

eduroam

Introduza a sua conta de utilizador para se ligar à rede "eduroam".

Nome de utilizador:

Senha:

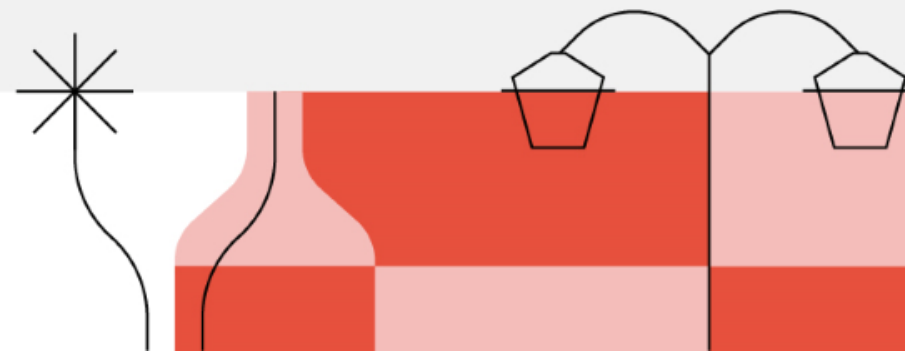
Cancelar

OK

# Segurança de credenciais em dispositivos + ReEDUROAM

Pedro Ribeiro – DSIC/IPLNet

pribeiro@net.ipl.pt



# Idealizado v.s. a realidade ...

- Repositórios de credenciais são “pote de mel” para *hackers*
- Sistemas e aplicações com potencial de intercepção de credenciais introduzidas
- Chaves colecionadas abusadas em “todas as portas que abrem”
- Regulamentações e legislação apontam para solução:
  - Acesso com autenticação *multi-fator*



# MFA em uso ...

- Responsáveis pedem que se implemente
  - Porque legislação e outros lhes dizem ser a solução
  - Fogem ao uso quando têm eles próprios de usar!
- MFA é vocacionado para a Web
  - Não é solução universal
  - Nem todas as aplicações são web
  - O incómodo extra promove comportamentos de risco
  - Alguns sistemas simplificam a ponto de anular a segurança acrescida
  - Frequente impasse quando a validação secundária está indisponível
  - O mundo tem que continuar a rolar quando não há SMS ou net ...
    - Ou a gestão de um TLD deixa as chaves DNSSEC expirarem (.de)



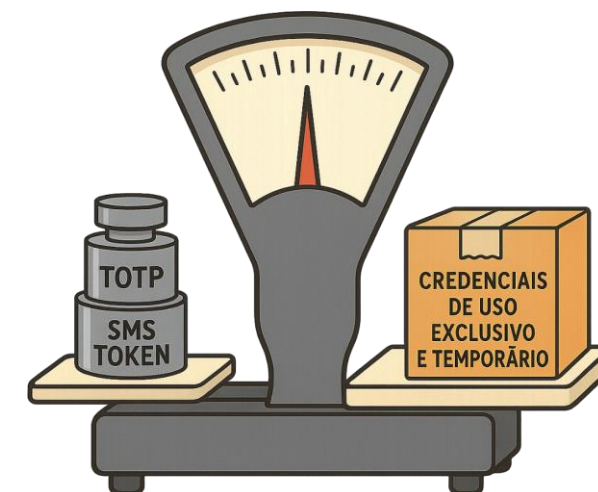
# Aplicações base da Internet e MFA

- Aplicações que realizem acessos ou autenticações regulares em nome do utilizador
  - Aplicações de acesso a e-mail
  - Sistemas que enviam ou recebem e-mail
  - Acessos VPN
  - Eduroam
    - Imaginam como seria a eduroam com MFA/TOTP ou similar?  
(no dia 4, um utilizador da presidência do IPL realizou 105 autenticações até às 18h)
- Sistemas em que ocorra autenticação com uma frequência tal que o uso de MFA afete significativamente o desempenho das tarefas
  - Ao gerir um parque de centenas de routers/*switch*, será viável MFA a cada acesso numa operação a realizar em grupos destes?



