



JENS NEUHALFEN

User Salary MAC*

| Alice | 0xabcd |
|-------|--------|
| Eve | 0x9876 |
| | |

2,718€

3,141€

3,141€

GOOD CRYPTOGRAPHY

DATA INTEGRITY & ASSOCIATION





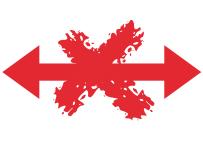
THE CHECKSUMS DON'T MATCH, PROMOTION IS DECLINED



Problem: Protected data can be "replayed". Solution: Cryptographically bind data to context.

* including the username in the hash/hmac

0xabcd...





DATA INTEGRITY & ASSOCIATION

0X123456...

Problem: Protected data can be "replayed".

Solution: Cryptographically bind data to context.

MAC* User Salary 3,141€ Alice 0xabcd... 3,141€ Eve THE CHECKSUMS DUN I MAICH, PRUMUTIUN IS DECLINED

* including the username in the hash/hmac

DATA INTEGRITY & ASSOCIATION

OX123456...

Problem: Protected data can be "replayed".

Solution: Cryptographically bind data to context.

Password Hash * User 0X123456... Alice • • • OXABCDEF... Eve * including the username in the hash/hmac