



Elektronická identifikačná karta

1. december 2009
Bratislava

Jozef Čapuška
Sekcia informatiky, telekomunikácií a bezpečnosti MV SR



OBSAH

- 1) Vývoj ID karty (OP)
- 2) Prečo OP ako eID, úlohy eID
- 3) Bezpečnostné prvky čistopisu
- 4) Čip a jeho obsah
- 5) Ochrana dát v čipe a bezpečnosť ich používania
- 6) Proces vydávania eID, zmeny oproti súčasnosti
- 7) Zhrnutie



Ministerstvo vnútra Slovenskej republiky

Vývoj ID kariet





Ministerstvo vnútra Slovenskej republiky

Prečo OP ako elektronická ID karta

- Snaha o integráciu a unifikáciu dokladov
- Potreba nielen elektronickej ale aj fyzickej bezpečnosti eID karty
- Využitie a zefektívnenie existujúcich procesov pri výrobe eID karty
- eID vznikne implementáciou kontaktného čipu do existujúceho OP

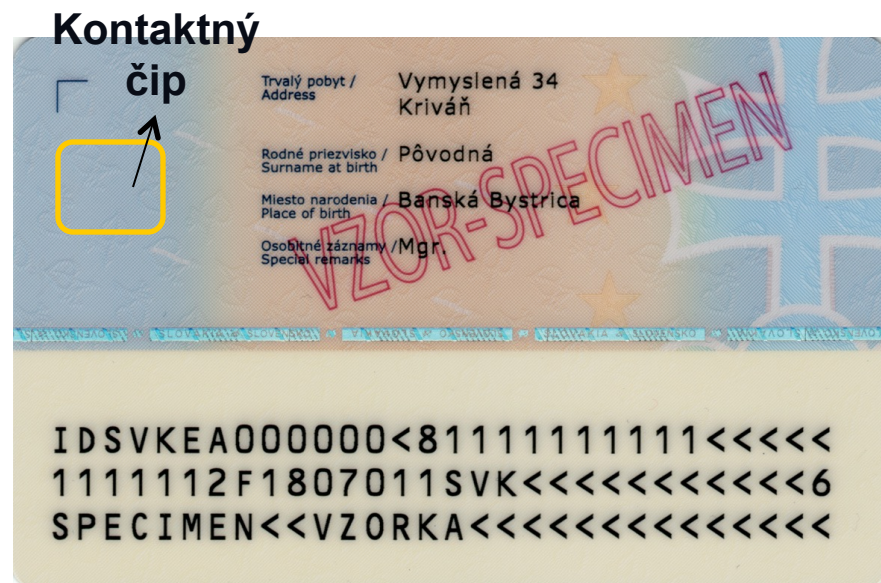


- eID karta bude identifikačným a autentifikačným prostriedkom pre využívanie elektronických služieb eGovernmentu
- eID karta bude certifikovaným dátovým nosičom pre uloženie kvalifikovaného certifikátu a SW nástrojov pre tvorbu ZEP a pre uloženie osobných údajov občana v elektronickej forme
- eID karta môže byť využitá nielen pre eGovernment služby ale aj pre súkromné služby (e-business, e-banking,...)
- súlad s európskou legislatívou a požiadavkami
- vytvorenie adekvátneho dokladu aj pre cudzincov s povoleným pobytom v SR

Ministerstvo vnútra Slovenskej republiky

Bezpečnostné prvky čistopisu

- Personalizovaná centrálna v Národnom personalizačnom centre
- Viacvrstvový polykarbonát vo formáte ID1

