УПУСТВО ЗА КОРИШТЕЊЕ
И ПРИБЛИЖАН ОПИС

РАСПАКИВАЊЕ АПЛИКАЦИЈА И БИБЛИОТЕКА ИНСТАЛАЦИЈА И КОНФИГУРАЦИЈА ТЕ ПОКРЕТАЊЕ

- РАСПАКОВАТИ ДАТОТЕКЕ КОДА И БИБЛИПТЕКА У NETBEANS ПРОЈЕКТНИ ДИРЕКТОРИЈУМ (УКОЛИКО СЕ КОРИСТЕ ИЗВРШНЕ ВЕРЗИЈЕ ПРЕКОМПАЈЛИРАТИ ЈАВА АРХИВЕ)
- ДОБИЈЕ СЕ ВИШЕ ПОВЕЗАНИХ ПРОЈЕКАТА ДВА СИСТЕМА БАЗА КОРИСНИКА И ПОДАЦИ КОРИСНИКА

- НАПРАВИТИ БАЗУ ПОДАТАКА ИЗВРШАВАЊЕМ SQL СКРИПТИ ЗА СЕРВЕР И СЕРВЕРСКЕ АПЛИКАЦИЈЕ ПРБАЦИТИ НА СЕРВЕРСКУ МАШИНУ
- КЛИЈЕНТСКЕ АПЛИКАЦИЈЕ ПРЕБАЦИТИ НА КЛИЈЕНТСКУ МАШИНУ
- ИЗКОНФИГУРАИСАТИ ПАРАМЕТРЕ СЕРВЕРА И БАЗЕ ПОДАТАКА (НПР. ШИФРА) ПОМОЋУ КОНФИГУРАЦИОНИХ АПЛИКАЦИЈА БАЗЕ КОРИСНИКА

- ИЗВРШИТИ СИСТЕМСКУ СКРИПТУ ЗА СЕРТИФИКАЦИЈУ СЕРВЕРА. ФОЛДЕР СА СКРИПТАМА КОПИРАТИ НА КОРИЈЕНСКИ ДИРЕКТОРИЈУМ СЕРВЕРСКЕ АПЛИКАЦИЈЕ
- СЛИЧНО ЗА КЛИЈЕНТ УРАДИТИ СА ДАТОТЕКОМ СА СЛИКАМА И КЛИЈЕНТСКОМ АПЛИКАЦИЈОМ

- ПОКРЕНУТИ СЕРВЕРСКУ АПЛИКАЦИЈУ (БАЗЕ КОРИСНИКА САМО ЗА РЕГИСТРОВАЊЕ И ПРИЈАВЕ, ДОК ПОДАЦИ КОРИСНИКА ВРШЕ И СЕРТИФИКАЦИЈУ И РАЗМЈЕНУ ПОРУКА ПО ПРОЈЕКТНОМ ЗАДАТКУ УЗ ПРЕДХОДНО)
- САДА СЕ МОГУ ПОКРЕТАТИ КЛИЈЕНТСКЕ КОНЗОЛНЕ ИЛИ ГРАФИЧКЕ АПЛИКАЦИЈЕ КЛИЈЕНАТА, (УКОЛИКО ЈЕ СЕРВЕР ПОДАТАКА КОРИСНИКА СВЕ, А БАЗЕ КОРИСНИКА САМО КЛИЈЕНТИ ЗА БАЗЕ КОРИСНИКА)

