U cacerts dodajemo sve CA sertifikate (ne sertifikate krajnjih korisnika) kojima nas server veruje.

Dodati rootCA.pem (root kojim je potpisan angular sertifikat) i root.pem (root kojim su potpisani sertifikati za siem agent i siem centar – generisani su pki-jem nasim) koji su u SIEM Agent/ certificates folderu.

1. Proveriti putanju do jre/jdk koji se koristi

Project -> Properties -> Java Build Path

ili

System.*getProperty*("java.home")

1. cacerts se nalazi u:

putanja\_do\_jre\_koji\_se\_koristi\lib\security

1. keytool.exe se nalazi u:

putanja\_do\_jre\bin

1. Komanda za dodavanje CA sertifikata u *cacerts* trust store:

keytool -importcert -file *path\_to\_our\_certificate* -alias *some\_alias* -keystore *path\_to\_cacerts* -storepass changeit

alias nije bitan sada, moze bilo koji da se lupi

“changeit” je default password za cacerts fajl

Cmd se pokrece u administratorskom rezimu!

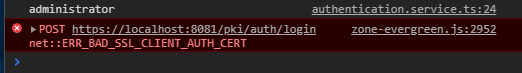
\* U application.properties siem centra i pki-ja je dodato:

server.ssl.client-auth=need

Bez ovoga ne proverava sertifikat klijenta.

Radi lepo siem agent – siem centar https komunikacija i siem agent – pki https komunikacija,

ali ne radi browser – pki. Iako je root dodat u cacerts izbacuje:



siem agent – pki radi i kad agent koristi browser sertifikate