Unapređenje sigurnosti pristupa za Oracle Forms aplikacije korištenjem eOI

Lovro Kudelić, mag. ing. inf. et comm. techn.

25. hroug godišnja konferencija

Hrvatski operator prijenosnog sustava d.o.o.

O predavaču

- Rođen u Zagrebu
- Završio Fakultet elektrotehnike i računarstva, Informacijska i komunikacijska tehnologija
- Od rujna 2019. zaposlen u HOPS d.o.o.

Tehnologije

- Linux OS (Red Hat, CentOS, Oracle Linux)
- Oracle i PostgreSQL baze podataka
- Apache Tomcat
- Apache Web Server
- Oracle F&R + Weblogic 12C
- Zabbix

Sadržaj

- Općenito o problematici kibernetičke sigurnosti (incidenti, NIS direktiva)
- Multifakorska autentifikacija
- eOI i zakonska regulativa
- Prikaz konfiguracije Oracle Forms-a i OHS-a (Oracle HTTP Server) kako bi isti koristili multifaktorsku autentifikaciju pomoću eOI

Kibernetički napadi

- Glavni krivac – čovjek (napadač i žrtva)
- Vrste napada:
  - Malware (Ransomware)
  - Phishing
  - DoS (Denial of Service) – DDoS (Distributed Denial of Service)
  - Krađe podataka
  - …
- Epidemija Covid-19 + rad od kuće – plodno tlo za sve veći broj napada

Incidenti

- US Colonial Pipeline
- INA
- ENTSO-E
- …

How a major oil pipeline got held for ransom

The largest petroleum pipeline in the country was reportedly breached by a single leaked password.

By Sara Morrison | Updated Jun 8, 2021, 12:50pm EDT

SHARE

Colonial Pipeline shut down its massive oil pipeline after a ransomware attack took some of its systems offline. Above, a Colonial facility in 2016. | Luke Sharrett/Bloomberg/Getty Images

Ransomware Attack Exposes Poor Energy-Sector Cybersecurity

An infection at a pipeline provider caused it to shut down for two days, DHS says

MOST POPULAR

A pipeline under construction. An alert from the Department of Homeland Security shows the energy sector's vulnerability to hackers.

PHOTO: MATT ROURKE/ASSOCIATED PRESS

Entso-E targeted in recent cyberattack

The European Network of Transmission System Operators for Electricity said on Monday that unidentified hackers recently targeted its computer networks.

MARCH 10, 2020 BRIAN PUBLICOVER

GRIDS & INTEGRATION | INSURANCE | MARKETS | MARKETS & POLICY | POLICY | TECHNOLOGY | TECHNOLOGY AND R&D | FINLAND | SWEDEN | WESTERN EUROPE

Image: Sfedor/Pixabay

Wind giant EDP hit by Ragnar Locker ransomware attack

Image: EDP

European energy giant Energias de Portugal (EDP) was hit by a ransomware attack on Easter Monday, the company has confirmed.

Austrijsko ministarstvo pod 'ozbiljnim kibernetičkim napadom'

Austrijsko ministarstvo vanjskih poslova pod "ozbiljnim je kibernetičkim napadom", priopćili su u subotu navečer te upozorili da bi odgovorna mogla biti neka druga država.

"S obzirom na težinu i narav napada, ne može se isključiti da je to cijani napad i da ga je izveo državni akter", objavio je ministarstvo u zajedničkoj izjavi s ministarstvom unutarnjih poslova nešto prije 23 sata te dodalo da napad još traje.

Traje snažan kibernetički napad na INA-u

INA Grupa izvijestila je u nedjelju da se nalazi pod kibernetičkim (foto ilustracija) napadom koji je započeo 14. veljače oko 22 sata.

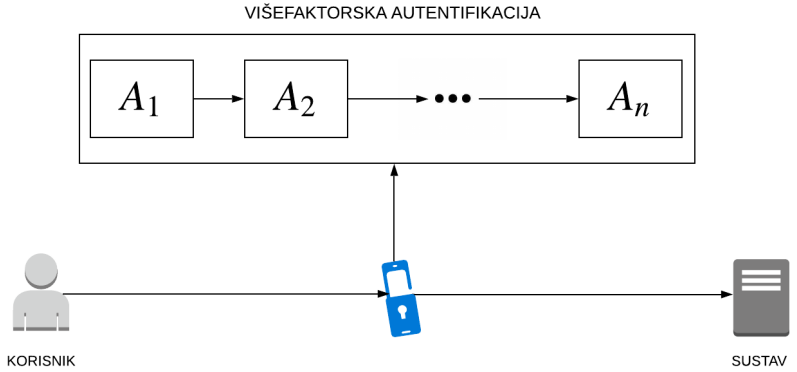
"U ovom trenutku je bitno reći da opskrba derivatima cijelog tržišta i prodaja našim kupcima na maloprodajnim mjestima cijelo ovo vrijeme radi neometano. Kupci, bez obzira plaćaju li gotovinom, bankovnim karticama ili karticama Ine, mogu kupovati na siguran način", izjavio je u ponedjeljak novinarima operativni direktor Industrijskih servisa Ine Goran Pavlović.

Rješenja

- Edukacija korisnika
- Zaštita kritične infrastrukture
- NIS2 direktiva:
  - Direktiva o sigurnosti mrežnih i informacijskih sustava (*engl. Network and Information Security Directive*)
  - Sektori: Energetski, Financijski, Transport, Distribucija pitke vode, Digitalne usluge, telekomunikacijske kompanije, upravljanje otpadnim vodama, svemir, proizvodnja kritičnih proizvoda, poštanske i kurirske usluge, hrana i javna uprava
  - Strože provođenje i nadzor mjera te uspostava administrativnih sankcija
- Korištenje isključivo korisničkog imena i lozinke više nije rješenje

Multifaktorska autentifikacija

- „Nešto što osoba zna” – lozinka, pin
- „Nešto što osoba je” – otisak prsta, lice
- „Nešto što osoba posjeduje” – token, pametna kartica



Pametne kartice

- eOI – Elektronička osobna iskaznica
- FINA osobni ili poslovni certifikat

Zakonska regulativa

- eIDAS (engl. electronic IDentification, Authentication and trust Services)
- Uredba Europske komisije kojom digitalni potpis dobiva pravnu snagu i izjednačava se s vlastoručnim potpisom
- U Hrvatskoj implementiran kroz zakon iz 2017. „Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ“

Oracle Forms

- „Oracle Forms nije mrtav”
- WebLogic 12c:
  - Napuštanje Java web start tehnologije (Java applet)
  - Pokretanje korištenjem Oracle Java JRE okoline
  - Omogućeno napredno korištenje certifikata s pametnih kartica
- Omogućavanje multifaktorske autentifikacije nad Oracle Forms aplikacijama bez potrebe za „pokretanjem Forms developer-a” (nije potrebno prilagođavati aplikacije)

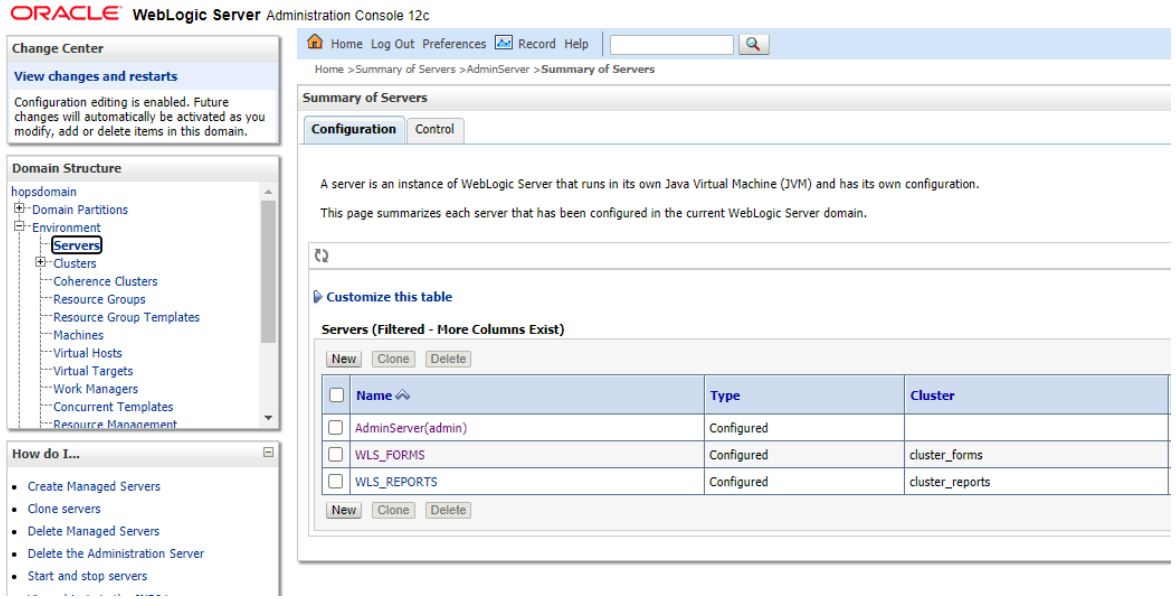
Koraci implementacije

- WebLogic Administration Console i Enterprise Manager
- Oracle HTTP Server (OHS)
- Zaštita Administration Console i Enterprise Manager-a korištenjem OHS-a kao reverse proxy
- Pokretanje Forms aplikacija korištenjem Windows keystore-a kao standalone aplikacije

