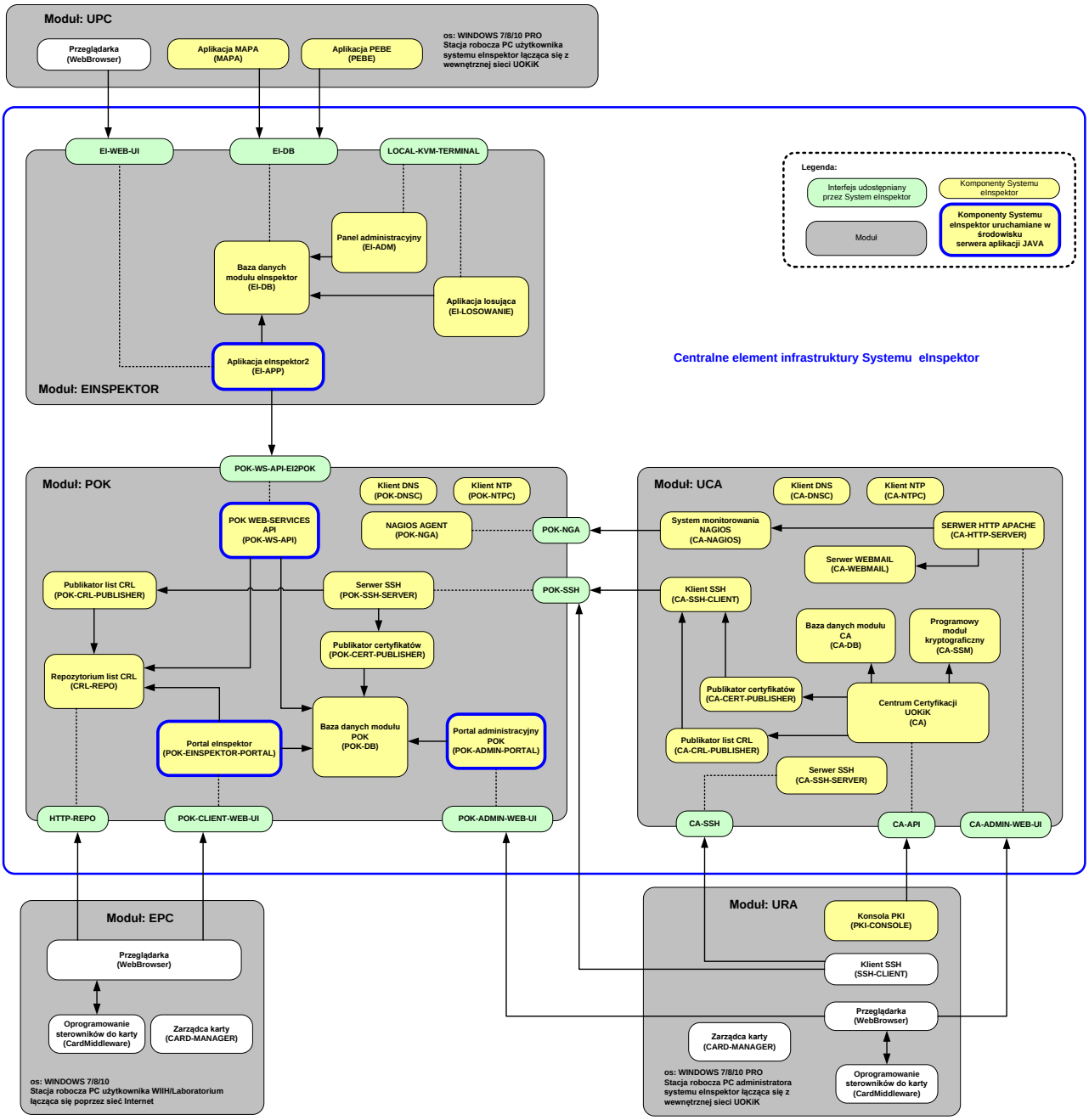
Architektura systemu eInspektor2

Spis treści

1 Architektura rozwiązania

1.1 Architektura logiczna systemu eInspektor

Na poniższym schemacie została zaprezentowana architektura logiczna systemu eInspektor.



