MAP karta

# Představení systému MAP

# Obsah prezentace

MAP karta

- Důvod vzniku systému MAP
- Nové prvky systému MAP
- Kde lze MAP kartu použít?
- Bezpečnost systému MAP karty
- Architektura systému
- Centrální MAP autorita
- Kompatibilita se současnými karetními systémy
- Kroky, které vedou k cíli

# Důvod vzniku systému MAP

MAP karta

- **Požadavky na straně ČD**
  - Lokálně navržené karetní systémy a s tím spojené nároky IDS na odbavovací zařízení ČD již neumožňují obsluhu dalšího IDS (SAM sloty, řešení black listů, …)
  - Každý lokální systém má vlastní SAM, aplikaci, jízdní doklad
  - Nemožnost sloučit více lokálních systémů na jednu kartu
  - Bezpečnost a rychlost lokálních systémů není na úrovni dnešních požadavků a potřeb, mnohde je bezpečnost ponížena z důvodu alespoň uspokojivé rychlosti práce s kartou

# Důvod vzniku systému MAP

- **Požadavky na straně PMDP - spojení přechodu na DESfire EV1 s novým pohledem na karetní systém**
  - Požadavky na bezpečnost systému
  - Požadavky na vzájemné sdílení aplikací na kartě
  - Nutnost návrhu centrální správy „sdílené“ karty
  - Nové funkce multiaplikační karty
- **Navazujícím krokem byl společný postup PMDP a ČD**
  - Smlouva o spolupráci
  - Společné výběrové řízení na dodavatele řešení

# Nové prvky systému MAP

- **Interoperabilita cestou sdílení aplikací**
  - V jediné tzv. multimodální dopravní aplikaci mohou být různé jízdní doklady různých jednoznačně identifikovatelných subjektů (dopravců, krajů, apod.)
- **Systém umožňující interoperabilitu v celostátním měřítku**
  - Na základě vzájemných obchodních dohod je systém MAP možno konfigurovat dle požadavků jednotlivých zapojených subjektů (vzájemné uznávání dokladů, apod.)
  - Vznik centrální autority s definovanými pravidly, dohlížející na sdílené komponenty systému (účastníci, klíče, kontrola autenticity transakcí, …)
- **Inteligentní SAM s dálkovou správou**
  - Dálková správa on-line i off-line aktualizací klíčů, apletů i konfigurací (oprávnění práce s aplikací pro jednotlivé subjekty zapojené do systému)

