EAP-TLS: Moving beyond usernames and passwords in eduroam?

Stefan Paetow, Federated Roaming Technical Specialist, Jisc

Networkshop

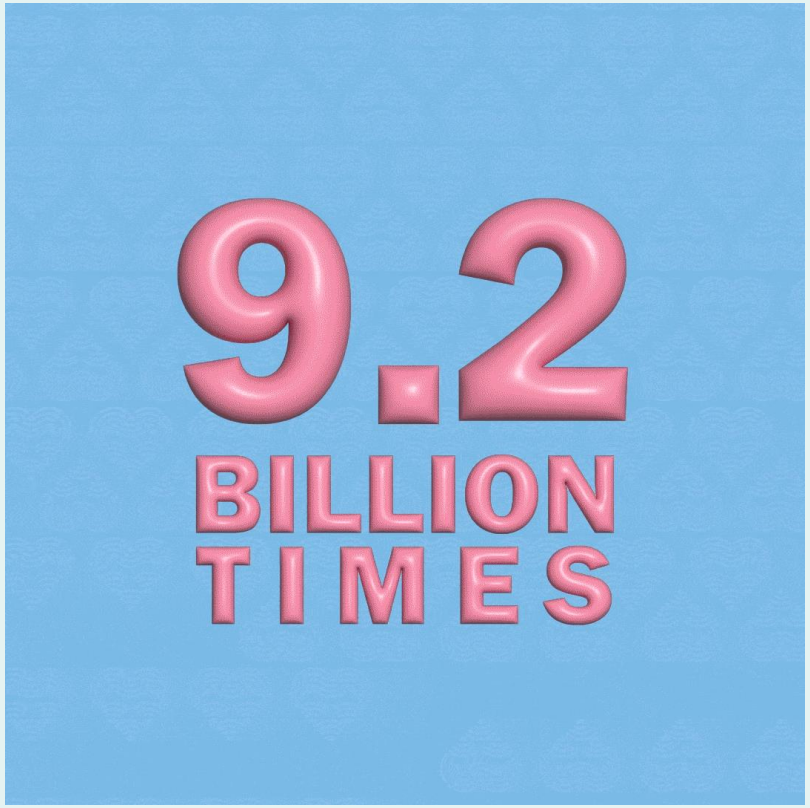
_2026

First – Happy birthday eduroam(UK)

Happy birthday eduroam(UK)

20 years of connecting UK R&E under the ‘eduroam’ name

- In 2025, eduroam world-wide hit 9.2 billion authentications
  - New record!
- UK is 20% of that!
  - 1,795,734,309 auths
- What does this mean?



- WE HAVE STICKERS!

