Mobilní platby

EurOpen

Martin Chlumský / říjen 2014

NFC telefony

NFC telefony

Použití a potřebné vybavení

- Telefon se chová jako bezkontaktní karta
- Určeno především k placení na POS terminálech
- Potřebné HW vybavení
  - NFC čip s anténou
  - Secure Element
- Potřebné SW vybavení
  - Platební aplikace
  - Mobilní aplikace
  - PPSE

NFC telefony

Near Field Communication

- Množina standardů pro bezkontaktní výměnu dat na krátkou vzdálenost
  - ISO/IEC 1443
  - ISO/IEC 18092
  - ISO/IEC 15693 – delší dosah, nižší přenosová rychlost
- Operační módy
  - Peer-to-Peer – výměna dat, sdílení souborů (konfigurace Wi-Fi apod.)
  - Reader/Writer – čtení a zapisování NFC tagů (reklamní plakáty, …)
  - Card Emulation – emulace bezkontaktní karty ISO/IEC 14443 (platby, hromadná doprava atd.)

NFC telefony

Hardware

- NFC čip s anténou
  - Umístění
    - Součást telefonu
    - microSD karta
    - Rámeček/obal na telefon
- Secure Element
  - Bezpečné uložení aplikací a dat
  - Tamper resistant HW, certifikace
  - Přímá komunikace s NFC čipem bez účasti CPU
  - Umístění
    - Součást telefonu
    - microSD
    - Rámeček/obal na telefon
    - SIM/UICC – největší standardizace

NFC telefony

Software – platební aplikace

- Ekvivalent platební karty
- Uložena včetně dat v SE
  - Aplikace
  - Nastavení aplikace
  - Údaje o držiteli a kartě
  - Klíče
- Podobnost s kartou
  - Bezkontaktní profil pro čipové i MSD transakce
  - Online i Offline použití
- Nové vlastnosti
  - mPIN
  - Objekty pro komunikaci s mobilní aplikací
  - Některá nastavení mobilní aplikace
  - Profil nemá podporu pro kontaktní rozhraní (EMV)

NFC telefony

Software – mobilní aplikace

- Grafické rozhraní
  - Historie transakcí
  - Výběr karty
  - Preference
  - Ověření držitele na telefonu
- Uložena v normální paměti, zpracování v CPU
- Aplikace pro jednu kartu vs. Mobilní peněženka (více karet, reklamy, kupóny)
- Komunikace s vydavatelem skrze MNO nebo Wi-Fi
- Další možnosti:
  - Dynamické generování CVV2
  - Zobrazení citlivých informací karty
  - Dobíjení kreditu
  - Jednorázová hesla (CAP/DPA)
- Vliv na konfiguraci PPSE

NFC telefony

Software – aplikace PPSE

- PPSE – Proximity Payment System Environment
- Katalog dostupných bezkontaktních aplikací – urychlení procesu výběru aplikace na terminálu
- Aktualizace podle aktivovaných platebních aplikací a potřeb držitele
- Správa PPSE
  - Přímo (External Mode) – změna konfigurace (datové struktury) přichází přímo z mobilní aplikace
  - Nepřímo (Internal Mode) – mobilní aplikace aktivuje/deaktivuje platební aplikaci, ta informuje CSR (GP Contactless Registry Service). Aplikace PPSE si upraví sama konfiguraci na základě notifikace z CSR
- Příklady obsahu PPSE
  - Více aplikací s preferencemi
  - Alespoň jedna aplikace v PPSE, pokud má být platba zahájena kdykoliv pouhým přiložením
  - Prázdné PPSE pokud držitel nechce, aby byla stále viditelná platební aplikace

NFC telefony

Správa Software – příklad rámečku na telefon

- Příklad použití obalu obsahujícího SE a NFC čip s anténou
- Důvod pro zvolený HW
  - Podpora iPhone
  - Nezávislost na MNO
- Personalizace v standardním personalizačním centru
  - Platební aplikace
  - PPSE
- Po převzetí HW si klient nainstaluje mobilní aplikaci z obchodu s aplikacemi dané platformy
- Aktivace

