PADERBORN UNIVERSITY

Join the Bonus Program but stay Private.

Practical Privacy-Preserving Point-Collection for Shopping

SFB 901 Transfer project (T2)

Diebold Nixdorf

C&K

SFB 901

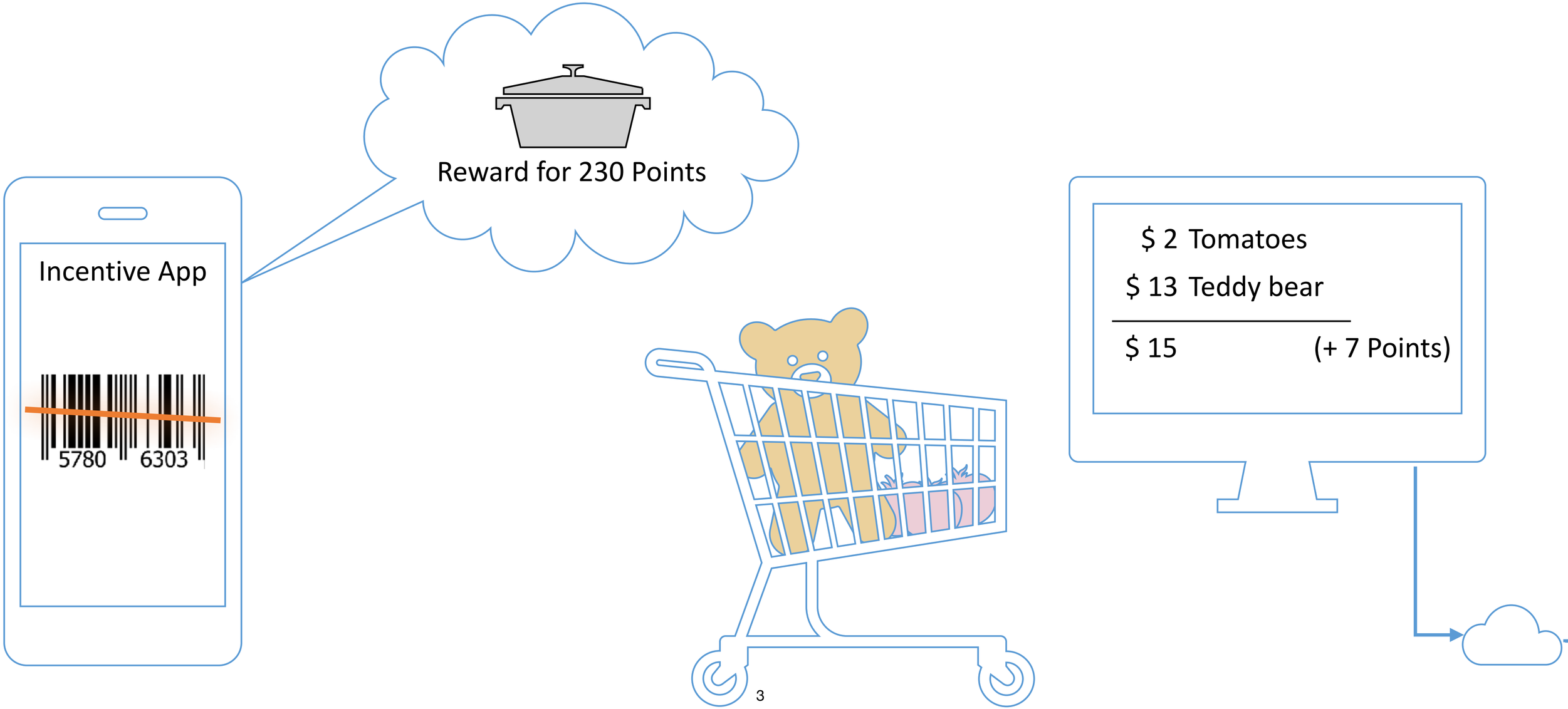
ON - THE - FLY COMPUTING

Johannes Blömer, Jan Bobolz, Paul Kramer, Patrick Schürmann, Fabian Eidens

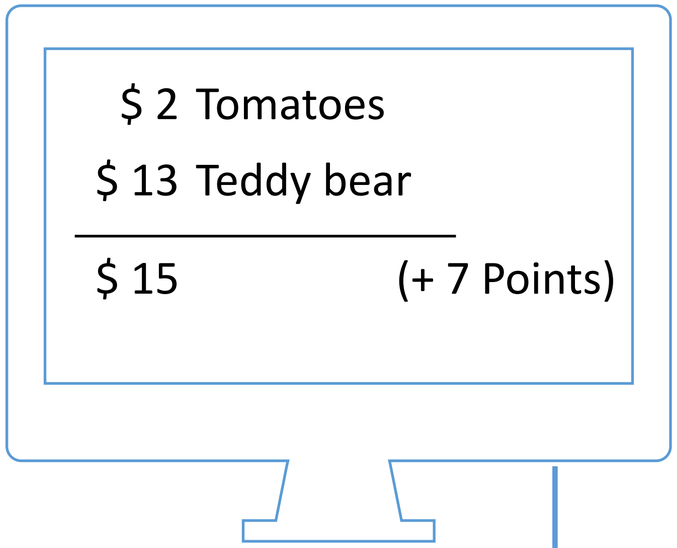
15.09.2022

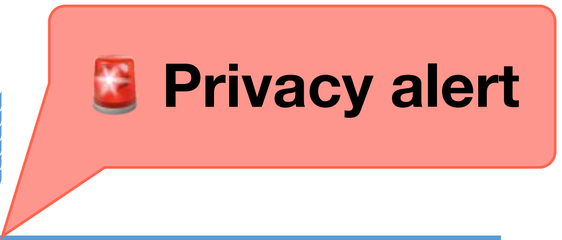
What are **incentive systems**?

Incentive Systems / Point Collection: In practice



Incentive Systems / Point Collection: In practice





