

Identifikaciona informacija – Primer

Neka je identifikaciona informacija sledeća:

Marko Marković

E-mail: marko.markovic@viser.edu.rs

Binarni zapis identifikacione informacije (pojednostavljen) neka taj niz bude:

$P = 1001010$

Generiše se n slučajnih nizova iste dužine kao P:

$S1 = 1101010$

$S2 = 0010100$

$S3 = 1110011$

Protokolom za deljenje tajne generišu se druge polovine parova:

$R1 = S1 \text{ XOR } P = 0100000$

$R2 = S2 \text{ XOR } P = 1011110$

$R3 = S3 \text{ XOR } P = 0111001$

Parovi:

R1 i S1

R2 i S2

R3 i S3

mogu otkriti poruku P (identifikacionu informaciju)- dok njihove polovine same ne otkrivaju ništa:

$$\mathbf{R1 \text{ XOR } S1 = 1001010 = P}$$

$$\mathbf{R1 \text{ XOR } S2 = 0110100 \neq P}$$

Za hash funkciju uzmimo, radi jednostavnosti, XOR funkciju:

$$\mathbf{R1 \text{ (hash)} = XOR (R1) = 0 \text{ XOR } 1 \text{ XOR } 0 \text{ XOR } 0 \text{ XOR } 0 \text{ XOR } 0 \text{ XOR } 0 = 1}$$

$$\mathbf{S1 \text{ (hash)} = XOR (S1) = \dots = 0}$$

$$\mathbf{R2 \text{ (hash)} = XOR (R2) = \dots = 1}$$

$$\mathbf{S2 \text{ (hash)} = XOR (S2) = \dots = 0}$$

$$\mathbf{R3 \text{ (hash)} = XOR (R3) = \dots = 0}$$

$$\mathbf{S3 \text{ (hash)} = XOR (S3) = \dots = 1}$$

Na novčanicu se zapisuju parovi:

R1 (hash) i S1 (hash)

R2 (hash) i S2 (hash)

R3 (hash) i S3 (hash)



Платите по овом чеку са рачуна бр. 908-20001-18

ДИН.