NFC telefony

Správa Software – příklad UICC & TSM

- Řešení založené na NFC telefonech s NFC SIM (UICC)
- Vlastníkem SE (SIM/UICC) je MNO!
- Sjednání služby v bance – držitel získá aktivační kód
- Vzdálená instalace a spuštění mobilní aplikace, držitel zadá aktivační kód
- Po validaci kódu zahájí TSM prostřednictvím MNO kontrolu vhodného HW vybavení (Eligibility Check)
- V případě vhodného vybavení
  - OTA vytvoření bezpečnostní domény banky v SE
  - OTA instalace SW a personalizace dat
  - Mobilní aplikace mezitím zobrazuje stav
  - Na závěr si držitel zvolí mPIN
- Správa prováděna prostřednictvím TSM (Trusted Service Manager)

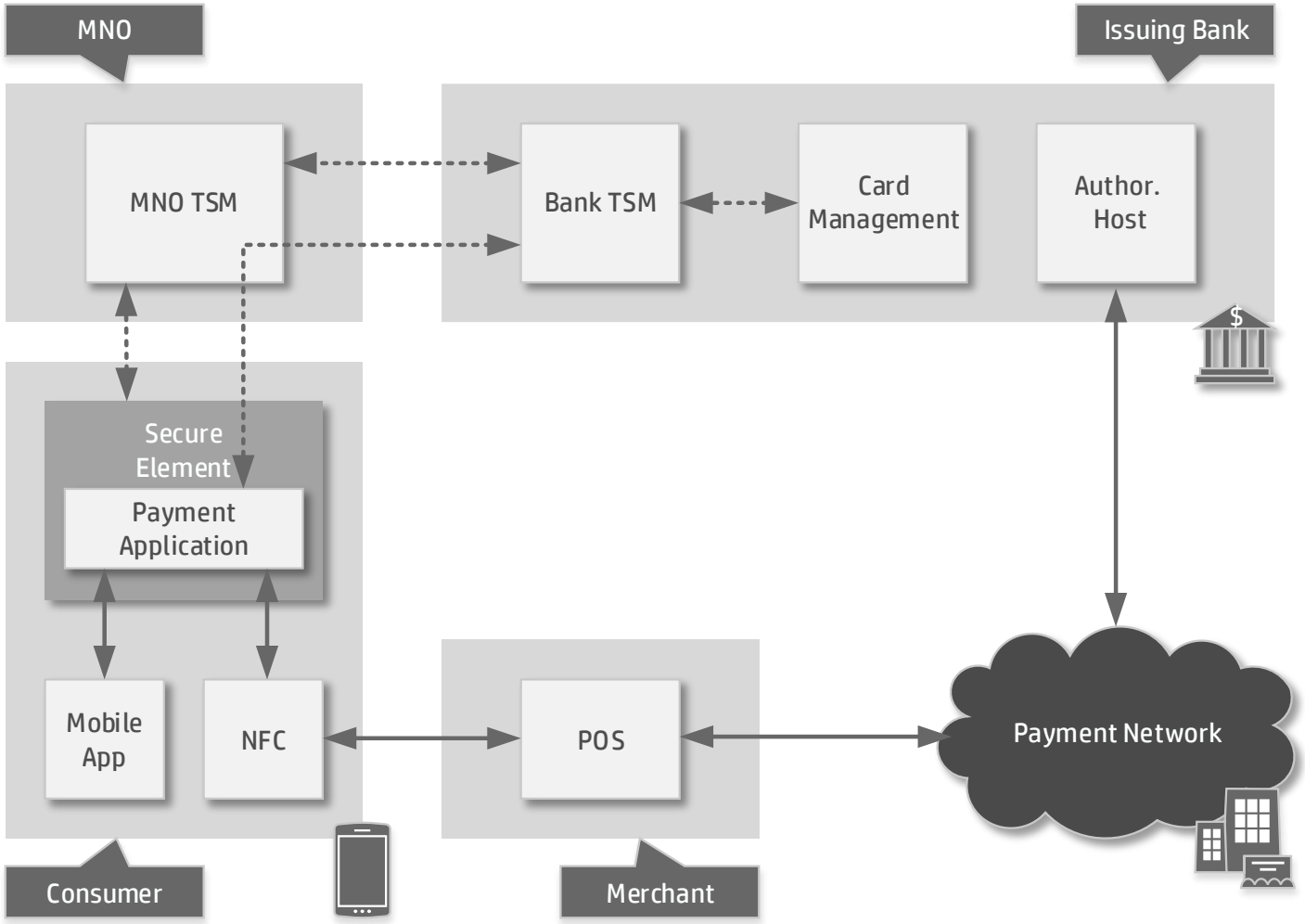
NFC telefony

TSM – Trusted Service Manager

- Vzdálená správa životního cyklu aplikací na SE se zachováním bezpečnosti
- Propojení vydavatelů SE (MNO) a poskytovatelů služeb (banky)
- Umožňuje poskytovateli služeb spravovat svou pronajatou oblast v SE, tj. instalovat a personalizovat aplikaci objednané služby
