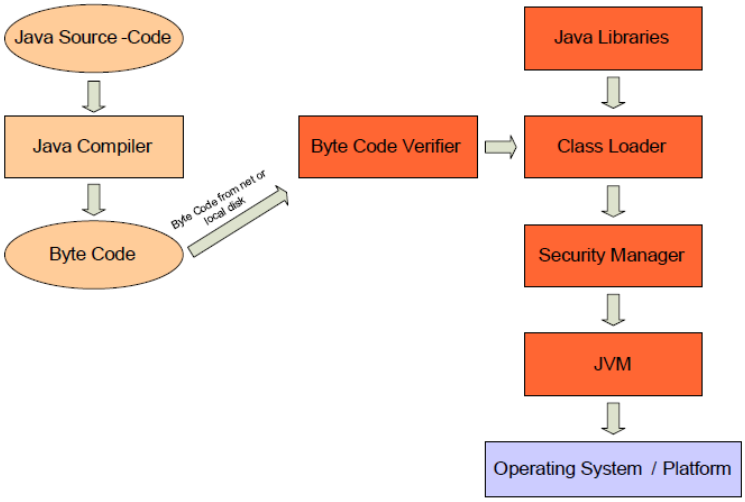
Survey Java Security

1. Wie überprüft die Java Plattform sicherheitstechnisch die Ausführung des Java Codes?



- *Java Interpreter überprüft Class File: See 0xCAFEBABE in .class*

(Folie 14)

2. Welche Sicherheit bietet der Java Class Loader?
   - *Class Loader und Namespaces*
   - *Trusted Class Libraries*
   - *Protection Domains*

   (Folie 16)

3. Was ist eine protected Domain?

   Jede Klasse wird einmalig bei ihrer Erzeugung einer ProtectionDomain zugeordnet
   Eine Protection Domain ist eine Zuordnung von Rechten zu bestimmten Code (CodeSource, Principal)
   Kann während der Lebenszeit einer Klasse nicht mehr geändert werden
   Kapselt CodeSource, Principal array, ClassLoader und PermissionCollection
   (Folie 19)

4. Worauf baut die Java Programmiersprache ihre Sicherheit auf?
   - *Keine Pointer sondern Objektreferenzen*
   - *Virtuelle Maschine - überwacht Programmausführung und Rechte*
   - *Strenge Typisierung*
   - *private, protected, package, public (Sichtbarkeiten)*
   - *Exceptions - definierte und kontrollierte Programmabbrüche*
   - *Strenge Arraygrenzen - kein Zugriff auf benachbarte Entitäten*

   (Folie 13)

5. Was ist JAAS?

   Java Authentication and Authorization Service
   - *Einführung eines Benutzerzentriertes Sicherheitsmodels!*
   - *Einführung eines deklaratives Sicherheitsmodels!*
   - *Java Platform Security – Zugriffskontrolle nach Herkunft des Codes (Codezentriertes Sicherheitsmodell)*
   - *Erweiterung der Java Platform Security mit JAAS (Benutzerzentriertes Sicherheitsmodell - vgl. Betriebssystem)*

- *JAAS ist für Multiuser-Applikationen wichtig*
- *JAAS ist die Standardimplementierung des JEE-deklarativen Sicherheitsmodells*

(Folie 29ff)

6. Erklären Sie deklarative und programmatische Sicherheit!

Deklarative Security

Im DD wird definiert wer auf welche EJB und/oder welche Methoden zugreifen kann oder welche URL aufrufen darf.

Programmatische Security

Innerhalb der Bean-Implementation kann auf die Identity zugegriffen werden, damit Context-spezifische Security angewendet werden kann

Deklarative und Programmatische Security werden typischerweise zusammen verwendet

Deklarative Security hat die höhere Priorität gegenüber der programmatische Security!

(Folie 37)

7. Welche Ziele verfolgen die Java EE Sicherheit Spezifikationen?

Portabilität:

„Write Once, Run Anywhere“

Transparenz:

Applikationsentwickler müssen keine tiefgründigen Kenntnisse über Security haben um ihre Applikationen zu entwickeln

Isolation/ Abstraktion:

Trennung von Business und Security – Der Deployer kann die Sicherheit hinzufügen

Erweiterbarkeit:

Die Portabilität der Applikation wird durch die Einbindung von Sicherheits-Services nicht behindert

Unabhängigkeit:

Die Einbindung von verschiedenen Sicherheitstechnologien soll möglich sein

(Folie 34)

8. Was ist ein Realm?

Realm, Wiki sagt: Realm steht im Englischen für Reich, Bereich, Domäne.

