MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

PLÁN OBNOVY

Financované
Európskou úniou
NextGenerationEU

Čo prináša verejná časť vládneho cloudu

Architektúra a technické možnosti

Úvod

- Cieľ prezentácie je vysvetliť technický a architektonický rámec vládneho cloudu.
- Zameriavame sa zodpovednosti, kompetencie, multicloud a exit stratégie, odporúčania a best practice.

Rozdelenie - privátna a verejná časť

Podľa bezpečnostnej úrovne

Privátna časť
Výhradne pod správou Ministerstva vnútra SR, ktoré prevádzkuje infraštruktúru a platformové služby vo vlastných datacentrách na území Slovenskej republiky.

Verejná časť
Je tvorená cloudovými službami zapísanými v katalógu služieb vládneho cloudu, ktorých prevádzkovateľmi a/alebo poskytovateľmi sú komerčné subjekty.

Bezpečnostné úrovne

Technické role a zodpovednosti

MIRRI SR – Centrálna architektúra a štandardy

- Definuje multicloud architektonické princípy
- Naming convention, Tagging
- Spravuje IPAM
- Prevádzkuje centrálne komponenty
- Koordinuje technické onboarding procesy OVM

Cloud provider - Platforma a infra vrstva

- Prevádzkuje infra, sieťové a platformové služby
- Zaisťuje bezpečnosť a SLA

OVM - Správa vlastného cloudového prostredia

- Riadi IAM lifecycle (identity, role, oprávnenia)
- Definuje si FW politiky
- Zodpovedá za aplikácie, dáta, konfigurácie, prevádzku a bezpečnosť
- Udržiava dokumentáciu ako auditnú stopu (verziované RBAC/FW šablóny)

Výhody multicloud prístupu

Multicloud prístup umožňuje vybrať cloud podľa technológie

Každý cloud má svoje silné stránky, preto je úplne logické priradiť riešenie tam, kde je:

- Najlepšia natívna integrácia
- Najlepší performance pre daný typ workloadu
- Najnižšie licenčné náklady
- Dostupná manažovaná verzia služby

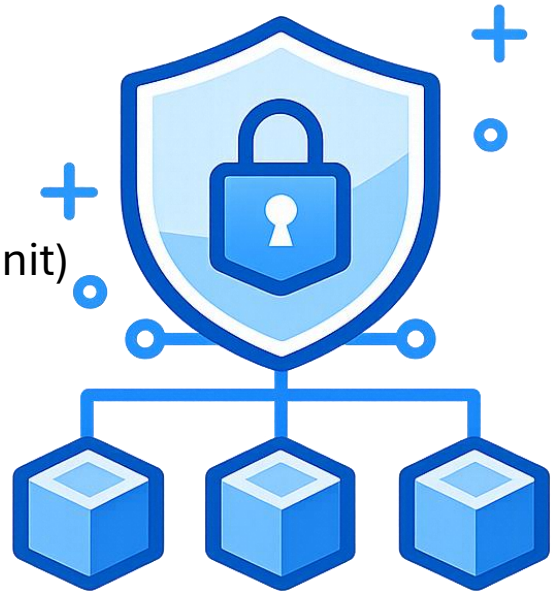
Je prirodzené ísť do cloudu toho poskytovateľa:

- Konfigurácia je jednoduchšia, pretože služba je manažovaná
- Dochádza ku konsolidácii licenčného modelu
- Jednoduchšia migrácia
- Zároveň klesá záťaž na interné tímy
- Hybridný model

Exit stratégia – odporúčania pre OVM

- Navrhovať riešenia cloud-native a cloud-agnosticky
- Používať otvorené štandardy pre dáta, API a integrácie
- Minimalizovať vendor lock-in a závislosti na proprietárnych službách
- Udržiavať prehľadnú a aktuálnu architektonickú dokumentáciu
- Preferovať platformovo prenositeľné PaaS služby
- Definovať RTO/RPO a pripraviť exit scenár už v návrhu

Prevádzkové “stavebné kamene”



Izolácia prostredí OVM

- Každé OVM má vlastné **izolované prostredie** (subscription / compartment / business unit)
- Prostredie je uzavreté – všetko je explicitne definované
- Základ princípu **„separation of duties“** a **„least privilege“**