- Z pohledu banky jde o mobilní personalizační centrum
- TSM
  - MNO TSM
  - Bank TSM
- Proces je interaktivní, nikoliv dávkový jako u výroby běžných karet
- TSM nemusí patřit nutně MNO -> výměna klíčů mezi TSM a MNO
- TSM se nijak neúčastní bezkontaktní transakce
- Složitá a drahá implementace

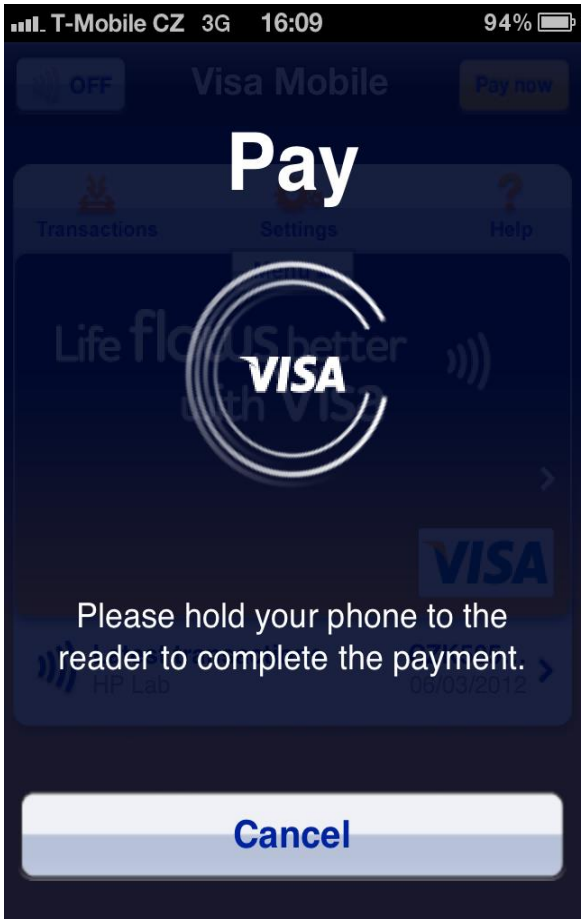
NFC telefony

Trusted Service Manager



NFC telefony

Placení na terminálech



- Platba jako s bezkontaktní kartou
- Podlimitní transakce bez ověření držitele
- Nad 500,- Kč požadována verifikace
  - mPIN/Passcode
    - ověření na telefonu
    - potřeba druhého přiložení
  - Online PIN
    - ověření na POS terminálu
- Verifikace může být požadována s každou platbou
- Na rozdíl od karet lze řídit chování telefonu po přiložení do elektromag. pole
  - Platba až při spuštěné mobilní aplikaci
  - Automatické spuštění mobilní aplikace
  - Možná platba s vypnutým telefonem

