Ensuring integrity with an HMAC

H_k("[request]debit=50")

H_k("[response]950")

H_k("[response]950")

Н, К

[request]debit=50
f89a73aa27f3ea6...

[response]950
ee5a49c19fc252f...

H_k("[request]debit=50")

Ensuring integrity with an HMAC

H, K

H, K

H_k("[request]debit=50")

[request]debit=50
f89a73aa27f3ea6...

H_k("[request]debit=50")

H_k("[response]950")

[response]950
ee5a49c19fc252f...

H_k("[response]950")

Security mechanisms

	Encryption	MAC	Authenticated Encryption
Confidentiality	✓	✗	✓
Integrity	✗	✓	✓