

Java Security

Inhoud

Deze cursus behandelt beveiligingselementen binnen het JAVA platform. Er wordt gestart met een algemene inleiding in de cryptografie en beveiliging. Nadien worden de specifieke beveiligingsvoorzieningen binnen het JAVA platform behandeld. De aandacht gaat hierbij vooral uit naar het gebruik van Security Policies en het digitaal ondertekenen van JAVA code.

Inhoudsopgave

- 1.1. Inleiding
- 1.2. Inleiding in de cryptografie
 - 1.2.1. Confidentialiteit
 - 1.2.1.1. Secret key cryptografie
 - 1.2.1.2. Public key cryptografie
 - 1.2.1.3. Combinatie
 - 1.2.2. Integriteit
 - 1.2.3. Authenticiteit en onweerlegbaarheid: digitale handtekening
 - 1.2.4. Sleutelbeheer
 - 1.2.4.1. Certification Authorities
 - 1.2.4.2. PGP (Pretty Good Privacy)
 - 1.2.5. Belgium EID
- 1.3. Beveiliging binnen het Java platform
 - 1.3.1. Het Java Security Model
 - 1.3.1.1. JDK 1.0 Security model
 - 1.3.1.2. JDK 1.1 Security model
 - 1.3.1.3. JDK 1.2 Security model
 - 1.3.2. De Security Manager
 - 1.3.2.1. Werken met beleidsbestanden (policy files)
 - 1.3.2.2. Een Security Manager schrijven
 - 1.3.3. Code met digitale handtekening
 - 1.3.3.1. Een certificaat genereren
 - 1.3.3.2. Code handtekenen en uitvoeren
 - 1.3.3.3. Getekende applets

Doelgroep

Deze cursus is bedoeld voor JAVA programmeurs die de beveiliging binnen het JAVA platform beter willen leren kennen.

Syllabus

Voor deze cursus wordt gebruik gemaakt van een op maat gemaakte syllabus waarin theorie wordt afgewisseld met praktische oefeningen. De syllabus werd ontwikkeld door Noël Vaes en is tevens apart verkrijgbaar via de website www.noel-vaes.be.

Taal

De syllabus en de lessen zijn in het Nederlands.

Duur

1 dag.

Voorkennis

Goede kennis van JAVA 1.4 of Java 5.