JENS NEUHALFEN

User	Salary	MAC*
Alice		0xabcd...
Eve		0x9876...
...	...	...

2,718€

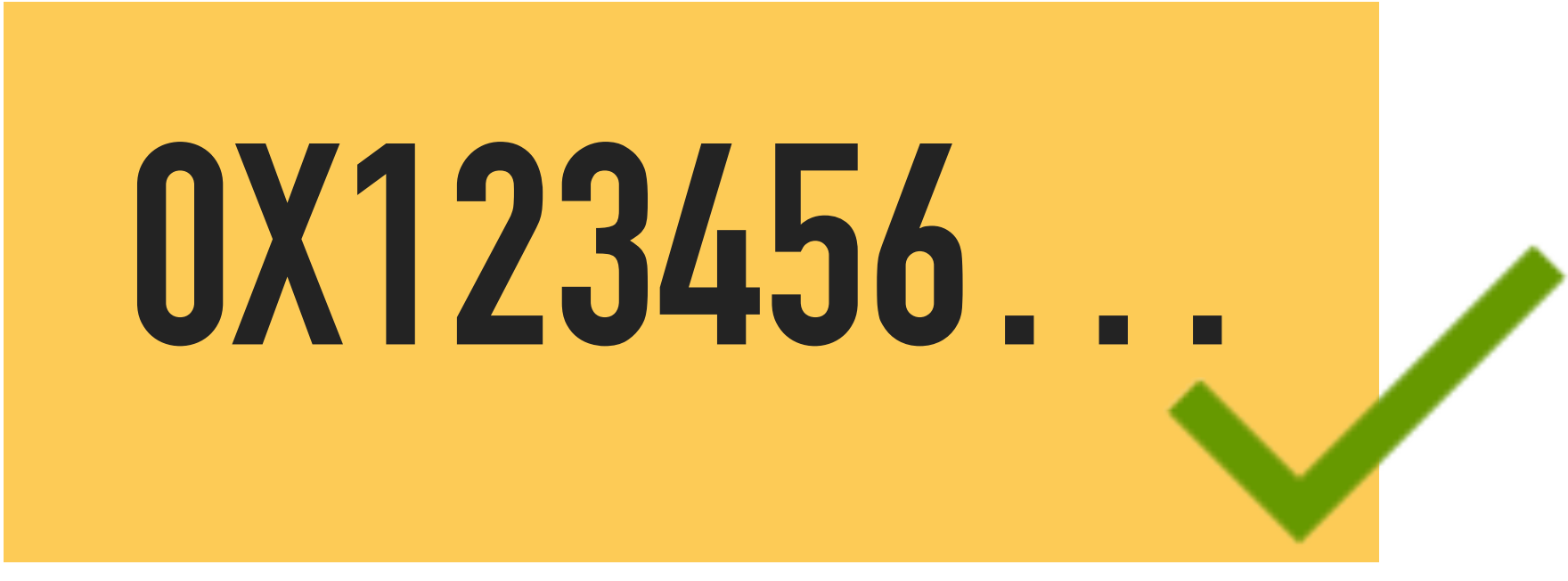
3,141€

3,141€

GOOD CRYPTOGRAPHY

DATA INTEGRITY & ASSOCIATION

THE CHECKSUMS DON'T MATCH, PROMOTION IS DECLINED


0X123456...

Problem: Protected data can be “replayed”.

Solution: Cryptographically bind data to context.

* including the username in the hash/hmac

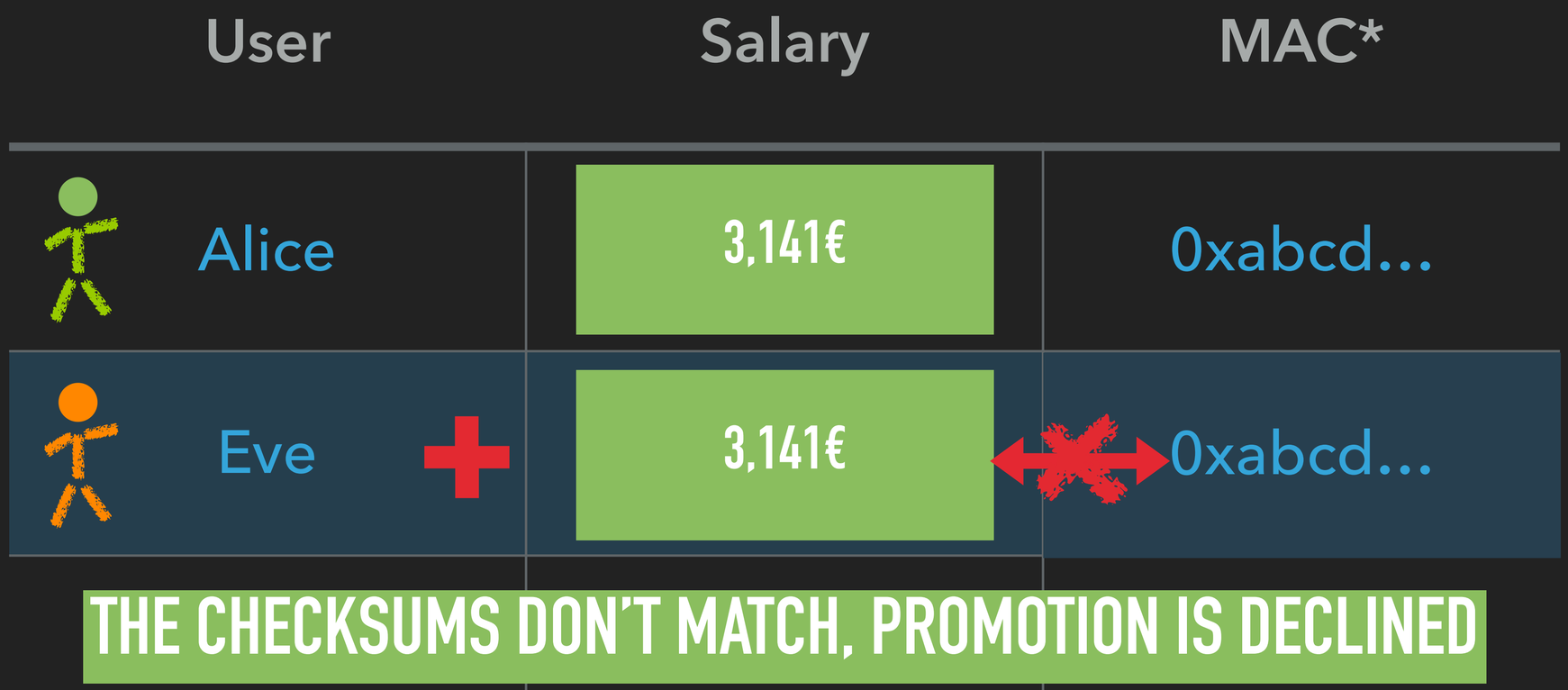
0xabcd...

DATA INTEGRITY & ASSOCIATION

0X123456…

Problem: Protected data can be “replayed”.

Solution: Cryptographically bind data to context.



* including the username in the hash/hmac

DATA INTEGRITY & ASSOCIATION

0X123456…

Problem: Protected data can be “replayed”.

Solution: Cryptographically bind data to context.

User	Password Hash *	…
Alice	0X123456…	…
Eve	0XABCDEF…	…
…	…	…

* including the username in the hash/hmac