19-09-2018

Deliverable D9.4
Evaluation of Certificate Provisioning Pilot

Deliverable D9.4

Contractual Date:	29-06-2018
Actual Date:	19-09-2018
Grant Agreement No.:	731122
Work Package/Activity:	9/JRA3
Task Item:	Task 4
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	RESTENA
Document ID:	GN4-2-18-134024
Authors:	S. Winter (RESTENA); P. Dekkers (SURFnet)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Abstract

This deliverable outlines investigations into improving the scalability and efficiency of certificate provisioning for server-to-server transport protection (RADIUS/TLS) in eduroam, currently supported by eduPKI. Approaches to adopting the principles of 'LetsEncrypt' to streamline this process, under the concept name 'LetsRadsec', are evaluated, and the results of the tests carried out are discussed.

Table of Contents

Executive Summary 1

1 Introduction 2

2 Pilot Review 4

2.1 Pilot Scope 4

2.2 Pilot Description 4

2.3 Pilot Results 6

3 Conclusions and Next Steps 8

References 9

Glossary 9

Table of Figures

Figure 1: Verification Mechanism for LetsRadsec 5

Executive Summary

This deliverable outlines the investigations that were carried out into improving the scalability and efficiency of certificate provisioning for server-to-server transport protection (RADIUS/TLS) in eduroam, including the concept itself and its concrete, technically viable, implementation. Currently certificates for transport protection are supported by eduPKI.

An approach to verify whether the principles of 'LetsEncrypt' [Let's Encrypt] could be adopted to streamline the certificate provisioning process in eduroam, under the concept name 'LetsRadsec' was evaluated. This LetsRadsec work aimed specifically to facilitate the issue and renewal of X.509 certificates for RADIUS server-to-server communication.

The validations of the technical pilot performed in actual deployments demonstrated that, while LetsRadsec performed well, its benefits were limited to one group of eduroam participants only, i.e. eduroam Identity Providers, who were less likely to see RADIUS/TLS deployment as a priority. Conversely, for eduroam National Roaming Operators (NROs), who have a more critical need for such certificates, a number of workarounds were required to make automatic provisioning with 'LetsRadsec' possible, making it an operationally suboptimal choice for this group. Where benefits were delivered, there was also a trade-off due to the need for more complex certificate management overall.

Due to these limitations, the pilot was concluded, and there are no plans to put this concept into production in the foreseeable future. Other ways of certificate provisioning that are more tailored to eduroam NROs are now being investigated instead and it is recommended that an alternative solution that better supports established delivery channels be developed as the next step.

1 Introduction

eduroam is a highly de-centralised roaming service which relies on several levels of aggregation of its roaming partners and their respective technical infrastructures.

eduroam Identity Providers and eduroam Service Providers are aggregated towards their respective eduroam National Roaming Operators (NROs), and eduroam NROs are in turn then aggregated in groups towards eduroam top-level servers, which often serve an entire continent or similarly large geographic region.

While eduroam authentications do not strictly require transport-level security for the server-to-server connections – the actual authentication payload is encrypted on a higher layer – there is some utility in providing a secured transport layer anyway. One reason for this is that without the transport-layer being encrypted, some important metadata is not encrypted. In addition, transport layer encryption along with other supporting measures makes it possible to bypass some aggregation layers ("dynamic discovery"), thereby removing dependencies on centralised aggregators and eliminating possible points of failure. Finally, bypassing proxies expedites the request forwarding, leading to quicker authentication for the end user.

All of these advantages were known before the pilot, but their practical application was progressing slowly. A factor that influences deployment is the complexity of getting a certificate.

To realise the benefits of transport layer encryption for RADIUS (RADIUS/TLS, a.k.a. RadSec), RADIUS servers need a X.509 certificate identifying them as an authorised eduroam Identity Provider (or proxy), or an authorised eduroam Service Provider (or proxy).

Currently, server operators request these certificates from the GÉANT eduPKI service. This service uses a workflow requiring significant amounts of human intervention as well as following strict administrative procedures – much like classical workflows to obtain web server certificates from a commercial provider. RADIUS/TLS is currently only used by about 15 major NROs (of almost 100 globally) and a small number of eduroam Identity Providers (less than 10 among several thousand). The goal of the present work was therefore to investigate whether the administrative burden of obtaining certificates via a semi-manual workflow could be reduced, thereby increasing take-up of RadSec.