Now – Let’s get into the meat and bones

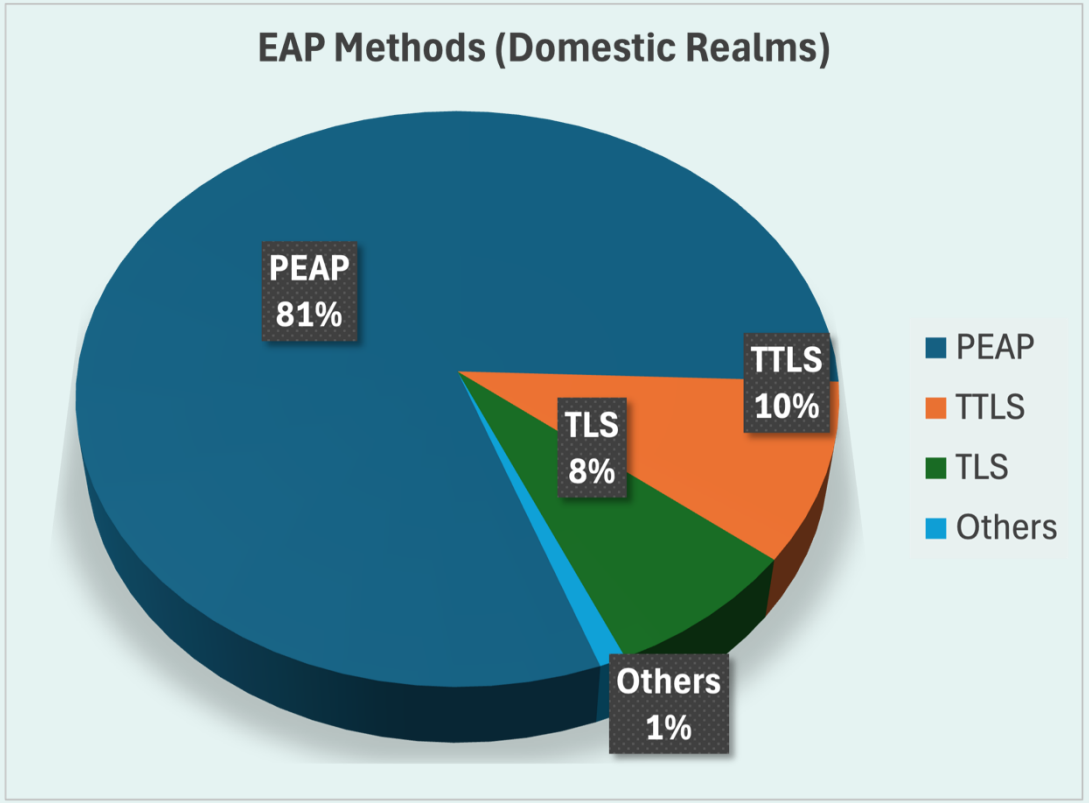
Challenges facing eduroamers in the UK

There's plenty!

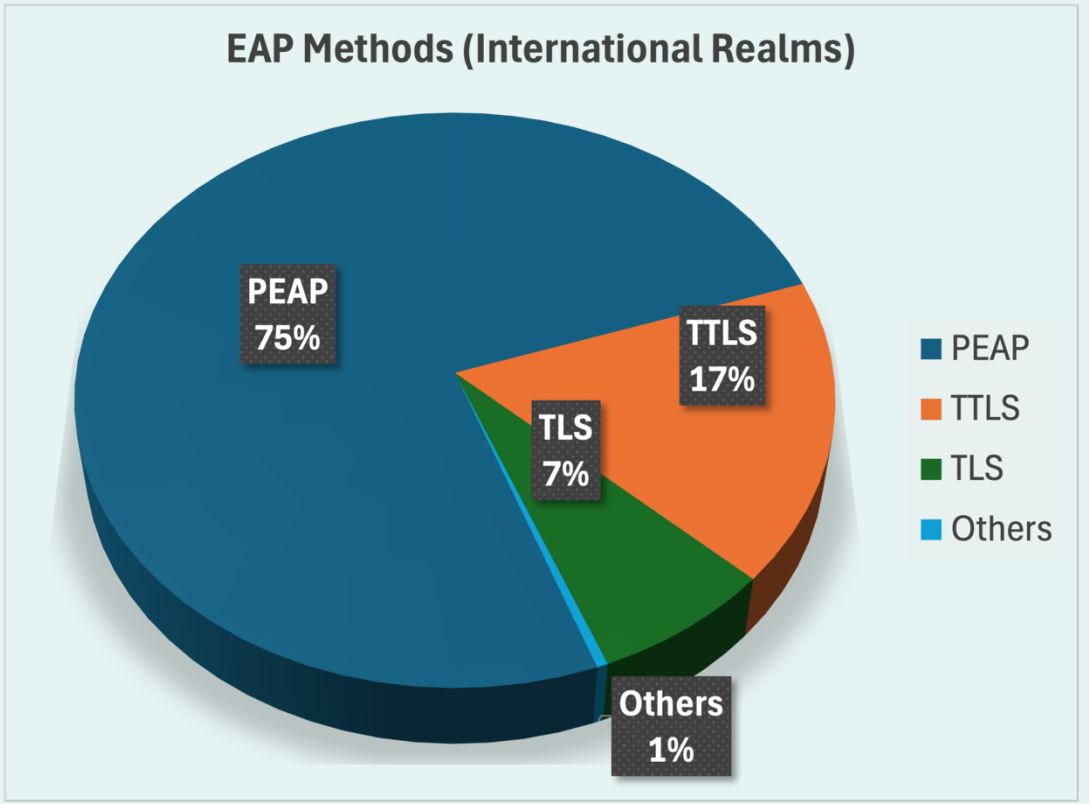
- CredentialGuard
  - We've seen this before, haven't we?
- Microsoft wants to kill off NTLM
  - We've seen the announcements
- Moving to cloud services
  - Not necessarily compatible with ActiveDirectory
- Usernames and passwords are a PITA
  - Change password, eduroam locks the account

