RUHR-UNIVERSITÄT BOCHUM

RUB

How to authenticate mobile devices in a web environment

- The SIM-ID approach -

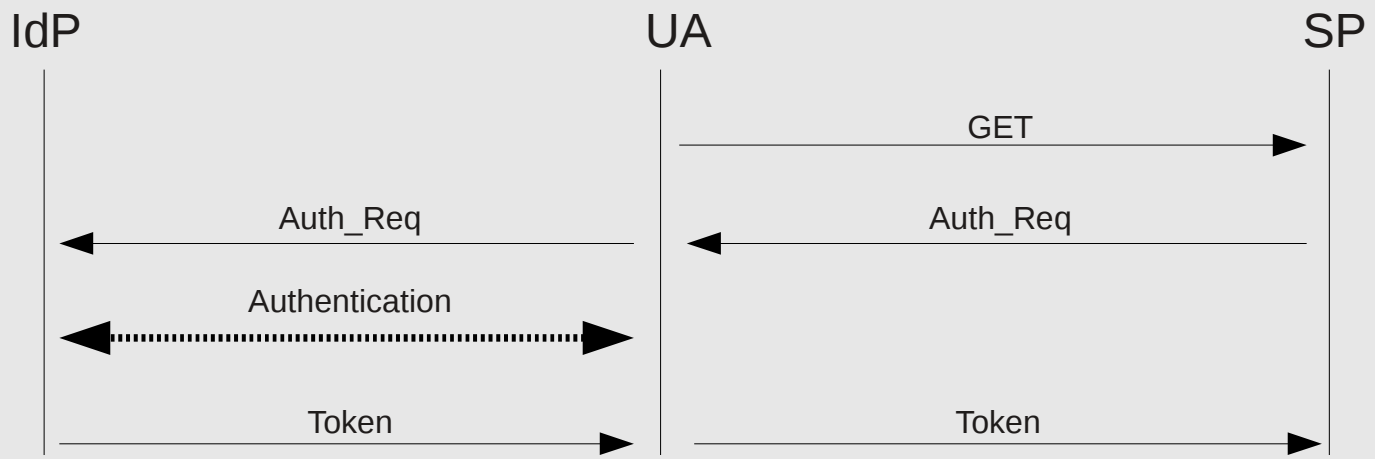
11.09.2013

Horst Görtz Institute for IT-Security
Chair for Network and Data Security

Authentication of Mobile Devices

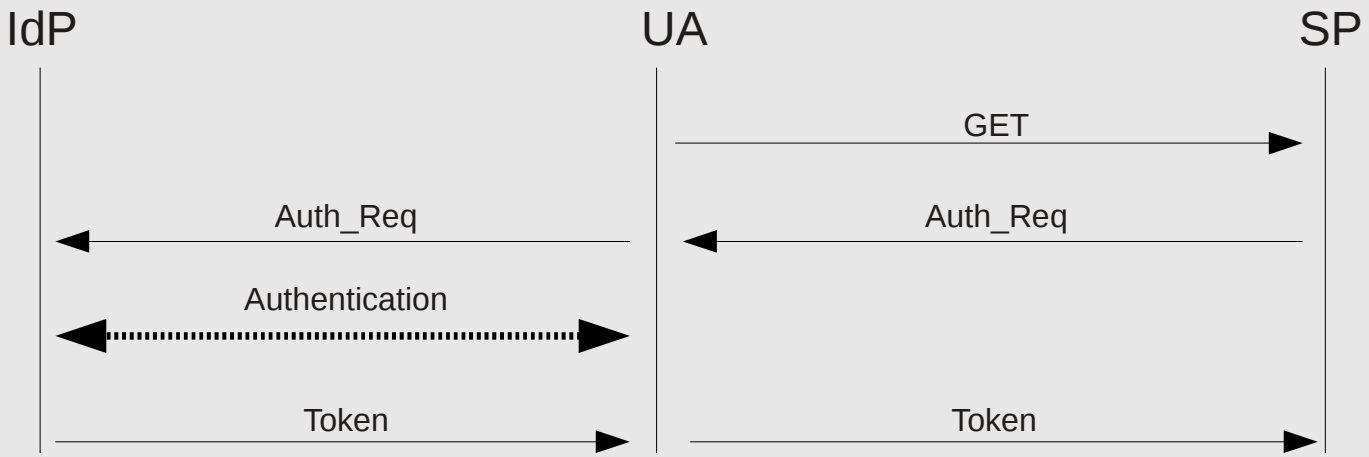
- Most basic form of authentication: username/password
- Passwords can be stolen (e.g. by malware)
- Strong authentication necessary
- NFC etc. not yet widespread