- *komplette „Datenbank“ mit Usern und Gruppen (Webapplikation)*
- *identifiziert valide User einer Applikation*

Realm-Typen:

- *File-Realm*
- *Certificate-Realm*
- *LDAP-Realm*
- *etc*

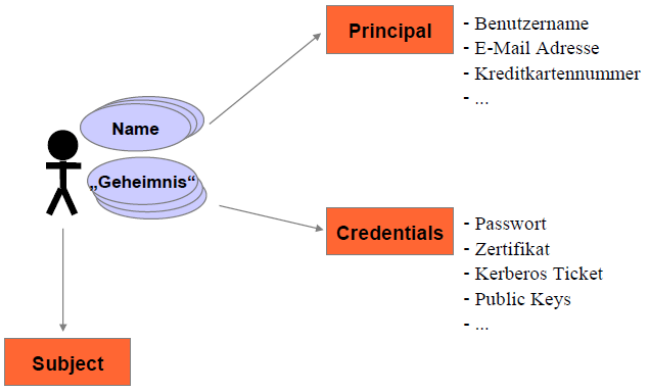
Bei einem Realm Wechsel wird das „Ziel“ gegen welches ein User autorisiert wird ausgetauscht.

(Folie 38)

9. Was sind die wichtigsten Objekte im JAAS?

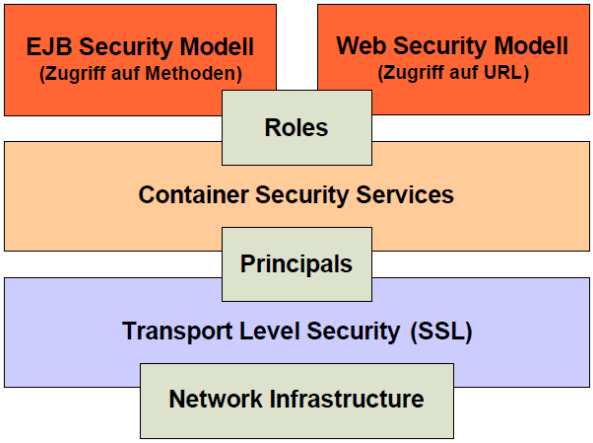
Benutzer sind entweder Personen oder Dienste (Subject) und können mehrere Identitäten (Principal) und Berechtigungen (Credential) besitzen

- *Subject*
- *Pricipal*
- *Credentials*



(Folie 30)

10. Zeichnen Sie die JEE Sicherheitsarchitektur!



(Folie 35)

11. Wie setzen Sie die deklarative Sicherheit für die Autorisation im EJB Tier um?

Steps für die Umsetzung im EJB-Tier:

1. *Der Deployer definiert die Rollen im Deployment Descriptor (kann auch über Annotations im Code hinterlegt werden)*
2. *Der Deployer definiert im Deployment Descriptor die Zugriffsrechte der Business-Methoden mittels zuweisen der Rollen (kann auch über Annotations im Code hinterlegt werden)*
3. *Deployer definiert das Mapping der Gruppen zu den deklarierten Rollen im herstellerspezifischen Deployment Descriptor*

(Folie 42)

12. Wie setzen Sie die programmatische Sicherheit für die Autorisation im EJB Tier um?

Steps für die Umsetzung im EJB-Tier:

1. *Applikationsentwickler implementiert die programmatische Authorizations-Logik innerhalb des Bean-Codes*
2. *Applikationsentwickler deklariert die abstrakte Security-Rolle im Deployment Descriptor der Bean*
3. *Der Deployer definiert das Mapping der abstrakten Security-Rollen zu den deklarierten Rollen (der spezifischen Umgebung) im Deployment Descriptor*
4. *Deployer definiert das Mapping der Gruppen zu den deklarierten Rollen im herstellerspezifischen Deployment Descriptor (optional)*

(Folie 49)