EAP methods seen on UK eduroam

Local Realms



International Realms



So – what do we do?

Passwords… Storing and using them with RADIUS

	Clear-text	NT Hash	MD5 Hash	Salted MD5 Hash	SHA1 Hash	Unix Crypt
PAP	✅	✅	✅	✅	✅	✅
CHAP	✅					
Digest	✅					
MS-CHAP	✅	✅				
PEAP	✅	✅				
EAP-MSCHAPv2	✅	✅				
LEAP	✅	✅				
EAP-GTC	✅	✅	✅	✅	✅	✅
EAP-MD5	✅					
EAP-SIM	✅					

So – what do we do? Part II

What else is there?

- Certificates!
  - Needs a Public Key Infrastructure (PKI)

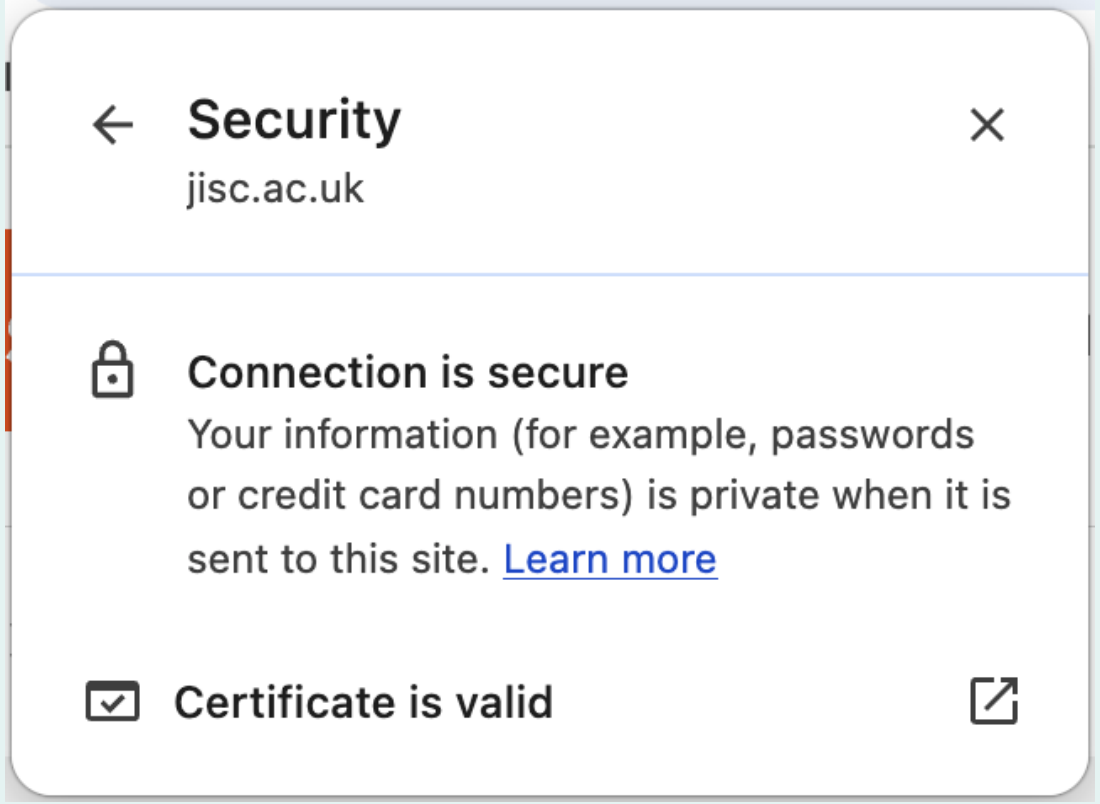
- But PKI! PKI!! ARGHHHH!
  - Certificates are HARD!! (are they?)