X.509 certificate provisioning for the web has been revolutionised in the recent past by a concept and service called 'LetsEncrypt' [Let's Encrypt], which automated large parts of certificate provisioning and renewal making getting a web server certificate almost effortless.

The pilot described in this deliverable mirrors the workflow of LetsEncrypt in the different context of RADIUS/TLS within eduroam and is called 'LetsRadsec'.

LetsRadsec leverages the established trust relationship that an eduroam Identity Provider already has with the eduroam consortium: an IdP is connected to the “traditional” RADIUS/UDP infrastructure. This is based on the traditional hierarchical structure of proxies, but for the present purposes serves as a vehicle to verify the authority of a requester in an automated way, and has an existing X.509 certificate and corresponding private key for the purpose of authenticating its own users (the ‘EAP server certificate’). While that EAP server certificate is unrelated to the RADIUS/TLS certificate that is to be provisioned, its private key can serve as proof-of-possession.

The trust relationship combined with the key make it possible to verify that a requested RADIUS/TLS certificate is authorised (existing connection to eduroam exists), and that the certificate request itself came from a legitimate eduroam administrator in the requesting organisation (the person requesting the RADIUS/TLS certificate has access to the private key of the EAP server certificate).

2 Pilot Review

2.1 Pilot Scope

The pilot's primary goal was purely technical in nature – to prove the feasibility of porting the LetsEncrypt concept towards a RADIUS/TLS certificate infrastructure.

Since the LetsRadsec concept focuses on TLS endpoints on the IdP side, a secondary goal was to gauge interest in the concept on the part of IdP participants and obtain feedback from other relevant eduroam participants (SPs, NROs, other proxy operators).

The primary success criterion defined was whether it would be possible to create a workable setup and have this setup tried out by at least two IdPs inside two distinct NROs. The tests run included the set-up of a (software-based, provisional) CA infrastructure to issue certificates, an API endpoint to receive new certificate requests, and a set of scripts for the IdP side to request new certificates and trigger certificate renewals.

The secondary aim of collecting feedback from various operators was achieved through dissemination of a survey that included questions to assess the usefulness and acceptability of the concept to users of the pilot and other interested parties.

2.2 Pilot Description

The core concept of LetsRadsec mirrors that of LetsEncrypt: certificates are requested semi-automatically, an out-of-band proof of possession verification is performed and, if this is successful, the certificate is generated and delivered.

The proof of possession algorithm is different from that of LetsEncrypt because the specificities of the eduroam architecture need to be considered, i.e. the system needs to find out whether the entity that requested a certificate is actually a registered, known and operational eduroam Identity Provider. The certificate then needs to be issued with the properties of the IdP so that any subsequent usage of it can be attributed to that IdP.

This verification mechanism is therefore specific to the eduroam consortium. Where Let'sEncrypt uses an ordinary IP connection to connect to the to-be-vetted web server over the internet, Let'sRadSec connects via the eduroam RADIUS proxy infrastructure to the to-be-vetted RADIUS server. This mechanism is depicted in Figure 1 below.