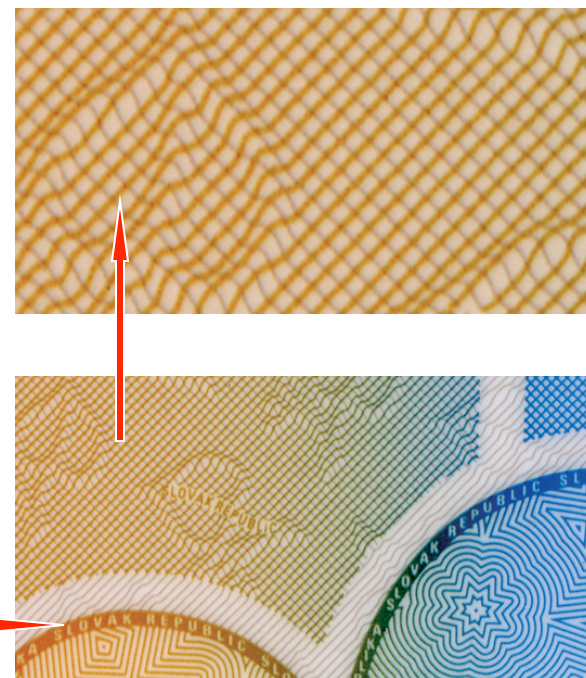




Ministerstvo vnútra Slovenskej republiky

Bezpečnostné prvky čistopisu

Gilošová ochranná podtlač s 3D prvkami, obsahuje aj antikopírovacie štruktúry.

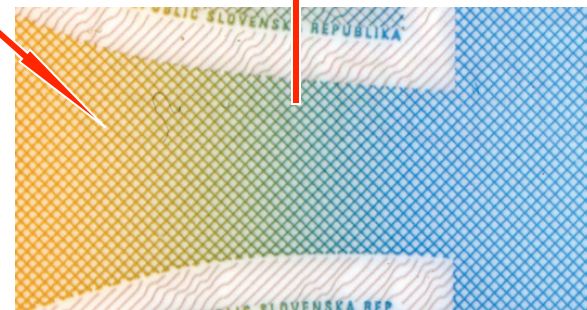
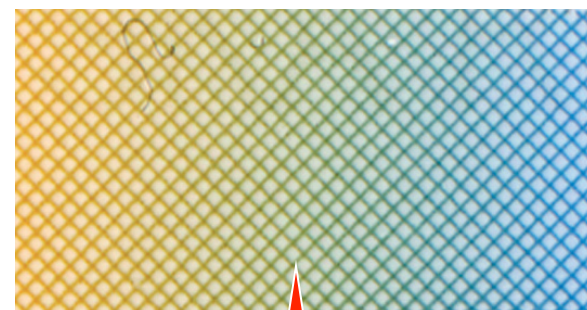




Ministerstvo vnútra Slovenskej republiky

Bezpečnostné prvky čistopisu

Irisová líniová tlač s plynulým farebným prechodom.





Ministerstvo vnútra Slovenskej republiky

Bezpečnostné prvky čistopisu

Pozitívny mikrotext - rozmerovo malé písmená tlačené v pozitívnom obraze, viditeľné len pod lupou.

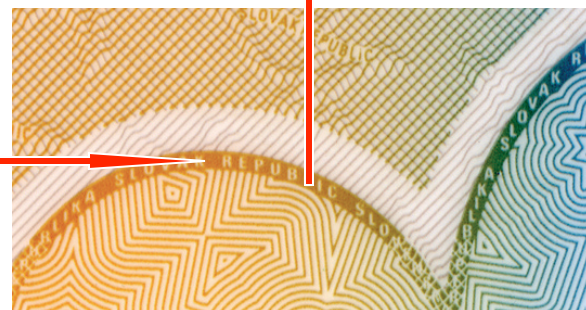
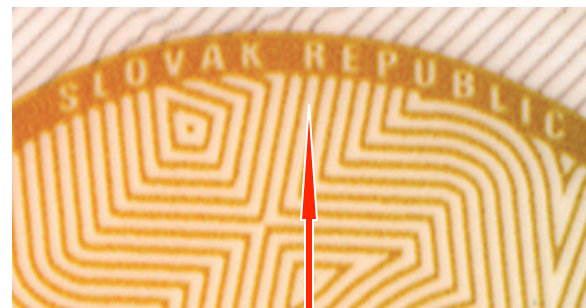




Ministerstvo vnútra Slovenskej republiky

Bezpečnostné prvky čistopisu

Negatívny mikrotext - rozmerovo malé písmená v negatívnom obraze, pôsobiace ako biele písmo na vytlačennom farebnom pozadí, viditeľné len pod lupou.