ПРИЈАВЕ КОРИСНИКА КАО УСЛОВ СЕРТИФИКАЦИЈЕ И РАЗМЈЕНА ПОРУКА

- ПРВО ЈЕ ПОТРБНО РЕГИСТРОВАТИ КОРИСНИКЕ НА СИСТЕМ, А ТО СЕ ОБАВЉА ПОД УНИЛАТЕРАЛНОМ КОМУНИКАЦИЈОМ ГДЈЕ СУ ПОДАЦИ ПРЕМА СЕРВЕРУ ЗАШТИЋЕНИ СЕРВЕРСКИ СЕРТИФИКАТОМ, ДОК ПРЕМА КЛИЈЕНТУ ЊЕГОВИМ СЛУЧАЈНИМ КЉУЧЕМ
- ПОТРЕБНО ЈЕ И ДА КЛИЈЕНТ ИМА ДОСТУПАН СЕРТИФИКАТ СЕРВЕРА У ИСТОИМЕНОМ ДИРЕКТОРИЈУМУ КАО И ГДЈЕ СУ СКРИПТЕ СЕРВЕРА (НПР. ДОБАВИО ГА ЈЕ СА СВОЈОМ КЛИЈЕНТСКОМ АПЛИКАЦИЈОМ)
- ПО РЕГИСТРАЦИЈИ КОРИСНИКА ДОСТУПНЕ СУ СВЕ ОПЦИЈЕ СЕРТИФИКАЦИЈЕ И РАЗМЈЕНЕ ПОРУКА
- КЛИЈЕНТСКЕ АПЛИКАЦИЈЕ ПОДАТАКА КОРИСНИКА БЕЗ ПРИЈАВЕ КОРИСНИКА МОГУ ОБАВИТИ САМО НЕКЕ ПРЕГЛЕДЕ ЛОКАЛНИХ ПОРУКА, ДОК СА СЕРВЕРОМ НЕ МОГУ КОМУНИЦИРАТИ
- ЗА ОПЦИЈЕ КРЕИРАЊА И ЧИТАЊА ПОРУКА ПОТРБНИ КОРИСНИЦИ КОМУНИКАЦИЈЕ МОРАЈУ БИТИ СЕРТИФИКОВАНИ
- ЗА ПРИЈАВУ И РЕГИСТРАЦИЈУ СЕ МОГУ КОРИСТИТИ И ГРАФИЧКИ КЛИЈЕНТИ БАЗЕ КОРИСНИКА
- ЗА ОСТАЛЕ ОПЕРАЦИЈЕ ИСКЉУЧИВО СИСТЕМ ПОДАТАКА КОРИСНИКА КОЈИ ЈЕ НАДСИСТЕМ ПРЕДХОДНОГ