IAM – identity a prístupy

- OVM si riadi vlastné identity
- RBAC podľa šablón MIRRI SR
- Oddelenie rolí: admin / operátor / auditor
- MFA povinné pre administratívne aj technické prístupy

Sieť & Firewall

- Centralizovaná topológia Hub & Spoke
- OVM si riadi vlastné FW pravidlá podľa šablón MIRRI SR
- Centrálne riadený IPAM

Žiadosti a potrebná dokumentácia

Ako získať cloudové služby v rámci eSKa Cloud

Žiadosť cez web MIRRI

Oficiálna stránka poskytuje všetky potrebné dokumenty.

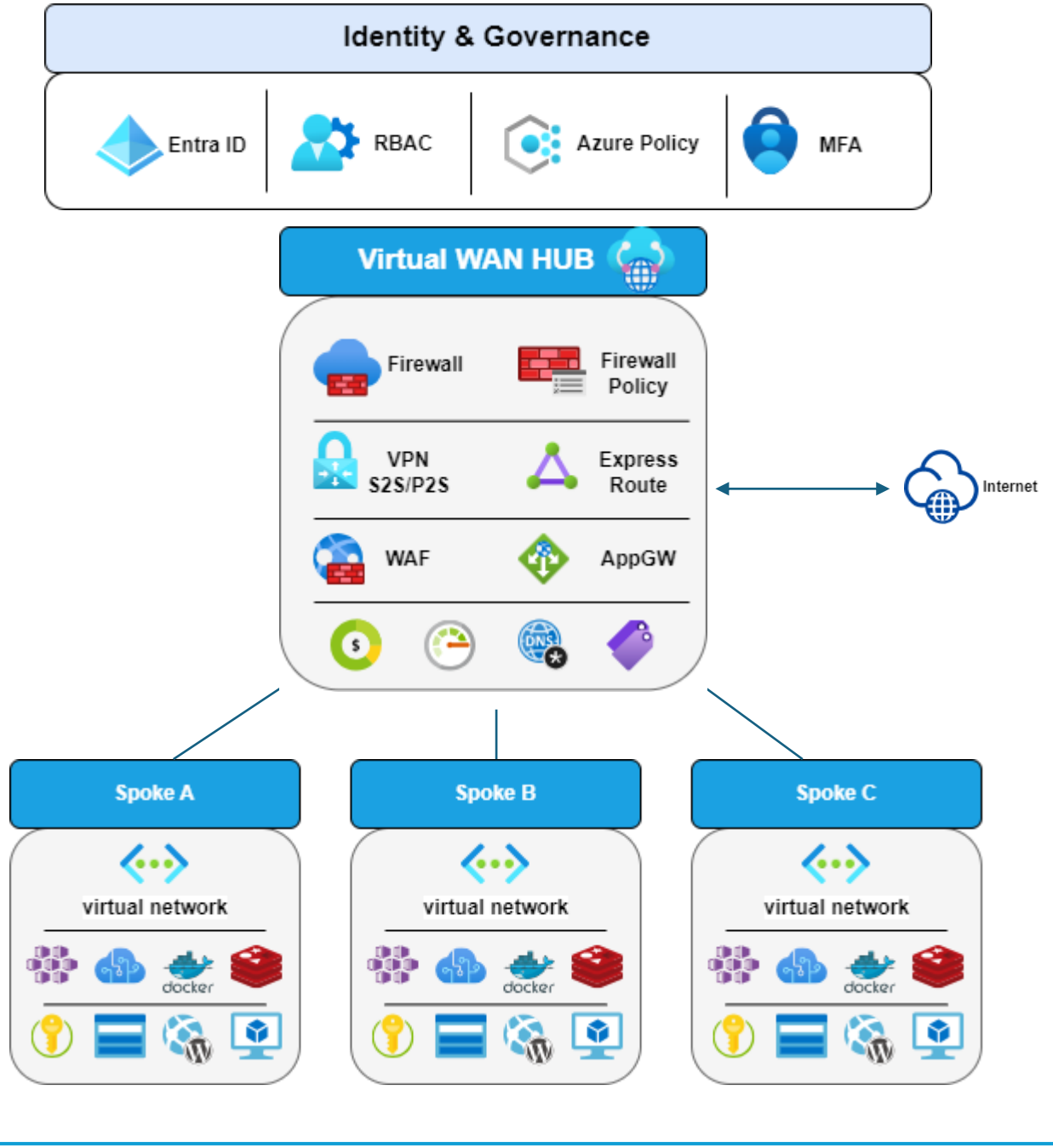
MS Azure
eSKa Cloud

Microsoft Azure – Landing Zone

Vrstva **Identity & Governance Microsoft Entra ID, RBAC, Policy a MFA** riadi prístup a bezpečnostné pravidlá naprieč prostredím.