Single Sign-On

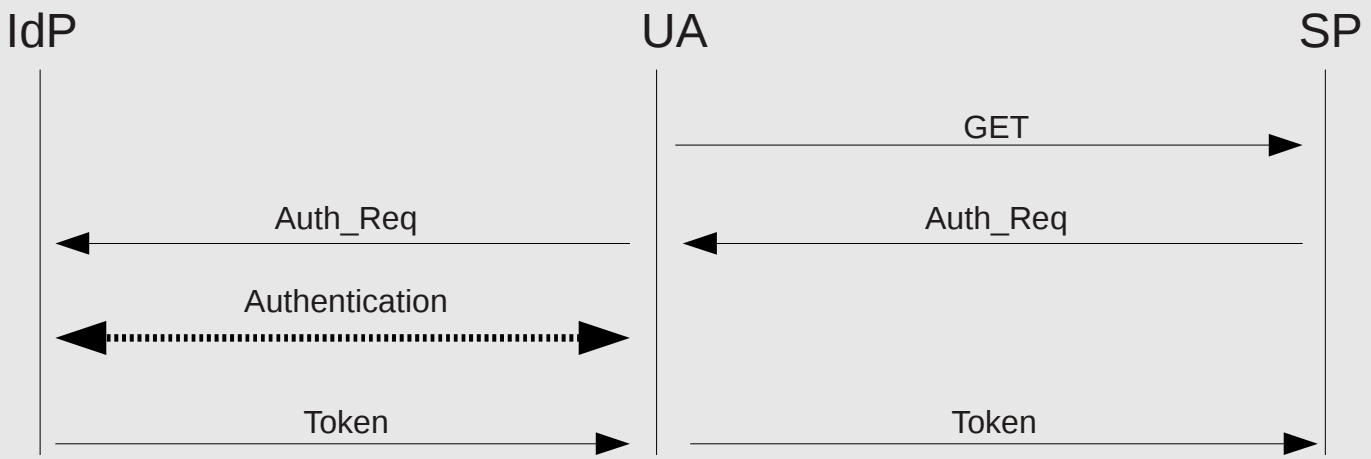


Single Sign-On with GAA and LAIFF

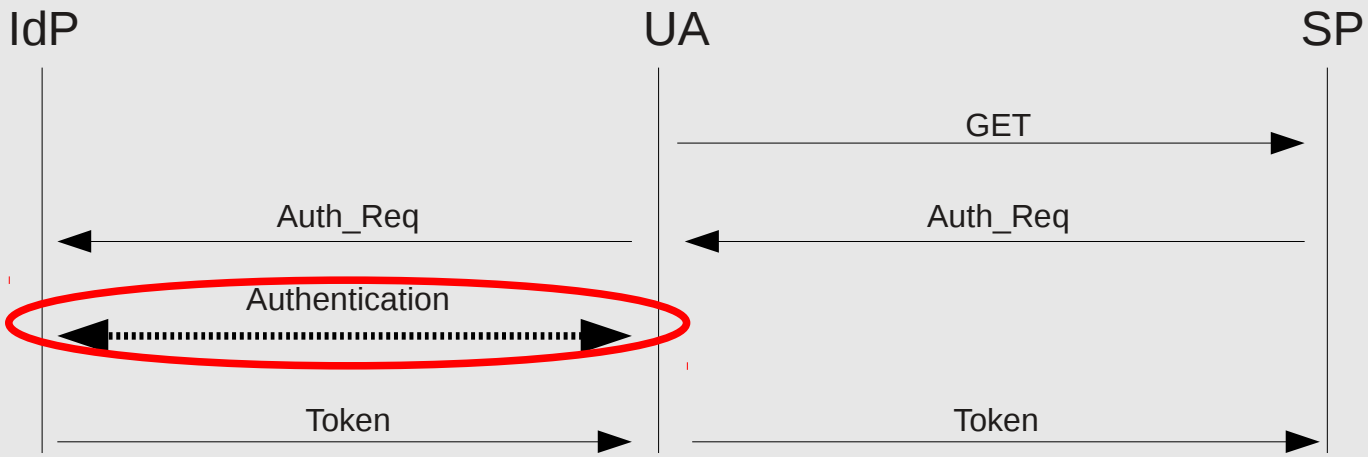
Mobile Service Provider: Mobile Device:



