Sekcia informačných technológií verejnej správy

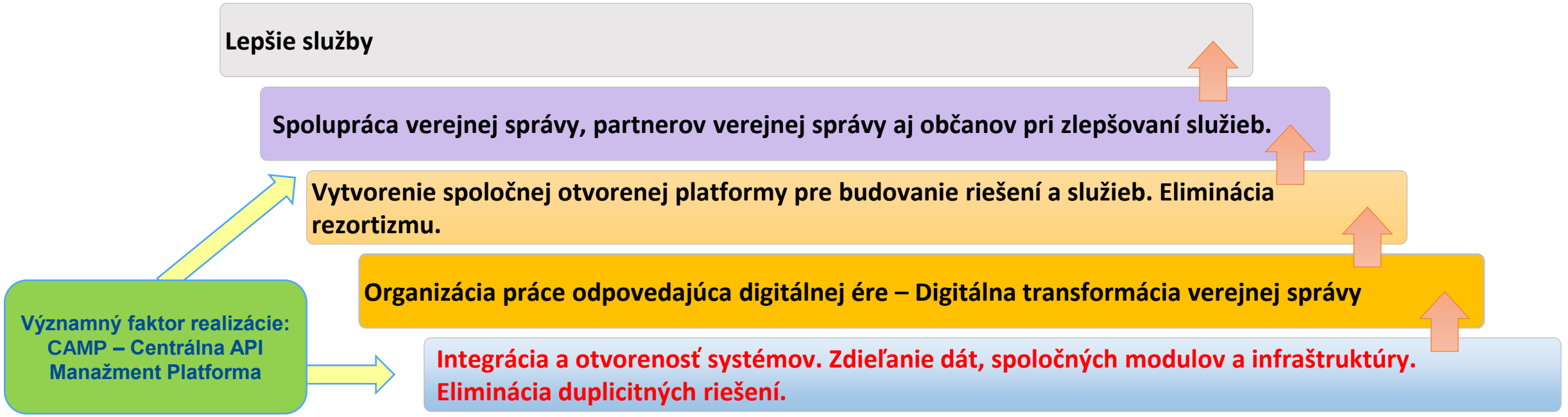
CAMP – Centrálna API manažment platforma

Anton Svetlošák
anton.svetlosak@mirri.gov.sk

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CAMP – Centrálna API manažment platforma

- NKIVS: Budovanie otvorenej platformy verejnej správy



Ciele a výstupy projektu CAMP

Ciele:

Centrálne manažované spístupnenie služieb ISVS poskytnutím integračnej platformy poskytujúcej služby pre lepšie riadenie a zjednodušenie publikácie služieb ISVS prostredníctvom Open API.

Chceme sprístupniť elektronické služby štátu cez Open API pre aplikácie v mobilných zariadeniach (Projekt Slovensko v Mobile) a umožniť modernizáciu ÚPVS.

Chceme zapojiť súkromný sektor a využiť jeho inovačný potenciál v prospech občana.

Chceme naplniť zákonnú povinnosť definovanú novelou zákona o e-Governmente.

Výstupy:

Vytvorenie centrálnej platformy pozostávajúcej z nakupovaných a parametrizovaných modulov

Sprístupnenie vybraných elektronických služieb VS v centrálnej API Manažment platforme - Služby UPVS, METAIS, MOU, CSRÚ

Sprístupnenie otvorených rozhraní služieb štátu a pripojenie **tretích strán** pre využívanie sprístupnených služieb

Sprístupnenie funkcionality API Manažment platformy pre **využitie subjektami VS pre interné rezortné využitie**

Motivácia pre tému Open API

- Open API je téma/produkt, ktorej cieľom je **umožniť komerčnému** aj **nekomerčnému sektoru využívať API služieb štátu**, aby mohli **vytvárať aplikácie s vysokou pridanou hodnotou pre koncového používateľa**.

- Aby bolo možné tento cieľ dosiahnuť je nutné:
  1. **Zverejňovať API**, o ktoré je záujem, majú **veľkú pridanú hodnotu** a teda budú **využívané tretími stranami**.
  2. Mať **technologické (centrálne) komponenty (CAMP)**, ktoré umožnia **API publikovať** a zároveň **jednoducho používať** tvorcom aplikácii a koncovým konzumentom.

