IMPLEMENTIMI I MOBILE BANKING NJË RAST STUDIMI

***KRASTAFILAKU E., XHINA E.**

Universiteti Tiranës, Fakulteti Shkencave të Natyrës, Departamenti Informatikës

e-mail: elona.krastafilaku@fshn.edu.al

Përmbledhje

Përdorimi i pajisjeve celulare në komunikimin e përditshëm është duke u rritur me shpejtësi. Risitë teknologjike si dhe zhvillimi i telefonave celularë ka krijuar mundësi për të ofruar komunikime të ndryshme si dhe të kryen transaksione biznesi duke përdorur telefonat celularë. Në përputhje me potencialin e rritjes së tregtisë në industrinë celulare është krijuar një shumëllojshmëri e përpunimit të pagesave celulare e cila përdoret në përputhshmëri me shërbimet e komunikimit si GPRS, USSD, NFC, SMS, Bluetooth, WAP, WI-FI etj. Në këtë artikull ne do të prezantojmë dhe analizojmë disa nga zgjidhjet e arkitekturës në transaksionet me celular dhe strukturat e procesimit të pagesave në transaksionet me celular si dhe do të paraqesim një rast implementimi në një nga bankat e nivelit të dytë.

Abstrakt

The usage of mobile devices in every day communication is growing. Technological innovations and developments of the mobile phones have created opportunities to provide several communications and conduct business transactions using mobile phones. In line with the potential growth in the mobile industry trade is created a variety of mobile payment processing that can be used in accordance with different communication services like GPRS, USSD, NFC,SMS, Bluetooth, WAP, WI-FI etc. In this article we will present and analyze some of the architecture solutions in mobile transactions and payment processing structures in mobile transactions and present a case of implementation in one of the commercial banks.

Fjalëkyçet: Mobile banking, SMS, USSD, WAP, NFC.

Hyrje

Në Shqipëri përdorimi i telefonisë së levizshme ka filluar në vitin 1996. Deri në vitin 2013 në treg ekzistojne 4 operatorë që ofrojnë shërbimin e telefonisë së lëvizshme. Ky shërbim nga viti në vit ka pësuar rritje dhe shifrat tregojnë se numri përgjithshem i numrave të telefonisë së lëvizshme tejkalon dhe numrin e përgjithshëm të popullsisë me përfarsisht 3.3 milion deri në gjysmën e vitin 2013. Sipas të dhënave të raportit vjetor 2012 nga AKEP numri përdoruesve celularë që përdorin internetin GRPS/EDGE në vitin 2012 është 1.4 milion.

Ky numër tregon që shqiptarët janë përdorues të mirë të telefonisë së lëvizshme dhe kjo shërben si një sinjal që institucionet financare duhet ta përdorin për te ofruar shërbime alternative.

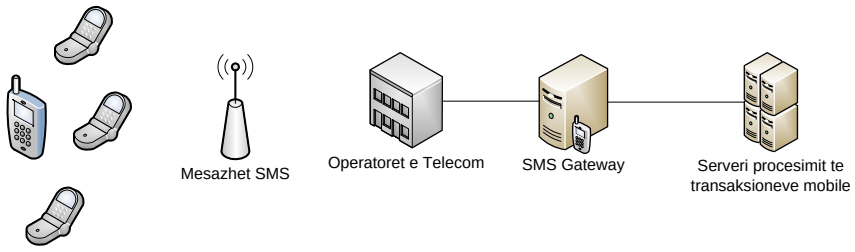
Kanalet Celulare

SMS: Mesazhet SMS suportohen në pothuaj të gjitha pajisjet celulare dhe shumica e përdoruesve mund të përdorin mesazhet SMS për të kryer transaksione mobile duke përdorur celularët e tyre. Ky kanal në përputhje me modelin e biznesit ka avantazhet dhe disavantazhet bazuar në aspektin rregullator të pajtueshmerisë. Është model i kushtueshëm në krahasim me kanalet e tjera alternative të lëvizshme. Transaksionet mobile të mbështetura në shërbimin SMS ofrojnë tekonologjinë e sigurisë më të ulët për shkak disa pikave ku të dhënat e SMS janë të aksesueshme në një format të pastër dhe të painkriptuar.