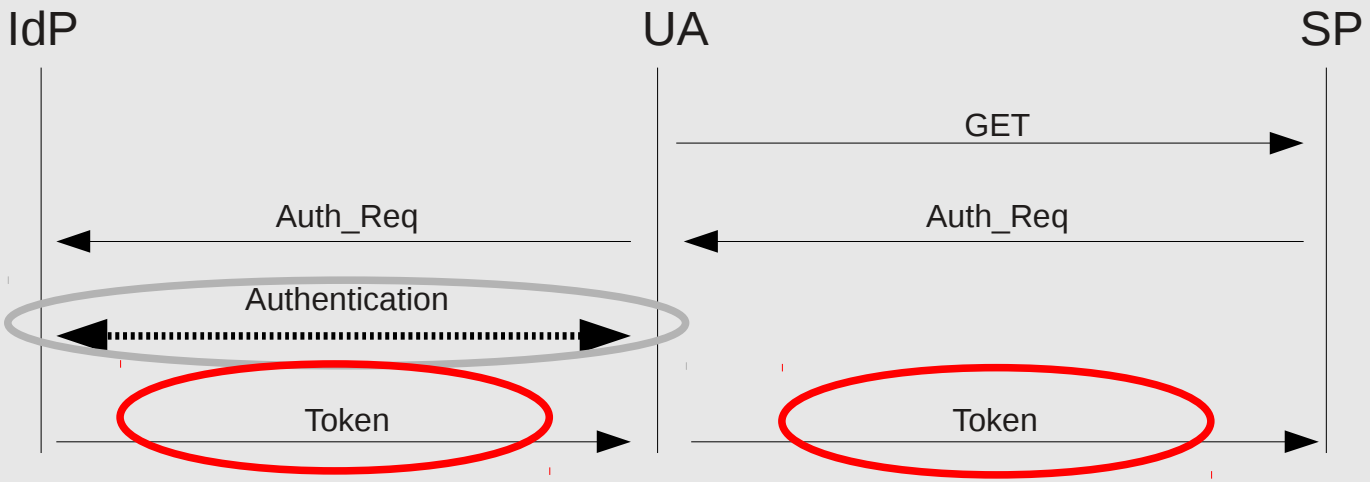
Single Sign-On – Attack Surfaces



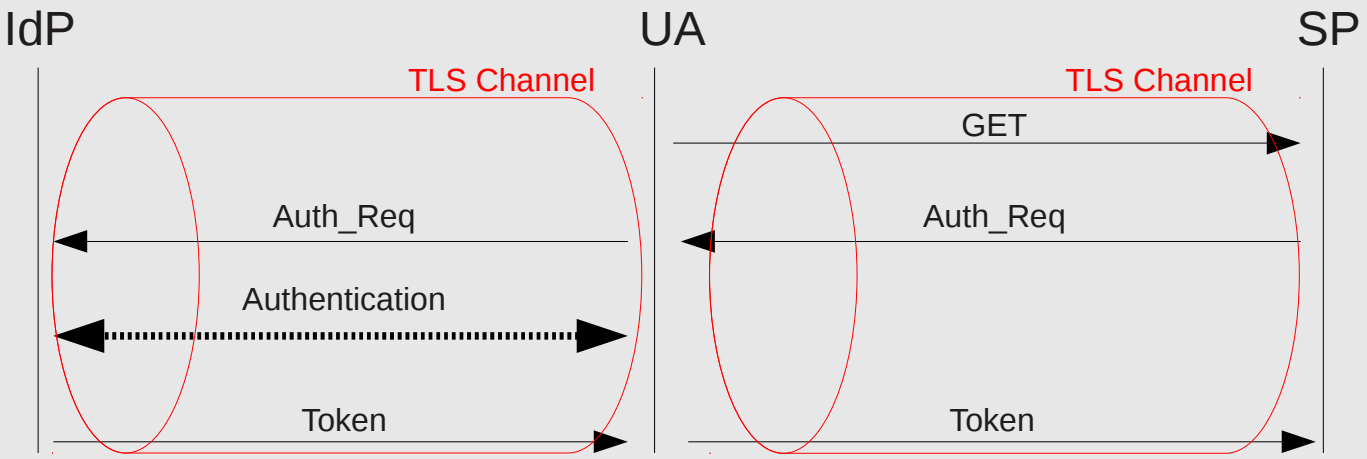
Single Sign-On – Attack Surfaces



Single Sign-On – Attack Surfaces



Solution: Transport Layer Security



Solution: Transport Layer Security?