Architektúra je postavená na **Hub-and-Spoke modeli** s centrálnym **vWAN Hubom**, ktorý zabezpečuje konektivitu, bezpečnosť a centralizované riadenie siete.

Všetky workloady sú umiestnené v izolovaných **Spoke VNetoch**, pričom sieťová komunikácia je riadená cez **Azure Firewall.**



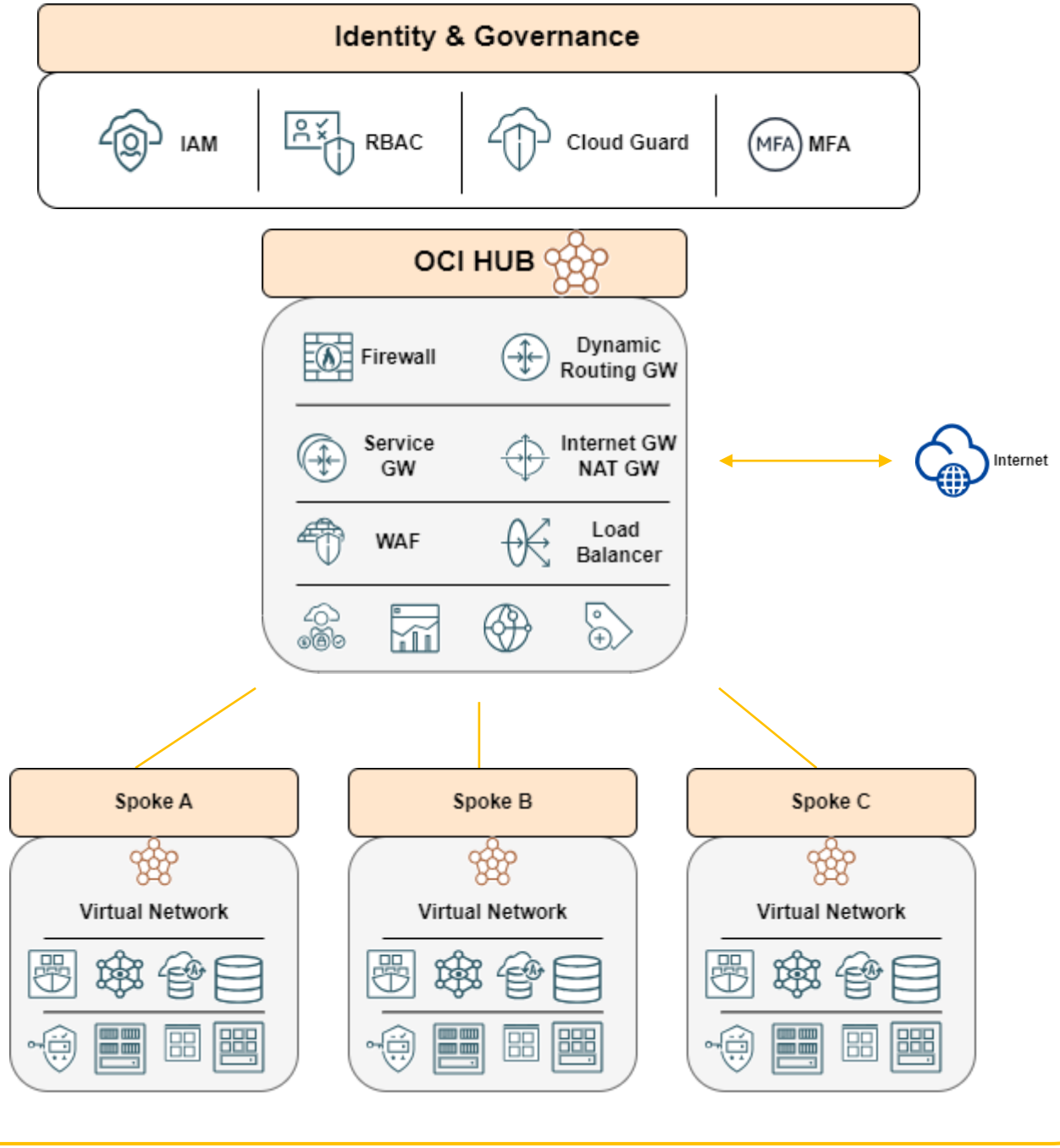
ORACLE OCI
eSKa Cloud

Oracle Cloud Infrastructure (OCI) – Landing Zone

Vrstva **IAM, Policies, Cloud Guard a MFA** zabezpečuje centralizovanú správu identity, compliance a bezpečnosti.

OCI architektúra využíva **Hub-and-Spoke topológiu** s centrálnym **DRG (Dynamic Routing Gateway)** pre riadenie konektivity medzi VCN sieťami a externým prostredím.