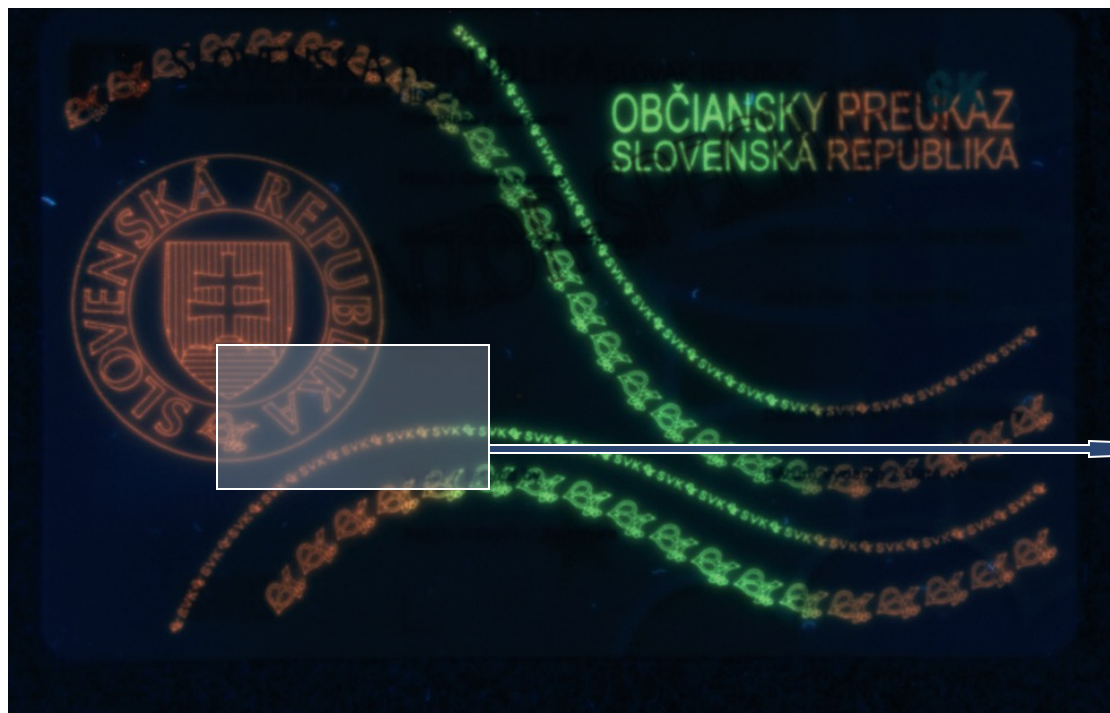




Ministerstvo vnútra Slovenskej republiky

Bezpečnostné prvky čistopisu

UV grafika - grafika viditeľná len v UV svetle vyhotovená dvoma farbami s plynulými farebnými prechodmi jednej farby do druhej.

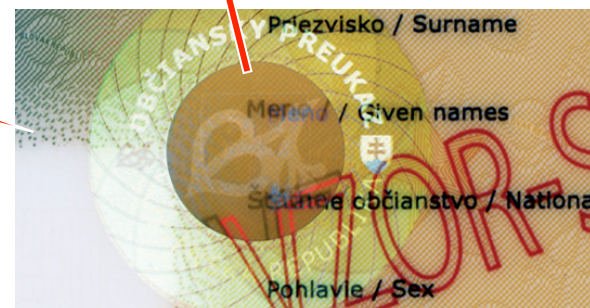




Ministerstvo vnútra Slovenskej republiky

Bezpečnostné prvky čistopisu

Priehľadný Kinegram® Patch - priehľadný opticky variabilný prvok čiastočne prekrývajúci podobu držiteľa. Vyznačuje sa kinetickými a farebnými efektmi.