Oracle WebLogic Server

WebLogic Administration Console

- Preduvjeti:
  - HTTPS certifikat i privatni ključ
  - Identity keystore
  - Trust keystore
  - Aktivirana pametna kartica i čitač pametne kartice

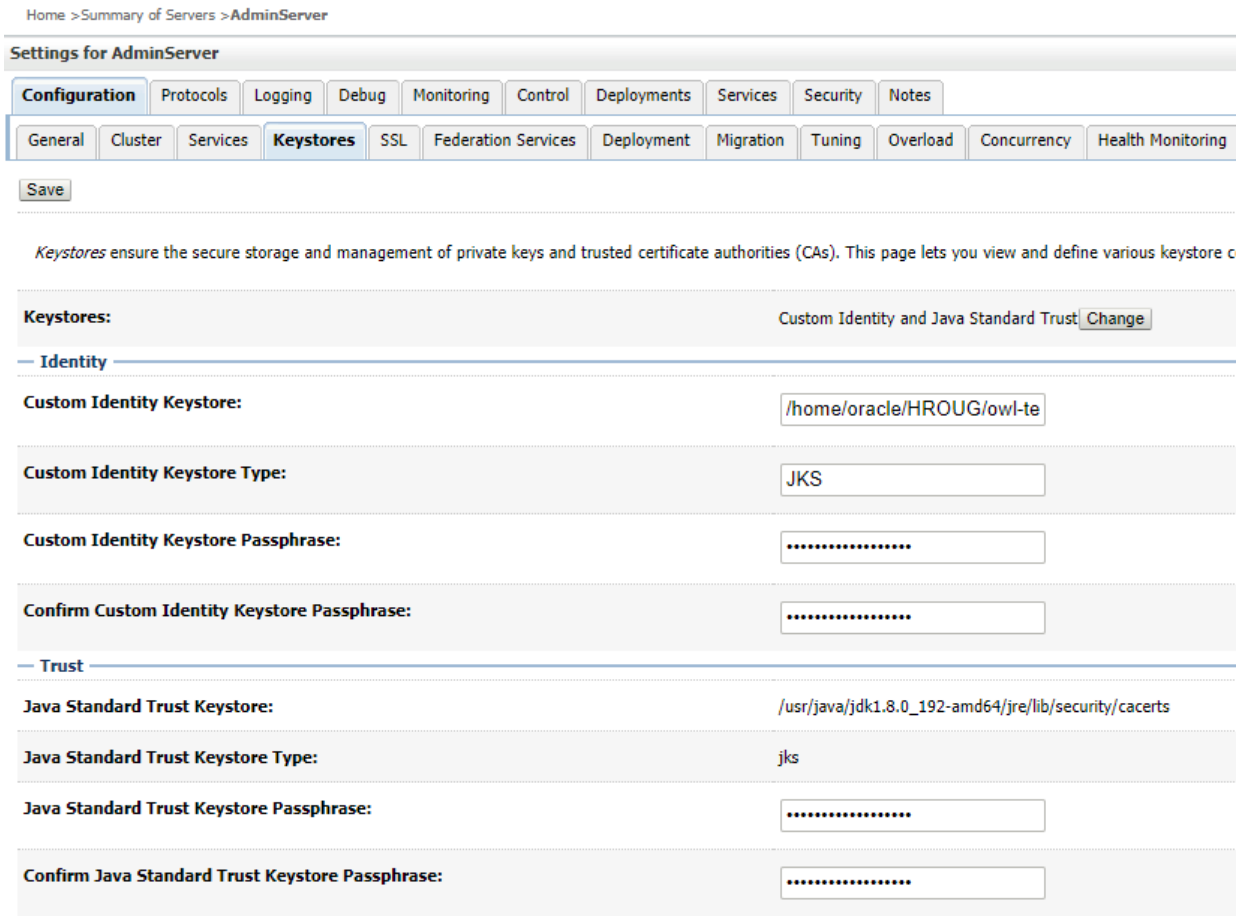


Priprema keystora

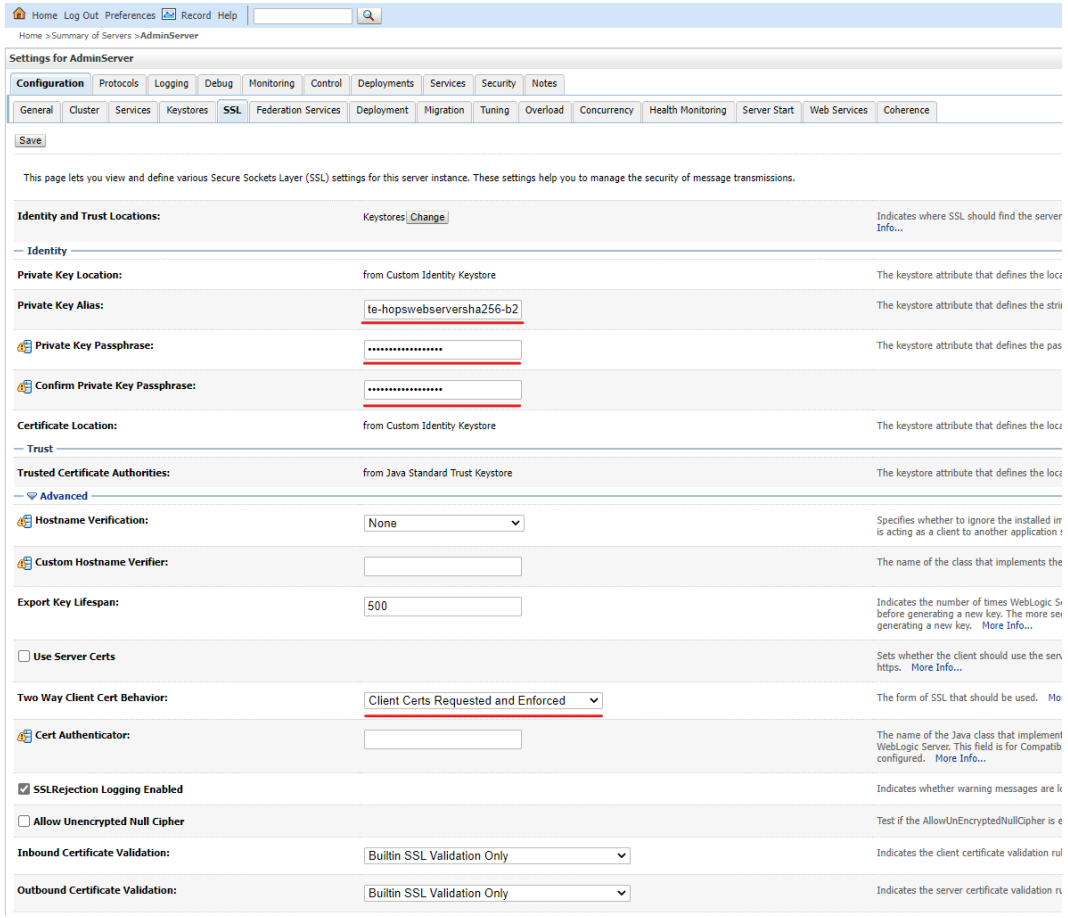
- PFX datoteka:
  - Sadrži certifikat u PKCS#12 formatu
  - Sastoji se od privatnog ključa, certifikata i intermediate certifikata
- Isti je potrebno pretvoriti u Java Key Store (JKS) – Identity store:
  - `keytool -importkeystore -srckeystore owl-test.pfx -destkeystore owl-test.jks -srcstoretype PKCS12 -deststoretype JKS`
- Java Trusted Key Store:
  - /usr/java/jdk1.8.0_192-amd64/jre/lib/security/cacerts

```
[oracle@owl-test HROUG]$ keytool -importkeystore -srckeystore owl-test.pfx -destkeystore owl-test.jks -srcstoretype PKCS12 -deststoretype JKS
Importing keystore owl-test.pfx to owl-test.jks...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias te-hopswebserversha256-d262bca6-8b67-4b32-9580-b4e496ea5aa4 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

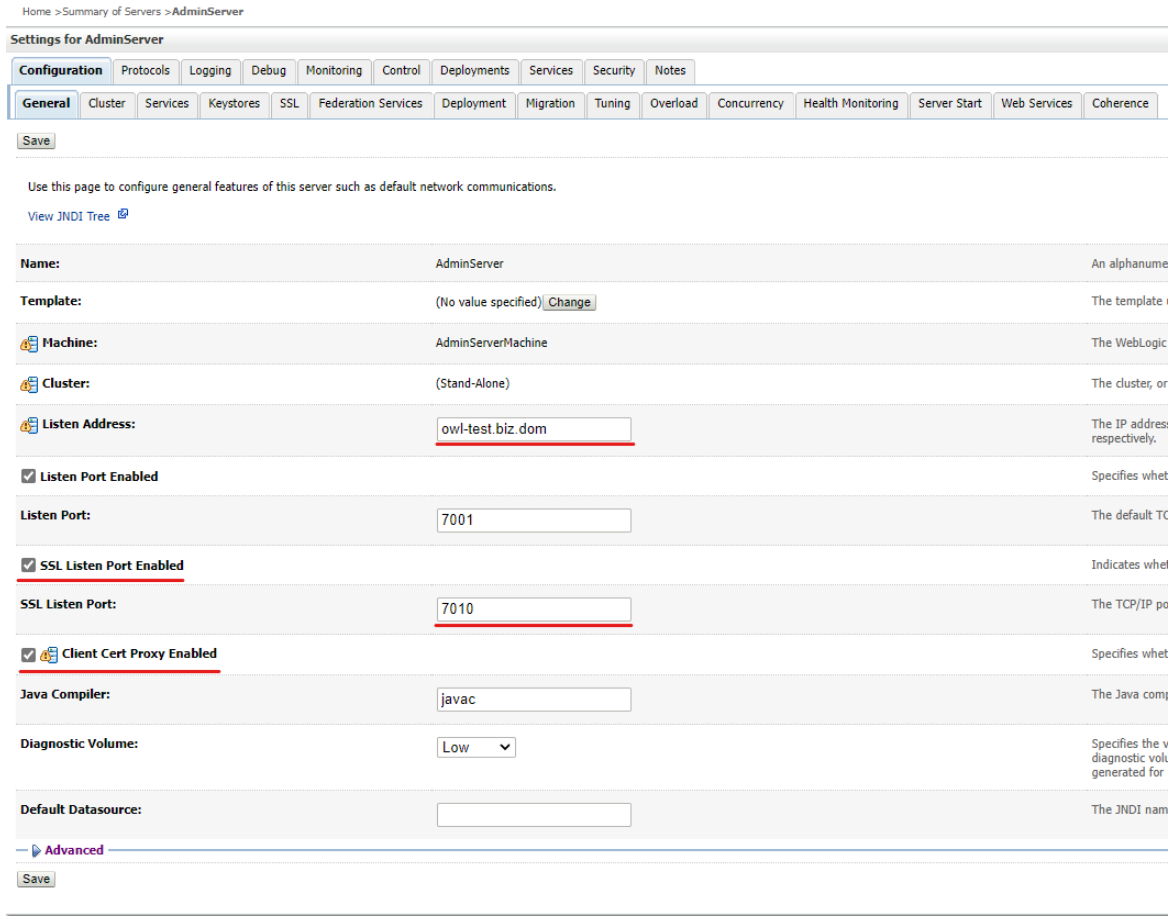
Oracle WebLogic Server – konfiguracija (1)



Oracle WebLogic Server – konfiguracija (2)



Oracle WebLogic Server – konfiguracija (3)



Oracle WebLogic Server – konfiguracija (4)

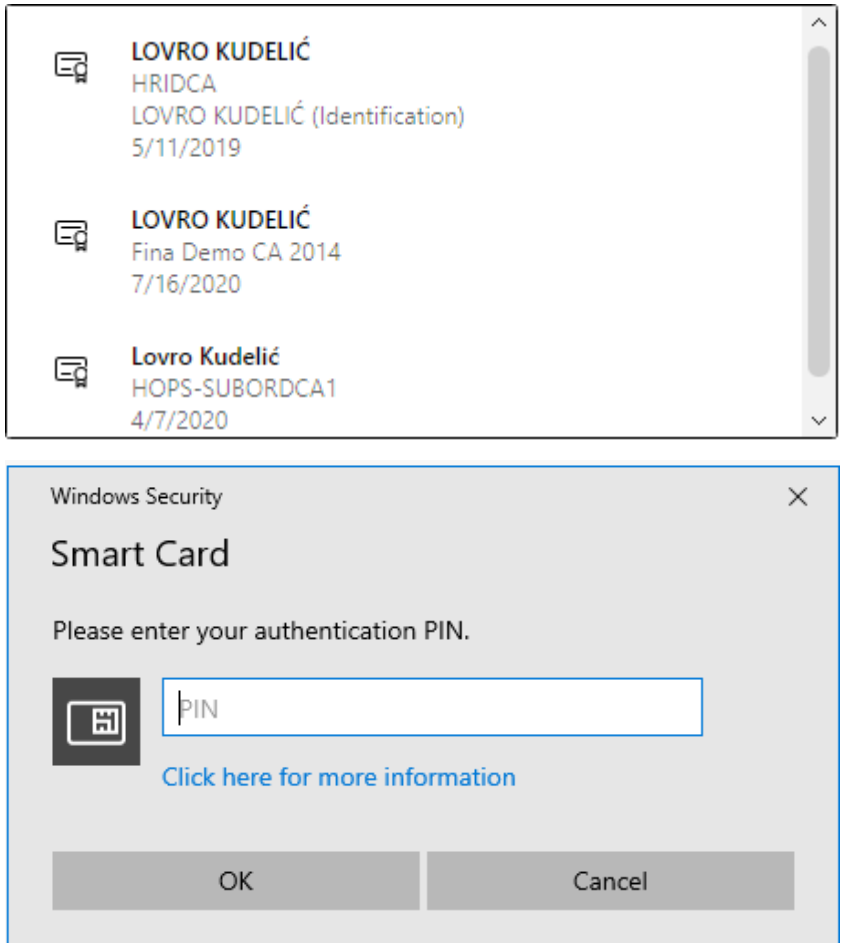
- Odabirom opcije „Client Certs Requested and Enforced” od klijenta se traži njegov klijentski certifikat
- U Java Trusted Keystore je potrebno dodati trusted certifikate kako bi odabrali kojim klijentima (certifikatima) vjerujete
- Alat KeyStore Explorer - https://keystore-explorer.org/
- Nakon svih navedenih izmjena, potrebno je napraviti restart cijele Oracle WebLogic okoline

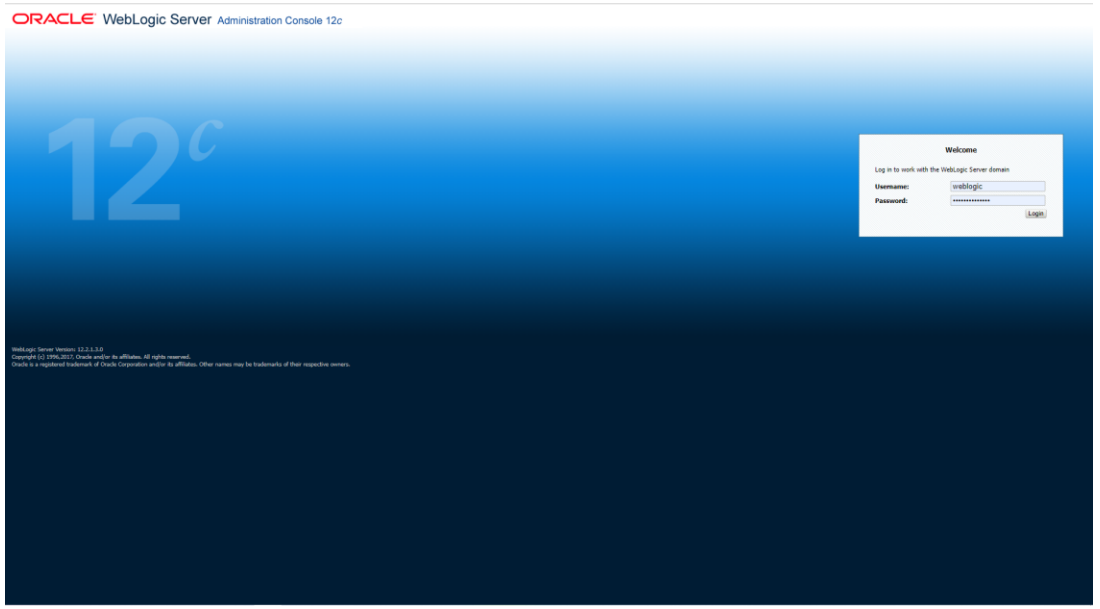
Oracle WebLogic Server – konfiguracija (5)

cacerts

T	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
-		affirmtrustpremiumca [jdk]	RSA	4096	31. 12. 2040. 15:10:36 CET	25. 08. 2016. 17:20:41 CEST
-		affirmtrustpremiumeccca [jdk]	EC	384	31. 12. 2040. 15:20:24 CET	25. 08. 2016. 17:20:21 CEST
-		akdca root	RSA	4096	19. 01. 2038. 04:14:07 CET	14. 09. 2020. 08:58:22 CEST
-		aolrootca1 [jdk]	RSA	2048	19. 11. 2037. 21:43:00 CET	25. 08. 2016. 17:20:26 CEST
-		aolrootca2 [jdk]	RSA	4096	29. 09. 2037. 16:08:00 CEST	25. 08. 2016. 17:20:25 CEST
-		baltimorecybertrustca [jdk]	RSA	2048	13. 05. 2025. 01:59:00 CEST	25. 08. 2016. 17:19:55 CEST
-		buypassclass2ca [jdk]	RSA	4096	26. 10. 2040. 10:38:03 CEST	25. 08. 2016. 17:19:53 CEST
-		buypassclass3ca [jdk]	RSA	4096	26. 10. 2040. 10:28:58 CEST	25. 08. 2016. 17:19:50 CEST
-		camerfirmachambersca [jdk]	RSA	4096	31. 07. 2038. 14:29:50 CEST	25. 08. 2016. 17:20:38 CEST