ПРОЦЕС СЕРТИФИКАЦИЈЕ

- КЛИЈЕНТ ПОШАЉЕ ЗАХТИЈЕВ СЕРВЕРУ ЗА СЕРТИФИКАТ, А ОВАЈ ГЕНЕРИШЕ СИСТЕМСКЕ СКРИПТЕ СА НАРЕДБАМА ЗА ГЕНЕРИСЊЕ СЕРТИФИКАТА И ЈОШ ОСНОВНИ KEY STORE. ОПЕРАТЕР НА СЕРВЕРУ РУЧНО ПОКРЕЋЕ СИСТЕМСКЕ СКРИПТЕ И ГЕНЕРИШЕ СЕРТИФИКАТ И ЊЕГОВ ПРИВАТНИ КЉУЧ (И ЈОШ НЕКЕ МЕЂУСЕРТИФИКАТЕ).
- КЛИЈЕНТ ПО НОВОМ ЗАХТИЈЕВУ ПРЕУЗМЕ СЕРТИФИКАТ И ПРИВАТНИ КЉУЧ (НА СЕРВЕРУ СЕ НЕ БРИШЕ НИ ЈЕДНА ДАТОТЕКА, ПРЕМ ДА БИ ТРЕБАЛО ИЗБРИСАТИ ДАТОТЕКЕ СА П.К.)
- СМАТРА СЕ ДА ЈЕ СЕРВЕР ОД ПОВЈЕРЕЊА, И ДА СЕ НЕЋЕ КОРИСТИТИ ПРИВАТНИ КЉУЧЕВИКЛИЈЕНТА, ИАКО ЈЕ БОЉА ВАРИЈАНТА ДА КЛИЈЕНТИ ГЕНЕРИШУ ПАР КЉУЧЕВА И ПОШАЉУ ЈАВНИ СЕРВЕРУ ГДЈЕ ГА ОВАЈ УГРАДИ У СЕРТИФИКАТ
- ПРИВАТНИ И ЈАВНИ КЉУЧ СЕ ШАЉУ СИГУРНОМ ЛИНИЈОМ КА КЛИЈЕНТУ (СЕРВЕРСКИ СЕРТИФИКАТ КОД КЛИЈЕНТСКЕ АПЛИКАЦИЈЕ И СЛАЊЕ СЛУЧАЈНОГ КЉУЧА КЛИЈЕНТА СЕРВЕРУ УЗ ТЕСТ СЕРВЕРА)
- САДА ЈЕ СЕРТИФИКАТ И КОРИСНИКОВ ПРИВАТНИ КЉУЧ КОД КЛИЈЕНТА
- ПРИВАТНИ КЉУЧ ЈЕ У JKS ФОРМАТУ И ШТИЋЕН ЈЕ ЛОЗИНКОМ КЛИЈЕНТА
- ЛОЗИНКЕ КЛИЈЕНТА СЕ ИНИЦИЈАЛНО ХЕШСАЛТУЈЕ КОД РЕГИСТРАЦИЈЕ И ТО НА СЕРВЕРСКОЈ СТРАНИ, ДОК СЕ ОТВОРЕНА СИГУРНИМ КАНАЛОМ ДОБАВИ ДО СЕРВЕРА
- ПРИ ЗАХТЈЕВУ СЕРТИФИКАТА ПОНОВО СЕ УНОСИ И ШАЉЕ СЕРВЕРУ ГДЈЕ СЕ ПРОВЈЕРАВА И ПРИХВАТА ЗА ПРИВАТНЕ КЉУЧЕВЕ (БЕЗ ТОГ СЕ СЕРТИФИКАТ НЕ МОЖЕ КРЕИРАТИ)
- ЗАНИМЉИВО ЈЕ ДА СЕ ЛОЗИНКА ПРИВАТНОГ КЉУЧА ПРЕПАКУЈЕ КОД КЛИЈЕНТА
- ИНИЦИЈАЛНО НА СЕРВЕРУ ЈЕ ФОРМАЛНА ЛОЗИНКА –СЕРВЕР- А П.К. СЕ ПРЕНОСИ СИГУРНИМ ЛИНИЈАМА, ДОК ЈЕ СЕРВЕР ОД ПОВЈЕРЕЊА (БАР ЗА П.К.)
- КОРИСНИК ПОСЕБНИМ ЗАХТИЈЕВОМ МОЖЕ ТРАЖИТИ СЕРТИФИКАТЕ (БЕЗ П.К.) ДРУГИХ КОРИСНИКА РАДИ СЛАЊА ПОРУКЕ
- НАПОМЕНА ЈЕ ДА СЕ ИЗВРШНЕ СКРИПТЕ ЗА СЕРТИФИКОВАЊЕ БРИШУ ПО ПРИЈЕМУ СЕРТИФИКАТА И ВИШЕ СЕ НЕ КРЕИРАЈУ ЗА СЕРТИФИКОВАНОГ КОРИСНИКА, ДОКЛЕ ГОД ОПЕРАТЕР НЕ ИЗБРИШЕ СЕРТИФИКАТ И ПРИВАТНИ КЉУЧ, А СМАТРА СЕ ДА ТО НЕЋЕ РАДИТИ.
- ЈОШ ТРЕБА НАПОМЕНУТИ ДА СУ КОРИСНИЧКИ СЕРТИФИКАТИ ПОТПИСАНИ СЕРВЕРСКИМ

ПРОЦЕС ПРИМОПРЕДАЈЕ ПОРУКА

- ПРИЈАВЉЕН И СЕРТИФИКОВАН КОРИСНИК МОЖЕ КРЕИРАТИ **ENC** ДАТОТЕКУ СА ДАТУМОМ КРЕИРАЊА И ИМЕНОМ ПРИМАОЦА И СА КРИПТОВАНОМ ПОРУКОМ BASE64 КОДОВАНОМ НА ПРЕГЛЕД КОРИСНИКА. УЗ ТУ ДАТОТЕКУ КРЕИРА СЕ **MSG** ДАТОТЕКА У КОЈОЈ ЈЕ ПОРУКА КРИПТОВАНА НА ПРИМАОЦЕВ СЕРТИФИКАТ И СЛУЖИ ЗА РЕВИДИРАЊЕ ПОРУКЕ ОД СТРАНЕ ПОШИЉАОЦА ПРИЈЕ СЛАЈА, ЗА РАЗЛИКУ ОД ПРЕДХОДНЕ КОЈА ТРЕБА ДА СЕ УГРАДИ У СЛИКУ И ШАЉЕ ПРИМАОЦУ. ЈОШ СЕ КРЕИРА И СИСТЕМСКА СКРИПТА ПОМОЋУ КОЈЕ КЛИЈЕНТ РУЧНО УГРАЂУЈЕ ПОРУКУ И ПОДАТКЕ ИЗ ENC У СЛИКУ.