Spoke projekty sú oddelené do samostatných **VCN**, pričom komunikácia je riadená cez **Network Firewall** a **DRG.**



aws eSKa Cloud

Amazon Web Services (AWS) – Landing Zone

Technické možnosti: od IaaS po SaaS

IaaS

- Virtuálne servery a siete
- Load balancery, VPN, brány
- Block/Object storage, snapshoty, backup
- OVM si sama spravuje operačný systém, aplikácie a dáta

PaaS

- Managed databázy (SQL, PostgreSQL, Oracle, NoSQL)
- Kontajnery a Kubernetes
- Serverless funkcie a integračné služby
- OVM sa sústredí už len na aplikáciu a dáta

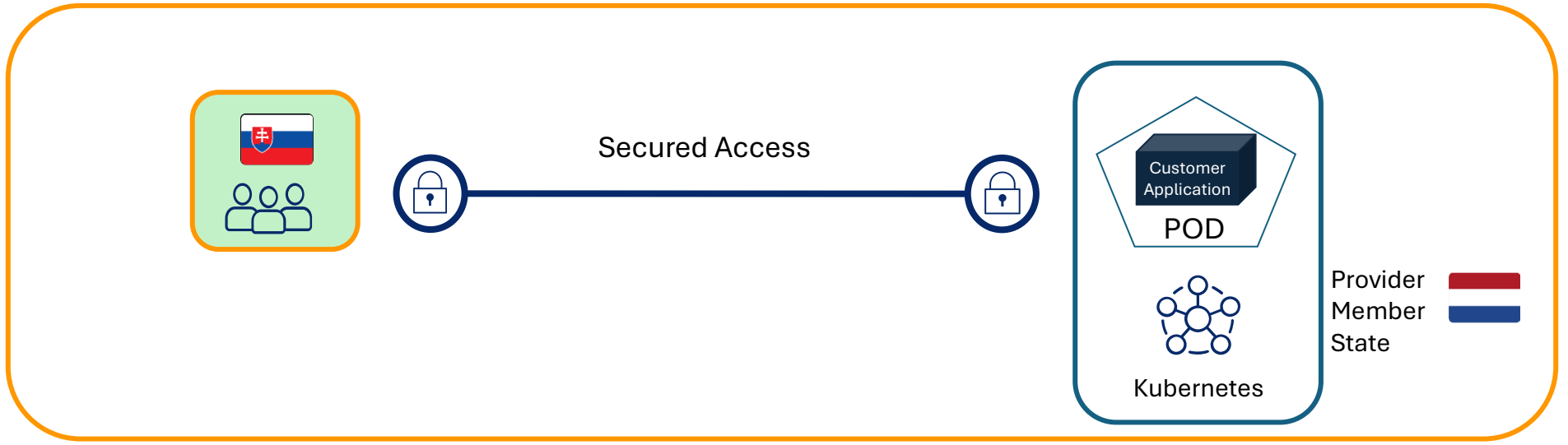
SaaS

- Hotové kancelárske a kolaboračné služby
- Špecializované aplikácie
- Plne spravované riešenia bez infraštruktúry
- OVM len používa službu