W ramach architektury logicznej systemu PKI można wyróżnić następujące moduły:

- Moduł EINSPEKTOR
- Moduł UCA

- Moduł POK
- Moduły UPC
- Moduły URA
- Moduły EPC

Ponadto, jako otoczenie systemu PKI wskazano moduł UOKIK zawierający usługi współpracujące z systemem eInspektor takie jak:

- DNS-SERVER
- NTP-SERVER

W kolejnych rozdziałach opisano składowe bloki funkcjonalne modułów oraz ich podstawowe funkcje.

1.2 Opis modułów logicznych architektury.

1.2.1 Moduł UCA

Moduł centrum certyfikacji UCA składa się z następujących bloków funkcjonalnych:

- Baza danych modułu CA (CA-DB)
- Centrum Certyfikacji UOKiK (CA)
- Programowy moduł kryptograficzny (CA-SSM)
- Publikator certyfikatów (CA-CERT-PUBLISHER)
- Publikator list CRL (CA-CRL-PUBLISHER)
- Server SSH (CA-SSH-SERVER)
- Klient SSH (CA-SSH-CLIENT)
- Klient NTP (CA-NTPC)
- Klient DNS (CA-DNSC)
- System monitorowania NAGIOS (CA-NAGIOS)
- Serwer WEBMAIL (CA-WEBMAIL)
- Serwer HTTP APACHE (CA-HTTP-RESVER)

Bloki funkcjonalne funkcjonujące w ramach modułu są odpowiedzialne między innymi za obsługę procesu rejestracji wniosków o wydanie certyfikatów, generacji certyfikatów w standardzie X.509 v3 (RFC 5280), wydawania certyfikatów, publikacji certyfikatów, unieważniania certyfikatów, generowania i publikacji list CRL, personalizacji kart, udostępniania informacji o statusie certyfikatu z zastosowaniem list CRL. Dodatkowo w ramach modułu UCA został zlokalizowany moduł monitorowania.

W kolejnych rozdziałach opisano wskazane składowe bloki funkcjonalne modułów oraz ich podstawowe funkcje

1.2.1.1 Baza danych modułu CA (CA-DB)

Blok funkcjonalny bazy danych modułu CA (CA-DB) pełni rolę systemu zarządzania relacyjną bazą danych dla bloku funkcjonalnego Urząd Certyfikacji CA i funkcjonuje w oparciu o oprogramowanie PostgreSQL.

1.2.1.2 *Centrum Certyfikacji UOKiK (CA)*

Blok funkcjonalny Centrum Certyfikacji UOKiK (CA) realizuje funkcje związane z infrastrukturą klucza publicznego PKI wg. standardu X.509 v3 (RFC 5280) oraz systemu personalizacji i zarządzania kartami. Blok ten współpracuje między innymi z blokami funkcjonalnymi takim jak: baza danych modułu CA, programowy moduł kryptograficzny, publikator certyfikatów, publikator list CRL, konsola PKI. Blok funkcjonalny funkcjonuje w oparciu o oprogramowanie MALKOM QR-CERT (moduły oprogramowania: CA-ENGIN, CA-GATEWAY, CA-PUBLISHER, KG-INIT).

1.2.1.3 *Programowy moduł kryptograficzny (CA-SSM)*

Programowy moduł kryptograficzny został wdrożony w oparciu o oprogramowanie MALKOM QR-CERT moduł SSM i współpracuje z modułem CA za pośrednictwem interfejsu w standardzie PKCS#11.