Používateľské scenáre pre tému Open API

- Ako tretia strana chcem do svojich služieb integrovať služby ver. správy a poskytnúť ich ako nový komplexný produkt
- Ako používateľ chcem používať aplikáciu tretej strany, ktorá integruje služby ver. správy. (natívna, mobilná alebo webová aplikácia tretej strany)
- Ako orgán riadenia ITVS chcem využívať služby spoločných ISVS (napr. služby ÚPVS)
- Ako orgán riadenia ITVS chcem využiť službu iného agendového ISVS orgánu ver. správy pre moje služby a procesy, alebo pre kooperáciu s iným orgánom pre zabezpečenie spoločnej komplexnej služby, napr. riešenie životnej situácie
- Ako orgán riadenia ITVS chcem publikovať svoje služby

Ako sa budú aplikácie tretích strán registrovať do CAMP?

Registrovanie aplikácií tretích strán umožní modul Manažment tretích strán pomocou prípadov použitia cez Service Desk (NASES):

- Registrácia organizácie
  - Registrácia vývojárov tretích strán a vývojárov ISVS na vývojársky portál
    - Self registrácia správcu organizácie
    - Self registrácia používateľa pre existujúcu organizáciu
    - Registrácia API
  - Registrácia aplikácie
    - Registrovanie a spracovanie požiadavky na prístup k API (aj samoobslužne)
      - Vytvorenie prístupu k API
      - Registrácia aplikačnej autentifikácie
    - Nastavovanie prístupu osobitne pre každého konzumera API
      - Zmena prístupových oprávnení (Aplikácia-Rola) Administrátorom organizácie
      - Požiadavka na zmenu prístupových oprávnení (Aplikácia-Rola) používateľom

Bezpečná autentifikácia používateľov v CAMP

Používateľ pristupuje k funkcionalite cez mobilnú, webovú aplikáciu alebo integrovaný ISVS (tretia strana). Pre prácu v musí byť používateľ autentifikovaný. Predpokladáme nasledujúce alternatívy autentifikácie (neplatí pre API, ktoré budú verejne prístupné a nebudú požadovať autentifikáciu):

1. Autentifikácia pre používateľa

a) Autentifikácia cez **mID** - Autentifikácia používateľa bude primárne riešená použitím riešenia mobilnej identity (mID). mID bude použité pri autentifikácii používateľa, ktorý bude pracovať s mobilnou aplikáciou „Slovensko v mobile“, prípadne s aplikáciou tretej strany, ktorá je s aplikáciou „Slovensko v mobile“ integrované priamo (deepLink / URL Schema). Pri autentifikácii cez mID je úroveň eIDAS „pokročilá“.

b) Autentifikácia cez **eID kartu** - v prípade, že bude používateľ pracovať s portálom, môže použiť na autentifikáciu eID kartu s kontaktnou čítačkou kariet, v prípade dostupnosti riešenia pre bezkontaktné eID 2.0 s NFC čipom, aj to. Autentifikácia cez eID kartu je EIDAS registrovaná schéma autentifikácie s vysokou úrovňou bezpečnosti. Rovnako to bude platiť aj pri pripravovanej eID2.0 karte.

c) Autentifikácia **email – heslo** (**OAuth2**, **JWT**) – pre testovacie účely a pre integrujúce sa tretie strany vyžadujúce úroveň autentifikácie nízka, bude poskytnutá autentifikácia ma báze email-heslo. Vystavené JWT tokeny budú obsahovať úroveň tejto autentifikácie.

Bezpečná autentifikácia používateľov v CAMP

2. Autentifikácia aplikácii

a) **OIDC(JWT, OAuth2)** - v prípade prístupu aplikácie, teda akýchkoľvek integrovaných ISVS (tretia strana), má ako možnosť autentifikácie využitia autentifikácie pomocou registrovaného kľúčového páru v JWK formáte v systéme CAMP.