- Bleichenbacher Million Question Attack
- Timing Attacks
- B.E.A.S.T. / C.R.I.M.E.
- Hash Collisions
- DigiNotar
- […] *(see Meyer and Schwenk, SoK: Lessons Learned from SSL/TLS Attacks)*

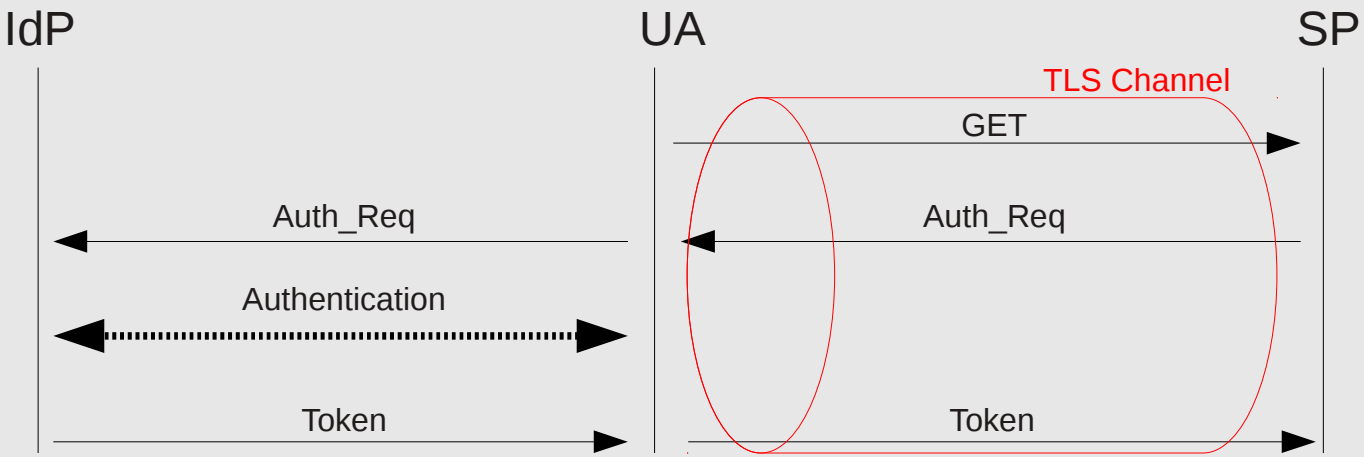
Solution: Transport Layer Security?

- Bleichenbacher Million Question Attack
- Timing Attacks
- B.E.A.S.T. / C.R.I.M.E.
- Hash Collisions
- DigiNotar
- […] *(see Meyer and Schwenk, SoK: Lessons Learned from SSL/TLS Attacks)*

Also:

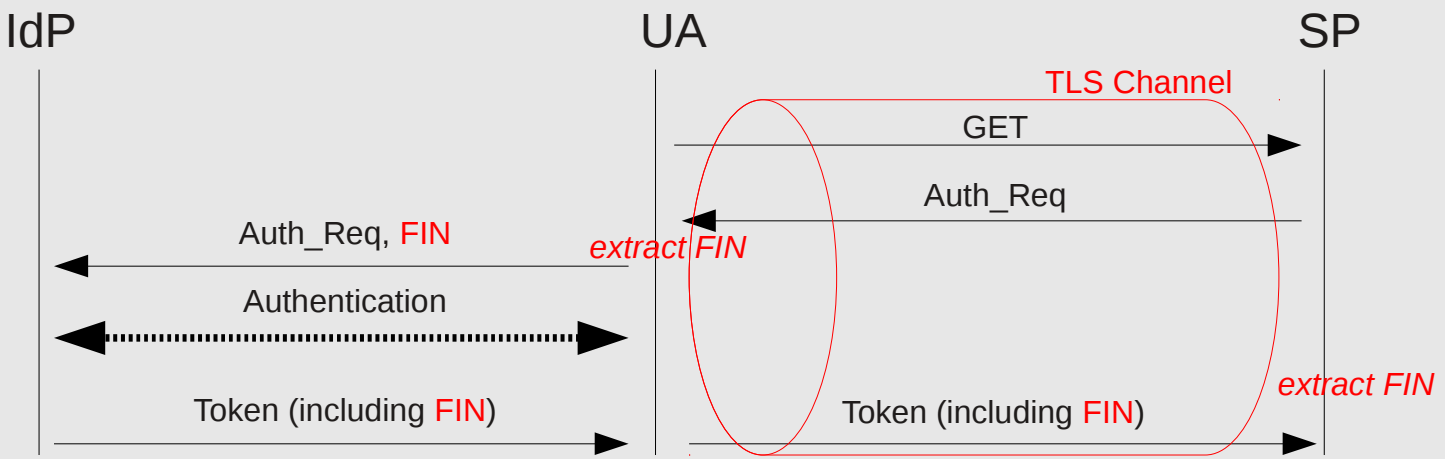
- Cross Site Scripting
- Clickjacking

Remedy: Cryptographic Bindings (RFC 5929)