user id	name	points	buying habits
…	…	…	…
5780 6303	Jimothy Halpert	~~200~~ 207	*Yesterday*: Pregnancy test *Today*: Tomatoes, teddy bear.
…	…	…	…

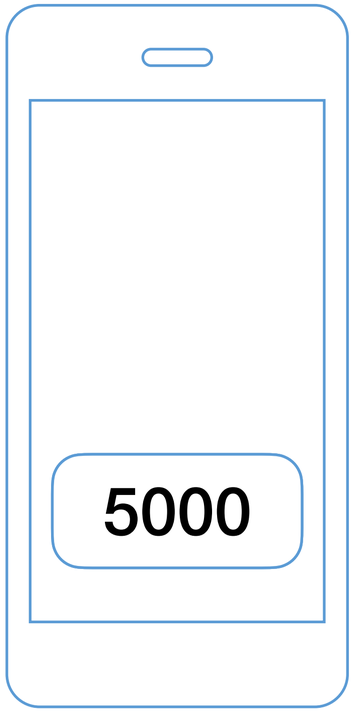
Rethinking the incentive system architecture for **privacy**

user id	name	points	buying habits
…	…	…	…
5780 6303	Jimothy Halpert	207	*Yesterday*: Pregnancy test *Today*: Tomatoes, teddy bear.
…	…	…	…

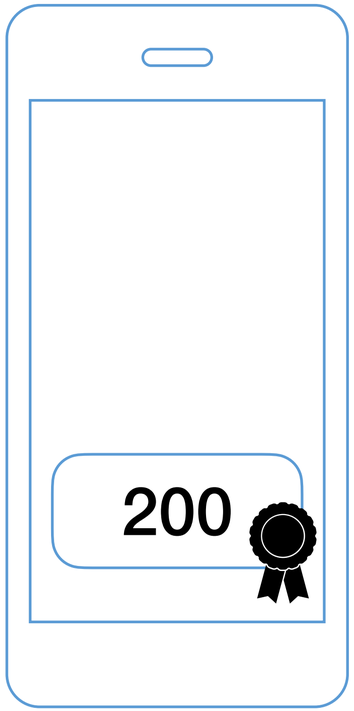
🙂 Privacy! Store does not get to see data. Cannot abuse, cannot leak.

🙃 Challenge! Database was convenient, need to rethink.

