



JENS NEUHALFEN

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



2,718 €

DATA INTEGRITY & ASSOCIATION

SLEEP BETTER WITH CONTENT ENCRYPTION

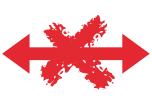




THE CHECKSUMS DON'T MATCH, PROMOTION IS DECLINED



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: Protected data can be "replayed".

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

DATA INTEGRITY & ASSOCIATION

OX123456...

Problem: Sensitive data can be manipulated.

Solution: Use cryptographic checksums with a secret.

Salary User MAC* Alice 0x4711... 3,141€ 0xabcd... 10,000 € Eve THE CHECKSUMS DON'T MATCH, PROMOTION IS DECLINED

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