-		camerfirmachamberscommerceca [jdk]	RSA	2048	30. 09. 2037. 18:13:44 CEST	25. 08. 2016. 17:19:58 CEST
-		camerfirmachambersignca [jdk]	RSA	4096	31. 07. 2038. 14:31:40 CEST	25. 08. 2016. 17:20:36 CEST
-		certplusclass2primaryca [jdk]	RSA	2048	07. 07. 2019. 01:59:59 CEST	25. 08. 2016. 17:20:12 CEST
-		certplusclass3pprimaryca [jdk]	RSA	2048	07. 07. 2019. 01:59:59 CEST	25. 08. 2016. 17:20:05 CEST
-		certumca [jdk]	RSA	2048	11. 06. 2027. 12:46:39 CEST	25. 08. 2016. 17:19:37 CEST
-		certumtrustednetworkca [jdk]	RSA	2048	31. 12. 2029. 13:07:37 CET	25. 08. 2016. 17:20:05 CEST
-		chunghwaepkirootca [jdk]	RSA	4096	20. 12. 2034. 03:31:27 CET	25. 08. 2016. 17:20:34 CEST
-		comodoaaaca [jdk]	RSA	2048	01. 01. 2029. 00:59:59 CET	25. 08. 2016. 17:20:22 CEST
-		comodoeccca [jdk]	EC	384	19. 01. 2038. 00:59:59 CET	25. 08. 2016. 17:20:46 CEST
-		comodorsaca [jdk]	RSA	4096	19. 01. 2038. 00:59:59 CET	25. 08. 2016. 17:19:25 CEST
-		deutschetelekomrootca2 [jdk]	RSA	2048	10. 07. 2019. 01:59:00 CEST	25. 08. 2016. 17:19:49 CEST
-		digicertassuredidg2 [jdk]	RSA	2048	15. 01. 2038. 13:00:00 CET	25. 08. 2016. 17:19:32 CEST
-		digicertassuredidg3 [jdk]	EC	384	15. 01. 2038. 13:00:00 CET	25. 08. 2016. 17:19:30 CEST
-		digicertassuredidrootca [jdk]	RSA	2048	10. 11. 2031. 01:00:00 CET	25. 08. 2016. 17:19:24 CEST
-		digicertglobalrootca [jdk]	RSA	2048	10. 11. 2031. 01:00:00 CET	25. 08. 2016. 17:20:13 CEST
-		digicertglobalrootg2 [jdk]	RSA	2048	15. 01. 2038. 13:00:00 CET	25. 08. 2016. 17:19:43 CEST
-		digicertglobalrootg3 [jdk]	EC	384	15. 01. 2038. 13:00:00 CET	25. 08. 2016. 17:19:43 CEST
-		digicerthighassuranceevrootca [jdk]	RSA	2048	10. 11. 2031. 01:00:00 CET	25. 08. 2016. 17:19:44 CEST
-		digicerttrustedrootg4 [jdk]	RSA	4096	15. 01. 2038. 13:00:00 CET	25. 08. 2016. 17:19:59 CEST
-		dtrustclass3ca2 [jdk]	RSA	2048	05. 11. 2029. 09:35:58 CET	25. 08. 2016. 17:19:52 CEST
-		dtrustclass3ca2ev [jdk]	RSA	2048	05. 11. 2029. 09:50:46 CET	25. 08. 2016. 17:20:44 CEST
-		entrust2048ca [jdk]	RSA	2048	24. 07. 2029. 16:15:12 CEST	25. 08. 2016. 17:20:34 CEST
-		entrustevca [jdk]	RSA	2048	27. 11. 2026. 21:53:42 CET	25. 08. 2016. 17:19:34 CEST
-		entrustrootcaec1 [jdk]	EC	384	18. 12. 2037. 16:55:36 CET	25. 08. 2016. 17:20:04 CEST
-		entrustrootcag2 [jdk]	RSA	2048	07. 12. 2030. 18:55:54 CET	25. 08. 2016. 17:19:39 CEST
-		fina rdc 2015 (fina root ca)	RSA	4096	25. 11. 2025. 11:43:30 CET	14. 09. 2020. 08:59:06 CEST
-		fina rdc-tdu 2015 (fina root ca)	RSA	4096	25. 11. 2025. 17:40:09 CET	14. 09. 2020. 08:59:11 CEST
-		fina root ca	RSA	4096	24. 11. 2035. 20:37:30 CET	14. 09. 2020. 08:59:16 CEST
-		geotrustglobalca [jdk]	RSA	2048	21. 05. 2022. 06:00:00 CEST	25. 08. 2016. 17:20:16 CEST
