

Integriteta in varnost podatkov

↳ ni napak, napačnih podatkov, podatki ne manjkajo
↳ dostop: kdo ima dostop? Kako zagotovimo ustrezen dostop.

Avtentikacija: uporabljeni se prijavijo

Zanesljivost dostopa:

Integriteta

Bankomat A

Bankomat B

Banka
€ 120

1) Stanje? →

2) ← 120

120

→ 3) Stanje?

4) Izdano €100

5) Dwig €100 → 20
← OK

-80

←

6) Izdano €100

7) Dwig €100

?!
..

→

ERROR!

↓
CAS

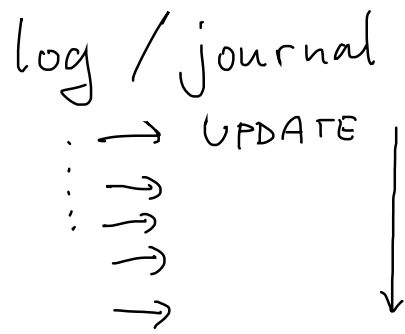
Transakcija

BEGIN ; transakcija se završava

SELECT , ..

UPDATE

SELECT



(a)

COMMIT

Uspješno završeno transakcija

(b)

ROLLBACK

prekinuto izvršavanje

(c)

zmanjena električna

⇒ ROLLBACK

Bankomat s transakcijo

Bankomat A

Banka

1) BEGIN

BEGIN

2) Stanje (SELECT) →

120

←

120

3) Insert →

20

4) Dajmo denar tipu

elektrika!

5) COMMIT

COMMIT

.
:
.
|

DEFERRED/IMMEDIATE

Osoba

ime

priimek

emiso NOT NULL
UNIQUE

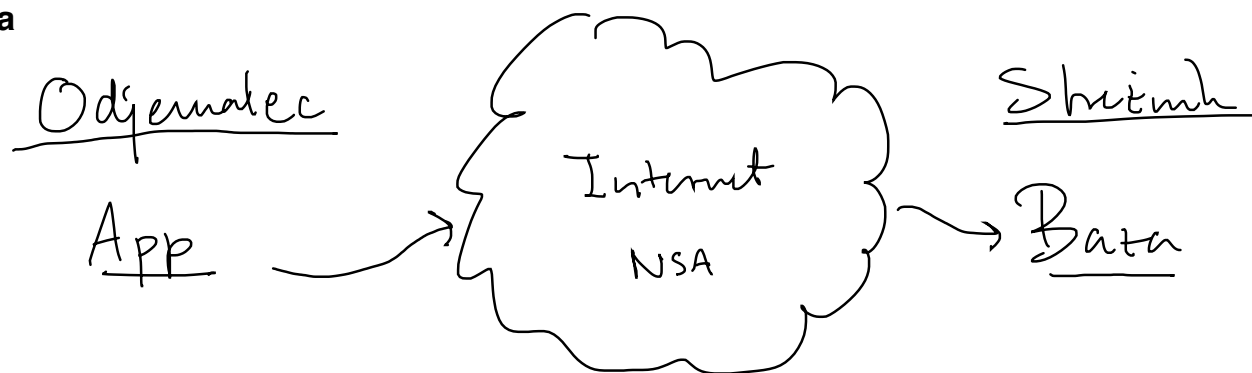
id KEY

	emiso	<u>id</u>
Joze	002	1
Micha	003	2
Jamet	070	3
Leopold		4

DEFERRED ~> preveri po COMMIT

IMMEDIATE ~> preveri takoj / sprati.

Avtentikacija



1) Odjemalec in baza vzpostavita zvezo

2) Odjemalec se avtentificira

- uporabnik / geslo

- ključi:

privatni ključ Pr

javni ključ Pub

Odjemalec

Baza

~~Z~~ ← $\text{decode}_{Pr}(Y)$

←
→

$\text{code}_{Pub}(X) = Y$

Z

$X = Z?$

Gesla

Uporabnik.

Username : Lojze

Geslo : *****
PStrežnikUporabnik

username

password

kripto hash

f(P)

Enosmerna funkcija

 $f : \text{String} \rightarrow \text{string}$ LAHKA f^{-1} TEŽKO RACUNATI :Če poznamo y , težko najdemotak x , da je $f(x) = y$.

GRANT/REVOKE

Nadtonijenski dostop do posameznih tabel :