- ПО ИЗВРШАВАЊУ УГРАДЊЕ НОВА СЛИКА СЕ СМИЈЕШТА У ПОСЕБАН ДИРЕКТОРИЈУМ И ЈОШ ЈЕ ИМЕНСКИ ОЗНАЧЕНА КАО OUTBOX ТЈ. ЗА СЛАЊЕ. САМО ОВАКО ОЗНАЧЕНЕ ПОРУКЕ СЕ МОГУ ПОСЛАТИ. ДАЉЕ КЛИЈЕНТ ИМА ОПЦИЈУ КОЈОМ ШАЉЕ ОВУ СЛИКУ НА СЕРВЕР. ПО СЛАЊУ ОНА СЕ НЕ БРИШЕ НА КЛИЈЕНТСКОЈ СТРАНИ, КАО НИ БИЛО КОЈЕ ДРУГЕ ДАТОТЕКЕ И ПОРУКЕ. НА СЕРВЕРУ СЕ ТА ДАТОТЕКА ПРЕИМЕНУЈЕ И ТАМО СТОЈИ ДО ЗАХТЈЕВА ЗА ПРИЈЕМ.

- ПРИМАОЦИ ТЈ. КЛИЈЕНТИ ИМАЈУ МОГУЋНОСТ ДА ОЧИТАЈУ ПОРУКЕ КОЈЕ СУ ПРИВРЕМЕНО НА СЕРВЕРУ И ДА КОПИРАЈУ БИЛО КОЈУ ПОРУКУ (УКОЛИКО СУ ПРИЈАВЉЕНИ) БЕЗ БРИСАЊА НА СЕРВЕРУ ИЛИ ДА ПРЕУЗМУ СВЕ ПОРУКЕ СА СЕРВЕРА КОЈЕ СУ ФОРМАТОМИМЕНА ЊИМА НАМЈЕЊЕНЕ. У ТОМ СЛУЧАЈУ СЕ БИЉЕЖИ ПРЕУЗИМАЊЕ НА СЕРВЕРУ, А ЛИСТА ДАТИХ СЕ МОЖЕ ЧИТАТИ ОД СТРАНЕ КЛИЈЕНАТА. ЈОШ ЈЕ ЗА НАПОМЕНУТИ ДА СЕ ПОРУКЕ ПРИ СЕРВЕРУ БРИШУ.

- ПО ПРИЈЕМУ ПОРУКЕ, ДА БИ ЈЕ ОЧИТАО ИЛИ ПОКУШАО ОЧИТАТИ КЛИЈЕНТ ЈЕ ПРВО МОРА ИЗДВОЈИТИ ИЗ СЛИКЕ. АПЛИКАЦИОНО МОЖЕ ГЕНЕРИСАТИ СИСТЕМСКЕ СКРИПТЕ КОЈИМА ЋЕ ТО УРАДИТИ. ФОРМАЛНА ШИФРА УКЛАПАЊА И ИЗВАЈАЊА ЈЕ КОРИСНИЧКО ИМЕ ПРИМАОЦА.

- ПРИ РАСПАКИВАЊУ СЕ КРЕИРА САМО ENC ДАТОТЕКА КОЈА ЈЕ СЛИЧНА ПРЕДХОДНОЈ. САМО СЕ У ИМЕНУ РАЗЛИКУЈЕ ДАТУМ КОЈИ НИЈЕ ВИШЕ ДАТУМ КРЕИРАЊА ПОРУКЕ, НЕГО ДАТУМ ПРИЈЕМА.

- ПРИ ОЧИТАВАЊУ ПОРУКЕ КЛИЈЕНТ КОМ ЈЕ ПОРУКА НАМИЈЕЊНА САМО ОН МОЖЕ ОЧИТАТИ ПОРУКУ. ЈОШ СЕ ПРОВЈЕРАВА И ПОТПИС КОЈИМ ЈЕ ПОШИЉАЛАЦ ПОТПИСАО И ТЕКСТ И КРИПТОВАНЕ ПОДАТКЕ (ЗАЈЕДНИЧКИ). ФОРМАТ ДАТОТЕКЕ ЈЕ ОДРЕЂЕН АПЛИКАЦИЈОМ. ЈОШ ЈЕДАН ВАЖАН ДАТУМ ЈЕ ДАТУМ ОЧИТАВАЊА.