About EAP-TLS

EAP-TLS

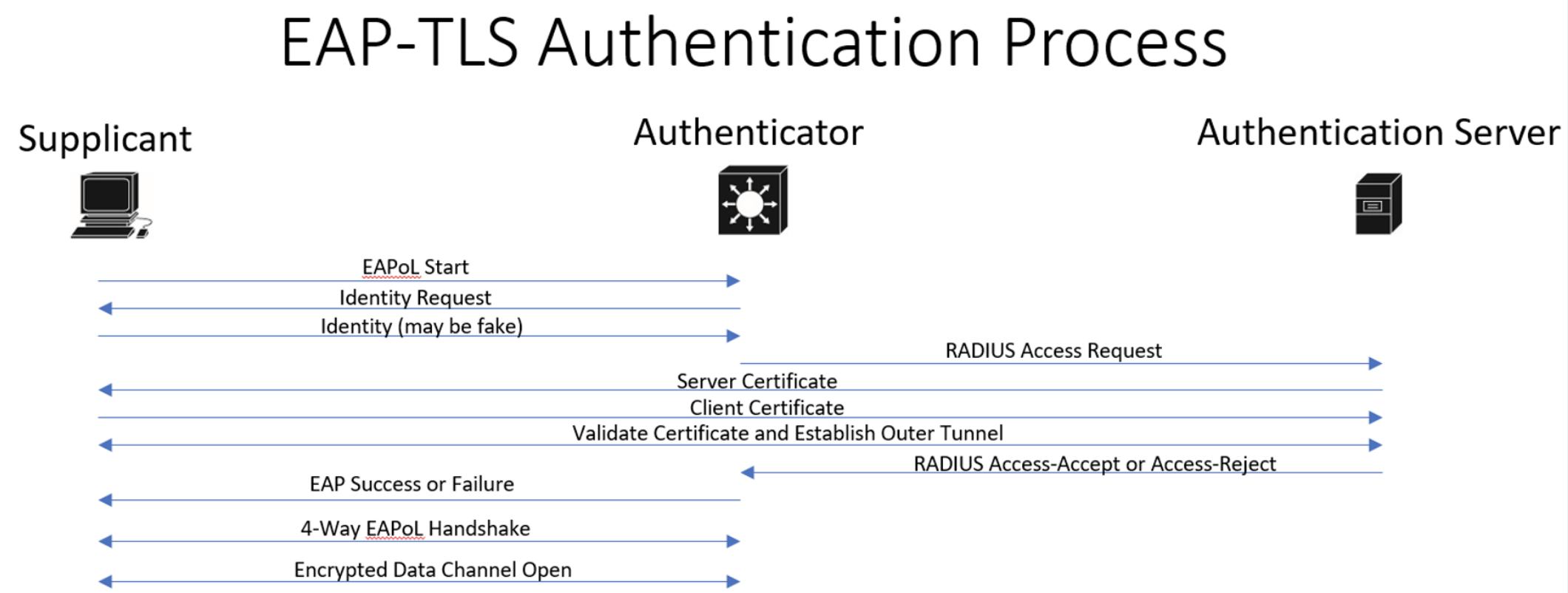
How does it work?