# Nové prvky systému MAP

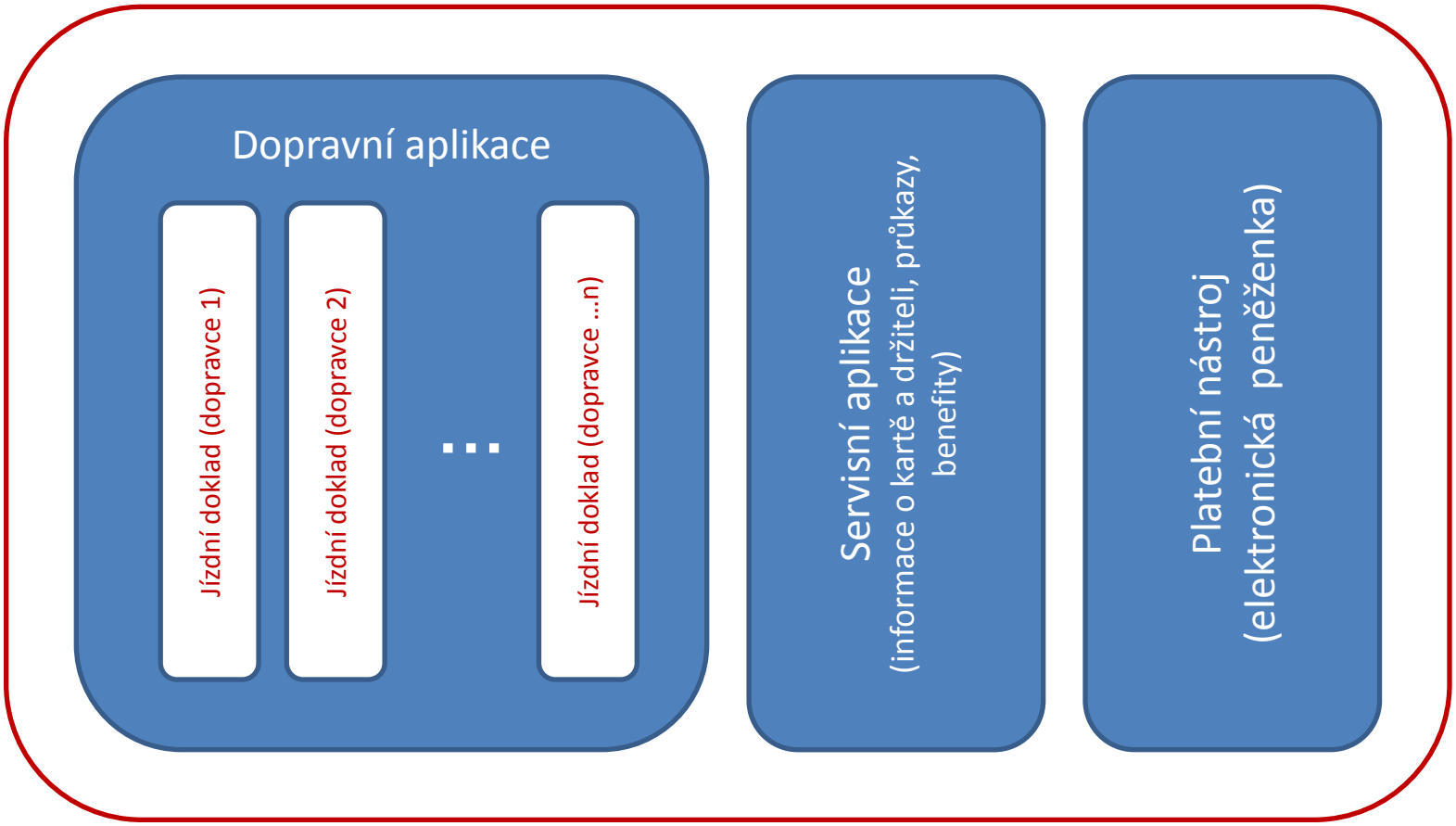
MAP karta

- **Zaručená autenticita transakcí**
  - SAMem podepsané transakce za využití asymetrické kryptografie (dodržení optimálního způsobu a času odbavení držitele karty)
- **Dynamická struktura dopravní aplikace**
  - variabilní délka a počet jízdních dokladů (jednoduché doklady zabírají méně místa než doklady se složitou strukturou)
  - čtení a zápis jen minimálního potřebného množství dat z/do karty
  - „neomezený“ počet subjektů, které mohou v rámci interoperability dopravní aplikaci využívat

# Nové prvky systému MAP

- **Komplexnost struktury karty - karta obsahuje ucelenou skupinu aplikací**
- **Možnost umístění aplikace jiného vydavatele karty (není nutné zakládat rezervní aplikace)**
  - Nutným předpokladem je obchodní dohoda jednotlivých subjektů
- **Ohled na rozvoj technologií i požadavků uživatelů**

# Nové prvky systému MAP



# Kde lze MAP kartu použít?

- **Ukládání jízdních dokladů jakéhokoli v ČR používaného typu**
  - IDS, drážní, PAD/LAD, …
  - Doklad může být vydáván různými dopravci / prodejci s možností vzájemného uznávání dokladů mezi dopravci
- **Prokazování nároku na slevu (profil držitele) nebo potvrzení identity držitele**
  - Elektronický žákovský průkaz, elektronický průkaz dítěte, zaměstnanecký průkaz, karta občana, knihovní průkaz
  - Vystavení průkazu/profilu pouze pro jednoho poskytovatele služeb/dopravce, pouze pro vybranou (tarifní či jinou) síť, popřípadě „národní“ průkaz