NFC telefony

Placení na Internetu

- K placení na Internetu obvykle potřebujeme číslo karty, platnost a hodnotu CVC2/CVV2 ze zadní strany karty
- Mobilní karta postrádá zadní stranu :-)
- Platební aplikace může obsahovat oblast s citlivými daty
- Zobrazení mobilní aplikací po verifikaci držitele
- Visa – možnost generování dynamické hodnoty nahrazující CVV2

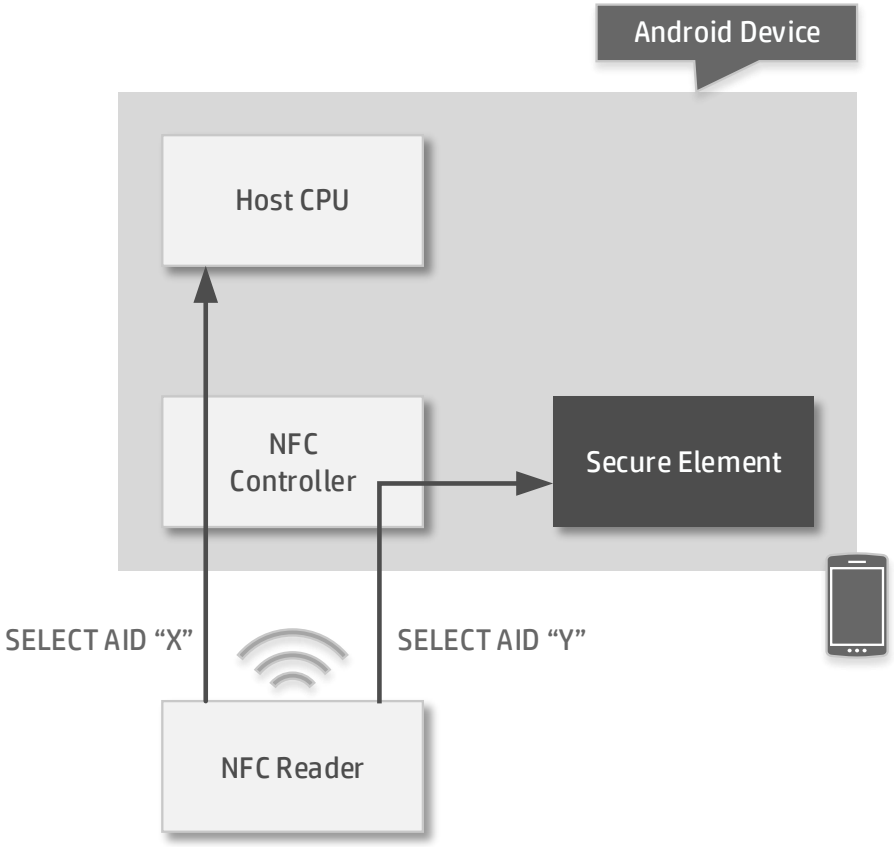
NFC telefony

Risk Management

- Offline transakce vyžadují offline akumulátory a čítače
  - Resetování těchto objektů probíhá běžně v kontaktním rozhraní
  - Telefony - druhé přiložení po transakci (někdy vlastně třetí)? Jen někdy? To není praktické
  - Resetování přes síť MNO nebo WiFi
    - Platební aplikace obsahuje příznaky indikující potřebu spojení s bankou
    - Spojení provedeno po transakci nebo na vyžádání
    - Generování ARQC, odeslání přes VISA Mobile Gateway nebo Reset Server do banky
    - Zpracování odpovědi a aktualizace objektů karty (popř. zpracování skriptů)
  - Potřeba ověření držitele – ochrana před dobíjením karty
- Čítače a akumulátory k ochraně před zneužitím telefonu
  - Po překročení limitů potřeba verifikace držitele, bez nutnosti spojení s bankou
- Ověření držitele (mPIN)
  - Opakovanému dotazování na mPIN během transakce či dokončení lze předejít nastavením platnosti (dané operace vs. stanovená doba)