- Browsers do half of this (using SSL/TLS)
  - Browser certificates
- RADIUS servers do half of this too
  - Server certificates
- EAP-TLS = EAP using certificates!
  - Send your personal (client) certificate back
  - RADIUS server checks it



EAP-TLS – How it works

A diagram…



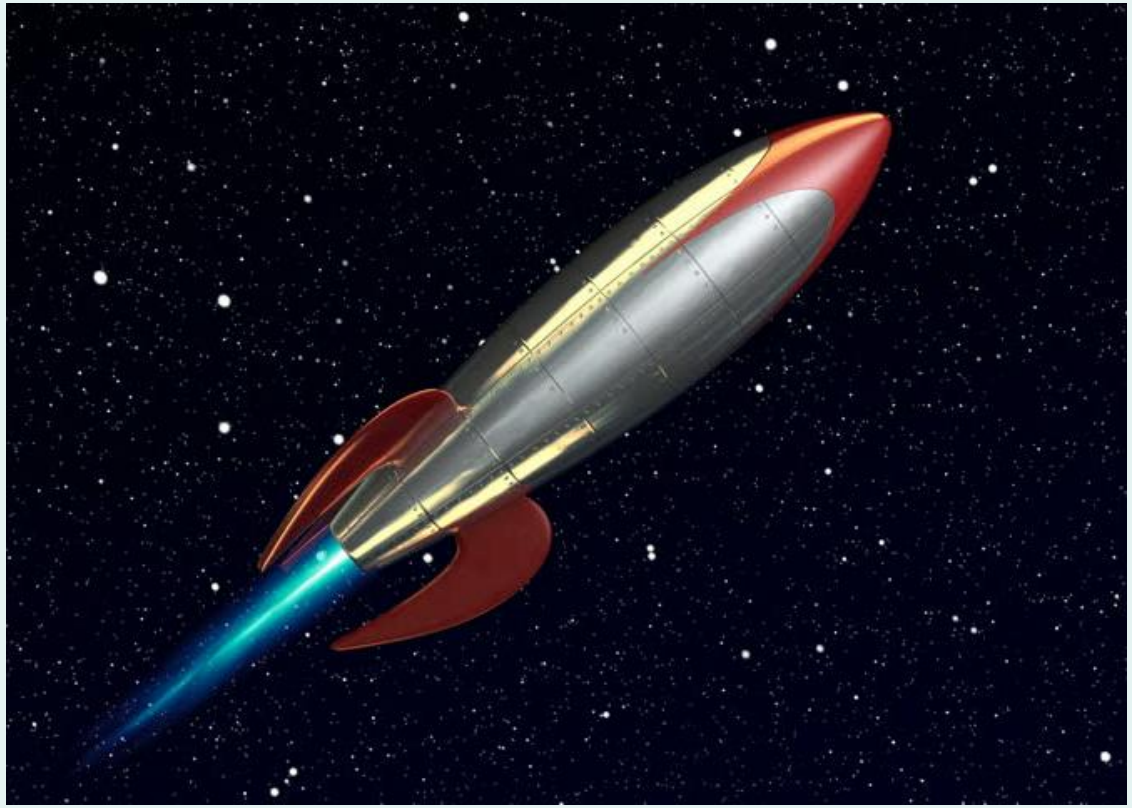
EAP-TLS – Is it faster?

A question of round-trips…

- Username/Password methods
  - Many (8-12) round trips!

- Is EAP-TLS better?
  - It depends!

- Some issues don’t change between EAP-TLS and other methods



EAP-TLS – Is it faster (part deux)?