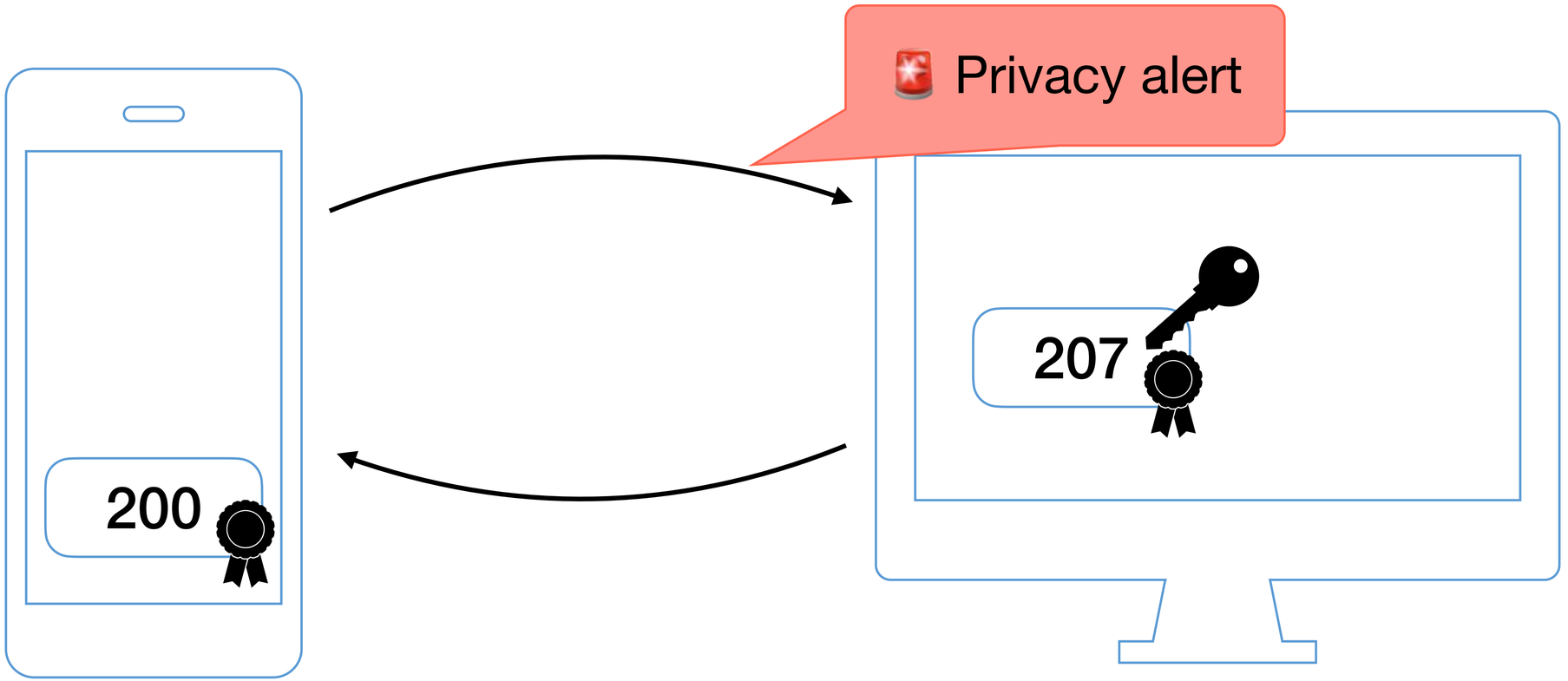
	🗃️ Central database (privacy ❌)	📱 Users store data (privacy ✅)
🪨 Users cannot illegally change data	Database does access control ✔️	User can just change point count



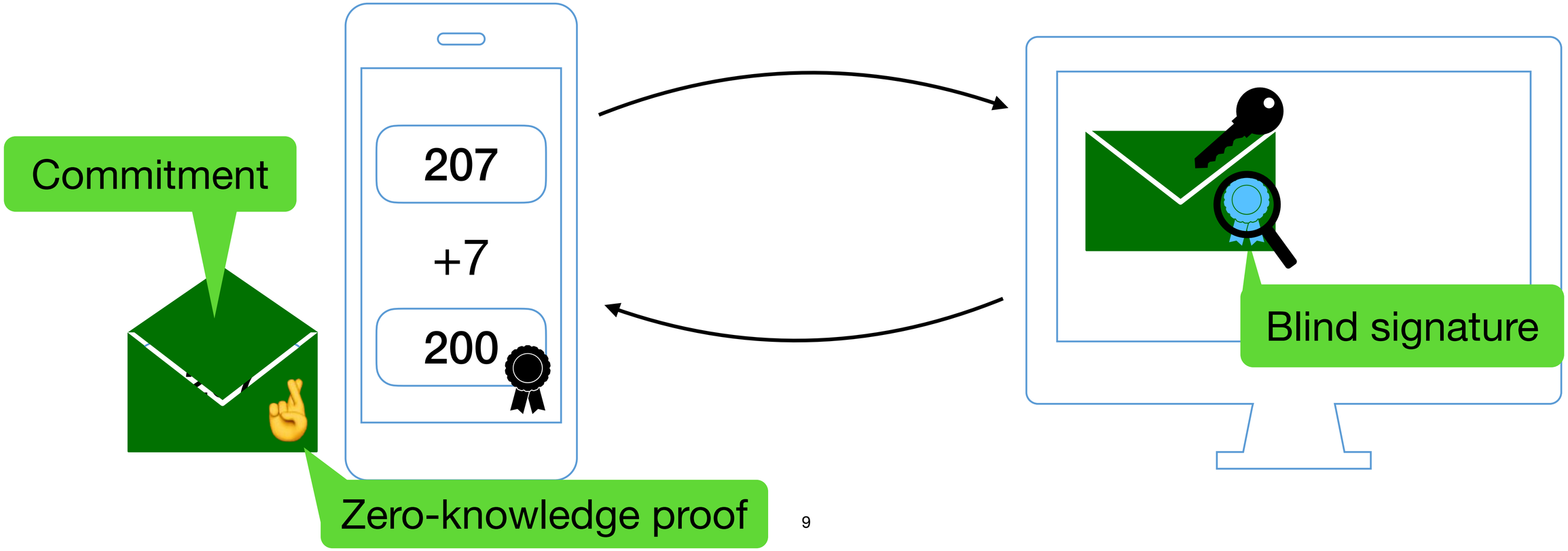
	🗃️ Central database (privacy ❌)	📱 Users store data (privacy ✅)
🪨 Users cannot illegally change data	Database does access control ✔️	Digital signature ✔️



