

draft-rieckers-eappparameterextension-00

# Problems with certificate checking in EAP-TLS

- ▶ certificate checks on supplicants known to be faulty
- ▶ Insecure defaults
  - ▶ disabled by default in Android (at least <7.0)
  - ▶ Current Androids: “Use system certificates” with “domain” input
  - ▶ User questioning on Windows/Mac OS/iOS
- ▶ EAP-TLS specification lacks a specific method to determine certificate validity for use in EAP-TLS
- ▶ supplicants must be able to determine validity for the intended use with information only defined by communication context.

## Suggested solution

- ▶ New Certificate extension
  - ▶ explicitly define a valid realm
  - ▶ Realm implicitly known from username
  - ▶ validatable by CAs if realm is a DNS name

## Other possible solutions

- ▶ RFC 7585 SubjectAltName:otherName:NAIRealm
  - ▶ Specified to help with roaming/federation connections
- ▶ Specific domain prefix in SubjectAltName:dnsName or even CN
  - ▶ e.g. eap-tls.uni-bremen.de for uni-bremen.de

## Feedback received, further work

- ▶ possibly reuse OID for RFC7585  
SubjectAltName:otherName:NAIRealm
- ▶ Adding specific ExtendedKeyUsage for EAP-TLS Server Authentication

Thoughts?