JENS NEUHALFEN

User	Salary	MAC*
Alice		0x4711...
Eve		0xabcd...
...	...	...

10,000 €

2,718 €

DATA INTEGRITY & ASSOCIATION

GOOD CRYPTOGRAPHY

THE CHECKSUMS DON'T MATCH, PROMOTION IS DECLINED

0X123456... ✓

3,141€

* Checksum with a secret: hmac, AEAD, public key signatures

Problem: Sensitive data can be manipulated.

Solution: Use cryptographic checksums with a secret.

DATA INTEGRITY & ASSOCIATION

0X123456... ✓

Problem: Sensitive data can be manipulated.

Solution: Use cryptographic checksums with a secret.

User	Salary	MAC*
Alice	3,141€	0x4711...
Eve	10,000 €	0xabcd...

THE CHECKSUMS DON'T MATCH, PROMOTION IS DECLINED

* Checksum with a secret: hmac, AEAD, public key signatures

DATA INTEGRITY & ASSOCIATION

0X123456... ✓

Problem: Protected data can be "replayed".

User	Salary	MAC*
Alice	3,141€	0x4711...
Eve	2,718 €	0xabcd...
...	...	...