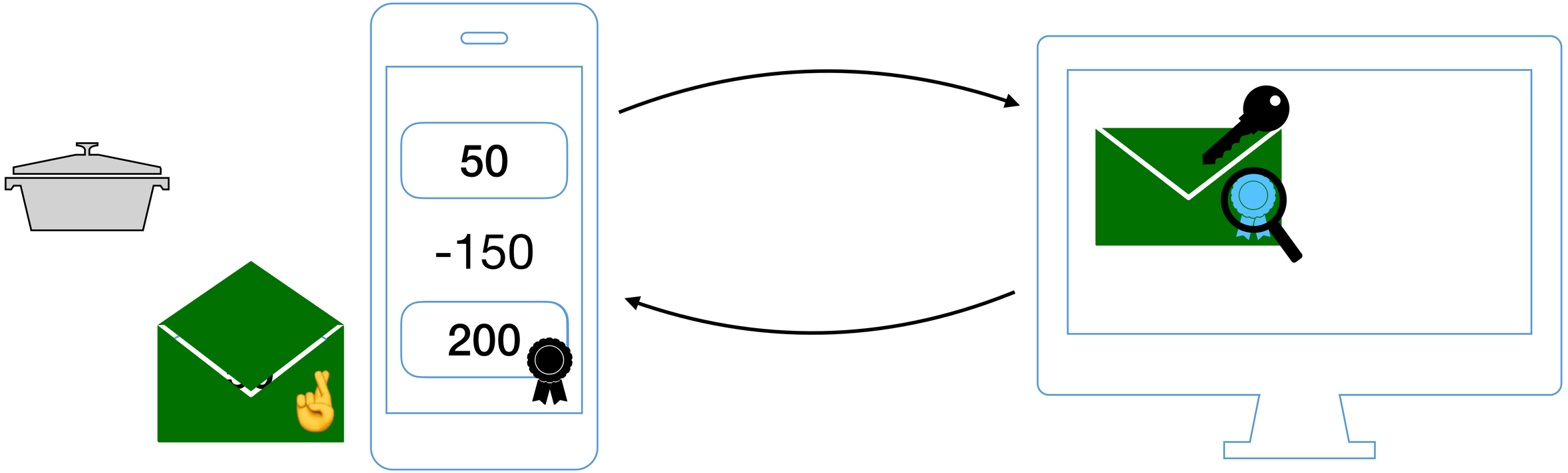
	🗃️ Central database (privacy ❌)	📱 Users store data (privacy ✅)
🪨 Users cannot illegally change data	Database does access control ✔️	Digital signature ✔️
✏️ Store can easily update data	`UPDATE tbl SET points = points + 7 WHERE user = 57806303` ✔️	How to do privacy-preserving update?