# Kde lze MAP kartu použít?

- **Možnost vytvoření systému bonusového programu**
  - Věrnostní karty pro oblast retailu a služeb v jedné multiaplikační kartě
- **Parkování (P+R parkoviště) a další služby navázané na cestování**
- **Vstupenky na kulturní a sportovní akce**
- **Samoobslužný prodej s využitím MAP Elektronické peněženky (EP) s možností PINu a limitu transakce**
- **Identifikační karty, ….**

# Bezpečnost systému MAP karty

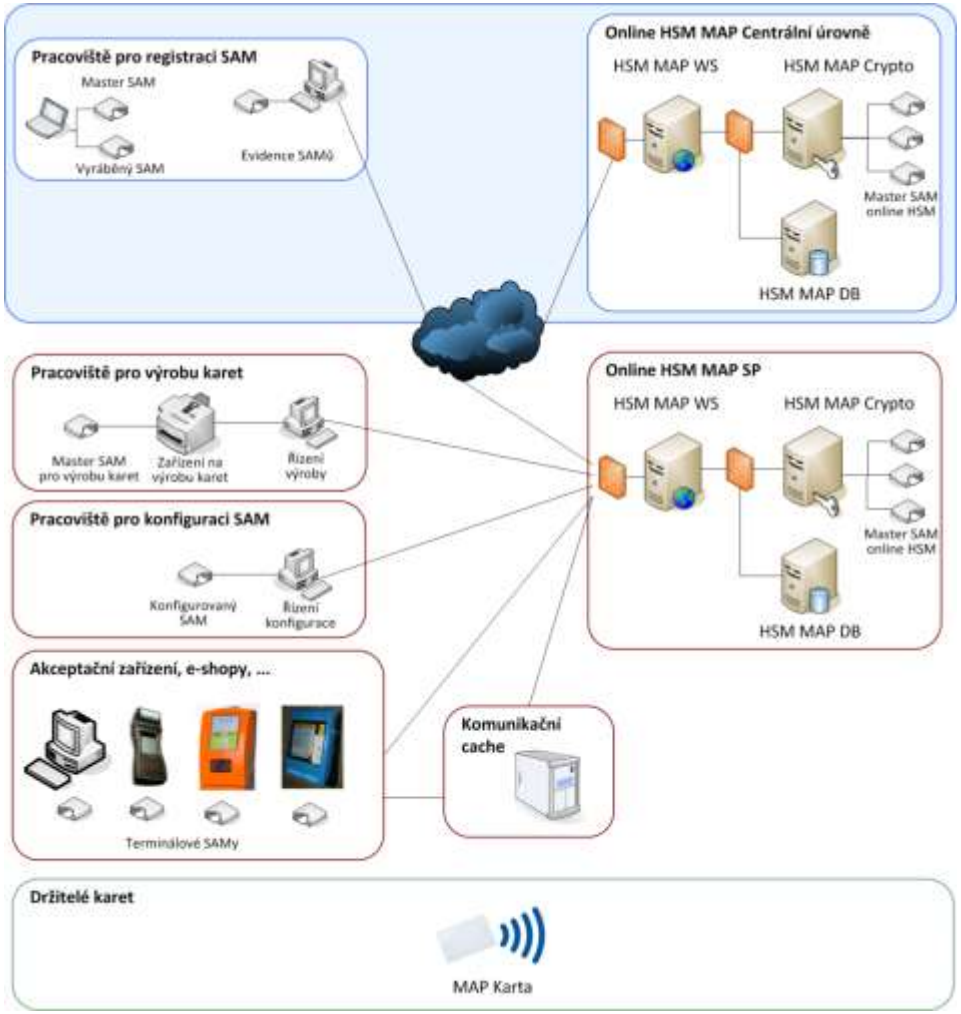
- **Zajištění bezpečnosti (integrity, nepopiratelnosti) dat**
  - Konkrétní data jsou dostupná jen pro odpovědné subjekty
  - Data na kartě jsou dostupná jen prostřednictvím logiky SAMu
- **Bezpečnost je řešena z hlediska důvěrnosti a nemožnosti zneužití systému**
  - „Prolomení systému“ např. formou podvržení cizích zařízení, karet nebo SAMů
  - Ochranu systému proti kompromitaci komunikace (SAM vs. HSM)
- **Citlivé údaje jsou uloženy výhradně v HSM nebo v SAM**
- **Systém zohledňuje bezpečnostní nedokonalosti karty DESFire EV1**
  - Řeší riziko podvržení příkazů CommitTransaction nebo AbortTransaction
  - Řeší riziko oddálení karty z pole čtečky / vypnutí pole čtečky