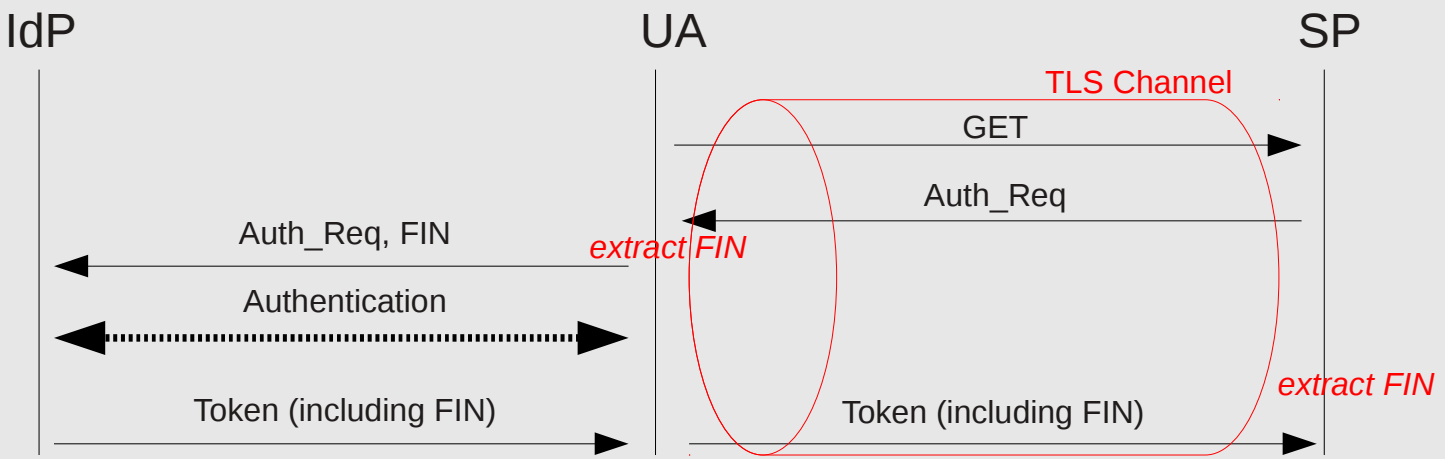
- Here: *tls-unique* channel binding

Remedy: Cryptographic Bindings (RFC 5929)



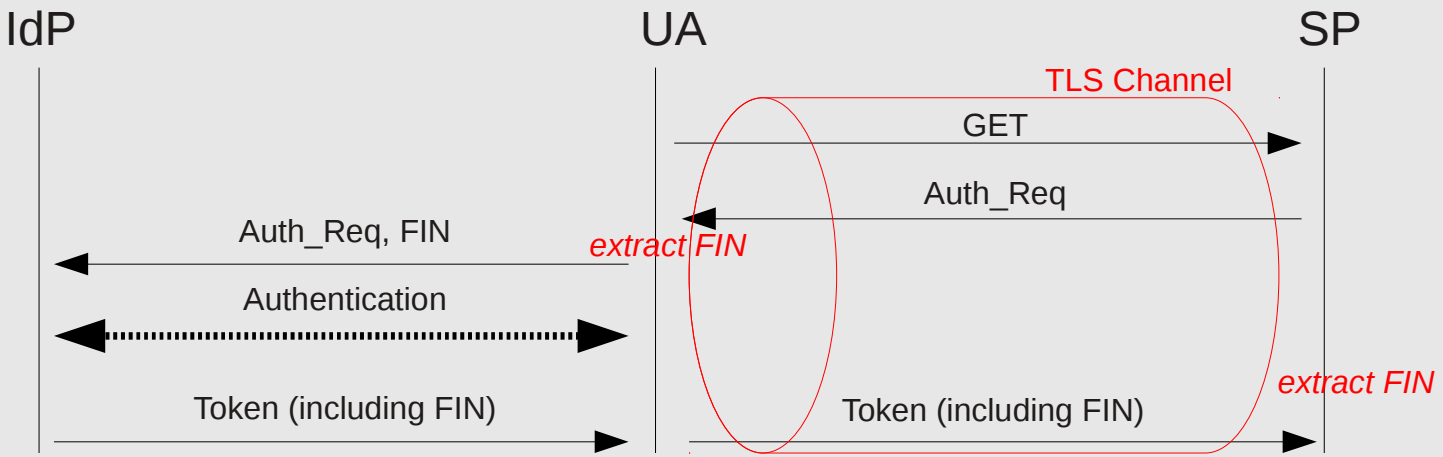
- Here: *tls-unique* channel binding

Remedy: Cryptographic Bindings (RFC 5929)