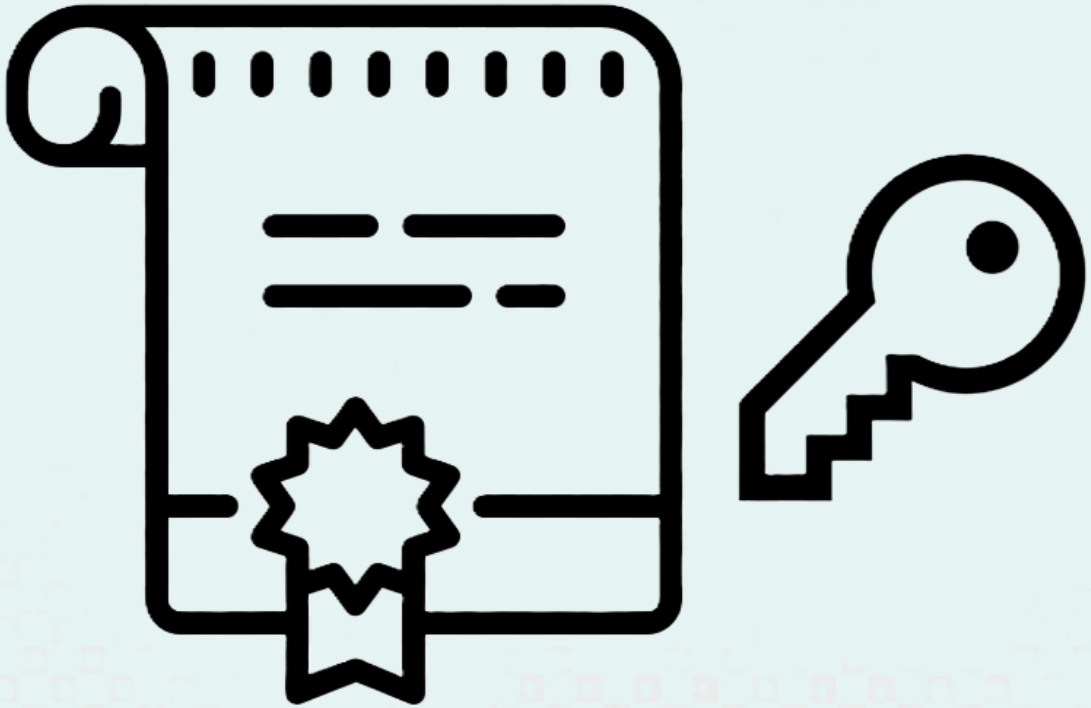
Certificate chains and key sizes (all methods)

- Long chains = more fragments
- More fragments = more packets
- More packets = more round-trips
- Bigger keys (for RSA) = more round-trips
- Post-quantum cryptography = more round-trips
- More fragments = problematic with some firewalls and SSL inspection.

EAP-TLS – But… Is it better?