# Uma solução de compromisso ...

- Que evite introdução de códigos em cada acesso
- Que minimize a possibilidade de reutilização de credenciais roubadas
- Que não signifique voltarmos às contas locais em cada serviço



# Em desenvolvimento no IPLisboa (1)

- Uma lógica de validação de acessos complementar no uso de contas institucionais .ipl.pt
- Paralelos identificáveis com técnicas usadas no “MBNET” pelo sistema bancário
  - Geração de cartões com validade reduzida
  - Geração de cartões para apenas um comerciante
  - Invalidação de cartões em anomalias de uso



# Em desenvolvimento no IPLisboa (2)

- Possibilidade de criação pelo utilizador de novos pares utilizador/palavra-chave que são processados internamente como se a conta base se tratasse
  - Critérios automatizados de expiração (ex. inatividade ou tentativa de uso indevido)
  - Uso apenas em determinado serviço (ex. envio e-mail)
  - Uso apenas em determinado dispositivo (ex. endereço MAC do dispositivo eduroam)
  - Uso apenas a partir de determinada rede ou grupo de redes
  - Possibilidade de autoaprovisionamento no primeiro acesso usando 2FA/TOTP

# Exemplo com credenciais de serviço

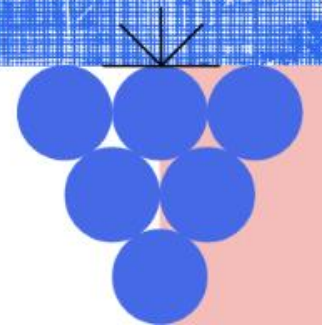
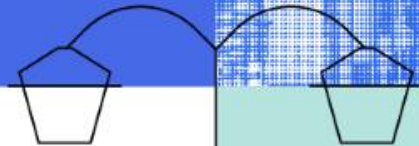
- Utilizador acede a painel de controlo de conta e solicita geração de credencial de serviço.
  - Obtenção via canal robusto validado com TOTP ou CC/CMD
  - Só visível durante um tempo limitado
- No primeiro uso com sucesso
  - Sistema regista em *cache* elementos adicionais de “impressão digital” do serviço/dispositivo/aplicação
- Acessos posteriores aceites se as condições do acesso forem mantidas
- Credencial é invalidada se a “impressão digital” se alterar