-		geotrustprimaryca [jdk]	RSA	2048	17. 07. 2036. 01:59:59 CEST	25. 08. 2016. 17:19:51 CEST
-		geotrustprimarycag2 [jdk]	EC	384	19. 01. 2038. 00:59:59 CET	25. 08. 2016. 17:20:32 CEST
-		geotrustprimarycag3 [jdk]	RSA	2048	02. 12. 2037. 00:59:59 CET	25. 08. 2016. 17:20:31 CEST
-		geotrustuniversalca [jdk]	RSA	4096	04. 03. 2029. 06:00:00 CEST	25. 08. 2016. 17:19:46 CEST
-		globalsignca [jdk]	RSA	2048	28. 01. 2028. 13:00:00 CET	25. 08. 2016. 17:20:14 CEST
-		globalsigneccrootcar4 [jdk]	EC	256	19. 01. 2038. 04:14:07 CET	25. 08. 2016. 17:19:37 CEST
-		globalsigneccrootcar5 [jdk]	EC	384	19. 01. 2038. 04:14:07 CET	25. 08. 2016. 17:19:36 CEST
-		globalsignr2ca [jdk]	RSA	2048	15. 12. 2021. 09:00:00 CET	25. 08. 2016. 17:20:12 CEST
-		globalsignr3ca [jdk]	RSA	2048	18. 03. 2029. 11:00:00 CET	25. 08. 2016. 17:20:07 CEST
-		godaddyclass2ca [jdk]	RSA	2048	29. 06. 2034. 19:06:20 CEST	25. 08. 2016. 17:20:39 CEST
-		godaddyrootg2ca [jdk]	RSA	2048	01. 01. 2038. 00:59:59 CET	25. 08. 2016. 17:20:47 CEST
-		gtecybertrustglobalca [jdk]	RSA	1024	14. 08. 2018. 01:59:00 CEST	25. 08. 2016. 17:20:08 CEST
-		hridca (akdca root)	RSA	4096	01. 06. 2030. 17:08:08 CEST	14. 09. 2020. 08:58:31 CEST
-		identrustcommercial [jdk]	RSA	4096	16. 01. 2034. 19:12:23 CET	25. 08. 2016. 17:20:40 CEST

Oracle WebLogic Server – Administration Console





Nedostaci

- Nema filtriranja korisnika
- Potencijalni sigurnosni problem ako se ne koristi zadnja verzija – iskustvo iz HOPS-a
- Rješenje:
  - Stavljanje Oracle WebLogic komponenti u localhost
  - Korištenje Oracle HTTP servera kao reverse proxy za Oracle WebLogic Server

Oracle HTTP Server (OHS)

Oracle HTTP server (OHS)

- Web server komponenta za Oracle Fusion Middleware
- Sadrži listener za Oracle WebLogic Server
- Poslužuje statičke i dinamičke web stranice i web aplikacije
- Dijeli sličnost u konfiguraciji s Apache Web Server-om uz određene razlike – Oracle Wallet
- Preduvjeti:
  - HTTPS certifikat i privatni ključ
  - Oracle Wallet
  - Aktivirana pametna kartica i čitač pametne kartice

Oracle Wallet (1)

- Oracle Wallet – Spremište koje pohranjuje vjerodajnice poput certifikata, zahtjeva za certifikatima i privatnih ključeva koji se koristi kako bi OHS mogao od korisnika zatražiti certifikat željenog izdavatelja
- Koraci:
  - Kreiranje .p12 PKCS#12 datoteke iz prethodno kreiranog Java Identity Store-a
  - Kreiranje auto_login_only wallet-a
  - Import .p12 datoteke u auto_login_only wallet
  - Import trusted certifikata u kreirani wallet

Oracle Wallet (2)

- `keytool -importkeystore -srckeystore owl-test.jks -srcstoretype JKS -deststoretype PKCS12 -destkeystore ewallet.p12`