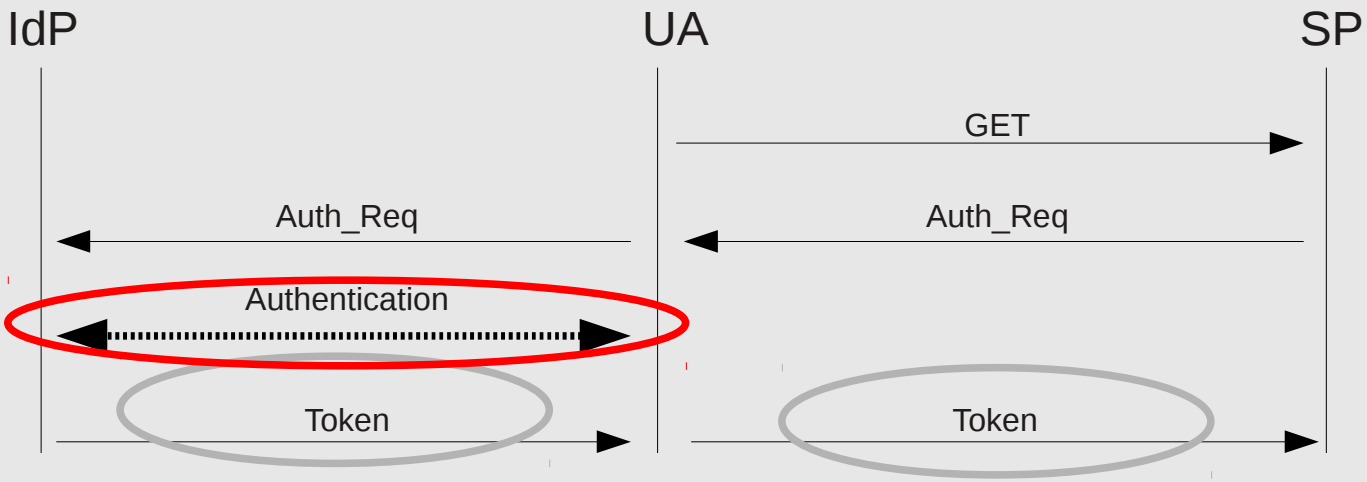
- Here: *tls-unique* channel binding
- FIN: Hash value uniquely identifying a specific TLS channel

Remedy: Cryptographic Bindings (RFC 5929)