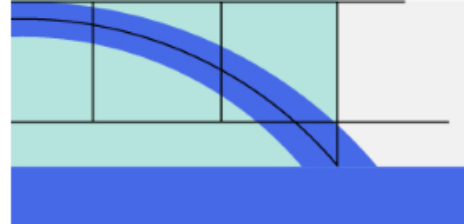


A1:B2:3C:4D:5E:6F

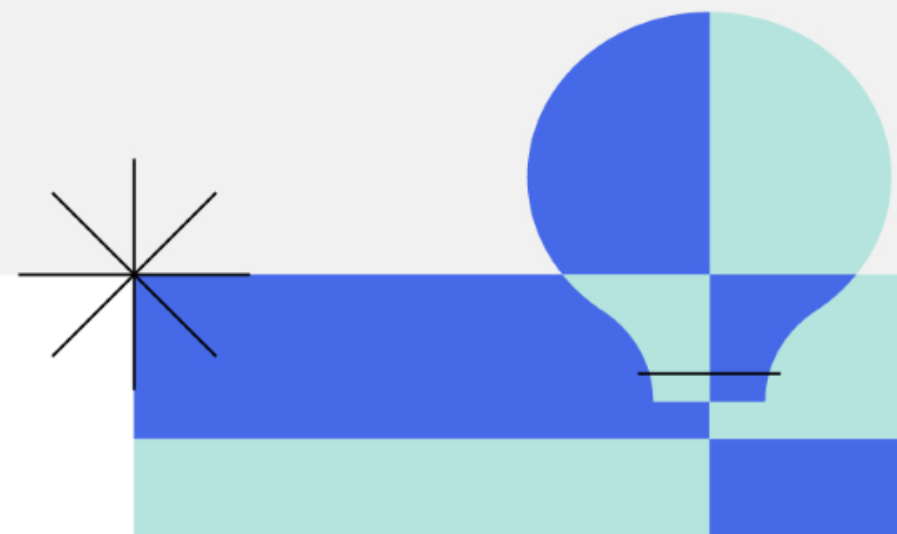
# “Impressão digital” de serviços

- Elementos que permitam, com determinado âmbito funcionar como identificação adicional do serviço e/ou dispositivo
- Potenciais elementos usáveis
  - E-mail: Serviço, país GeoIP, IP ASN, IMAP ID, TLS Suite, porto local TCP, autenticação PLAIN/LOGIN
  - VPN: Serviço, País GeoIP, IP ASN, MSCHAP ID, TLS Suite, tipo VPN L2TP/IPSEC ou SSTP, autenticação MSCHAP/PAP/EAP
  - eduroam: Serviço, MAC, EAP TLS Suite, autenticação EAP MSCHAP/GTC





# Evoluções para convergência NIS2



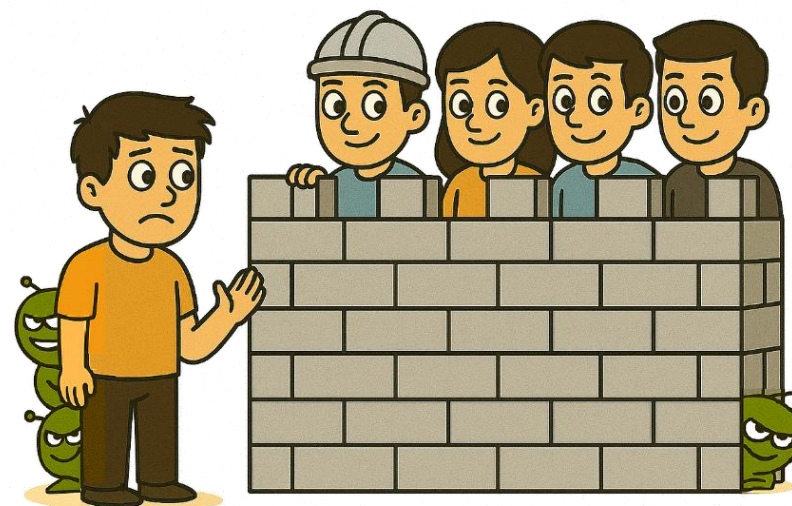
# Porquê?