```
[oracle@owl-test HROUG]$ keytool -importkeystore -srckeystore owl-test.jks -srcstoretype JKS -deststoretype PKCS12 -destkeystore ewallet.p12
Importing keystore owl-test.jks to ewallet.p12...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias te-hopswebserversha256-d262bca6-8b67-4b32-9580-b4e496ea5aa4 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
[oracle@owl-test HROUG]$ ls -l
total 32
-rw-r--r-- 1 oracle oinstall 1423 Sep 27 08:58 akdcaroot.crt
-rw-r--r-- 1 oracle oinstall 3267 Sep 27 09:36 ewallet.p12
-rw-r--r-- 1 oracle oinstall 1806 Sep 27 08:58 FinaRDCCA2015.cer
-rw-r--r-- 1 oracle oinstall 1811 Sep 27 08:58 FinaRDC-TDUCA2015.cer
-rw-r--r-- 1 oracle oinstall 1396 Sep 27 08:58 FinaRootCA.cer
-rw-r--r-- 1 oracle oinstall 1770 Sep 27 08:58 hridca.crt
-rw-r--r-- 1 oracle oinstall 2764 Sep 27 07:36 owl-test.jks
-rw-r--r-- 1 oracle oinstall 3267 Sep 27 07:35 owl-test.pfx
[oracle@owl-test HROUG]$
```

Oracle Wallet (3)

- `/u01/app/oracle/product/12.2.1/oracle_common/bin/orapki wallet create -wallet . -auto_login_only`

```
[oracle@owl-test HROUG]$ /u01/app/oracle/product/12.2.1/oracle_common/bin/orapki wallet create -wallet . -auto_login_only
Oracle PKI Tool : Version 12.2.1.3.0
Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights reserved.