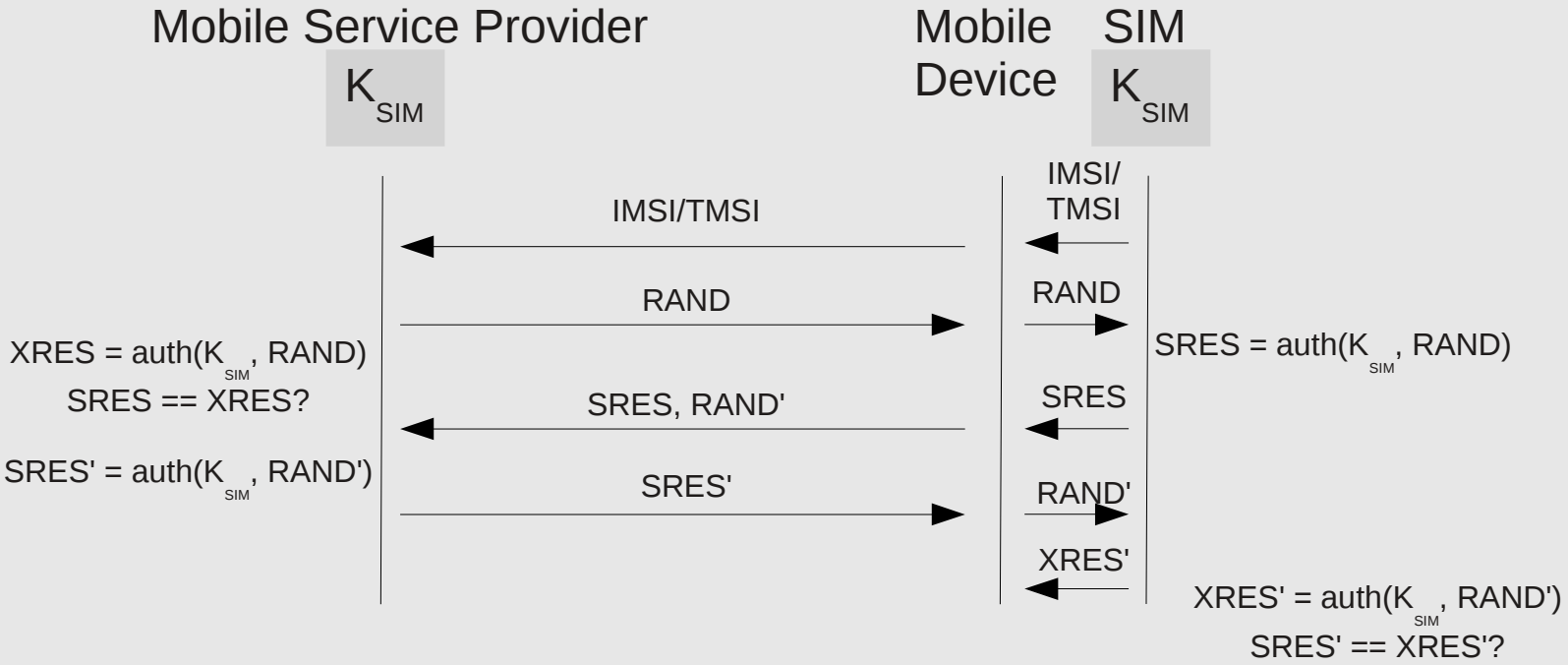


- Here: *tls-unique* channel binding
- FIN: Hash value uniquely identifying a specific TLS channel
- Token bound to that specific TLS channel