Ministerstvo vnútra Slovenskej republiky

Bezpečnostné prvky čistopisu

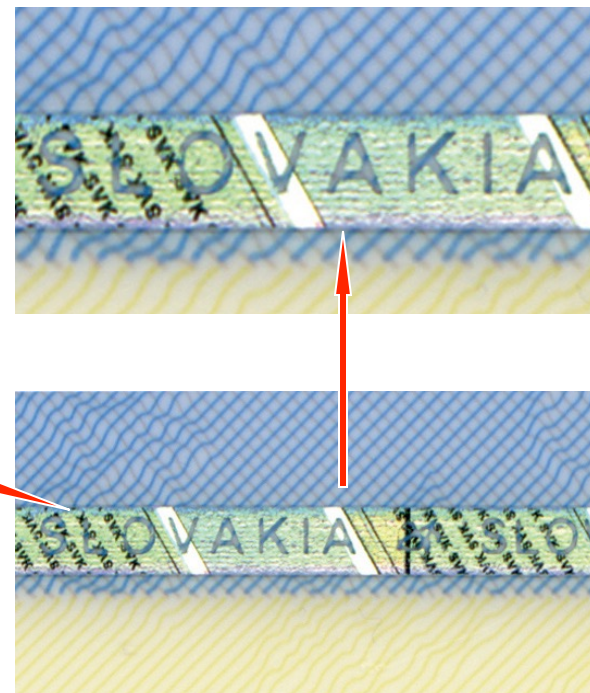
Opticky variabilná farba (OVI) - písmená „SK“ sú vytlačené špeciálnou farbou vyznačujúcou sa zmenou farebného odtieňa (z purpurovej do zelenej) v závislosti od zmeny uhla pohľadu.