Operation is successfully completed.
```

Oracle Wallet (4)

- `/u01/app/oracle/product/12.2.1/oracle_common/bin/orapki wallet import_pkcs12 -wallet . -pkcs12file ewallet.p12 -auto_login_only`
- `orapki wallet display -wallet cwallet.sso`

```
[oracle@owl-test HROUG]$ /u01/app/oracle/product/12.2.1/oracle_common/bin/orapki wallet import_pkcs12 -wallet . -pkcs12file ewallet.p12 -auto_login_only
Oracle PKI Tool : Version 12.2.1.3.0
Copyright (c) 2004, 2017, Oracle and/or its affiliates. All rights reserved.

Enter PKCS#12 file password:
orapki command import_pkcs12 executed successfully.
```

```
[oracle@owl-test HROUG]$ orapki wallet display -wallet cwallet.sso
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

Requested Certificates:
User Certificates:
Subject:        EmailAddress=dba@hops.hr,CN=owl.biz.dom,OU=HOPS ICT,O=HOPS d.o.o.,L=Zagreb,ST=Zagreb,C=HR
Trusted Certificates:
[oracle@owl-test HROUG]$ ls -l
total 36
-rw-r--r-- 1 oracle oinstall 1423 Sep 27 08:58 akdcaroot.crt
-rw------- 1 oracle oinstall 3005 Sep 27 10:00 cwallet.sso
-rw------- 1 oracle oinstall    0 Sep 27 10:00 cwallet.sso.lck
-rw-r--r-- 1 oracle oinstall 3267 Sep 27 10:00 ewallet.p12
-rw------- 1 oracle oinstall    0 Sep 27 10:00 ewallet.p12.lck
-rw-r--r-- 1 oracle oinstall 1806 Sep 27 08:58 FinaRDCCA2015.cer
-rw-r--r-- 1 oracle oinstall 1811 Sep 27 08:58 FinaRDC-TDUCA2015.cer
-rw-r--r-- 1 oracle oinstall 1396 Sep 27 08:58 FinaRootCA.cer
-rw-r--r-- 1 oracle oinstall 1770 Sep 27 08:58 hridca.crt
-rw-r--r-- 1 oracle oinstall 2764 Sep 27 07:36 owl-test.jks
-rw-r--r-- 1 oracle oinstall 3267 Sep 27 07:35 owl-test.pfx
[oracle@owl-test HROUG]$
```

Oracle Wallet (5)

- `orapki wallet add -wallet cwallet.sso -cert hridca.crt -trusted_cert -auto_login_only`
- `orapki wallet add -wallet cwallet.sso -cert akdcaroot.crt -trusted_cert -auto_login_only`
- `orapki wallet add -wallet cwallet.sso -cert FinaRDC-TDUCA2015.cer -trusted_cert -auto_login_only`
- `orapki wallet add -wallet cwallet.sso -cert FinaRootCA.cer -trusted_cert -auto_login_only`
- `orapki wallet add -wallet cwallet.sso -cert FinaRDCCA2015.cer -trusted_cert -auto_login_only`
- `orapki wallet display -wallet cwallet.sso`

Oracle Wallet (6)

```
[oracle@owl-test HROUG]$ orapki wallet add -wallet cwallet.sso -cert hridca.crt -trusted_cert -auto_login_only
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

[oracle@owl-test HROUG]$ orapki wallet add -wallet cwallet.sso -cert akdcaroot.crt -trusted_cert -auto_login_only
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

[oracle@owl-test HROUG]$ orapki wallet add -wallet cwallet.sso -cert FinaRDC-TDUCA2015.cer -trusted_cert -auto_login_only
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

[oracle@owl-test HROUG]$ orapki wallet add -wallet cwallet.sso -cert FinaRootCA.cer -trusted_cert -auto_login_only
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

[oracle@owl-test HROUG]$ orapki wallet add -wallet cwallet.sso -cert FinaRDCCA2015.cer -trusted_cert -auto_login_only
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

[oracle@owl-test HROUG]$ orapki wallet display -wallet cwallet.sso
Oracle PKI Tool : Version 12.1.0.2
Copyright (c) 2004, 2014, Oracle and/or its affiliates. All rights reserved.

Requested Certificates:
User Certificates:
Subject:        EmailAddress=dba@hops.hr,CN=owl.biz.dom,OU=HOPS ICT,O=HOPS d.o.o.,L=Zagreb,ST=Zagreb,C=HR
Trusted Certificates:
Subject:        CN=Fina RDC-TDU 2015,O=Financijska agencija,C=HR
Subject:        CN=AKDCA Root,2.5.4.97=VATHR-58843087891,O=AKD d.o.o.,C=HR
Subject:        CN=Fina RDC 2015,O=Financijska agencija,C=HR
Subject:        CN=HRIDCA,2.5.4.97=VATHR-58843087891,O=AKD d.o.o.,C=HR
Subject:        CN=Fina Root CA,O=Financijska agencija,C=HR
[oracle@owl-test HROUG]$
```

OHS – konfiguracija (1)

- nano /u01/app/oracle/config/domains/hopsdomain/config/fmwconfig/components/OHS/instances/ohs1/ssl.conf

```
SSLVerifyClient require
SSLWallet "/home/oracle/HROUG"
<LocationMatch ”/forms/*”>
      <RequireAll>
         Require expr %{TIME_HOUR} -ge 9 && %{TIME_HOUR} -le 17
         <RequireAny>
            Require expr %{SSL_CLIENT_S_DN} =~ /OIB/
        </RequireAny>
      </RequireAll>
</LocationMatch>
```

OHS – konfiguracija (2)

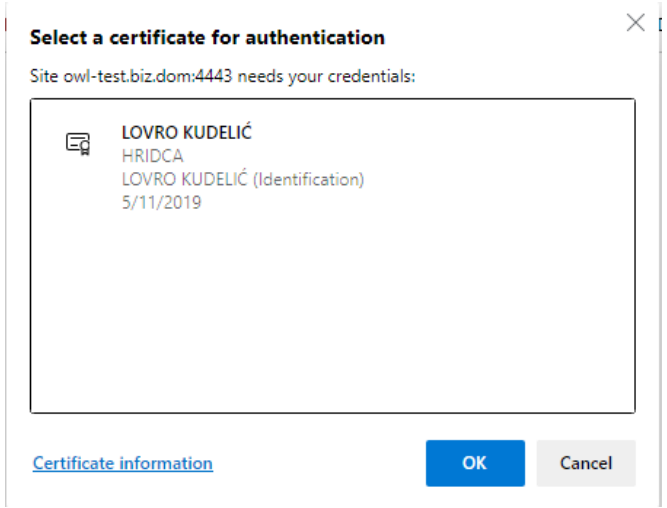
```
##
## SSL Virtual Host Context
##
#[VirtualHost] OHS_SSL_VH
<VirtualHost owl-test.biz.dom:4443>
  <IfModule ossl_module>
   #  SSL Engine Switch:
   #  Enable/Disable SSL for this virtual host.
   SSLEngine on

   #  Client Authentication (Type):
   #  Client certificate verification type and depth.  Types are
   #  none, optional and require.
   SSLVerifyClient require

   #  SSL Protocol Support:
   #  Configure usable SSL/TLS protocol versions.
   SSLProtocol ALL

   #  SSL Cipher Suite:
   #  List the ciphers that the client is permitted to negotiate.
   SSLCipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_

   # SSL Certificate Revocation List Check
   # Valid values are On and Off
   SSLCRLCheck Off

   #Path to the wallet
   SSLWallet "/home/oracle/HROUG"

   <FilesMatch "\.(cgi|shtml|phtml|php)$">
      SSLOptions +StdEnvVars
   </FilesMatch>

   <Directory "${ORACLE_INSTANCE}/config/fmwconfig/components/${COMPONENT_TYPE}/instances/${COMPONENT_NAME}/cgi-bin">
      SSLOptions +StdEnvVars
   </Directory>


<LocationMatch "/forms/*">
      <RequireAll>
        Require expr %{TIME_HOUR} -ge 9 && %{TIME_HOUR} -le 17
         <RequireAny>
            Require expr %{SSL_CLIENT_S_DN} =~ /OIB/
         </RequireAny>
      </RequireAll>
</LocationMatch>

   BrowserMatch "MSIE [2-5]" \
         nokeepalive ssl-unclean-shutdown \
         downgrade-1.0 force-response-1.0