EuroCloud - Overview of the PoC

Provisioning a Kubernetes Cluster

PoC1: Provisioning of Kubernetes POD
with a Customer Application



The infrastructure service will provide access to a (single) POD with a “customer application image” already deployed – We could propose a simple Web Page

CZ IT GR LV NL RO SK

Bezpečnostné minimum pre OVM

Security Baseline

- MFA
- Backup stratégia
- Oddelené prostredia (DEV/TEST/PROD)
- Žiadne public IP
- Pravidelné revízie účtov a FW pravidiel
- Patching pri IaaS službách

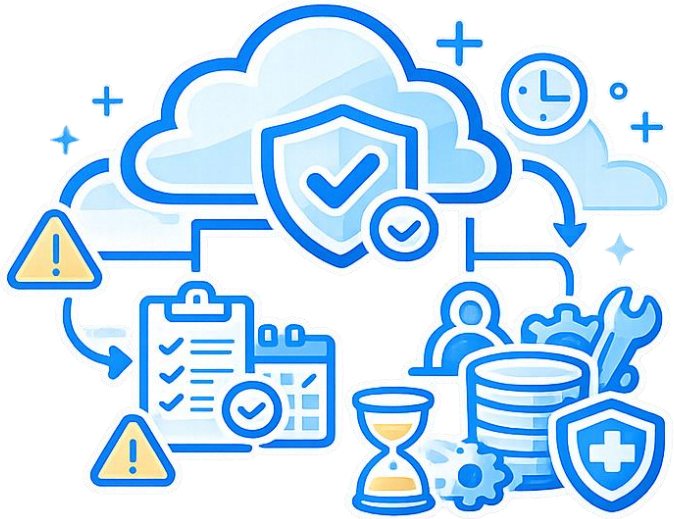
Monitoring & Observability

- Logy
- Metriky, tracing, auditné logy
- Povinné alerty pre kritické služby

Cloud IAM Best Practices

- Zákaz nepoužívať shared accounts
- Princípy
  - Role-Base Access Control RBAC
  - Least Privileges
  - Separation of Duties
- Time-bound prístupy pre admin operácie
- Oddelenie identity od infra účtov

DR/BCP – Disaster Recovery a Business Continuity



On-premise DR je finančne náročný

- Dodatočný HW/SW
- Replikácia infraštruktúry
- Vysoké prevádzkové náklady (energia, housing, SLA)

Cloud prináša zásadné zjednodušenie

- Infraštruktúru netreba kupovať vopred
- Služby sú on-demand
- Vstavaná replikácia a automatizované obnovy

Výhody verejného Vládneho cloudu

Prečo sa oplatí využívať vládne cloudové služby verejnej časti

Bezpečnosť a štandardy
Zabezpečené podľa GDPR, ISO 27001, HIPAA a iných medzinárodných štandardov.

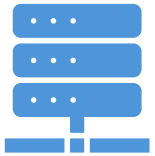
Finančná efektívnosť
PAYG model umožní presné riadenie nákladov.

Rýchle nasadenie
Projekty nemusia prechádzať zdĺhavým verejným obstarávaním.

Centralizované služby
Firewall, DNS, VPN brány, WAF a aplikačné brány sú poskytované centrálne MIRRI SR – bez nutnosti duplicity.

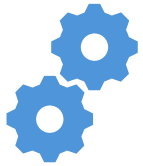
Záver a výzva k akcii

Vládny cloud ako základ k digitalizácii



Stabilná a bezpečná infraštruktúra
Vládny cloud predstavuje moderný základ pre fungovanie verejnej správy s dôrazom na kybernetickú bezpečnosť.

Škálovateľné riešenia pre všetkých
Umožňuje malým i veľkým inštitúciám využívať výhody cloudu bez vysokých vstupných nákladov.



Nástroj digitálnej transformácie
Kľúčový komponent pri plnení priorít štátu v oblasti elektronizácie služieb a efektívneho riadenia IT.

Výzva na zapojenie
Aktívne využívať možnosti vládneho cloudu a sandboxov.

Ďakujeme

eSKa Cloud

SLOVENSKEJ REPUBLIKY

PLÁN OBNOVY

cestovná mapa k lepšiemu Slovensku