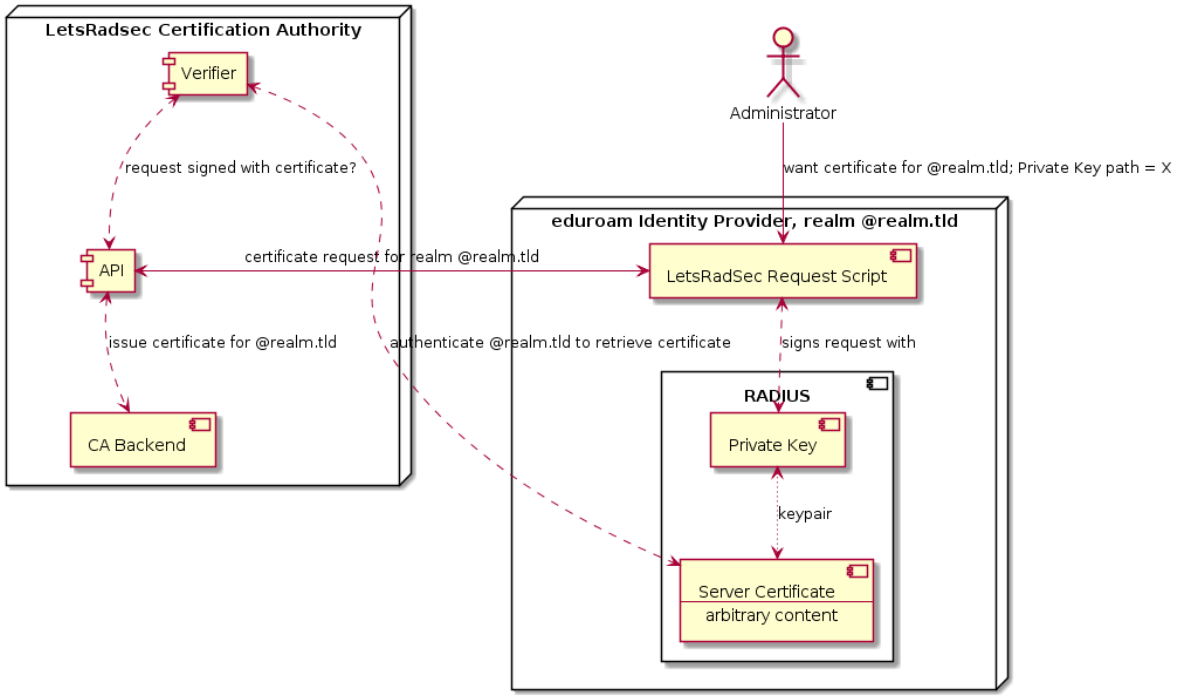

Figure 1: Verification Mechanism for LetsRadsec

The core features of the process are:

- The authorised administrator of a given eduroam realm @realm.tld has access to the corresponding EAP server certificate's private key (which no one else has access to).
- The administrator also knows the realm of their own IdP server in the eduroam infrastructure.
- With that information, the LetsRadsec request script can generate a Certificate Signing Request (CSR) with the realm @realm.tld as part of the certificate name; it can also sign the request using the private key of that realm's EAP server certificate.
- An eduroam authentication request for realm @realm.tld will be delivered via the eduroam infrastructure to the IdP EAP Server.
- The verification component of the LetsRadsec Certification Authority can retrieve the public key of the @realm.tld EAP server via a (made-up) authentication request to the EAP server and can use the public key to verify that the CSR was created with the private key that matches the public key.

This concept ensures that the person who requests a RADIUS/TLS certificate for a realm in eduroam is in possession of the EAP server for that same realm. This proves the authorisation of the requester to get a RADIUS/TLS certificate for the eduroam realm in question.

2.3 Pilot Results

The concept as described in the previous section was implemented successfully on a technical level and all steps verified.

A total of six eduroam NROs were issued at least one LetsRadsec certificate each for an Identity Provider in their constituency. Ten certificates were issued in total.

A total of 44 responses to the complementary survey were received. The majority of respondents were eduroam NROs, followed by eduroam IdP operators. Of those already supporting RadSec, the majority use eduPKI for the purpose. The essential findings of the survey and additional informal interviews with pilot participants were:

- As a general remark, eduroam Identity Providers noted that having to watch over an eventually expiring certificate is a step back compared to the previous “eternal” RADIUS shared secrets. This means that an introduction of LetsRadsec on the IdP level raises the operational complexity of an eduroam IdP deployment.

- eduroam Identity Providers noted that RADIUS servers with the eduroam IdP function are sometimes not exposed to the internet: RADIUS requests from the outside world are delivered to a proxy first, sanitised, and only then forwarded to the actual IdP server. In such deployment scenarios, the proxy server is the one in need of a RadSec certificate, but it does not have the private key of the actual EAP server itself. There are easy workarounds to that by copying the private key to the proxy (for the duration of the certificate request only; the key can safely be deleted afterwards).