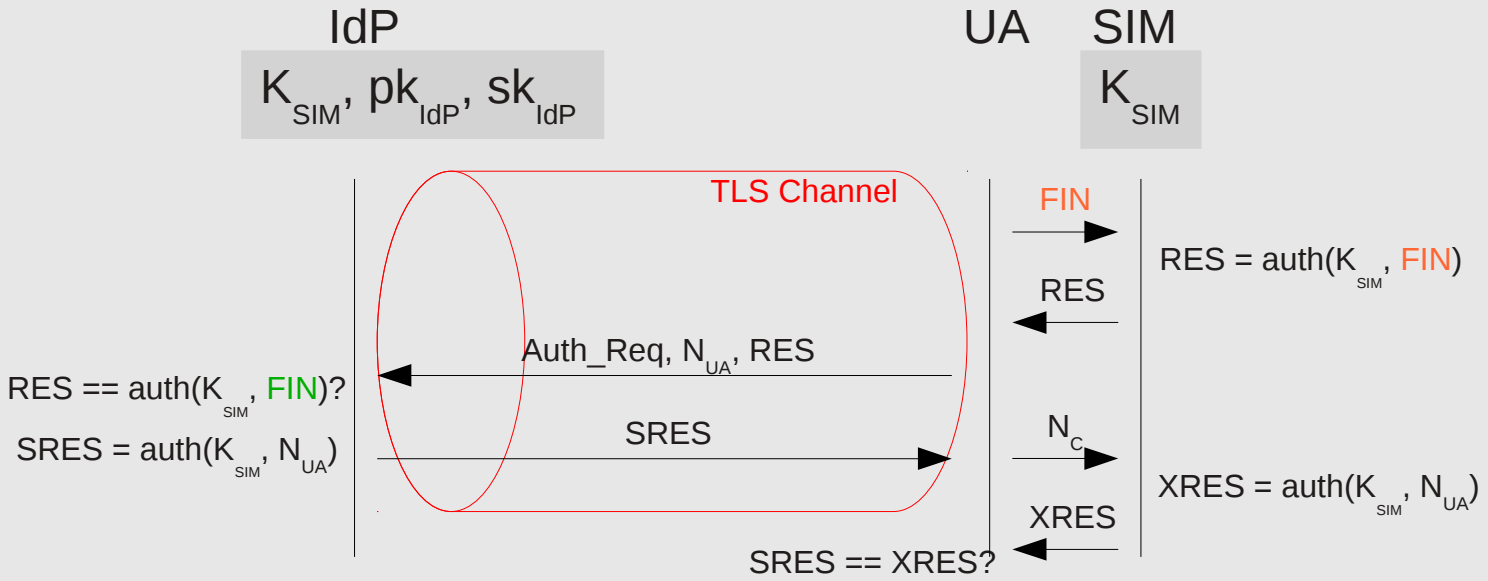
Securing Authentication

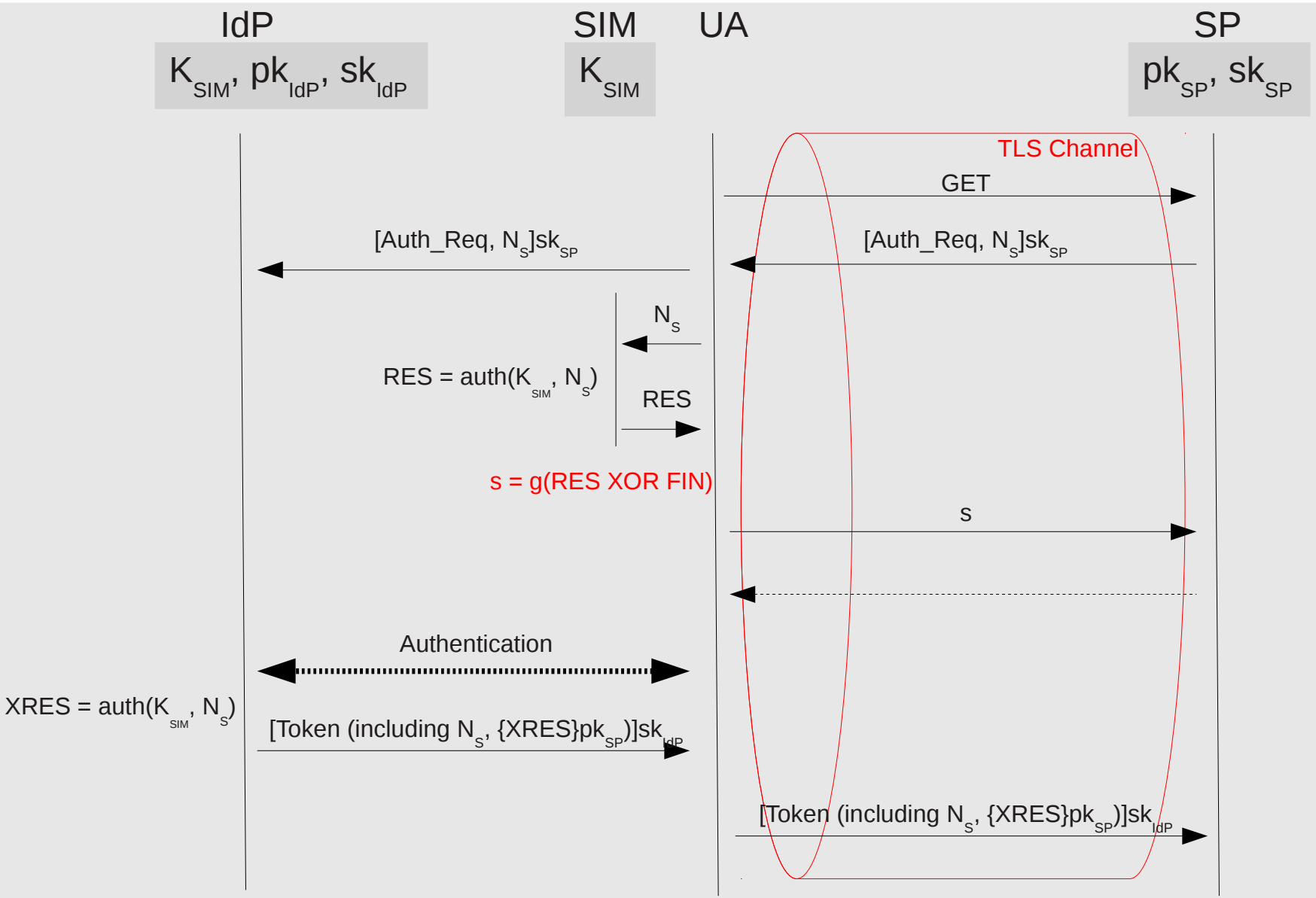


UMTS Authentication



Authentication With Secure Binding




IdP
K_{SIM}, pk_{IdP}, sk_{IdP}
SIM
K_{SIM}
UA
SP
pk_{SP}, sk_{SP}
TLS Channel
GET
[Auth_Req, N_S]sk_{SP}
[Auth_Req, N_S]sk_{SP}
N_S
RES = auth(K_{SIM}, N_S)
RES
s = g(RES XOR FIN)
s
Authentication
XRES = auth(K_{SIM}, N_S)
[Token (including N_S, {XRES}pk_{SP})]sk_{IdP}
[Token (including N_S, {XRES}pk_{SP})]sk_{IdP}
s == g(XRES XOR FIN)?

Conclusion

- Authentication of mobile device against Service Provider
- No credentials can be stolen
- Stolen token cannot be used by attacker

- Only Mobile Service Provider can function as IdP (cannot delegate)
- Malware on the device can still log in to SP

Thank you very much!

- Any questions?

Florian Feldmann
florian.feldmann@rub.de
http://www.nds.rub.de