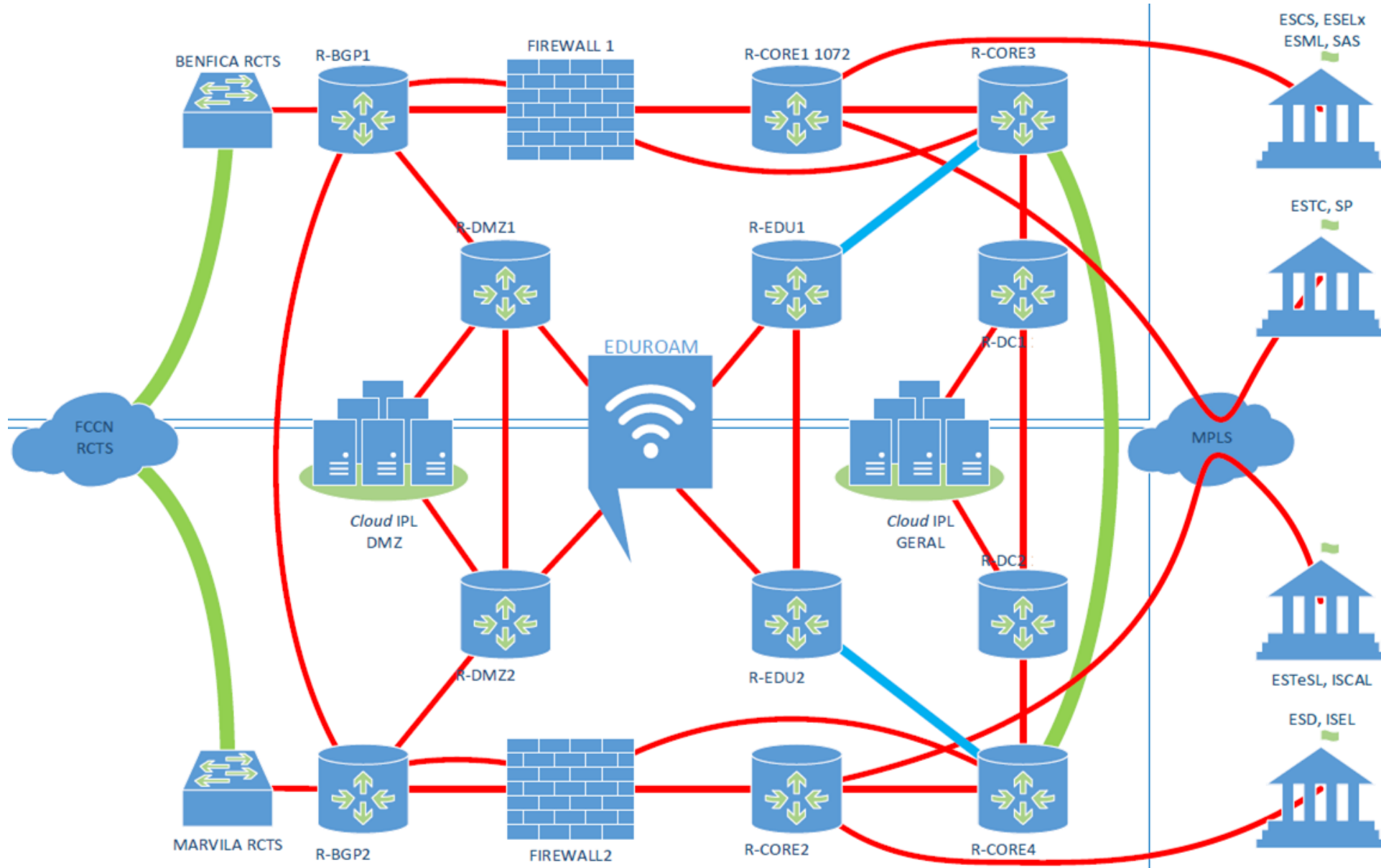
- Inviável a inclusão dos dispositivos de utilizadores no relatório anual de CS/CNCS
- Necessidade de maior controlo sobre os dispositivos com privilégios Intranet
- Próximo de 100% dos dispositivos detetados como “infetados”/comprometidos estão ligados na eduroam
  - Maioritariamente visitantes (já em DMZ)
- A quase totalidade dos dispositivos não acede a recursos Intranet



# Estrutura de redes eduoam atual

- Segregação de utilizadores por VLAN
  - Escalabilidade e segurança
  - Atribuição no momento do acesso
- 3 redes L2 em contexto DMZ (pré-firewall)
  - Com L3 central
- 11 redes L2 em contexto Intranet
  - 1 com L3 central usada para picos de uso e apoio a manutenções
  - 10 com L3 local à escola/serviço que servem