# Bezpečnost systému MAP karty

MAP karta

- **Systém zohledňuje možnost odcizení SAM**
  - SAM je vybaven sadou čítačů, povolujících provedení pouze určitého množství operací daného typu
  - Zařízení se musí před prací k SAMu autentizovat, přičemž autentizační klíč se mění v průběhu času
- **Systém počítá se zapojením většího počtu subjektů (poskytovatelů služeb)**
  - Důvěryhodnost transakcí
  - Provozní číselníky: blacklisty karet / aplikací, blacklisty SAM, apod.
  - Distribuce kryptografických klíčů

# Architektura systému

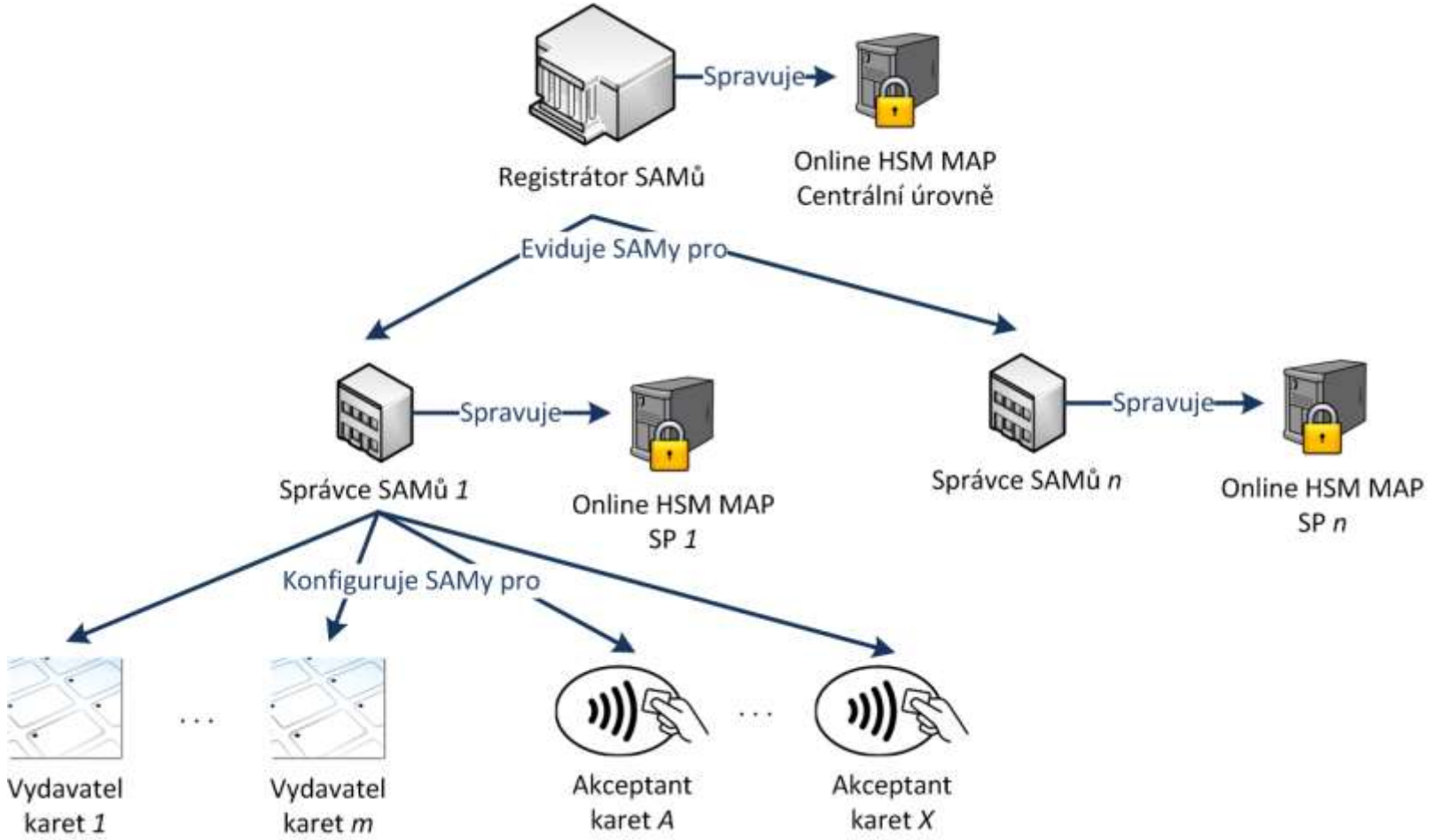


# Architektura systému

MAP karta

- **Centrální úroveň (HSM MAP)**
  - Zajišťuje funkční řízení Systému jako celku na „centrální / interoperabilní úrovni“ (po administrativní a bezpečnostní stránce zajišťuje integraci a vzájemnou komunikaci libovolného počtu poskytovatelů služeb i vydavatelů karet)
  - Zajišťuje registraci SAMů v definovaném prostředí formou dohodnutého postupu (klíčový prvek bezpečnosti celého systému s více zapojenými subjekty)
- **Úroveň poskytovatelů služeb (HSM SP)**
  - Úroveň MAP systému z pohledu správy (sdílejících aplikací karty) jednotlivých poskytovatelů služeb
  - Výroba karet dle vlastní potřeby
  - Konfigurace SAM dle vlastní potřeby
  - Nastavení konkrétních procesů dle vlastní potřeby

# Architektura systému



# Centrální MAP autorita

- **MAP autorita je zde chápána jako technický pojem a nepředjímá jakoukoli formu (právní, organizační)**
- **MAP autorita je předpokladem interoperability založené na sdílení aplikací a plní základní úlohy:**