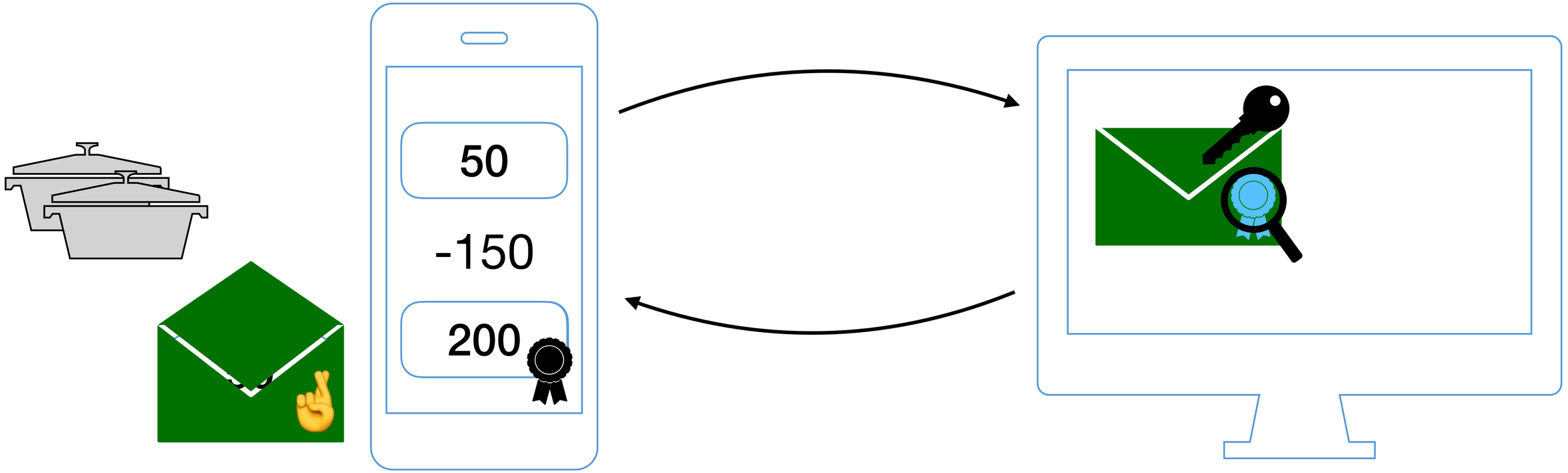
	🗃️ Central database (privacy ❌)	📱 Users store data (privacy ✅)
🪨 Users cannot illegally change data	Database does access control ✔️	Digital signature ✔️
✏️ Store can easily update data	`UPDATE tbl SET points = points + 7 WHERE user = 57806303` ✔️	Privacy-preserving update protocol ✔️



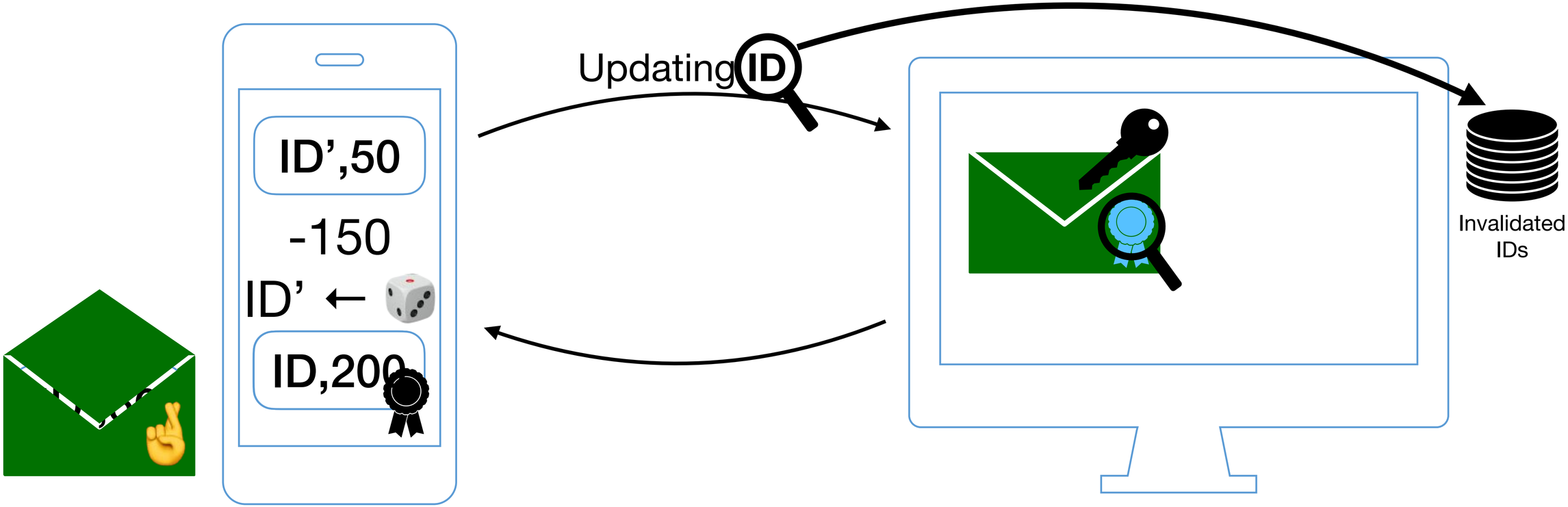
	🗃️ Central database (privacy ❌)	📱 Users store data (privacy ✅)
🪨 Users cannot illegally change data	Database does access control ✔️	Digital signature ✔️
✏️ Store can easily update data	`UPDATE tbl SET points = points + 7 WHERE user = 57806303` ✔️	Privacy-preserving update protocol ✔️
⚛️ Updates are read/write consistent	Database does ACID ✔️	User can keep using old data state



