



JENS NEUHALFEN

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

10,000 €

2,718 €

DATA INTEGRITY & ASSOCIATION

GOOD CRYPTOGRAPHY

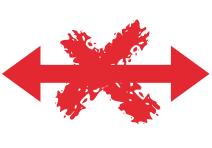




THE CHECKSUMS DON'T MATCH, PROMOTION IS DECLINED



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.

MAC* User Salary Alice 0x4711... 3,141€ Eve 10,000 € THE CHECKSUMS DUN I MAICH, PRUMUTIUN 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
• • •	• • •	• • •