Arkitektura e kanaleve SMS

Në këtë model mesazhet hyrëse dhe dalëse dërgohen dhe merren nga një gateway SMS e cila përdoret si një ndërfaqe ndërmjet përdoruesit dhe server-it. Të gjitha SMS hyrëse pranohen nga gateway SMS dhe ruhen në bazën e të dhënave në të cilën mesazhet janë lexuar nga shtresa e përpunimit. Mesazhet dalëse shkruhen në bazën e të dhënave nga e cila SMS gateway dërgon mesazhet për përdoruesit. Skema më poshtë paraqet arkitekturën SMS:

Figura1: Arkitektura SMS

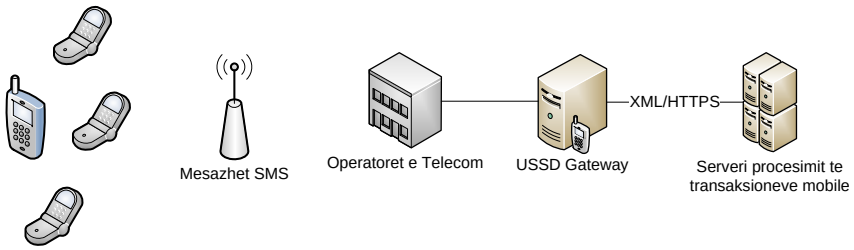


USSD: Kanali USSD mund të suportohet nga modele të ndryshme pajisjesh celulare. Është më e sigurt krahasuar me SMS por është e ndryshme dhe e varur nga ofruesit e Telecom që do të thotë se ka një kosto të lartë implementimi.

Arkitektura e kanalit USSD

USSD është një shërbim i orientuar nga sesioni. Përdoruesi mund të dërgojë dhe të marrë mesazhe me serverat USSD duke përdorur komandat USSD. Skema në vazhdim përshkruan rrjedhën e arkitekturës USSD.

Figura2: Arkitektura USSD



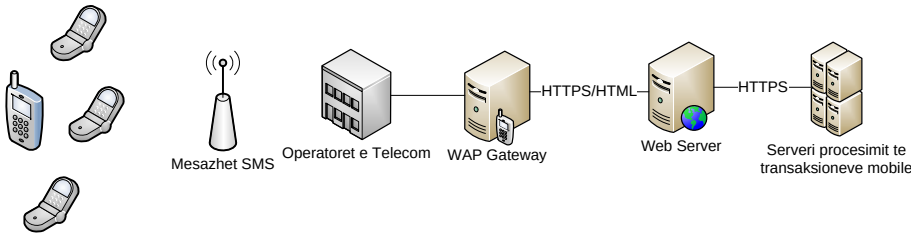
Browser-at Mobile: Browser-i mobile përdoret për të akesuar WAP ose aplikimet web për kryerjen e transaksioneve të biznesit në celular. Ky lloj kanali është i lehtë për tu përshtatur me shpjetësi për pajisjet mobile.

Arkitektura e Mobile browser

Një ndër standartet e përdorura për integrimin mobile browser është WAP i cili akseson përmbajtjen e WAP nëpërmjet WAP browser-ave. Bowser-i WAP është në gjendje të njohë përmbajtjen WML dhe ta shfaqë atë në pajisjen celulare. WAP dërgohet dhe merret nëpërmjet WAP gateway e cila përdoret për të konvertuar WAP në HTTP/HTTPS ndërmjet WAP gateway dhe web server-it i cili është hostuar në proçesuesin e transaksionit mobile.

Skema në vijim përshkruan arkitekturën WAP.

Figura3: Arkitektura WAP



NFC dhe komunikimi pa kontakt: Ky kanal mund të suportohet nëse NFC është e aktivizuar në pajisjet celulare.