- eduroam National Roaming Operators noted that their NRO infrastructure has the most significant need for LetsRadsec certificates. However, NRO servers are typically pure proxies, do not terminate any EAP conversations themselves and thus do not have a private key at all. This makes the LetsRadsec deployment process impractical for NRO-level infrastructure. A workaround of medium complexity exists: reconfigure the NRO-level server to serve a dedicated RADIUS realm as an endpoint that is used solely for the purposes of provisioning LetsRadsec on the device.

- When applying the workarounds for proxies, a further reported complication was that a certificate may be issued towards a specific realm (and that realm is also embedded in the certificate as a subjectAlternativeName property), but the server may serve more than one realm. When the subjectAlternativeName property is enforced, the proxies will appear unauthorised for any other realm they serve. A workaround for this issue was found to be very difficult to implement. One possible approach would be wildcard realms, combined with the ability to enumerate several realms in one certificate. However, all such realms would need to be verified simultaneously during the provisioning (which is conceptually difficult with wildcards), and the certificate would need to be re-issued whenever the list of served realms changes.

- Some eduroam National Roaming Operators want to exercise tight control over all authentication traffic in their country or territory. LetsRadsec however allows individual eduroam IdPs to set up a direct dynamic discovery endpoint, bypassing their NRO-level server

on a technical level. This is inherent to the fully automated provisioning process of LetsRadsec. These NROs noted that it would be preferable to disable the certificate generation altogether for their top-level domain.

- Some participants voiced a fear of losing visibility of statistics at a national and/or international level. While it is true that such an information loss may occur, it is important to stress that eduroam has already implemented a statistics system which does not rely on static request routing of eduroam authentication transactions: F-Ticks, the "federated ticker system", uses out-of-band signalling using Syslog. It aggregates statistics without having to aggregate the corresponding authentication traffic and was created precisely to counter possible information loss. Future attempts at decentralising the eduroam infrastructure should include better communication about its existing ability to gather statistics.

- Participants cited the workload/overhead involved as a significant reason why RadSec has not been adopted, and also expressed a preference for a self-service portal as the primary mechanism for this purpose.

Participants' remarks were then combined with technical analyses to produce recommendations for further work.

3 Conclusions and Next Steps

Overall, the technical implementation of the LetsRadsec pilot was a success. With an actual working concept at hand, all the relevant actors in eduroam were able to evaluate the practicality of the approach.

However, user feedback indicated that while the concept technically works, it does not deliver the expected benefit. the main points that emerged from the feedback received in this respect can be summarised as follows:

- LetsRadsec delivers the ability to perform fully automated provisioning of TLS certificates for RADIUS server interconnection on the IdP level; however, that feature is not considered a high priority by many.

- LetsRadsec does not deliver an easy provisioning for non-IdP participants (regional/national proxies, pure eduroam SP deployments); however, these participants are those who profit the most from having a TLS interconnection. For proxies with a need to maintain full control over all national traffic, it is possible to deploy RADIUS over TLS in a lightweight mode which ensures that they are still seeing the traffic on the national level. Those proxies would need to disable LetsRadsec administratively to retain their operational model.

- There is still demand for easier deployment of RadSec, in particular using a self-service portal. This needs to be considered in the context of wider questions about the decentralisation of eduroam and the relative advantages and disadvantages to NROs and other key participants.

The LetsRadsec concept is therefore not recommended for production deployment within eduroam, and alternative ways of supporting TLS deployment which more accurately reflect the federated delivery model of eduroam will be investigated.

The priority will be to focus on the use case to enable issuing RADIUS/TLS certificates to NROs rather than directly to IdPs. One approach currently of interest is to leverage the existing NRO operator privilege level within the eduroam Configuration Assistant Tool (CAT), allowing such privileged NRO operators to request their certificates directly from the web interface at the click of a button.

References

[Let's Encrypt] https://letsencrypt.org/

Glossary

CA	Certificate Authority
CSR	Certificate Signing Request
EAP	Extensible Authentication Protocol
eduroam CAT	eduroam Configuration Assistant Tool
IdP	Identity Provider
NRO	National Roaming Operator
RADIUS	Remote Authentication Dial-In User Service
RadSec	A protocol for transporting RADIUS datagrams over TCP and TLS
SP	Service Provider
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
X.509 certificate	A standard format of public key certificate used in many Internet protocols