  </IfModule>
</VirtualHost>

</IfModule>
```

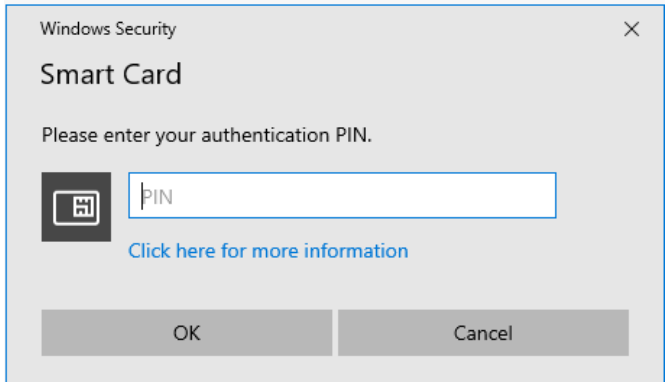
OHS – konfiguracija (3)

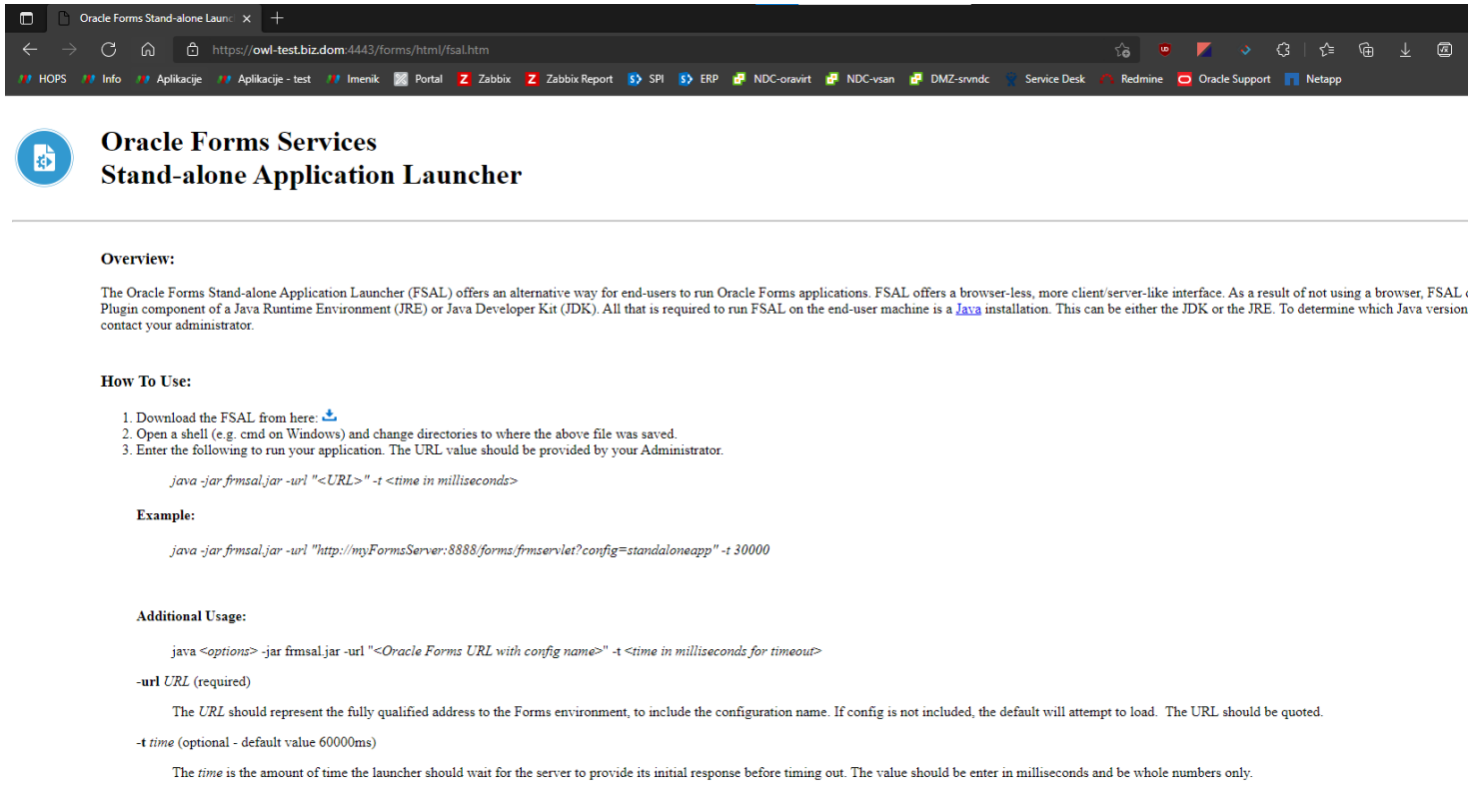
- Restart OHS-a:

```
$DOMAIN_HOME/bin/stopComponent.sh ohs1
$DOMAIN_HOME/bin/startComponent.sh ohs1
```

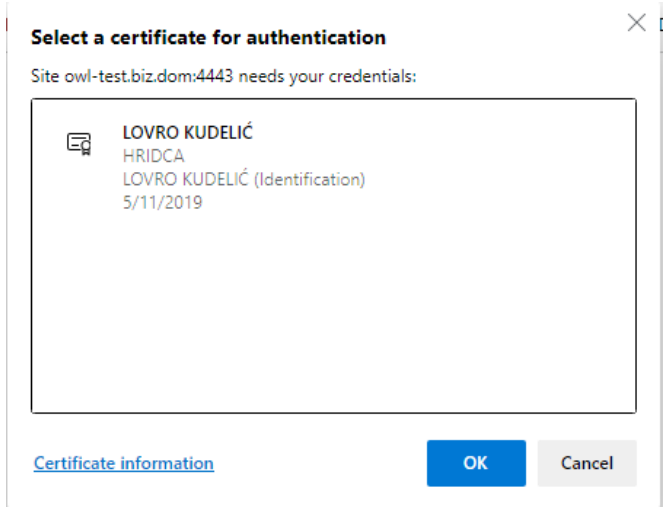
OHS – Pristup stranici - uspješno

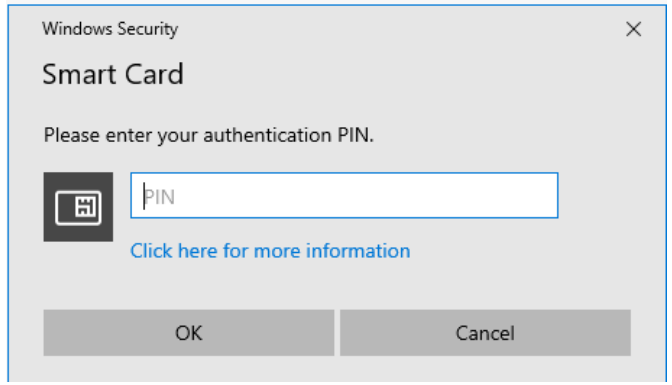


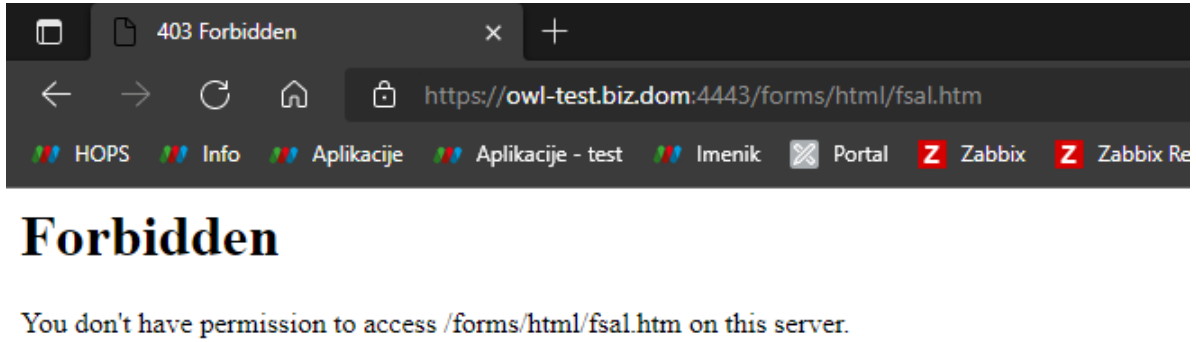




OHS – Pristup stranici – neuspješno



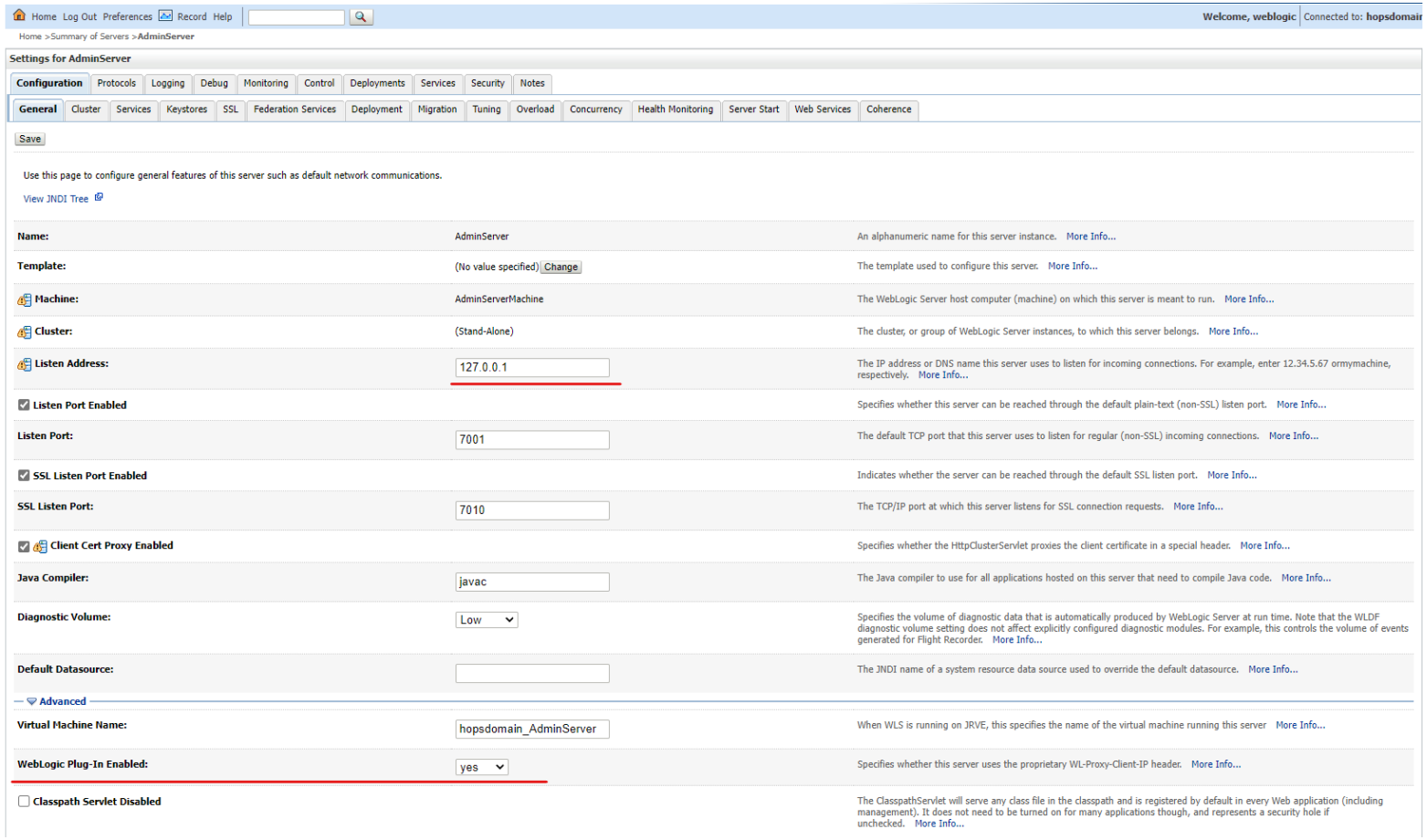




OHS kao reverse proxy za WebLogic Server

- Rješenje za problem filtriranja certifikata i korisnika
- Rješenje za potencijalne sigurnosne probleme WebLogic Servera
- Postavljanje kroz Administration Console-u i OHS

OHS kao reverse proxy – konfiguracija (1)



OHS kao reverse proxy – konfiguracija (2)

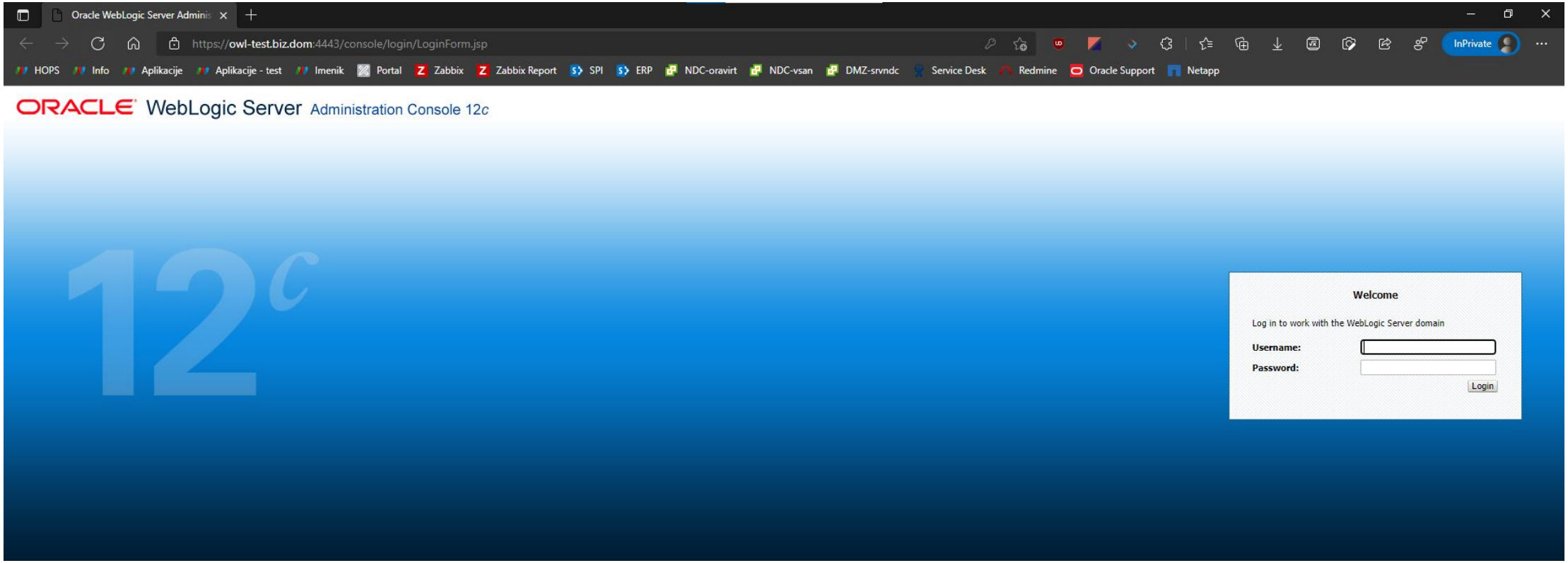
- nano /u01/app/oracle/config/domains/hopsdomain/config/fmwconfig/components/OHS/instances/ohs1/mod_wl_ohs.conf