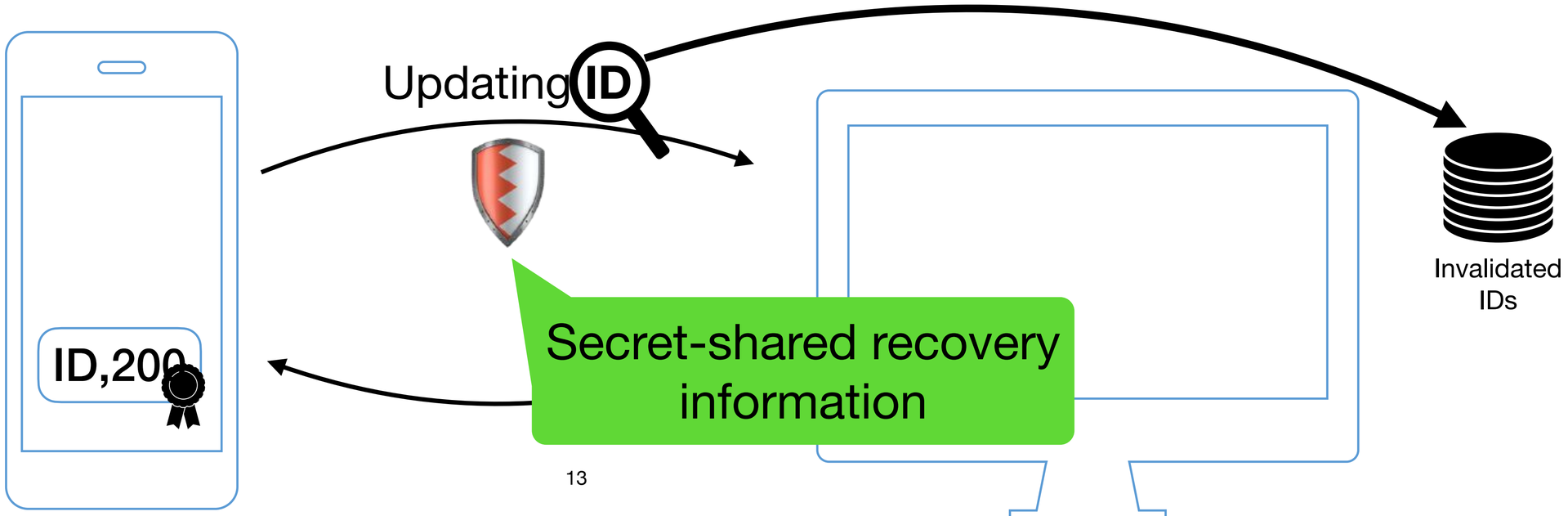
	🗃️ Central database (privacy ❌)	📱 Users store data (privacy ✅)
🪨 Users cannot illegally change data	Database does access control ✔️	Digital signature ✔️
✏️ Store can easily update data	`UPDATE tbl SET points = points + 7 WHERE user = 57806303` ✔️	Privacy-preserving update protocol ✔️
⚛️ Updates are read/write consistent	Database does ACID ✔️	User can keep using old data state