Arkitektura NFC

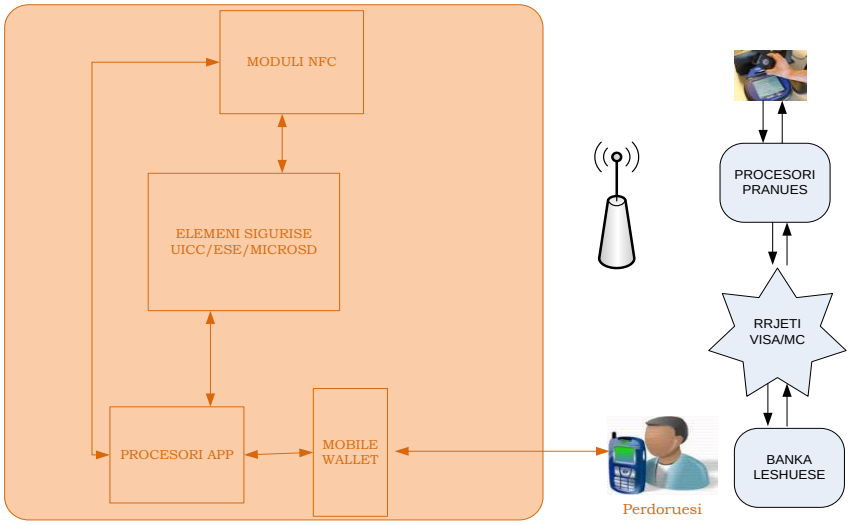
Ky është një komunikim me distancë të shkurtër dhe funksionon në pajisjet mobile që e kanë të aktivizuar NFC e cila mund të ndërveprojë me një POS që ka të aktivizuar NFC dhe të kryejë transaksionin nëpërmjet komunikimit NFC. Detajet e kartës dhe të PIN-it janë të ruajtura në kontrollerin e NFC në pajisjen celulare. Ekzistojnë tre modele të sigurisë per NFC:

UICC janë promovuar nga operatorët celularë; UICC përdoret si një element i sigurt për ruajtjen e informacionit në rrjet. UICC komunikon me kontrollerin NFC të celularit duke përdorur protokollin Single Wire (SWP). Të dy UICC dhe kontrolleri NFC krijon një mjedis të sigurt.

Hardware i integruar është një kartë smart e cila është pjesë e telefonit mobile dhe nuk mund të hiqet. Ky chip është vendosur në momentin e prodhimit dhe duhet të jetë i personalizuar mbasi pajisja jepet përdoruesit.

Kartë memorije e sigurtë (SMC) përbëhet nga një kombinim i kartës memorie dhe një karte smart. Kjo kartë ofron të njëjtën nivel sigurie me një kartë smart dhe është në përputhje me standartet kryesore si EMV, ISO. Si një kartë e lëvizshme dhe me memorie kapaciteti të lartë të lejon të hostosh një numër te madh aplikacionesh.

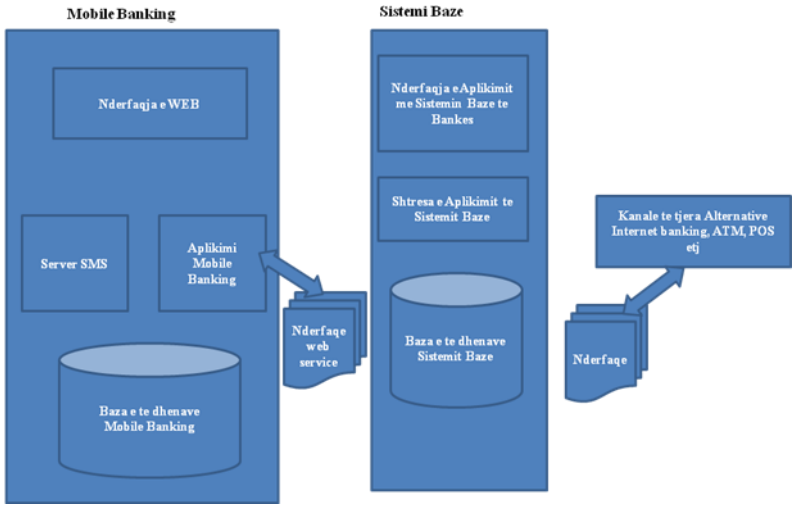
Figura4: Arkitektura e një telefoni celular me NFC e aktivizuar



Implementimi i Mobile banking

Ofrimi i shërbimeve financiare nëpërmjet telefonisë së lëvizshme (mobile banking) u lejon përdoruesve të kryejnë veprime financiare pa qënë e nevojshme prezenca fizike e klientit. Institucionet financiare ofrojnë këtë shërbim alternativ duke u perpjekur të zëvendësojnë transaksione që mund të kryhen me prezencë fizike duke ndërvepruar pavarësisht pozicionit të klientit dhe orarit të kryerjes së veprimeve.