NFC telefony

Host Card Emulation



- Android 4.4 KitKat a BlackBerry 10
- Na základě směrovací tabulky (NFC čip) lze v režimu Card Emulation směrovat data z NFC do SE nebo CPU (default je CPU)
- Platební aplikace nemusí být tedy nutně v SE
- Obvykle se předpokládá umístění dat v Cloudu, popř. v TEE
- Nezávislost na MNO
- Není potřeba TSM

NFC telefony

Porovnání HCE a SE

HCE NFC

- Instalace jako u standardní aplikace
- Závislost na online spojení
- mPIN – bezpečné uložení?
- Nelze s vybitou baterií
- Citlivé informace v datovém centru
- Nutná vícevrstvá bezpečnost
  - Jednorázová data
  - White-box kryptografie
  - Real-time analýza transakcí
  - Kontrola otisku mobilního zařízení
- Tokenizace – virtualizace čísla karty

SE NFC

- Potřeba SIM SE, správa prostřednictvím TSM
- Placení za všech okolností jako s kartou
- Podpora mPIN
- Možnost platby s vybitým telefonem
- Citlivé informace v SE
- SE poskytuje bezpečnost jako karta
- Zralost technologie a standardů

NFC telefony

Apple Pay

- Po neúspěšných pokusech naděje pro NFC
- Příkladná spolupráce Apple, Visa, MasterCard a Amex na novém “modelu” celého ekosystému
- Využití různých stavebních kamenů
  - iPhone 6
    - SE vlastněný Apple
    - NFC čip s anténou
  - Tokenizace (prováděna na straně asociací)
  - mPIN nahrazen otiskem prstu
- NFC nebude přístupné jiným aplikacím
- Placení v mobilních aplikacích
- Apple nedrží historii transakcí
- Pokusí se i ostatní výrobci (Samsung, HTC, LG, ...), když je prostředí připravené?

MasterCard Mobile

MasterCard Mobile

Použití a potřebné vybavení

- Telefon se netváří jako karta, ale nabízí přístup ke kartám v digitální peněžence
- Nejčastěji viditelné při placení na Internetu
- Možné platby přímo z mobilních aplikací
- Historie transakcí, seznam obchodníků

- Nevyžaduje žádné speciální vybavení jako SE nebo NFC
- Postačí běžný moderní telefon nebo tablet
  - s OS Android nebo iOS
  - a fotoaparátem
- Nutný přístup k Internetu (MNO, Wi-Fi)

MasterCard Mobile

Instalace SW vybavení

- Implementace v ČR – WN Wallet od společnosti Wincor Nixdorf
- Instalace z obchodu s aplikacemi dané platformy
- Každé instanci aplikace na telefonu je přidělen jednoznačný identifikátor
- Identifikátor je spojen s virtuální peněženkou, která je během instalace založena v datovém centru SP (PCI-DSS)
- Aktivace aplikace na základě kódu zaslaného prostřednictvím SMS
- Před dokončením instalace zvolen mPIN
  - Přístup do aplikace
  - Potvrzení platby vybranou kartou
- Aktivace ukončena výměnou komunikačních klíčů mezi telefonem a SP
- Opakovaná instalace vede k novému identifikátoru aplikace a nové peněžence u SP!

MasterCard Mobile

Vložení karet

- Kartu lze vložit bez jakékoliv žádosti v bance
- Lze zaregistrovat libovolnou kartu (MasterCard, Maestro, Visa, Visa Electron, Diners Club)
- Uživatel vloží číslo karty, platnost a CVC2/CVV2 – tyto informace nejsou uloženy do telefonu, nýbrž do virtuální peněženky u SP
- V telefonu je k dispozici pouze maskované číslo karty, přiřazené jméno a barva
- Při vkládání provedena transakce na 1 Kč
  - 3DS ověření transakce – výsledek ověření je ihned k dispozici, karta je okamžitě aktivní
  - V opačném případě je karta aktivována až po vložení kódu získaného z bankovního výpisu nebo eBankovnictví