1.2.1.4 *Publikator certyfikatów (CA-CERT-PUBLISHER)*

Publikator certyfikatów (CA-CERT-PUBLISHER) został wdrożony jako skrypt w języku PYTHON, który wykorzystuje mechanizm klienta SSH w celu transportu zleceń publikacji certyfikatu przekazywanych przez moduł CA do modułu POK.

1.2.1.5 *Publikator list CRL (CA-CRL-PUBLISHER)*

Publikator list CRL (CA-CRL-PUBLISHER) został wdrożony jako skrypt w języku PYTHON, który wykorzystuje mechanizm klienta SSH w celu transportu zleceń publikacji list CRL przekazywanych przez moduł CA do modułu POK.

1.2.1.6 *Server SSH (CA-SSH-SERVER)*

Blok funkcjonalny Serwer SSH (CA-SSH-SERVER) pełni rolę mechanizmu udostępniającego interfejs SSH do zarządzania modułem UCA oraz mechanizmu transportu certyfikatów i list CRL. Blok został wdrożony z wykorzystaniem oprogramowania OpenSSH Server.

1.2.1.7 *Klient SSH (CA-SSH-CLIENT)*

Klient SSH (CA-SSH-CLIENT) pełni rolę mechanizmu transportu certyfikatów i list CRL do serwera POK. Blok został wdrożony z wykorzystaniem oprogramowania OpenSSH Client.

1.2.1.8 *Klient NTP (CA-NTPC)*

Klient NTP (CA-NTPC) pełni rolę mechanizmu synchronizacji z serwerem czasu NTP

1.2.1.9 *Klient DNS (CA-DNSC)*

Klient DNS (CA-DNSC) pełni rolę mechanizmu rozwiązywania nazw na adresy IP w oparciu o serwer DNS.

1.2.1.10 *System monitorowania NAGIOS (CA-NAGIOS)*

System monitorowania NAGIOS (CA-NAGIOS) został wdrożony w oparciu o oprogramowanie NAGIOS i NAGVIS. Jego podstawową funkcją jest monitorowanie pracy systemów operacyjnych modułów POK i UCA oraz wybranych usług funkcjonujących w ramach tych modułów.

1.2.1.11 *Serwer WEBMAIL (CA-WEBMAIL)*

Serwer WEBMAIL (CA-WEBMAIL) został wdrożony w oparciu o oprogramowanie Roundcube. Podstawową funkcją bloku jest udostępnianie zgromadzonych na serwerze komunikatów diagnostycznych poczty elektronicznej za pośrednictwem interfejsu WWW.

1.2.1.12 Serwer HTTP APACHE (CA-HTTP-SERVER)

Blok funkcjonalny serwer HTTP APACHE (CA-HTTP-SERVER) pełni rolę bramy dostępowej udostępniającej usługi bloków CA-NAGIOS i CA-WEBMAIL za pośrednictwem protokołu HTTP (interfejs CA-ADMIN-WEB-UI) i funkcjonuje w oparciu o oprogramowanie Apache HTTP Server.

1.2.2 Moduł eINSPEKTOR2

Moduł EINSPEKTOR składa się z następujących bloków funkcjonalnych:

- Baza danych modułu eInspektor (EI-DB)
- Aplikacja eInspektor 2 (EI-APP)
- Panel administracyjny (EI_ADM)
- Aplikacja losująca (EI-LOSOWANIE)

1.2.2.1 Baza danych modułu eInspektor (EI-DB)

Blok funkcjonalny bazy danych modułu eInspektor (EI-DB) pełni rolę systemu zarządzania relacyjną bazą danych dla bloków funkcjonalnych: aplikacja eInspektor, panel administracyjny, aplikacja losująca, aplikacja mapa, aplikacja PEBE. Blok ten udostępnia interfejs EI-DB na potrzeby bloków aplikacja mapa, aplikacja PEBE.
Blok ten został wdrożony z wykorzystaniem oprogramowania Microsoft SQL Server.