```
LoadModule weblogic_module   "${PRODUCT_HOME}/modules/mod_wl_ohs.so"
<IfModule weblogic_module>
<Location /console>
       WLSRequest On
       WebLogicHost localhost
       WeblogicPort 7001
</Location>
<Location /em>
       WLSRequest On
       WebLogicHost localhost
       WeblogicPort 7001
</Location>
</IfModule>
```

OHS kao reverse proxy – konfiguracija (3)

```
# NOTE : This is a template to configure mod_weblogic.

LoadModule weblogic_module   "${PRODUCT_HOME}/modules/mod_wl_ohs.so"

# This empty block is needed to save mod_wl related configuration from EM to this file when changes are made at the Base Virtual Host Level
<IfModule weblogic_module>

<Location /console>
       WLSRequest On
       WebLogicHost localhost
       WeblogicPort 7001
</Location>

<Location /em>
       WLSRequest On
       WebLogicHost localhost
       WeblogicPort 7001
</Location>

#      WebLogicHost <WEBLOGIC_HOST>
#      WebLogicPort <WEBLOGIC_PORT>
#      MatchExpression *.jsp
</IfModule>

# <Location /weblogic>
#      SetHandler weblogic-handler
#      PathTrim /weblogic
#      ErrorPage  http:/WEBLOGIC_HOME:WEBLOGIC_PORT/
#  </Location>
```

OHS kao reverse proxy – Administration Console



Oracle Forms Standalone Launcher

Forms standalone aplikacije

- Napuštena podrška JAVE u preglednicima kao Java applet
- Napuštena Java web start tehnologija (Java 11 LTS)
- Jedini način koji ostaje je pokretanje Forms aplikacija kroz samostalni pokretač (engl. Standalone Launcher)
- Preduvjeti:
  - frmsall.jar
  - Aktivirana pametna kartica i čitač pametnih kartica
- Prikazani mehanizmi se mogu primijeniti i za druge Java aplikacije koje pristupaju resursima na poslužiteljima putem HTTPS protokola

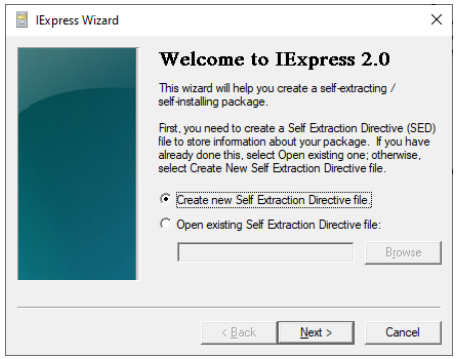
Forms standalone aplikacije – konfiguracija (1)

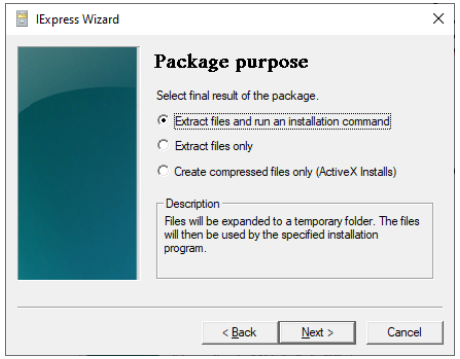
- Primjer za HOPS aplikaciju FIN
- Preuzeti frmsall.jar datoteku
- Kreirati .bat datoteku sa sadržajem:

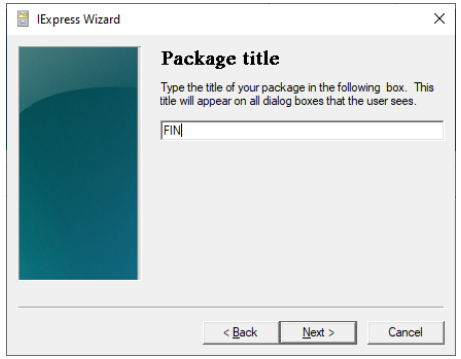
```
Title HOPS ERP
start "HOPS ERP„
"C:\Program Files (x86)\Java\jdk1.8.0_301\jre\bin\javaw.exe" ^
-Djavax.net.debug=ssl,handshake ^
-Djavax.net.ssl.keyStoreType=Windows-MY ^
-jar "C:\Users\lkudelic\Documents\Kuharice\Forms\frmsal.jar" ^
-url https://owl1.biz.dom:4443/forms/frmservlet?config=c3_fin
```

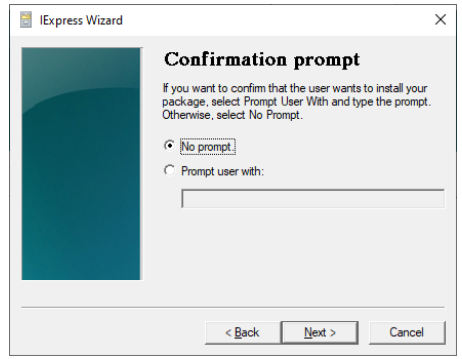
Forms standalone aplikacije – konfiguracija (2)

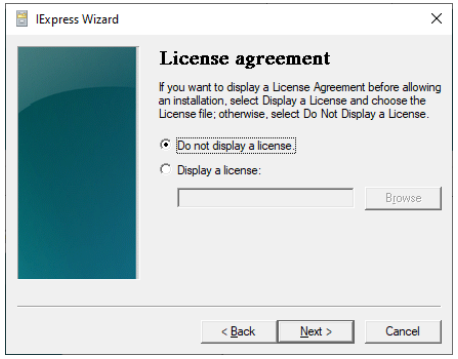
- Korištenjem programa iexpress na Windows računalima, kreira se exe datoteka pomoću koje ćemo pokretati Forms aplikaciju

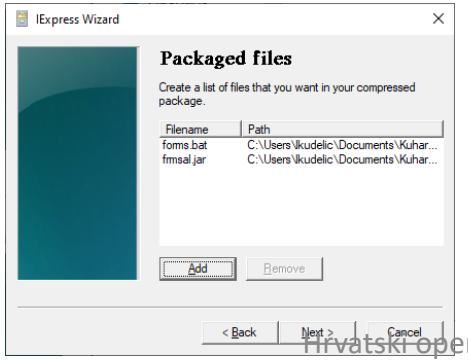


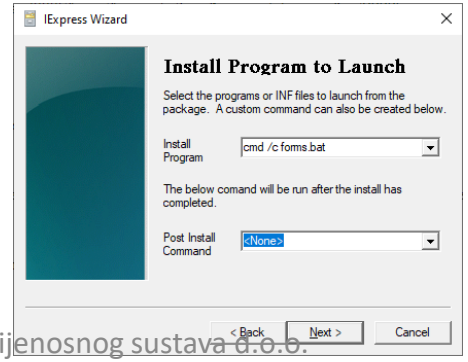


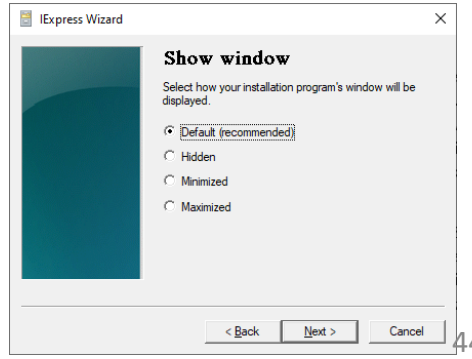




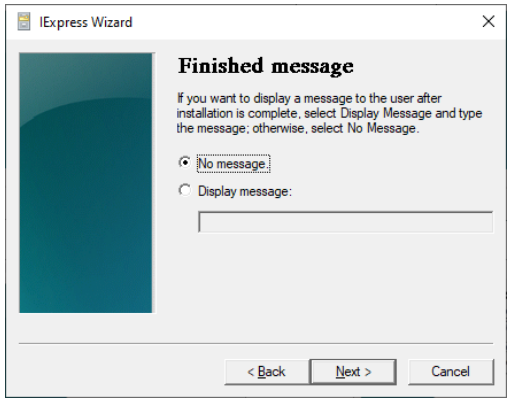


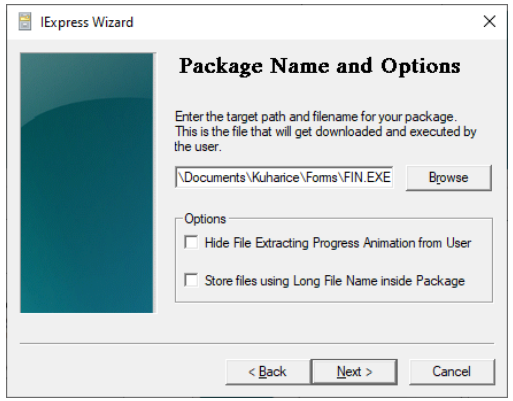


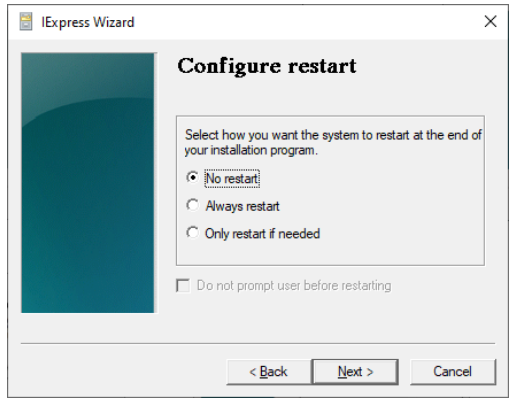


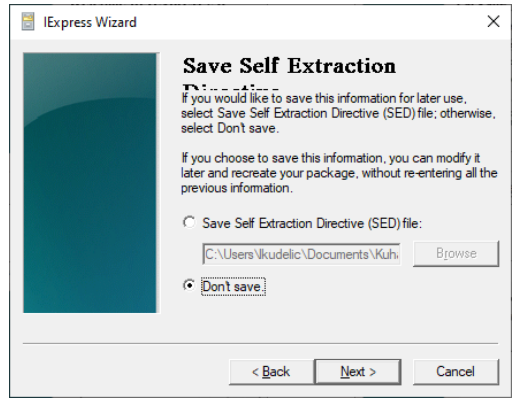


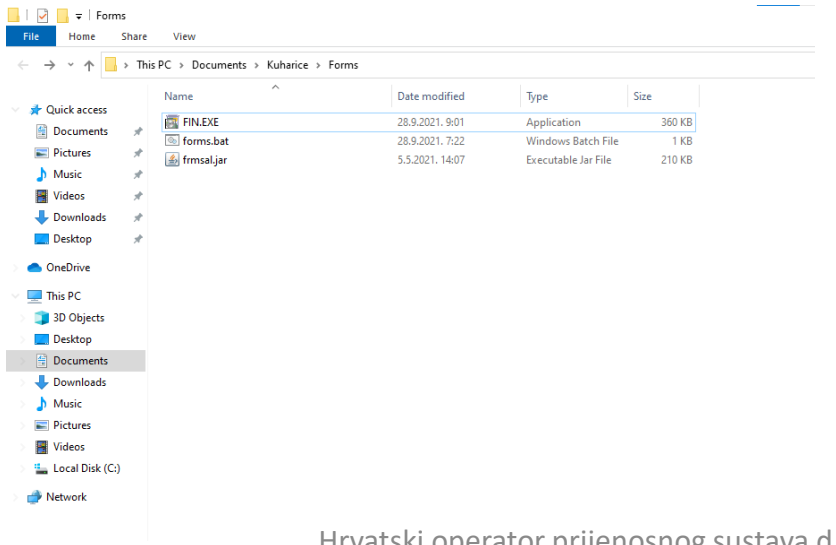
Forms standalone aplikacije – konfiguracija (3)





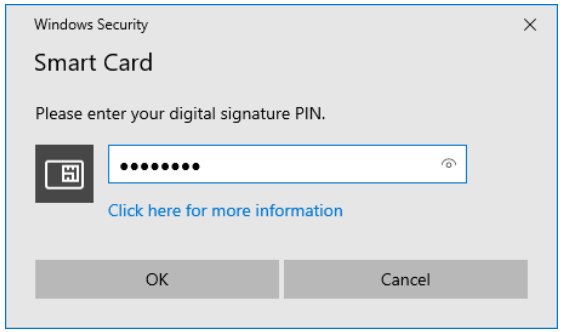


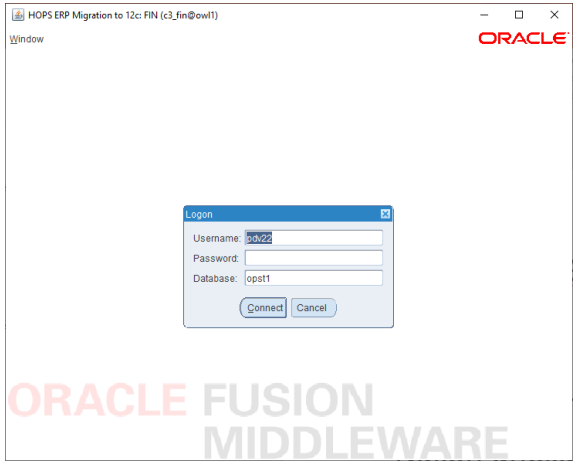




Forms standalone aplikacije

- Pokretanjem exe datoteke u pozadini se odvija provjera umetnute pametne kartice i ako je ona ispravna pojavi se prozor za unos PIN-a
- Nakon unosa PIN-a provjerava se OIB u korisničkom certifikatu i ako isti odgovara postavljenom na OHS-u korisniku se dozvoljava ulaz u aplikaciju





Prednosti i mane navedenih mehanizama

- Prednosti:
  - Visoka razina sigurnosti
  - Interoperabilnost
  - Niska cijena implementacije
  - Navedeni mehanizmi ne zahtijevaju promjene na aplikativnome nivou
- Mane:
  - Prilagodba korisnika na nove mehanizme autentifikacije
  - Politika tvrtke
  - Upravljanje certifikatima

Zaključak

- Prikazani mehanizmi pružaju izrazito visoku razinu kibernetičke sigurnosti
- Mogu se koristiti u implementaciji zahtjeva NIS2 (Direktiva o sigurnosti mrežnih i informacijskih sustava) direktive kako bi izbjegli uspostavu administrativnih sankcija, uključujući kazne za povrede pri upravljanju rizicima i upravljanju kibernetičkom sigurnošću.
- Navedene konfiguracije se mogu primijeniti i za sve druge web bazirane aplikacije koje poslužuje Apache Web Server (npr. Oracle Apex aplikacije)

Hvala Vam na pažnji!