Federação de Identidade RCTS

Perfil Tecnológico eduroam

1. Introdução

Este documento define o Perfil Tecnológico eduroam incorporado na Politica da FEDERAÇÃO DE IDENTIDADE RCTS e descreve a utilização do eduroam [1] na federação.

2. Requisitos

- Todos os FORNECEDORES DE IDENTIDADE e os FORNECEDORES DE SERVIÇO têm OBRIGATORIAMENTE de cumprir as regras da Política da Confederação Europeia eduroam [2].
- Os MEMBROS têm OBRIGATORIAMENTE de disponibilizar acesso à rede de acordo com as Definições do Serviço eduroam [3].
- Os MEMBROS NÃO PODEM cobrar qualquer valor pelo acesso à rede através do eduroam.
- Os MEMBROS têm OBRIGATORIAMENTE de apoiar os utilizadores da confederação a solucionar problemas e a gerir incidentes que envolvam o roaming.
- Os MEMBROS são OBRIGATORIAMENTE um FORNECEDOR DE SERVIÇO, isto significa que TÊM DE disponibilizar acesso à rede baseado na autenticação 802.1x.
- Os Realms associados aos servidores de Radius TEM DE ser uma string igual a um domínio de DNS, sendo o MEMBRO titular desse domínio.
- Os MEMBROS TÊM de ter em funcionamento pelo menos um servidor de Radius, de acordo com as regras eduroam, e DEVEM ter, pelo menos, um servidor adicional para garantir redundância.
- Os servidores de Radius dos MEMBROS TÊM de manter uma relação técnica de confiança com os servidores de Radius Nacionais de topo, geridos pela FCT | FCCN.
- Os FORNECEDORES DE SERVIÇOS TÊM de configurar pelo menos um mecanismo de autenticação baseada em EAP e encaminhar os restantes, que não pertençam aos seus utilizadores, para a hierarquia nacional de Radius.
- Os FORNECEDORES DE SERVIÇO TÊM de configurar o SSID eduroam, sem qualquer alteração, e DEVEM, sempre que possível anunciá-lo e torna-lo visível para os utilizadores.
- Os FORNECEDORES DE SERVIÇO TÊM DE disponibilizar acesso à rede eduroam através da cifra WPA2.

- Os FORNECEDORES DE SERVIÇO TÊM de gerar e registar a seguinte informação de Accounting:
    - User-Name
    - NAS-Port
    - NAS-IP-Address
    - Framed-IP-Address
    - NAS-Identifier
    - Acct-Authentic
    - Acct-Status-Type
    - Acct-Input-Octets
    - Acct-Output-Octets
    - Acct-Input-Packets
    - Acct-Output-Packets
    - Acct-Terminate-Cause
    - Acct-Session-Time
    - Acct-Delay-Time
    - Calling-Station-Id
    - Called-Station-Id
    - Timestamp
    - Status-Type

- Os FORNECEDORES DE SERVIÇO TÊM de transmitir informação de Accounting dos utilizadores em mobilidade para os respetivos FORNECEDORES DE IDENTIDADE;

- Os FORNECEDORES DE SERVIÇO TÊM de incluir nos pacotes de autenticação gerados o atributo Calling-Station-ID, e este deve ser preenchido com pelo menos o endereço mac (identificador do hardware) do dispositivo que está a realizar o acesso à rede;

- Os FORNECEDORES DE IDENTIDADE TÊM de gerar e registar a seguinte informação de Autenticação:
    - A data e hora que o pedido foi recebido;
    - O identificador do pedido;
    - O resultado do pedido de autenticação (Aceite ou Rejeitado);
    - A razão pela qual o pedido foi rejeitado, se aplicável;

- Os FORNECEDORES DE SERVIÇO TÊM de gerar e registar os seguintes registos relacionados com o serviço de DHCP:
    - A data e hora da atribuição do endereço IP via DHCP;
    - O endereço MAC do cliente;
    - O endereço IP atribuído ao cliente.

- Os MEMBROS TÊM de garantir a retenção dos registos de Autenticação, Accounting e DHCP num período não inferior a seis meses.