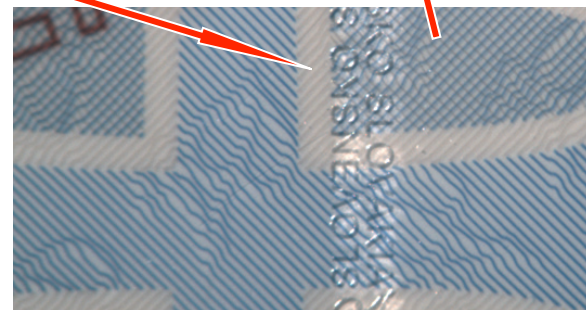
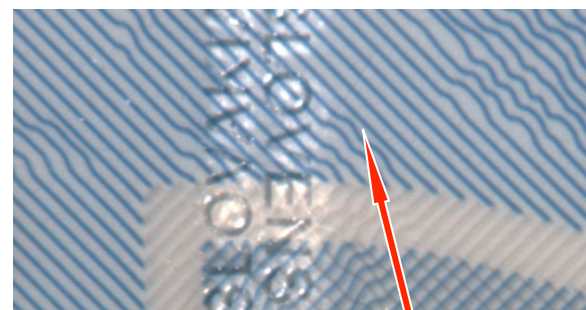
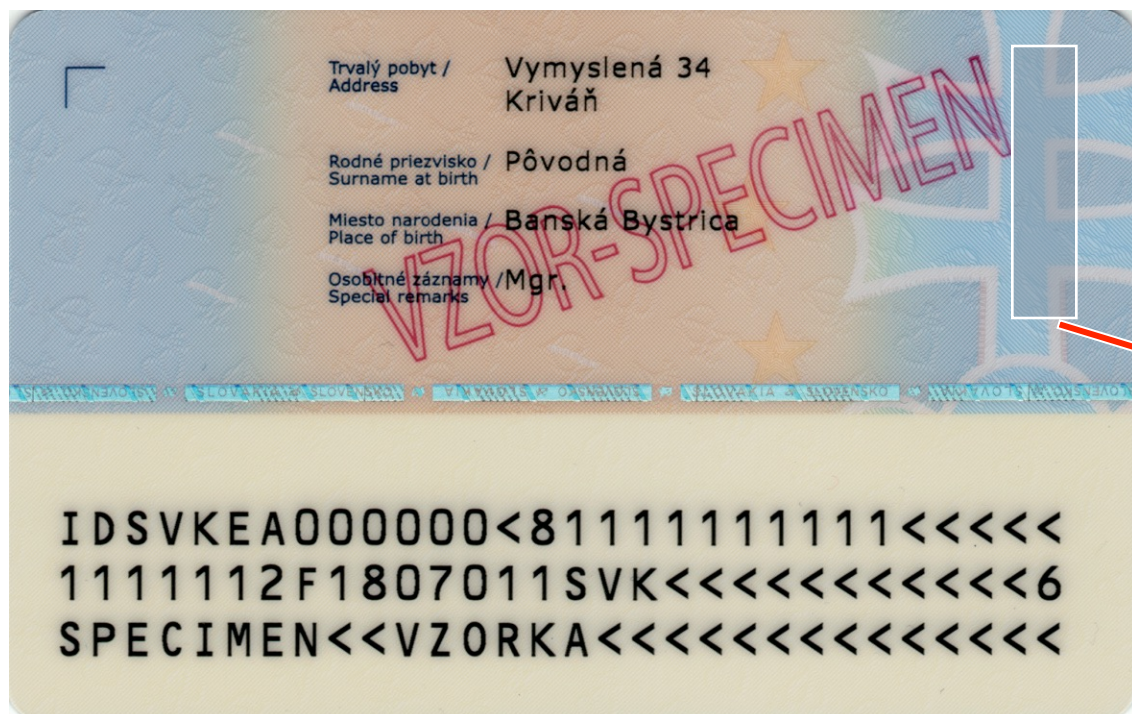


Bezpečnostné prvky čistopisu

Metalizovaný holografický ochranný prúžok aplikovaný na karte vo vodorovnom smere. Prúžok má demetalizované plochy obsahujúce mikrotext a motív lipového listu.



Reliéfny prvok - obsahuje text a motív lipového listu.





- Kontaktný čip s operačným systémom
- Podpora kryptografických funkcií
- Certifikácia NBÚ SR
- 3 dátové sektory

SEKTOR 1

- kvalifikovaný certifikát pre ZEP
- autentifikačný certifikát
- šifrovací certifikát

SEKTOR 2

- základné dáta o občanovi (meno, priezvisko, dátum narodenia, rodné číslo / BIFO, adresa,...)

SEKTOR 3

- prázdny, ponechaný pre budúce využitie (napr. emergency set)