Skema 1: Arkitektura e implementimit të mobile banking



Siguria dhe Autentifikimi

Autentifikimi dhe siguria janë dy elementet kryesore në një aplikim mobile banking. Përveç inkriptimit në nivel web protokolli është e nevojshme autentifikimi me dy faktorë për të mbrojtur përdoruesin nga rastet kur një fjalëkalim është vjedhur. Autentifikimi me dy faktorë kerkon që përdoruesi të përdore fillimisht fjalëkalimin e tij për t'u autentifikuar në sistemin mobile banking. Ky konsiderohet si faktori i pare per autentifikim.

Duke qënëse për shkaqe të ndryshme si pakujdesia e përdoruesit, ndërhyrje në rrjetin e komunikimit etj, fjalëkalimi i përdoruesit mund të vidhet nga ndonjë person i paautorizuar. Personi i paautorizuar mund të tentojë që me një tjetër pajisje të lidhet me sistemin mobile banking duke u identifikuar si përdoruesi që i është vjedhur fjalëkalimi. Në autentifikimin me dy faktorë sistemi mobile banking pasi përdoruesi është autentifikuar me fjalëkalim i dërgon atij një kod në numrin e tij të telefonit nëpërmjet një mesazhi SMS.

Për të përfunduar me sukses procesin e autentifikimit përdoruesi duhet të vendosë në hyrjen e sistemit mobile banking edhe këtë kod që është dërguar atij me SMS. Kodi është i vlefshëm vetëm një herë gjë që e bën atë te papërdorshëm për ndonjë ndërhyrës pasi është përdorur nga përdoruesi real. Dërgimi i një kodi të dytë nëpërmjet kanalit të SMS-ve e pengon vjedhësin e fjalëkalimit që të përfundojë me sukses fazën e dytë të procesit të autentifikimit. Në të njëjtën kohë sinjalizon përdoruesin dhe bankën për mundësinë e një tentative keqëdashëse për autentifikim të pautorizuar në sistemin mobile banking.

Aktivizimi

Rasti konkret i implementuar në një nga bankat e nivelit të dytë ka përdorur si mjet aktivizimi të shërbimit mobile banking rregjistrimin e klientëve në internet banking. Një klient mund të aksesojë shërbimin mobile banking vetëm pasi të jetë rregjistruar fillimisht në internet banking.

Limite ose kufizime me qëllim rritjen e sigurisë

Për të rritur sigurinë banka për transaksione specifike mund të vendosë limite si në nivel banke ashtu dhe në nivel klienti. Klienti mund të përzgjedhë të ruajë të njëjtat limite me bankën ose të rrisë sigurinë duke vendosur kufizime dhe përcaktuar limitet e tij.

Konkluzionet

Numri i përdoruesve të telefonisë së lëvizshme dhe internetit nëpërmjet telefonit e ka shndëruar shërbimin e bankingut nëpërmjet internetit në celular një mundësi të re të një kanali interaktiv gjithmonë pranë klientit. Mjetet dhe teknikat që mundësojne ndërfaqësimin e përdoruesit me shërbimin e bankingut nëpermjet telefonave smart janë disponibël dhe mundësojne mënyra të ndryshme të ofrimit të këtij shërbimi. Në mënyrë të veçantë çështjet e sigurisë marrin rëndësinë për shkak të ndjeshmerisë së të dhënave të transmetuara dhe vështiresive në imponimin e procedurave standarte të sigurisë tek klienti fundor. Në këto kushte sistemet me siguri të shtuar si psh ato që kërkojnë një autentikim të dyfishtë janë kusht për ofrimin e këtij shërbimi të bankingut.

Literatura

AKEP (Raporti Vjetor 2012)

http://www.akep.al/images/stories/AKEP/publikime/2013/RAPORTI-VJETOR-2012.pdf

Igoe T., Coleman D., Jepson B. (2014): Beginning NFC

C.-K.Toh (2001): Ad Hoc Mobile Wireless Networks: Protocols and Systems