  - Provádí registraci MAP SAMů (tj. jejich zabezpečení a evidenci) pro poskytovatele služeb
  - Udržuje na administrativní úrovni všechny sdílené číselníky
  - Určuje vývoj Systému MAP karta (předchází konfliktům mezi zapojenými subjekty)
  - Navrhuje pravidla (včetně bezpečnostních), kterými se řídí všichni poskytovatelé služeb
  - Sleduje dodržování stanovených bezpečnostních a procesních pravidel
  - Zajišťuje rutinní běh a interoperabilitu centrálních Systém (garantuje důvěryhodnost při výměně transakcí, zajišťuje distribuci základních číselníků systému MAP)
  - Zajišťuje bezpečnostní a technologickou certifikaci partnerů přistupujících do systému MAP

# Kompatibilita se současnými systémy

MAP karta

- **Možnosti řešení zpětné kompatibility:**
  - Jeden SAM modul - na bázi více apletů, do MAP SAM je možno nahrát applet umožňující práci i s jinou kartou (Opuscard, Plzeňská karta)
  - Jeden SAM modul – na bázi jednoho společného apletu – MAP applet bude rozšířen o vybrané funkce SAMů jiných karet (řešení pro stávající In-kartu a Opencard)
  - Samostatný SAM – v případě dostatečného počtu volných SAM slotů v OZ

# Kroky, které vedou k cíli

- Spolupráce a společný postup při implementaci technického řešení MAP systému
- Proaktivní přístup při spolupráci a hledání dalších možností využití MAP systému

# Děkujeme za pozornost!

**Radomír Kozler**
Projektový manažer úseku Plzeňská karta

**Další informace Vám poskytne:**

**Zbyněk Proška**
Projektový manažer úseku Plzeňská karta
Plzeňské městské dopravní podniky, a.s.
email: proska@pmdp.cz