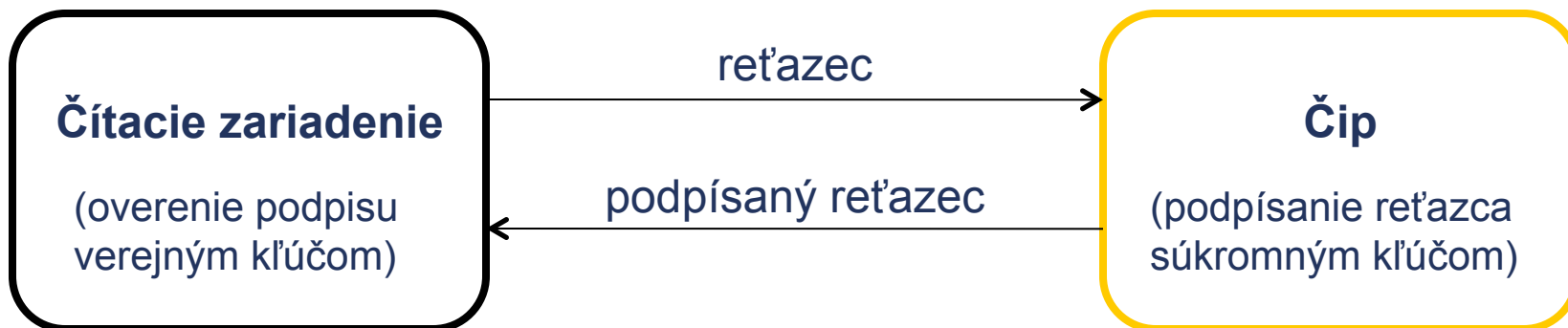


Pasívna autentifikácia – ochrana proti prepísaniu dát v čipe

Dáta v čipe budú podpísané elektronickým podpisom, bodom dôvery bude certifikačná autorita v správe NBÚ SR

Aktívna autentifikácia – ochrana proti klonovaniu čipu

- Challenge – response protokol medzi čítacím zariadením a čipom využívajúci asymetrickú kryptografiu
- Súkromný kľúč bezpečne uložený v secure memory čipu
- Verejný kľúč uložený v elektronicky podpísanom dátovom sete





Riadenie prístupu k osobným dátam

- Údaje na čipe nebude možné vyčítať bez súhlasu občana (ochrana PINom)
- Na čipe budú implementované špecializované funkcie pre ochranu citlivých údajov (vek, doba expirácie dokladu,..)

Riadenie dodatočného zápisu do 3.sektora

- Pre dodatočný zápis budú implementované špecializované funkcie, ktoré umožnia zapisovať iba oprávneným subjektom



Prijatie žiadosti na JP

Personalizácia v NPC

Odovzdanie dokladu držiteľovi spolu
so sprievodnou dokumentáciou,
vydanie kvalifikovaného certifikátu



Prijatie
písomnej
žiadosti

Stotožnenie
a
preverenie
žiadateľa

Zosnímanie
fotografie a
podpisu

Odoslanie
el. žiadosti
do NPC



Súčasťou projektu je:

- úprava mobilných pracovísk pre vydávania eID aj pre handicapovaných občanov
- zabezpečenie role registračných autorít





Ministerstvo vnútra Slovenskej republiky

Personalizácia v NPC

Prijatie el.
žiadosti

Laserové
gravírovanie

Zápis do čipu

Tlač a
obáľkovanie
sprievodných
dokumentov
(PIN)