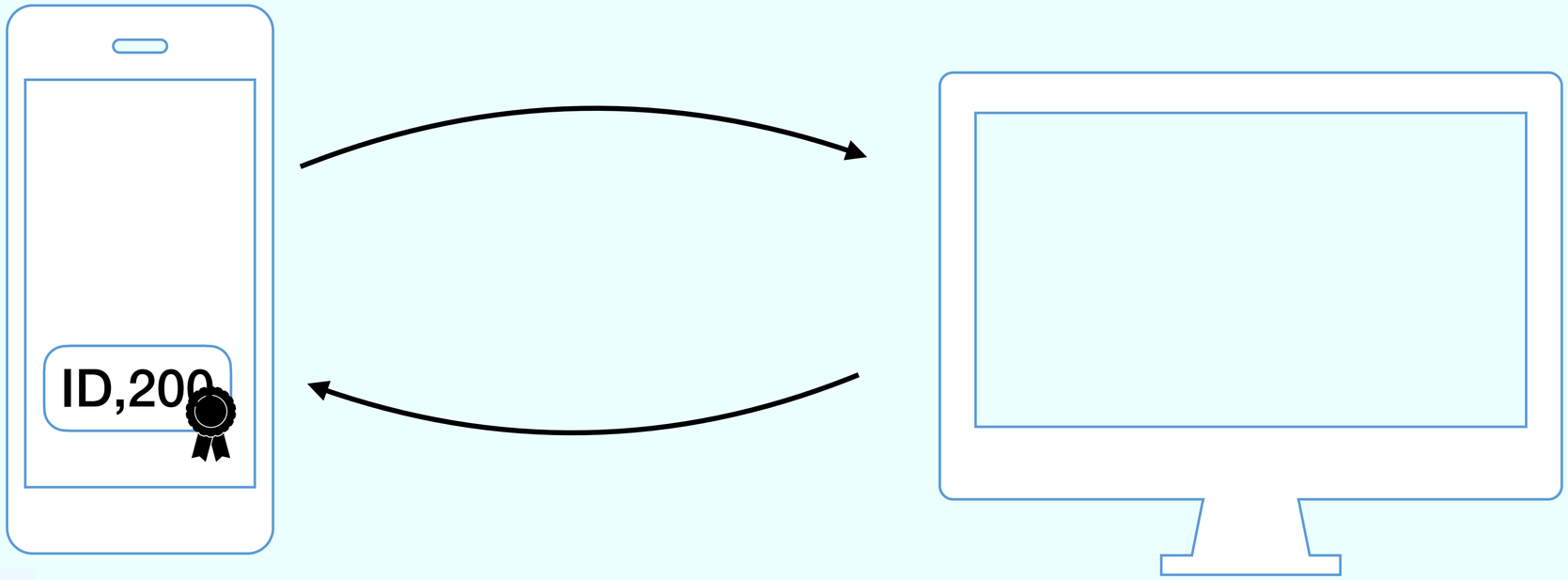


	🗃️ Central database (privacy ❌)	📱 Users store data (privacy ✅)
🪨 Users cannot illegally change data	Database does access control ✔	Digital signature ✔
✏️ Store can easily update data	`UPDATE tbl SET points = points + 7 WHERE user = 57806303` ✔	Privacy-preserving update protocol ✔
⚛️ Updates are read/write consistent	Database does ACID ✔	Data entry has unique ID, store can check if ID outdated ✔



	🗃️ Central database (privacy ❌)		📱 Users store data (privacy ✅)	
🪨 Users cannot illegally change data	Database does access control	✅	Digital signature	✅
✏️ Store can easily update data	`UPDATE tbl SET points = points + 7 WHERE user = 57806303`	✅	Privacy-preserving update protocol	✅
⚛️ Updates are read/write consistent	Database does ACID	✅	Data entry has unique ID, store can check if ID outdated	✅
🌍 Support for offline stores	No ability to check/change data	❌	Can be offline if you can *temporarily* tolerate old data	✅





The system in **action.**

13:00 LTE 100 %

Cryptimeleon Rewards

Nutella Promotion 2

Streak Promotion 1

VIP Promotion NONE

Dashboard Scan Basket

13:00 LTE 100 %

My Basket

	Price
2 x Nutella	4,78 €

Nutella Promotion
Get a free Nutella for 4 points!

Collect 2 points

Get a free Nutella for 4 points!
Nutella

Streak Promotion
Increase your streak

VIP Promotion
Collect 478 points

Total (2 Items): **4,78 €**

ShowPromotion Privacy Details

Checkout

Dashboard Scan Basket

Nutella Promotion
Collect 2 points

Collect 2 points

Get a free Nutell for 4 points!
Nutella

```
Store's view:
Choice: "Earn"
 score_new = score_old + 2
Data only you know:
 score_old = 2 → score_new = 4
```

```
 ├── score_old + 2 ≥ 4
 └── score_new = score_old + 2 - 4
Data only you know:
 score_old = 2 → score_new = 2 - 4 = 0
```

13:00 LTE 100 %

Cryptimeleon Rewards

Nutella Promotion 2

Streak Promotion 1

VIP Promotion NONE

Dashboard Scan Basket

13:00 LTE 100 %

My Basket

	Price
2 x Nutella	4,78 €

Nutella Promotion
Get a free Nutella for 4 points!