MasterCard Mobile

Placení na Internetu

- Po přesměrování na platební bránu je k dispozici logo/tlačítko MasterCard Mobile
- Po zvolení této platby je zobrazen QR kód – identifikátor transakce ve WN Wallet
- Držitel nastartuje aplikaci MasterCard Mobile a naskenuje QR kód
- Na telefonu se zobrazí informace o transakci (částka, měna, obchod)
- Držitel zvolí kartu z peněženky a zadá mPIN
- Po verifikaci mPIN a požadavku u SP jsou platební bráně bezpečně předány informace o zvolené kartě
- Proběhne standardní eCommerce transakce

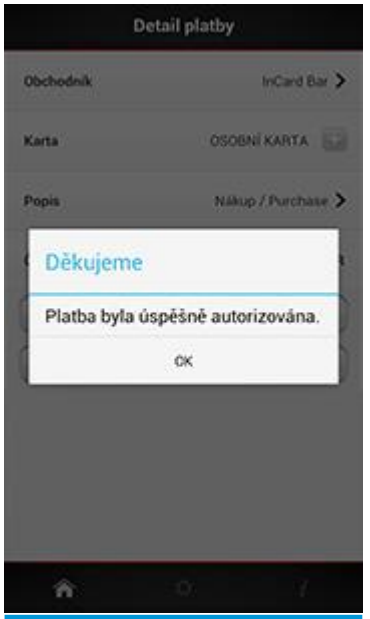
MasterCard Mobile

Placení na Internetu

Detaily transakce

Výběr karty

Verifikace držitele



Výsledek transakce

MasterCard Mobile

eCommerce Transakce

- Držitel u obchodníka vloží zboží do virtuálního nákupního košíku a přistoupí k platbě
- Přesměrování na platební bránu, bezpečný kanál (SSL/TLS)
- Platební brána zaeviduje transakci do systému, provede základní kontroly a vrátí částečně vyplněný HTML formulář zákazníkovi, aby mohl doplnit údaje o platební kartě
- Odeslání formuláře s vyplněným číslem a platností karty, včetně kódu CVC2/CVV2 ze zadní strany karty
- Brána pošle obchodníkovi bezpečným kanálem k revizi informace o transakci. Tento krok slouží jako potvrzení, že nedošlo k modifikaci dat transakce
- Obchodník potvrdí platební bráně správnost dat