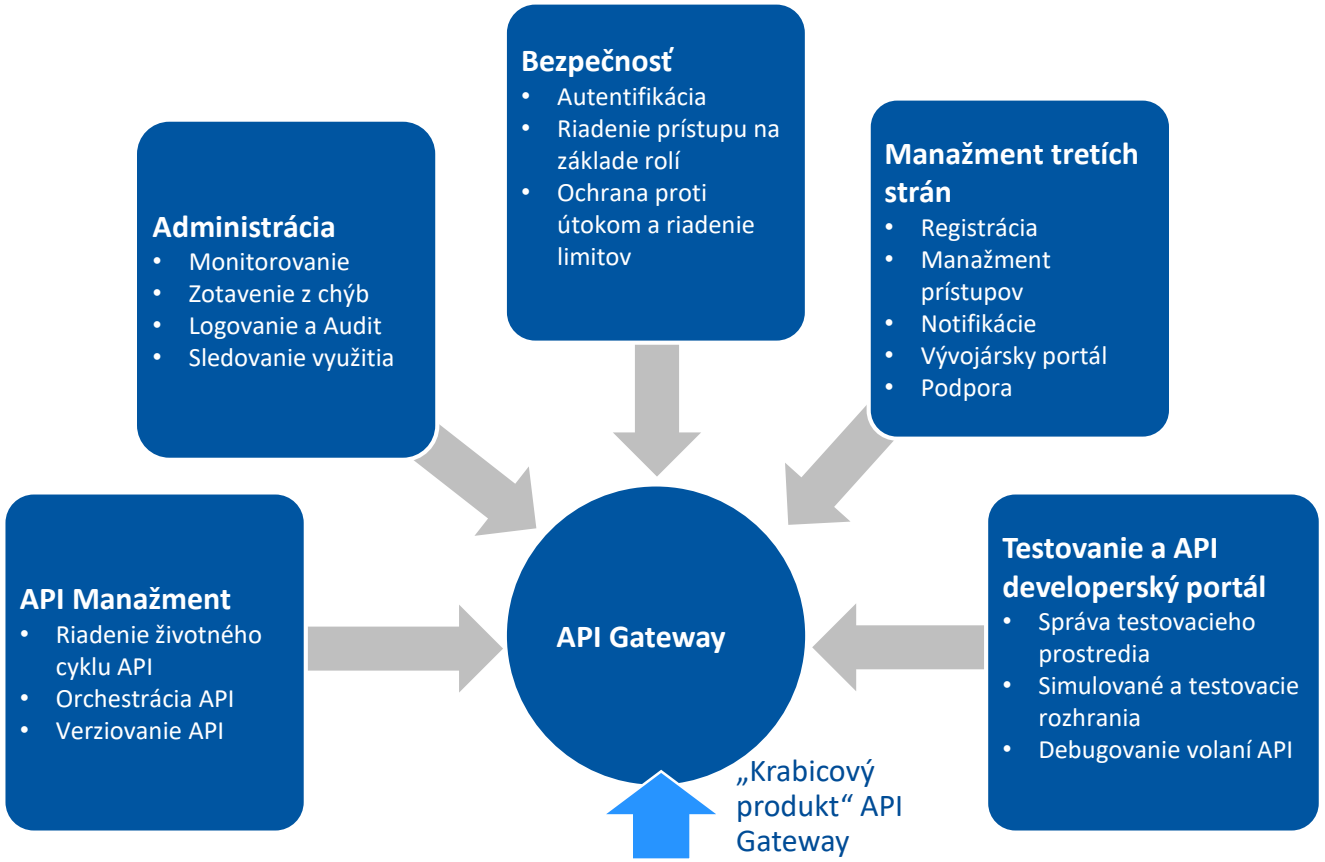
b) **mTLS s BASIC autentifikáciou** - v prípade prístupu aplikácie, teda akýchkoľvek integrovaných ISVS (tretia strana), má možnosť autentifikácie využitia mutual TLS (mTLS) autentifikácie v kombinácii s BASIC autentifikáciou pomocou meno a hesla administrátorských účtov. BASIC autentifikácia bude vyžadovaná len pri prístupe aplikácii na administrátorské API rozhrania.

c) **APIKey-PrivateKey autentifikáciou** - v prípade prístupu aplikácie, teda akýchkoľvek integrovaných ISVS (tretia strana), má možnosť autentifikácie s využitím symetrického šifrovania pomocou API kľúča generovaného systémom a vloženého privátneho kľúča pri registrácii aplikácie. Pri využívaní deepLink resp. URL schém je to nevyhnutná autentifikácia.

