

Uporabnost in varnost mobilnih tehnologij v bančništvu

Jure Bogadi



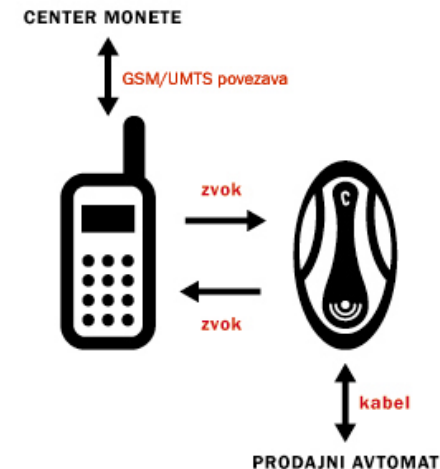


Posamezne črke gesla

- Klic s kateregakoli telefona, uporabnik na zahtevo pove nekaj črk svojega gesla
- Primer storitve:
 - Klic na klicni center banke

GSM/UMTS zaščita

- Prenos preko govornega kanala, telefonska številka kot sredstvo identifikacije
- Primeri storitev:
 - Glasovni kanal Monete
- Varnost
 - Nadomestna bazna postaja
 - Algoritma GSM A5/1 in UMTS A5/3
 - UMTS telefon in SUPERSIM





Enkratno geslo prek SMS

- Uporabnik prejme SMS z enkratnim geslom na mobilni telefon
- Primeri storitev:
 - Urejanje razmerja
- Varnost
 - Ločen kanal (SMS)
 - Zagotovilo, da ima uporabnik ta telefon pri sebi



Simetrični ključi na SIM kartici

- Bančni strežnik komunicira s SIM kartico preko šifriranih SMS sporočil
- Primer storitve:
 - Mobilno bančništvo
- Tehnologija:
 - SIM Toolkit
 - Deluje na vseh telefonih



Digitalno potrdilo na pametnem telefonu

- Certifikat je podobno, kot na računalniku, nameščen na operacijskem sistemu pametnega telefona
- Primer storitve:
 - Spletno (mobilno) bančništvo
- Varovanje:
 - SSL
 - Kraja certifikata?





Digitalno potrdilo na mini prenosniku





EMV – CAP čitalec

- Čitalec generira enkratno geslo
- Primeri storitev:
 - Plačilo prek spleta
 - Prijava v domeno, v spletno banko
- Varovanje:
 - Ločena naprava glede na uporabo
- Izziv za proizvajalca



M:certifikat na SIM kartici

- Bančni strežnik komunicira s SIM kartico preko SMS sporočil
- Podpis, avtentikacija, *asimetrično šifriranje*
- Primeri storitev:
 - Urejanje naročniškega razmerja (dvig limita na Moneti)
 - 1-2-3 Plačam
- Varovanje:
 - X.509, RSA, 1024 bit
 - Števec poslanih / prejetih sporočil
 - Ločen kanal glede na uporabo



Primerjava

- Posamezne črke gesla, enostavno, manj varno
- GSM/UMTS zaščita, enostavno, manj varno
- Simetrični ključi na SIM, potrebna menjava SIM, dela na vseh tel., varno
- Certifikat na pametnem telefonu, težavna namestitev, enostavna uporaba, majhno št. telefonov, vprašljivo varno
- Certifikat na mini prenosniku, identična up. izkušnja, majhno št. prenosnikov, varno
- EMV-CAP čitalec, uporabnik mora imeti čitalec s sabo, zelo varno
- M:Certifikat, potrebna menjava SIM, dela na vseh tel., omogoča podpis, zelo varno



Brezkontaktna plačila

- Brezkontaktna kartica na telefonu
- Primer storitve:
 - Brezkontaktno plačevanje
 - Pilotni projekt z Banko Koper in MasterCardom
- Varovanje na nivoju aplikacije



Hvala za pozornost!

Jure.Bogadi@mobitel.si