- Os FORNECEDORES DE SERVIÇO TÊM de garantir a Atribuição de um endereço IP público a cada utilizador em mobilidade;
- Os FORNECEDORES DE SERVIÇO TÊM de garantir os seguintes serviços para os utilizadores em mobilidade:
    - Acesso VPN (Virtual Private Network) para fora da instituição visitada, nomeadamente com as tecnologias IPSec, PPTP, L2TP e outras, sem prejuízo para outras tecnologias existentes ou que venham a existir;
    - Acesso a serviços de messaging;
    - Acesso aos serviços de voz sobre IP (VoIP);
    - Acesso de dentro do hotspot para fora da INSTITUIÇÃO VISITADA aos seguintes serviços de rede:
        - FTP (porto 20 e 21);
        - HTTP (porto 80, 443, 3128, 8080);
        - IMAP (porto 143 e 993);
        - POP3 (porto 110 e 995);
        - SMTP e SMTP AUTH (porto 25) pelo menos para os blocos de endereços da RCTS, nomeadamente 139.83.0.0/16; 146.193.0.0/19; 146.193.32.0/19; 146.193.64.0/18; 146.193.128.0/17; 158.162.0.0/18; 158.162.64.0/19; 158.162.96.0/20; 158.162.112.0/21; 158.162.128.0/18; 158.162.192.0/18; 192.12.232.0/24; 192.104.48.0/24; 193.136.0.0/15; 194.117.0.0/20; 194.117.16.0/21; 194.117.32.0/22; 194.117.40.0/22; e 194.210.0.0/16;
        - SSH (porto 22);
        - TELNET (porto 23);
        - SMTPS (porto 465);
        - SFX (9003)

- Sempre que os FORNECEDORES DE SERVIÇO sejam capazes de disponibilizar os serviços acima referidos, sem o recurso à atribuição de endereçamento IP público, esta requisito pode ser revisto.

- A FCT | FCCN TEM de operar pelo menos dois servidores de Radius, para encaminhar os pedidos para os MEMBROS.

- A FCT | FCCN TEM de disponibilizar e atualizar estatísticas de acordo com o estabelecido no ponto 2.2.3 das Definições do Serviço eduroam [3]

- Os MEMBROS TÊM de enviar para a FCT | FCCN a seguinte informação gerada nos processos de autenticação e accounting:
    - **Identificador** - Identificador do processo de autenticação no Radius. Por ser um valor numérico este não é único em todos os registos de autenticação;
    - **Timestamp** - Registo, no formato Unix, do momento em que o processo foi realizado
    - **Realm** - Domínio associado à autenticação do utilizador;
    - **Calling-Station-Id** - Endereço Mac do dispositivo que realizou a ligação;
    - **Called-Station-Id** - Endereço Mac do ponto de acesso onde com o qual a ligação foi estabelecida;

- **User-Name** - Nome de utilizador sobre o qual a sessão está a ser realizada e que serviu de autenticação. Este campo é cifrado (hashed com MD5) antes de ser transmitido;
- **NAS-IP** - IP do Access Point utilizado na autenticação do utilizador;
- **Resultado** - Resultado final da autenticação. Deve apresentar apenas um dos dois valores possíveis (OK ou FAIL);
- **Acct-Session-Time** – Tempo de duração da sessão;
- **Acct-Input-Octets/Acct-Output-Octets** – Número de octetos recebidos e enviados pelo utilizador durante a sessão;
- **Acct-Input-Packets/Acct-Output-Packets** - Número de pacotes recebidos e enviados pelo utilizador durante a sessão;
- **Acct-Input-Gigawords/Acct-Output-Gigawords** – Contador de grupos de 4 octetos de dados, transmitidos pelo utilizador durante a sessão;
- **Acct-Status-Type** – Tipo de pacote de accounting (Start, Alive, Stop);

- Os MEMBROS TÊM de cifrar toda a informação enviada para a FCT | FCCN, garantindo assim a privacidade dos utilizadores e dos seus dados, impedindo que seja possível fazer qualquer tipo de identificação ou localização dos mesmos, quer no espaço quer no tempo.

- Os MEMBROS TÊM de utilizar os mecanismos de envio de informação disponibilizados pela FCT | FCCN.

- A FCT | FCCN compromete-se a processar a informação recebida e a apresentar uma análise geral da utilização e qualidade da rede eduroam no sítio web eduroam.pt e outros sites associados quer à FCT | FCCN quer ao eduroam.

- A FCT|FCCN compromete-se ainda a fornecer uma análise mais detalhada de cada MEMBRO, garantindo que o acesso é restrito aos responsáveis por eles nomeados.

3. Referências

[1]http://www.eduroam.org
[2]https://www.eduroam.org/wp-content/uploads/2016/05/GN2-07-328-eduroam-policy-for-signing-Final2-2.pdf
[3]https://www.eduroam.org/wp-content/uploads/2016/05/GN2-07-327v2-DS5_1_1-_eduroam_Service_Definition.pdf

Lisboa, _____ de _____ de _____

_____	_____
NOME DA ENTIDADE	FCT – Fundação para a Ciência e a Tecnologia, IP
Cargo: CARGO DESEMPENHADO	