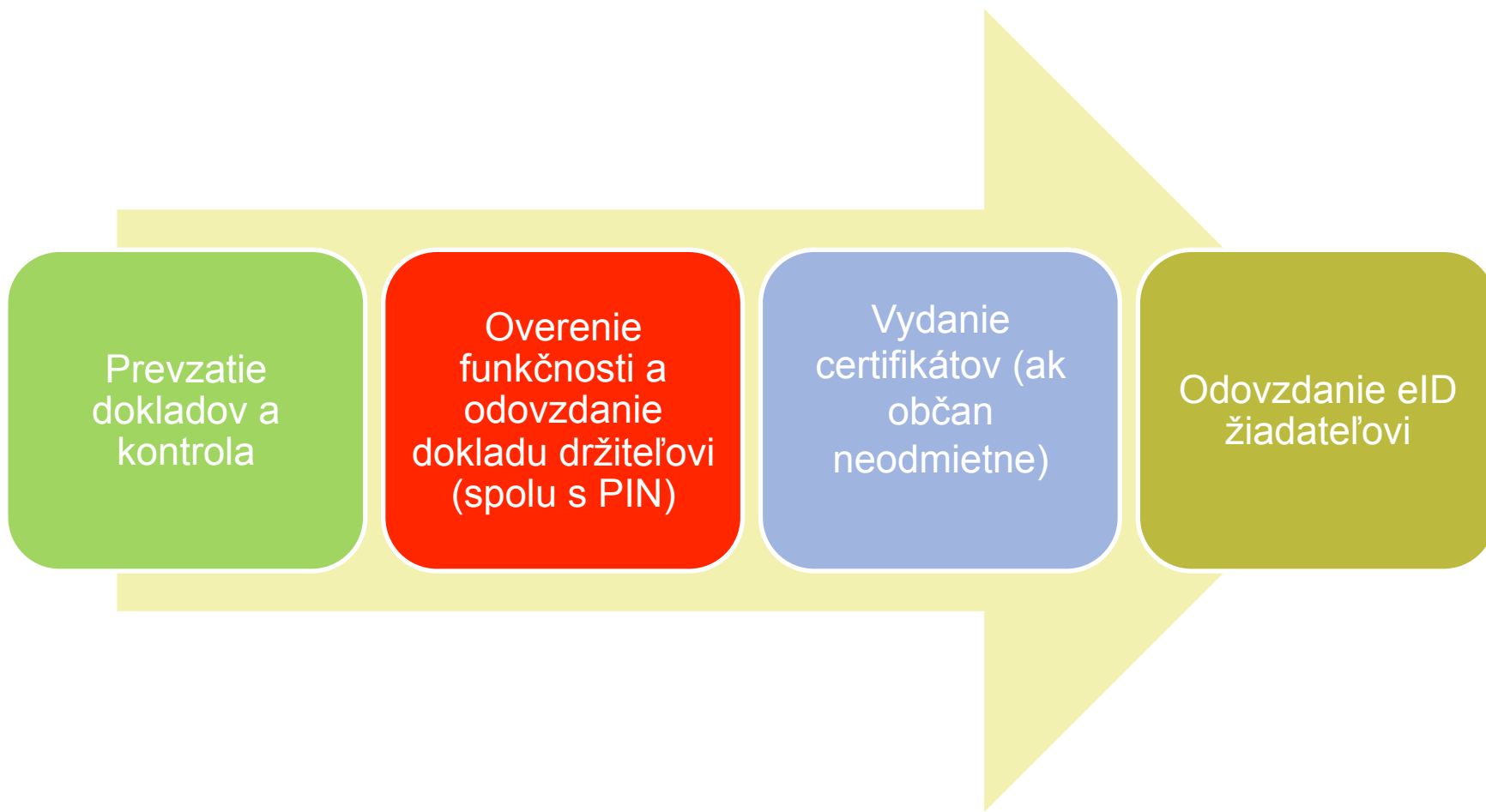
Kontrola
kvality a
distribúcia na
JP

Súčasťou projektu je aj zabezpečenie 100%-nej dostupnosti vydávania eID vybudovaním záložného NPC v okruhu 100km



Ministerstvo vnútra Slovenskej republiky

Vydanie dokladu na JP





Ministerstvo vnútra Slovenskej republiky

Prijatie žiadosti na JP

Súčasťou projektu je:

- vydanie prvého kvalifikovaného certifikátu pre ZEP každému občanovi bezplatne
- zabezpečenie možnosti okamžitého zneplatnenia certifikátov





- eID karta vznikne implementáciou kontaktného čipu do čistopisu súčasného občianskeho preukazu
- bude slúžiť na autentifikáciu občana pri využívaní eGovernment služieb
- bude slúžiť ako bezpečné úložisko pre kvalifikovaný certifikát a SW pre tvorbu ZEP
- prvý kvalifikovaný certifikát dostane občan zadarmo (ak ho neodmietne)
- bude obsahovať osobné dáta zabezpečené špecializovanými funkciami
- celý proces bude občan vybavovať na jednom mieste

Ďakujem za pozornosť!