# Redes eduroam DMZ (atual)

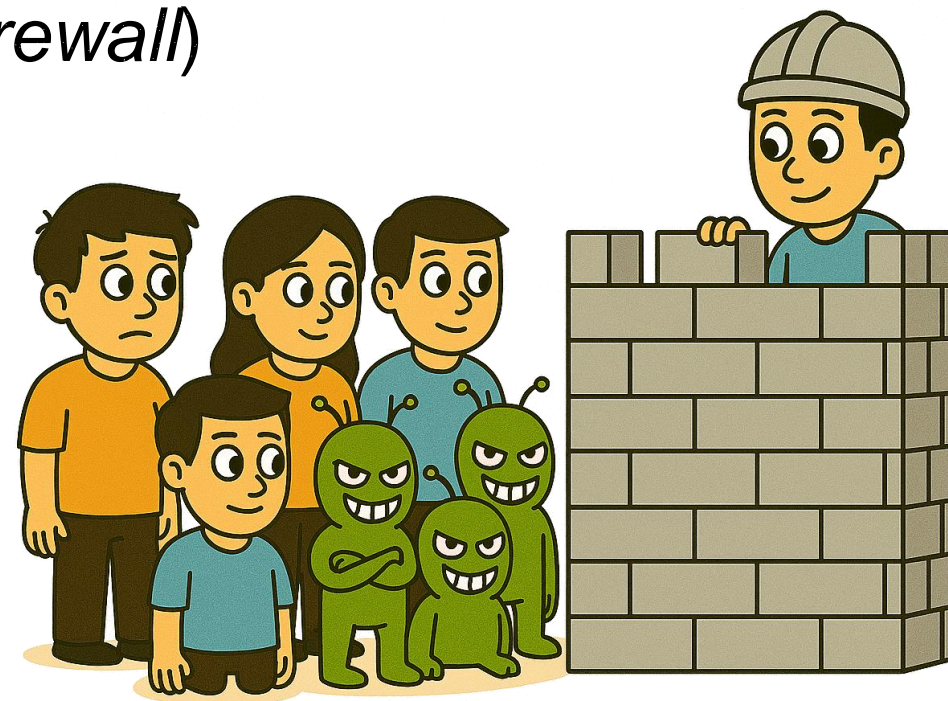
- Atribuídas a contas:
  - de *roamers* eduroam
  - contas locais de visitante @ipl.local
  - acessos com identidade anónima
- Separação por motivos de escalabilidade
  - 1000 dispositivos por rede
  - DMZ1 – Campus Marvila
  - DMZ2 – Campus Benfica
  - DMZ3 – Restantes pólos
- Endereçamento IP privado com mapeamento NAT M:N sobre um bloco /22 (~1k endereços públicos)
- Capacidade agregada de 10Gbit/s

# Redes eduroam Intranet (atual)

- Atribuídas às restantes contas
- Cerca de 4000 dispositivos suportados por rede
- Endereçamento IP privado com mapeamento NAT M:N sobre um bloco /20 e um bloco /21 (~6k endereços públicos)
- Capacidade de 10Gbit/s por rede

# Redes eduoam em preparação

- 4 redes L2 em contexto DMZ (pré-*firewall*)
  - Com L3 central
- 4 redes L2 em contexto Intranet
  - Com L3 central



# Redes eduroam DMZ (Q3 2026)

- Atribuídas por omissão a todas as contas
  - DMZ1 a 3 para contas internas
  - DMZ4 para *roamers* e visitantes com contas locais
  
- ~4000 dispositivos por rede
  
- Endereçamento IP privado com mapeamento NAT M:N sobre um bloco /20 (4k endereços)
  
- Capacidade de 10 ou 25Gbit/s por rede

# Redes eduroam Intranet (Q3 2026)

- Cerca de 250 dispositivos suportados por rede
- Endereçamento IP privado com mapeamento NAT M:N sobre um bloco /21 (~2k endereços)
- Capacidade de 25Gbit/s por rede
- Uso limitado a dispositivos elegíveis

# Eligibilidade eduroam Intranet

- Acessos pontuais podem usar VPNIntra
- Acessos regulares (ex. serviços administrativos)
  - Utilizadores sinalizam a necessidade no painel de controlo da conta
  - Equipamentos auditados por agente *endpoint* sempre que possível
  - Somente usando endereços MAC de fabricante (BIA)
  - Escolas/serviços terão de manter listagens dos dispositivos sob que assumem responsabilidade para a opção ficar disponível
    - Com MAC e demais dados posteriormente usados para o relatório de CS

Pedro Ribeiro  
*pribeiro@net.ipl.pt*

# Obrigado!

[jornadas.fccn.pt](http://jornadas.fccn.pt)

[fccn.pt](http://fccn.pt)



Imagens: LLM Copilot