Collect 2 points

Get a free Nutella for 4 points!
Nutella

Streak Promotion
Increase your streak

VIP Promotion
Collect 478 points

Total (2 Items): **4,78 €**

ShowPromotion Privacy Details

Checkout

Dashboard Scan Basket

Streak Promotion
Increase your streak

```
Store's view:
Choice: "Increase or Reset Streak"
Update Tree:
 AND
 ├─ new_lastdate = 2022-08-25
 └─ OR
    ├─ new_streak = 1
    └─ AND
       ├─ new_streak = old_streak + 1
       └─ 2022-08-25 - old_lastdate ≤ 7 days
Data only you know:
 lastdate: 2022-08-25 → 2022-08-25
 streak: 1 → 2
```

13:00 LTE 100 %

Cryptimeleon Rewards

Nutella Promotion 2

Streak Promotion 1

VIP Promotion NONE

Dashboard Scan Basket

13:00 LTE 100 %

My Basket

Price

2 x Nutella 4,78 €

Nutella Promotion
Get a free Nutella for 4 points!

Collect 2 points

Get a free Nutella for 4 points!
Nutella

Streak Promotion
Increase your streak

VIP Promotion
Collect 478 points

Total (2 Items): **4,78 €**

ShowPromotion Privacy Details

Checkout

Dashboard Scan Basket

VIP Promotion
Collect 478 points

```
Store's view:
Choice: "Earn"
 score_new = score_old + 478
Data only you know:
 vip_level = NONE
 score_old = 1056 → score_new = 1534
```

Cryptimeleon

- Library for prototyping privacy construction.
- Pairings, ZK proofs, …

https://cryptimeleon.org

Cryptimeleon protocols

$$\begin{aligned}
&\mathsf{ZKP}[(usk, v, z, z^*, t, t^*, u^*, esk, [esk^*_{\mathrm{usr}}]_\rho, (r_i)_{i\in[\rho]}, esk^*_{\mathrm{usr}}, dsrnd_0, dsrnd_0^*,\\
&dsrnd_1, dsrnd_1^*) : c_0 = usk\cdot\gamma + dsrnd_0 \ \wedge\ c_1 = esk\cdot\gamma + dsrnd_1\\
&\wedge\ dsid = w^{esk} \wedge\ C = (h_1^{usk}\cdot h_2^{esk}\cdot h_3^{dsrnd_0}\cdot h_4^{dsrnd_1}\cdot h_5^{v}\cdot h_6^{z}\cdot h_7^{t}, g_1)\\
&\wedge\ C^{(\mathrm{pre})} = ((h_1^{usk}\cdot h_2^{esk^*_{\mathrm{usr}}}\cdot h_3^{dsrnd_0^*}\cdot h_4^{dsrnd_1^*}\cdot h_5^{v-k}\cdot h_6^{z^*}\cdot h_7^{t^*})^{u^*}, g_1^{u^*})\\
&\wedge\ v \geq k \wedge\ ctrace = (w^{r_i}, (w^{r_i})^{esk}\cdot w^{esk^*_{\mathrm{usr},i}})_{i\in[\rho]}\\
&\wedge\ esk^* = \textstyle\sum_{i=0}^{\rho-1} esk^*_{\mathrm{usr},i}\cdot base^i \ \wedge [\textstyle\bigwedge_{i=0}^{\rho-1} esk^*_{\mathrm{usr},i} < base]
\end{aligned}$$

```
var eskDecVarVector = ExponentExpressionVector.generate(i -> builder.addZnVariable("eskStarUserDec_" + i, zn), pp.getNumEskDigits());

for (int i = 0; i < pp.getNumEskDigits(); i++) {
    builder.addSubprotocol("eskDigitSetMembership" + i,
        new SetMembershipFragment(pp.getEskBaseSetMembershipPp(), eskDecVarVector.get(i))
    );
}
```

Privacy-by-design is **feasible**.
We have the technology.

user id	name	points	buying habits
…	…	…	…
5780 6303	Jimothy Halpert	207	*Yesterday*: Pregnancy test *Today*: Tomatoes, teddy bear.
…	…	…	…