Disadvantages

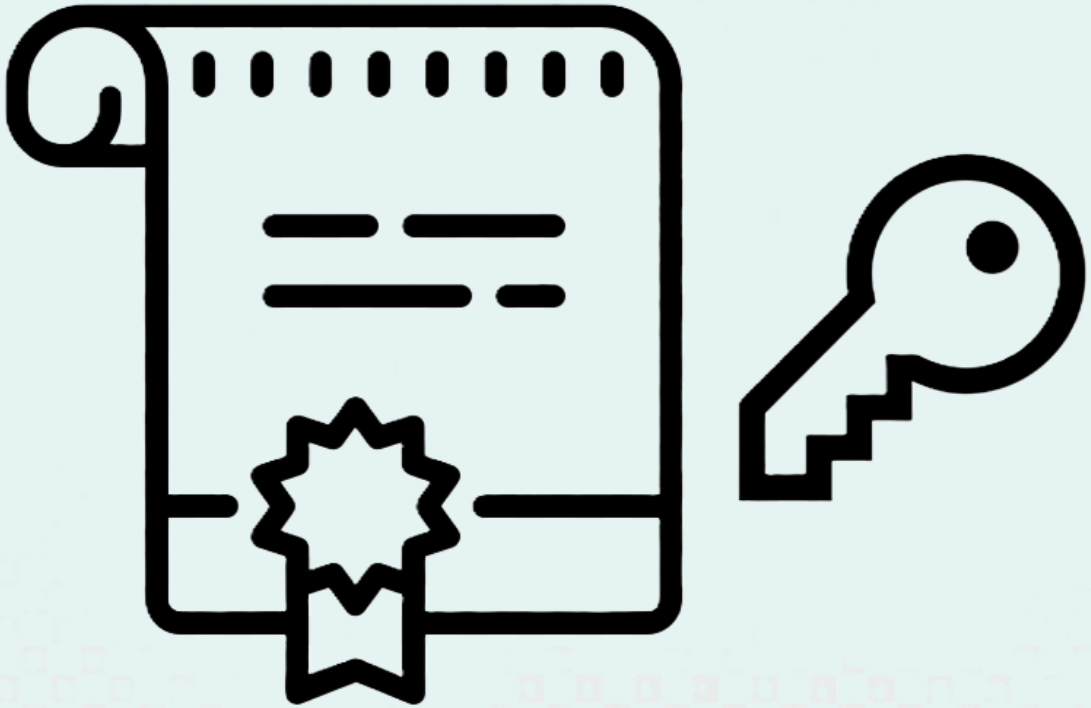
- Usernames are often exposed:
  - Subject: /C=GB/…/CN=username@realm
  - Use CN=anonymous@realm or tls@realm and stuff things into subjectAltName
- Fragments could be problematic
  - Especially with certs with large keys
- How to get certs + keys onto end user devices!!



EAP-TLS – Is it better?

Advantages

- Certificates are decoupled from directories
  - Fixed length validity
  - Independent of passwords
- Easily deployable through MDM
  - Perfect for corporate devices/creds
- Can hide user details
  - Use ‘pseudonymous’ information into subjectAltName that only *you* can link back to your users
- Supported by all devices and configurations (think OpenRoaming)



EAP-TLS – Requirements I

Certificate Format

- You ***must*** use the userID@realm.name format for the cert subject/CN!
  - eduroam requirement cannot be changed!

- What's the deal about the format?
  - Device certs are usually "host/<fqdn>"
  - Change to "host/<fqdn>@realm.name"?

- Consider PQC, use ECDSA certs before that (small but powerful)

EAP-TLS – Requirements II

What do you need?

- A PKI issuing certificates
  - Already have one in Windows CA Service!
  - Use Azure Cloud PKI/Amazon?
- A RADIUS Server and the above's root certificate!
- ACME/SCEP/portal to get certs issued!
- Way to pick up certificate revocation from ACME/SCEP/portal (for RADIUS to reject revoked certs)

EAP-TLS – Provisioning

How?

- For corporate
  - Use InTune, JAMF, Group Policy (!)
  - Remember the certificate name format!!
  - Regularly push updated certs
- For BYOD
  - All major vendors have tools!
  - geteduroam's Let's Wi-Fi portal!
    - Integrates with geteduroam app!
  - Both integrate into your SSO

What next for you?!

What next?

Things to consider

- What's your plan and what timeline do you have?
- Talk to vendors:
  - Price, device support, user experience (the granny test)
  - N.B. How do their tools deal with off-boarding (when your staff/students leave)
  - PKI Management! Point-and-click?
- How confident are you using an Open Source alternative (geteduroam/Let's Wi-Fi)?
- Try it with a few devices (pilot it)
- Try it with corporate devices (maybe IT staff first)
- Try it with BYOD users (staff again)
- Roll it out?

Questions?!

Email help@jisc.ac.uk or the use eduroam Support portal help request form!

Also consider Trust & Identity Consulting: trustandidentity@jisc.ac.uk

Thank you

Stefan Paetow

Federated Roaming Technical Specialist

Stefan.Paetow@jisc.ac.uk

help@jisc.ac.uk

0300 300 2212

jisc.ac.uk

@jisc.bsky.social

@jiscsocial

linkedin.com/company/jisc