3. Autentifikácia administrátorov

a) **Meno-heslo** - v prípade prístupu administrátorov do administračných služieb vystavených cez API, teda akýchkoľvek administrátorov integrovaných ISVS ako aj administrátorov systému CAMP, bude poskytnutá autentifikácia pomocou mena a hesla registrovaného v LDAP systému CAMP.

CAMP – Moduly

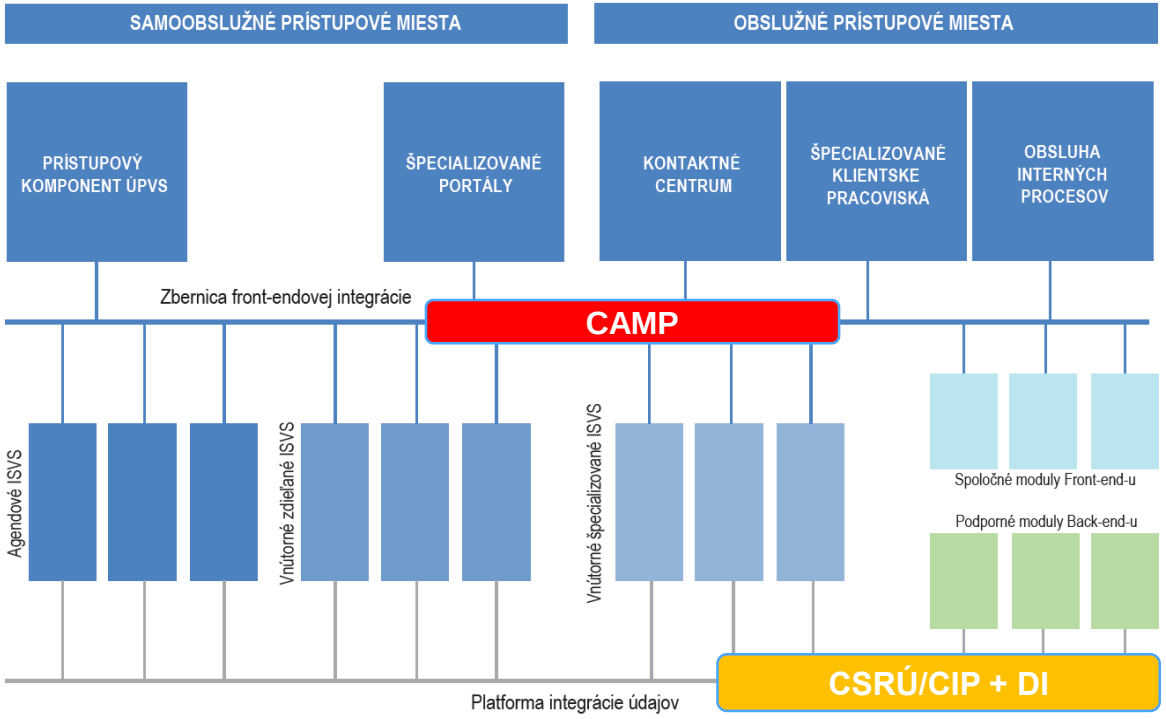

Bezpečnosť
• Autentifikácia
• Riadenie prístupu na základe rolí
• Ochrana proti útokom a riadenie limitov
Administrácia
• Monitorovanie
• Zotavenie z chýb
• Logovanie a Audit
• Sledovanie využitia
Manažment tretích strán
• Registrácia
• Manažment prístupov
• Notifikácie
• Vývojársky portál
• Podpora
API Manažment
• Riadenie životného cyklu API
• Orchestrácia API
• Verziovanie API
API Gateway
Testovanie a API developerský portál
• Správa testovacieho prostredia
• Simulované a testovacie rozhrania
• Debugovanie volaní API
„Krabicový produkt“ API Gateway

CAMP – Iniciálne publikované služby

- SVM
  - MID
  - PACHO (notifikácie)
- CSRU
- MOU (Manažment osobných údajov)
- MetaIS
- UPVS
  - IAM
  - EKR/eDESK
  - CEP
  - MDU
  - G2G
  - MEP

CAMP – Jednoduchý prípad použitia

Referenčná architektúra Integrovaného informačného systému verejnej správy a CAMP a CIP/CSRÚ