СИГУРНОСНИ КАНАЛИ

- ТРЕБА РАЗЛИКОВАТИ СИГУРНОСНИ КАНАЛ РАЗМЈЕНЕ ПОДАТАКА ИЗМЕЂУ КЛИЈЕНТА И СЕРВЕРА УНИЛАТЕРАЛНОМ КОМУНИКАЦИЈОМ СЕРТИФИКАТОМ СЕРВЕРА И РЕГУЛИСАНИУ ПРОТОКОЛОМ SECURE PROPIS (PROTOKOL RAZMJENE OSNOVNIH PODATAKA I SERTIFIKATA) НАСЛЕДНИКОМ SECURE BKSP (BAZA KORISNIKA SIMPLE PROTOCOL)
- ОД МЕХАНИЗМА РАЗМЈЕНЕ ПОРУКА ПРЕКО СЕРВЕРА КОЈИ ЈЕ ИНВАРИЈАНТАН НА ПРОТОКОЛ КОМУНИКАЦИЈЕ (МОЖЕ БИТИ И ОТВОРЕНА ЛИНИЈЕ, АЛИ НИЈЕ АПЛИКАЦИОНО ЈЕ SECURE PROPIS) , А КРИПТОВАЊЕ И ПОТПИСИВАЊЕ СЕ ВРШИ КОРИСНИЧКИМ СЕРТИФИКАТИМА БЕЗ СЕРВЕРА

СИСТЕМСКИ И АПЛИКАЦИОНИ ЗАХТЈЕВИ ЗА СЕРВЕР

- JAVA 8 JRE + JAVA FX 8 (I KEYTOOL)
- WINDOWS/LINUX+BASH OS
- OPENSSL
- MYSQL

СИСТЕМСКИ И АПЛИКАЦИОНИ ЗАХТЈЕВИ ЗА СЕРВЕР

- JAVA 8 JRE + JAVA FX 8 (I KEYTOOL)
- WINDOWS/LINUX+BASH OS
- STEGHIDE

ДОДАТНИ РАЗВОЈНИ ЗАХТЈЕВИ

- NETBEANS
- JAVAFXSCENEBUILDER
- MYSQLWORKBENCH

ПРИБЛИЖНИ ОПИСИ ДИЈЕЛОВА КОДА И ПРОЈЕКАТА

BAZA KORISNIKA CERT – АПЛИКАЦИОНА БИБЛИОТЕКА СА СИСТЕМСКИМ ФУНКЦИЈАМА
BAZA KORISNIKA-(ПОД)СИСТЕМ ЗА УПРАВЉАЊЕ ПРИЈАВОМ И РЕГИСТРАЦИЈОМ КОРИСНИКА
PODACI KORISNIKA –СИСТЕМ ЗА РЕАЛИЗАЦИЈУ ЈЕДНОСТАВНЕ PKI И СЕРТИФИКАЦИЈЕ
PODACI KORISNIKA – СИСТЕМ ЗА РАЗМЈЕНУ ПОРУКА КОРИШТЕЊЕМ СЕРТИФИКАТАКА
PODACI KORISNIKA – РЕАЛИЗАЦИЈА ПРОЈЕКТНО ЗАДАТКА И КРИПТОГРАФИЈЕ ...
PODACI KORISNIKA – НАДСИСТЕМ ЗА БАЗУ КОРИСНИКА
+SISTEM KORISNIKA – ВЕБ JSF БЛИСКА АПЛИКАЦИЈА ЗА РЕАЛИЗОВАЊЕ ГРУПА КОРИСНИКА (И БАЗЕ КОРИСНИКА)

НЕМА ГАРАНЦИЈЕ ЗА НЕПОСТОЈАЊЕ ПРАВОПИСНИХ ГРШАМА И ПОГРЕШНО ПОСТАВЉЕНИХ РЕЧЕНИЦА ИЛИ СИНТАГМИ