1.2.2.2 Aplikacja eInspektor 2 (EI-APP)

Blok funkcjonalny aplikacja eInspektor (EI-APP) realizuje funkcje związane z obsługą systemu kontroli jakości paliw. Komponent ten udostępnia interfejs EI-WEB-UI dla pracowników UOKiK, do którego dostęp uzyskuje się za pomocą przeglądarki internetowej. Komponent ten łączy się również do modułów POK w celu replikacji danych słownikowych oraz pobierania kart kontroli przygotowanych w module POK.
Blok został wdrożony z wykorzystaniem aplikacji dedykowanej eInspektor2 zainstalowanej na serwerze aplikacji JAVA o nazwie TOMCAT.

1.2.2.3 Panel administracyjny (EI-ADM)

Blok funkcjonalny Panel administracyjny (EI-ADM) realizuje funkcje związane z zarządzaniem użytkownikami i ich uprawnieniami oraz dostępem do rejestru zdarzeń dla modułu EINSPEKTOR.
Blok został wdrożony z wykorzystaniem aplikacji dedykowanej eInspektor2 - Panel administracyjny.

1.2.2.4 Aplikacja losująca (EI-LOSOWANIE)

Blok funkcjonalny Aplikacja losująca (EI-LOSOWANIE) realizuje funkcje związane z obsługą procesu losowania podmiotów dot. kontrolami paliw.
Blok został wdrożony z wykorzystaniem aplikacji dedykowanej eInspektor2 - Losowanie.

1.2.3 Moduł POK

Moduł POK składa się z następujących bloków funkcjonalnych:

- Baza danych modułu POK (POK-DB)
- Portal eInspektor (POK-EINSPEKTOR-PORTAL)
- Portal administracyjny POK (POK-ADMIN-PORTAL)

- POK WEB-SERVICES API (POK-WS-API)
- Repozytorium list CRL (CRL-REPO)
- Publikator list CRL (POK-CRL-PUBLISHER)
- Publikator certyfikatów (POK-CERT-PUBLISHER)
- Serwer SSH (POK-SSH-SERVER)
- Klient NTP (POK-NTPC)
- Klient DNS (POK-DNSC)
- NAGIOS AGENT (POK-NGA)

1.2.3.1 Baza danych modułu POK (POK-DB)

Blok funkcjonalny Baza danych modułu POK (POK-DB) pełni rolę systemu zarządzania relacyjną bazą danych dla następujących bloków funkcjonalnych: Portal eInspektor (POK-EINSPEKTOR-PORTAL), Portal administracyjny POK (POK-ADMIN-PORTAL), POK WEB-SERVICES API (POK-WS-API). Komponent został wdrożony z zastosowaniem oprogramowania PostgreSQL.

1.2.3.2 Portal eInspektor (POK-EINSPEKTOR-PORTAL)

Blok funkcjonalny Portal eInspektor (POK-EINSPEKTOR-PORTAL) realizuje funkcje związane z obsługą kart kontroli paliw stałych oraz wyników badań próbek paliw stałych. Komponent ten udostępnia interfejs POK-CLIENT-WEB-UI dla pracowników WIIH oraz pracowników laboratoriów, do którego dostęp uzyskuje się za pomocą przeglądarki internetowej.
Blok został wdrożony z wykorzystaniem aplikacji dedykowanej eInspektor Portal zainstalowanej na serwerze aplikacji JAVA o nazwie WildFly.

1.2.3.3 Portal administracyjny POK (POK-ADMIN-PORTAL)

Blok funkcjonalny Portal administracyjny POK (POK-ADMIN-PORTAL) realizuje funkcje związane z administracją kontami i uprawnieniami modułu aplikacji webowych POK. Komponent ten udostępnia interfejs POK-ADMIN-WEB-UI dla pracowników UOKiK oraz administratora UOKiK, do którego dostęp uzyskuje się za pomocą przeglądarki internetowej.
Blok został wdrożony z wykorzystaniem aplikacji dedykowanej eInspektor Portal zainstalowanej na serwerze aplikacji JAVA o nazwie WildFly.