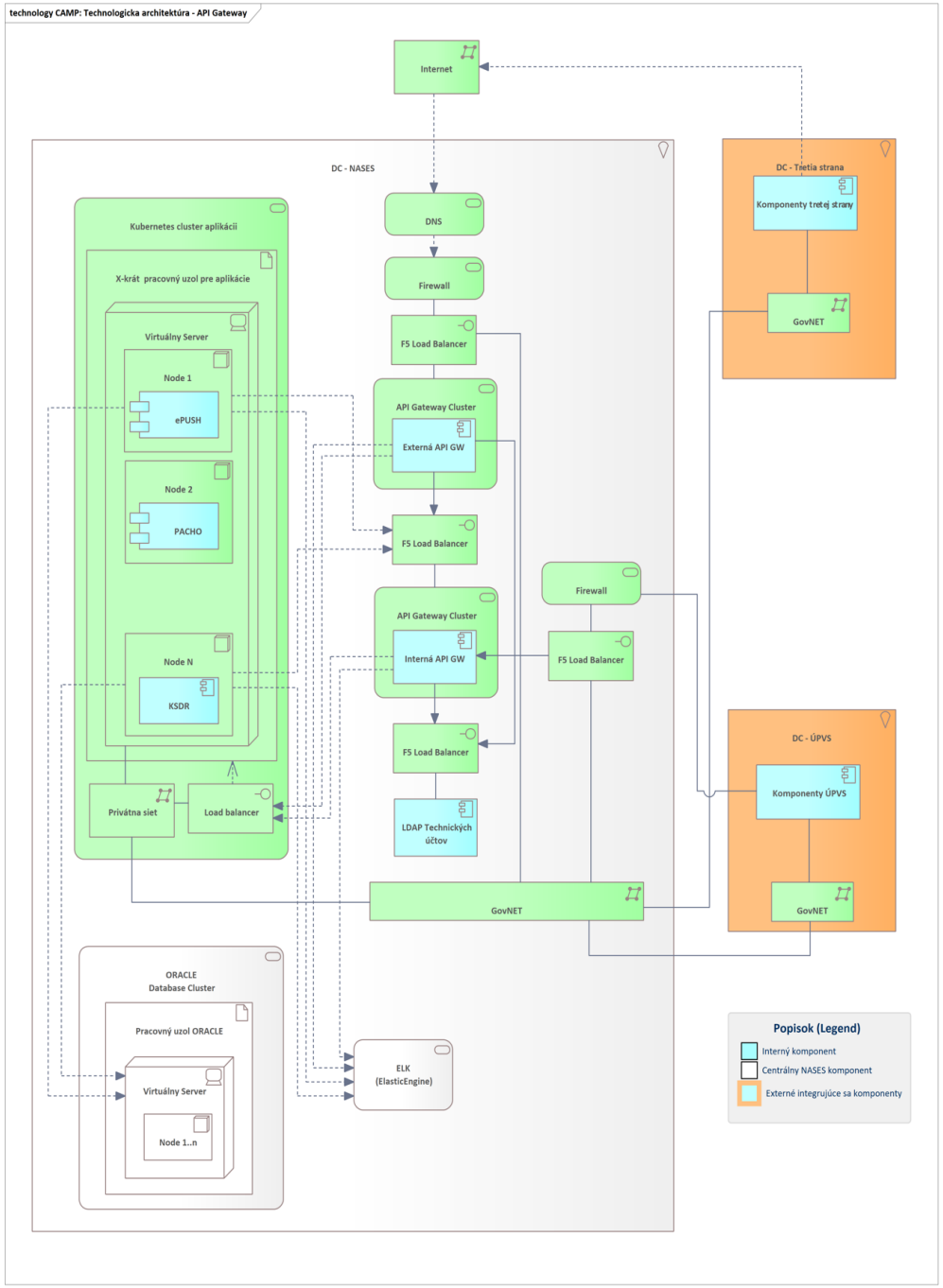


Centrálna API Manažment Platforma
(METAIS: projekt_514)

Cent. Systém Referenčných Údajov/ Centrálna Integračná Platforma + Dátová Integrácia
(METAIS: projekt_346 + projekt_327)