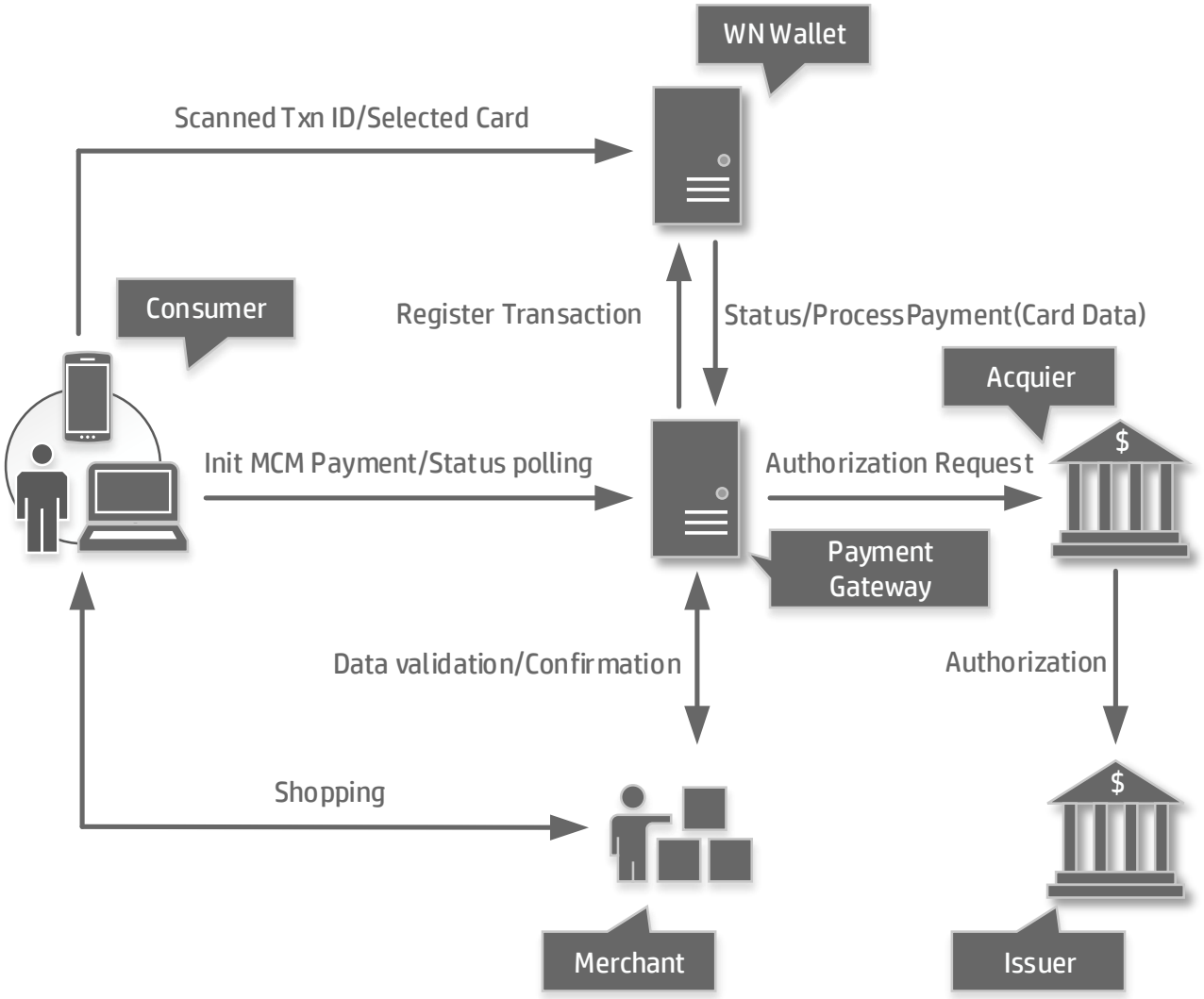
MasterCard Mobile

eCommerce Transakce – pokračování

- Pokud brána podporuje program 3-D Secure, je proveden pokus o autentizaci držitele:
  - Brána pošle dotaz do adresářové služby asociace, zda je karta zapojena do programu 3-D Secure
  - Pokud ano, dojde k přesměrování držitele na ACS (Access Control Server) vydavatelské banky
  - ACS obvykle vygeneruje jednorázový kód, který je zaslán držiteli prostřednictvím SMS
  - Držitel přepíše získaný kód do formuláře, ACS ověří kód a s podepsaným výsledkem přesměruje držitele zpět na platební bránu
  - Brána provede verifikaci výsledku ověření a na základě výsledku autentizace se rozhodne o pokračování v transakci
- Brána pošle transakci k autorizaci do vydavatelské banky
- Na základě odpovědi z autorizačního centra vydavatele platební brána transakci schválí nebo zamítne
- Obchodník i držitel jsou informování o provedení a výsledku transakce
- Webový prohlížeč je přesměrován zpět na stránky obchodníka

MasterCard Mobile

Integrace MCM do eCommerce transakce



MasterCard Mobile

Integrace MCM do eCommerce transakce

Po zvolení MCM platby proběhnou následující kroky:

- Platební brána provede prostřednictvím WS (Web Service) registraci transakce u SP
- SP přidělí a odešle zpět unikátní ID. Toto ID je zobrazeno v prohlížeči jako číslo a QR kód
- Prohlížeč začne periodicky zjišťovat stav transakce v platební bráně
- Držitel nastartuje mobilní aplikaci MCM, zadá mPIN a naskenuje QR kód
- Telefon odešle ID poskytovateli služby MCM -> spárování peněženky se zaregistrovanou transakcí. Na telefou zobrazeny podrobnosti transakce.
- SP pošle do platební brány informaci, že transakce byla naskenována
- Držitel vybere na mobilním telefonu kartu. Současně může být znovu dotázán na mPIN
- SP provede verifikaci požadavku z telefonu a poté zašle do platební brány pokyn k vykonání transakce s informacemi o zvolené kartě (číslo karty, platnost, CVC2/CVV2)
- Platební brána změní stav transakce a zajistí autorizaci u vydavatele karty. Webový prohlížeč periodickými dotazy zjistí, že transakce je již vybavována a zobrazí pokyn k vyčkání na výsledek
- Po obdržení autorizační odpovědi je SP informován o výsledku transakce

MasterCard Mobile

Přímé platby z telefonu

- Obchodníci mají vlastní aplikace pro tablety a telefony (bez Webového prohlížeče)
- MCM podporuje přímé platby z mobilních aplikací
  - Z aplikace provedena registrace platby u SP
  - Poté automaticky nastartována aplikace MCM na telefonu s přiděleným identifikátorem transakce
  - Po potvrzení transakce a verifikaci držitele zaslán požadavek SP k provedení autorizace
  - Po provedení platby předáno řízení zpět aplikaci obchodníka
  - Aplikace zašle dotaz SP na výsledek platby
- Modely komunikace s SP (registrace, dotaz na výsledek)
  - Backend-to-backend – zabezpečená komunikace serverů obchodníka a SP. Telefon komunikuje pouze se serverem obchodníka, který obsahuje klíče pro podepisování zpráv.
  - Server obchodníka pro generování podpisů – komunikace mezi telefonem a SP, potřebné podpisy zpráv zajistí pro telefon vyhrazený server obchodníka
  - Přímá komunikace – privátní klíč uložen v telefonu. Nejsložitější na bezpečnost

MasterCard Mobile

Zabezpečení

- Komunikace aplikace MCM a SP chráněna protokolem TLS
- Každý požadavek je na straně SP ověřován (MAC a otisk mPIN)
- Do MAC vstupuje
  - Identifikátor aplikace
  - Otisk mPIN
  - Data požadavku
  - Symetrický klíč
- Symetrický klíč je s každým požadavkem měněn
- Obě strany pracují výhradně s otiskem mPIN
- Po třech neúspěšných pokusech o verifikaci mPIN dochází k blokaci na 24 h
- Pokud se ani poté nepovede třikrát ověření, trvalá blokace => nová instalace a registrace všech karet

MasterCard Mobile

Zabezpečení

- Komunikace aplikace SP a platební brány prostřednictvím WS
- Zabezpečení protokolem TLS
- Standard WS-Security
  - Šifrování citlivých XML elementů (PAN, platnost, CVC2, tel. číslo)
  - Digitální podpis zpráv
  - Security token - X.509 certifikáty

MasterCard Mobile

Budoucnost

- SP je v ČR a SR společnost Wincor Nixdorf
  - Aplikace nefunguje v ostatních zemích, nutné nainstalovat jinou aplikaci
  - Bylo by vhodné propojení prostřednictvím asociace MasterCard
- Další použití
  - Placení složenek
  - Dárcovské platby
  - Dobíjení kreditu
  - Posílání peněz mezi kartami
- Teoreticky možné platit na POS terminálech
  - Skenování QR kódu z displeje POS nebo mPOS
  - Využití NFC k přenosu identifikátoru zaregistrované transakce
- Bude MMRP nahrazeno DSRP (Digital Secure Remote Payment)?
  - Podobný model používání – QR kódy skenované telefonem a placení z mobilních aplikací
  - EMV kryptografie – v závislosti na možnostech obchodníka a Acquiera bude transakce čipová nebo eCommerce
  - SE, tokenizace

Děkuji za pozornost

Martin Chlumský
<martin.chlumsky@hp.com>