1.2.3.4 POK WEB-SERVICES API (POK-WS-API)

Blok funkcjonalny POK WEB-SERVICES API (POK-WS-API) realizuje funkcje związane z wymianą danych w sposób automatyczny z modułem EINSPEKTOR. Komponent ten udostępnia interfejs POK-WS-API-EI2POK dla modułu EINSPEKTOR.
Blok został wdrożony z wykorzystaniem aplikacji dedykowanej eInspektor Portal zainstalowanej na serwerze aplikacji JAVA o nazwie WildFly.

1.2.3.5 Repozytorium list CRL (CRL-REPO)

Blok funkcjonalny Repozytorium list CRL (CRL-REPO) pełni rolę serwera udostępniającego listę CRL za pośrednictwem protokołu HTTP (interfejs HTTP-REPO) i funkcjonuje w oparciu o oprogramowanie Apache HTTP Server.

1.2.3.6 Publikator list CRL (POK-CRL-PUBLISHER)

Blok funkcjonalny Publikator list CRL (POK-CRL-PUBLISHER) pełni funkcję mechanizmu dystrybucji lisy CRL otrzymywanej z modułu UCA. Komponent został

wdrożony jako skrypt w języku PYTHON, który publikuje listy CRL przekazywane za pośrednictwem kanału SSH do odpowiedniego katalogu komponentu CRL-REPO.

1.2.3.7 Publikator certyfikatów (POK-CERT-PUBLISHER)

Blok funkcjonalny Publikator certyfikatów (POK-CERT-PUBLISHER) pełni funkcję mechanizmu dystrybucji certyfikatów otrzymywanych z modułu UCA. Komponent został wdrożony jako skrypt w języku PYTHON, który publikuje certyfikaty przekazywane za pośrednictwem kanału SSH do odpowiedniego katalogu komponentu CRL-REPO.

1.2.3.8 Serwer SSH (POK-SSH-SERVER)

Blok funkcjonalny Serwer SSH (POK-SSH-SERVER) pełni rolę mechanizmu udostępniającego interfejs SSH do zarządzania modułem UCA oraz mechanizmu transportu certyfikatów i list CRL. Blok został wdrożony z wykorzystaniem oprogramowania OpenSSH Server.

1.2.3.9 Klient NTP (POK-NTPC)

Klient NTP (POK-NTPC) pełni rolę mechanizmu synchronizacji z serwerem czasu NTP

1.2.3.10 Klient DNS (POK-DNSC)

Klient DNS (POK-DNSC) pełni rolę mechanizmu rozwiązywania nazw na adresy IP w oparciu o serwer DNS.

1.2.3.11 NAGIOS AGENT (POK-NGA)

Blok funkcjonalny NAGIOS AGENT (POK-NGA) pełni rolę agenta raportującego stan parametrów systemu operacyjnego i wybranych usług modułu POK do komponentu System monitorowania NAGIOS.

1.2.4 Moduł URA

Moduł URA składa się z następujących bloków funkcjonalnych:

- Konsola PKI (PKI-CONSOLE)
- Klient SSH (SSH-CLIENT)
- Przeglądarka (WebBrowser)
- Oprogramowanie sterowników do karty (CardMiddleware)
- Zarządca karty (CARD-MANAGER)

1.2.4.1 Konsola PKI (PKI-CONSOLE)

Blok funkcjonalny Konsola PKI (PKI-CONSOLE) pełni rolę interfejsu konsoli zarządzania blokiem funkcjonalnym Centrum Certyfikacji UOKiK (CA). Komponent został wdrożony z wykorzystaniem oprogramowania MALKOM QR-CERT (moduły oprogramowania: OPERATOR).