Odkaz na referenčnú architektúru IIS VS: https://www.mirri.gov.sk/sekcie/informatizacia/egovernment/sprava-architektury/referencna-architektura-isvs/index.html

Technologická architektúra integračnej zóny CAMP



CAMP – Hlavné časti aplikácie

- **Externá APIGW -** Verejná API Gateway vystavená pre prístup zo verejného Internetu
- **Interná APIGW –** Neverejná API Gateway vystavená pre prístup len z GOVNET siete
- **API Developer Portál** – komponent správy systému a publikovania API
- **Servis desk** - súčasť **CA Servise Managment**
- **LDAP technických a aplikačných účtov**
- **IdP CAMP, IdP mID** – Identity provider CAMP systému integruje autentifikačné metódy eID, mID a OAuth2
- **SwaggerHub –** Umožní návrhy a testing API v špecifikácie OpenAPI (OAS)
- **ELK** – Logovací komponent v NASES
- **Kafka** – Event broker pre publikovanie zmien nad aplikáciami a ich nastaveniami
- **Oracle RAC** – Oracle databázový server v infraštruktúre NASES

Figma - demo

https://www.figma.com/proto/c8kEUNFNpEb7dpEX5VNAR8/CAMP-(Demo)-(Texty)?node-id=366-1412&scaling=min-zoom&page-id=365%3A1336&starting-point-node-id=366%3A1412

Odkaz na dokumentáciu

https://metais.vicepremier.gov.sk/detail/Projekt/7d974952-97c2-4365-881a-e25f9dce9e6c/cimaster?tab=documentsForm

https://architektura.statneit.sk/centralne-projekty-mirri-sr/ a https://architektura.statneit.sk/wp-content/uploads/2023/04/DNR-CAMP.zip

Legislatívna podpora

- Vyhláška 547/2021 Z. z. o elektronizácii agendy verejnej správy (§ 5, ods. 5)
  - MIRRI pomocou vlastnej vyhlášky vedie tvorcov IS (OVM), aby robili používateľské prieskumy pre každý projekt. To zahŕňa aj aplikačné rozhrania. Každý projekt by teda mal zmapovať, aké služby a dáta budú chcieť využívať používatelia (tretie strany, tvorcovia aplikácii) a **výsledok** má byť dokonca **dostupný už v projektovom zámere** alebo **projektovom iniciálnom dokumente**.
- Zákon e-Governmente 305/2013 Z. z. (§ 25, ods. 7)
  - Všetky **podania** (aj **na UPVS** aj **špecializovaných portáloch**) sa musia dať **vytvoriť** aj **podať pomocou API**.

SLA

- Prevádzka bude zabezpečená v NASES,
  - vrátane L1 a L2 podpory, L3 dodávateľ
  - Zabezpečenie kyberbezpečnostného auditu pred spustením do prevádzky
  - RTO množstvo času potrebné pre obnovenie dát a celého prevádzky nedostupného systému - vytvorenie prostredí s minimálne 2 zastupujúcimi sa servermi v každej vrstve. Doba obnovenia systém je stanovená na 1 minútu.
  - RPO je stanovené na 1 minútu. Aplikovaný bude variant s vytváraním synchrónnych replík dát.
  - Dostupnosť nových služieb okrem plánovaných výpadkov je 99% v režime 24/7,
    - Plánovaný výpadok je oznámený minimálne 14 dní vopred,
    - Plánovaný výpadok nie je dlhší ako 8 hodín a je prioritne medzi 18 - 06:00, sobota alebo nedeľa.
    - Nasadzovanie nového API bude bez výpadku.

CAMP – Harmonogram

Legenda:

- Implemetácia, testovanie
- Nasadenie

Výhody pre Orgány riadenia

- Jedno miesto na ktorom sú publikované API rozhrania
- Jednotný manažement, procesy
- Jednotný prístup k autentifikácií a autorizácií ako služba
- Zjednodušenie DIZ
- Využitie pri implementácií agendových systémov
- Business funkcionalita jednotlivých modulov – bezpečnosť, manažment verzií, monitoring a analytika, testovanie a developer portál, manažment tretích strán atď.

S Open API môže byť spokojný každý

spokojní podnikatelia

Mobilné aplikácie, desktop aplikácie, responzívne weby

spokojný štát

spokojní občania

OTÁZKY / DISKUSIA