Словима

Кориснику чека

Који овај чек не може пренети на треће лице



Место и датум издавања чека

Потпис издаваоца чека

Серијски број

☒

Број текућег рачуна

☒

Износ

☒

В. жолт

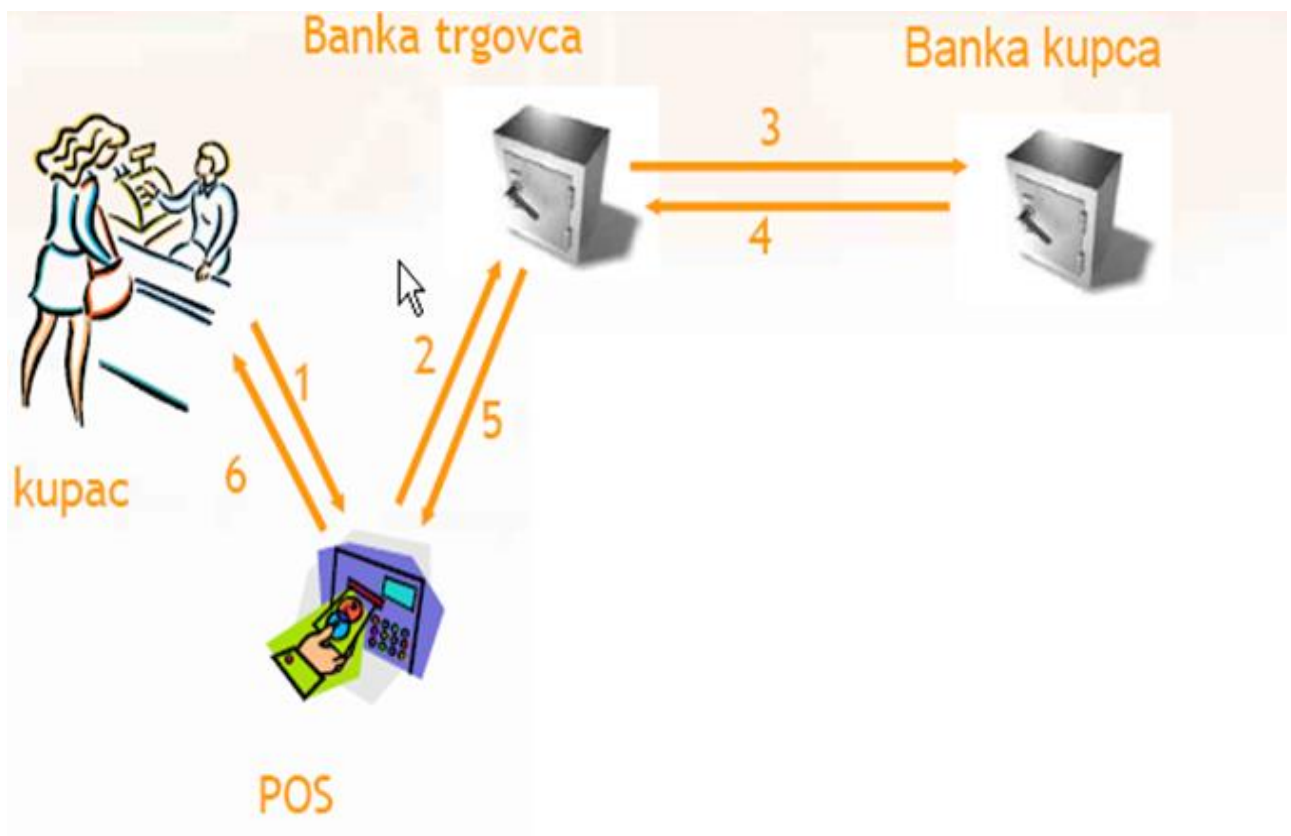
73308160

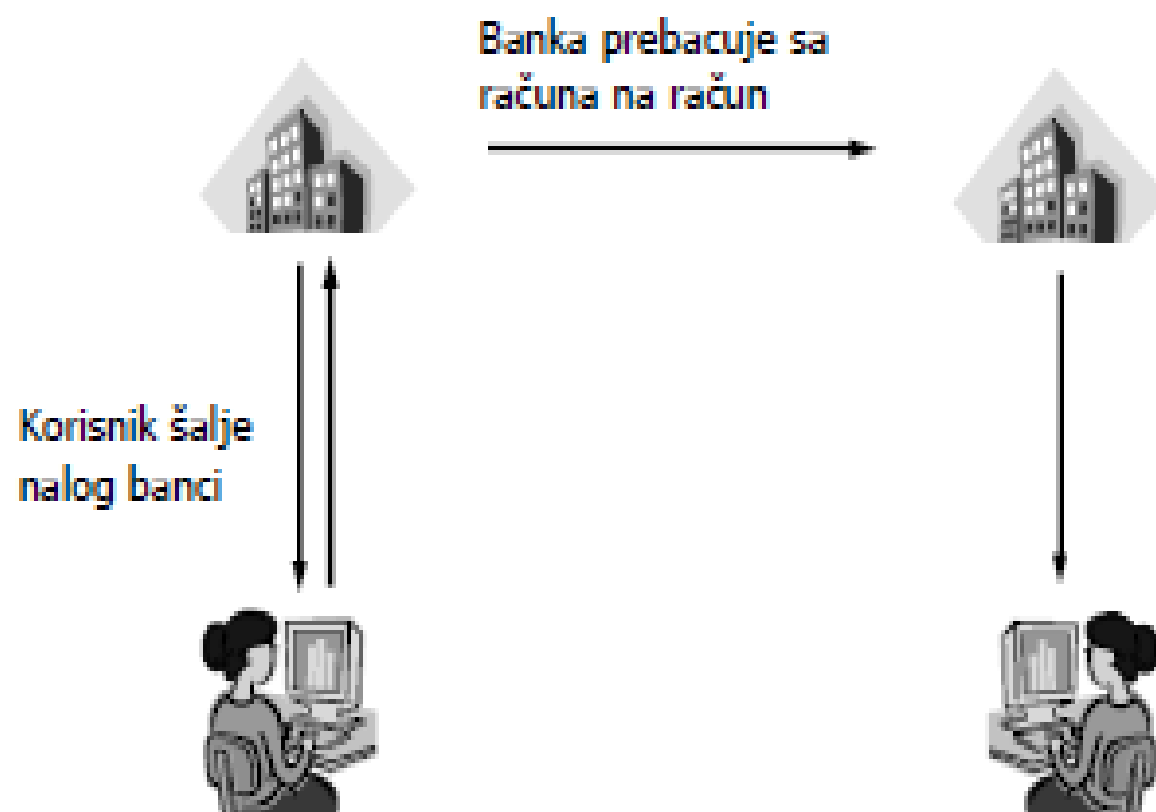
200 2603799 35

15H

Образац бр. 19-ц

По овом пољу не писати и не стављати печате.







Vendor	Value	ID#	Cust ID#	Expires	Props	Stamp	Secret
wellsfargo.com	/ 0.005usd	/ 0081432	/ 101861	/ 19961218	{co=us/st=ca}	1d7f4a734b7c02282e48290f04c20	