1.2.4.2 Klient SSH (SSH-CLIENT)

Blok funkcjonalny Klient SSH (SSH-CLIENT) pełni rolę interfejsu konsoli zarządzania blokami funkcjonalnymi systemu eInspektor takimi jak: serwery fizyczne i wirtualne: pok, uca.
Komponent został wdrożony z wykorzystaniem oprogramowania PuTTY.

1.2.4.3 Przeglądarka (WebBrowser)

Blok funkcjonalny Przeglądarka internetowa WWW (WebBrowser) pełni rolę interfejsu konsoli zarządzania blokiem funkcjonalnym CA-HTTP-SERVER oraz POK-ADMIN-PORTAL i funkcjonuje w oparciu o oprogramowanie Microsoft EDGE oraz Microsoft Internet Explorer.

1.2.4.4 Oprogramowanie sterowników do karty (CardMiddleware)

Blok funkcjonalny Oprogramowanie sterowników do karty (CardMiddleware) pełni rolę interfejsu API umożliwiającego dostęp z poziomu systemu operacyjnego do kluczy i certyfikatów zawartych na karcie.

1.2.4.5 Zarządca karty (CARD-MANAGER)

Blok funkcjonalny Zarządca karty (CARD-MANAGER) pełni rolę aplikacji do zarządzania kartą a w szczególności do zmiany kodu PIN karty i odblokowania karty w przypadku zablokowania kodu PIN. Blok funkcjonalny został zrealizowany z użyciem oprogramowania MALKOM QR-CARD MANGER.

1.2.5 Moduł UPC

Moduł UPC składa się z następujących bloków funkcjonalnych:

- Aplikacja MAPA (MAPA)
- Aplikacja PEBE (PEBE)
- Przeglądarka (WebBrowser)

1.2.5.1 Aplikacja MAPA (MAPA)

Blok funkcjonalny Aplikacja MAPA (MAPA) pełni rolę aplikacji zapewniającej wizualizację kontroli wylosowanych w aplikacji losującej oraz umożliwia ręczne dodawanie podmiotów do kontroli.
Komponent został wdrożony z zastosowaniem dedykowanego oprogramowania eInspektor Mapa Kraju, który do wizualizacji wykorzystuje oprogramowanie MapXtreme firmy Pitney Bowes.

1.2.5.2 Aplikacja PEBE (PEBE)

1.2.5.3 Przeglądarka (WebBrowser)

Blok funkcjonalny Przeglądarka internetowa WWW (WebBrowser) pełni rolę interfejsu użytkownika podczas korzystania z komponentu Aplikacja eInspektor2 (EI_APP) i funkcjonuje w oparciu o oprogramowanie Microsoft EDGE oraz Microsoft Internet Explorer.

1.2.6 Moduł EPC

Moduł EPC składa się z następujących bloków funkcjonalnych:

- Przeglądarka (WebBrowser)
- Oprogramowanie sterowników do karty (CardMiddleware)
- Zarządca karty (CARD-MANAGER)

1.2.6.1 *Przeglądarka (WebBrowser)*

Blok funkcjonalny Przeglądarka internetowa WWW (WebBrowser) pełni rolę interfejsu użytkownika podczas korzystania z komponentu Portal eInspektor i funkcjonuje w oparciu o oprogramowanie Microsoft EDGE oraz Microsoft Internet Explorer.

1.2.6.2 *Oprogramowanie sterowników do karty (CardMiddleware)*

Blok funkcjonalny Oprogramowanie sterowników do karty (CardMiddleware) pełni rolę interfejsu API umożliwiającego dostęp z poziomu systemu operacyjnego do kluczy i certyfikatów zawartych na karcie.

1.2.6.3 *Zarządca karty (CARD-MANAGER)*

Blok funkcjonalny Zarządca karty (CARD-MANAGER) pełni rolę aplikacji do zarządzania kartą, a w szczególności do zmiany kodu PIN karty i odblokowania karty w przypadku zablokowania kodu PIN. Blok funkcjonalny został zrealizowany z użyciem oprogramowania MALKOM QR-CARD MANGER.