X509v3 EAP Parameter Extension  
draft-rieckers-eapparameterextension-00

Abstract

This document specifies an extension to X509v3 certificates for EAP-TLS servers to mitigate some flaws in the specification to the use of TLS in EAP as specified in RFC5216. The specified extension enables clients to decide whether to trust the certificate presented by the EAP-TLS server by including information implicitly defined by login credentials or communication context in the server certificate.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 5, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
1. Introduction

Logging in with EAP-TLS based methods is a widely used mechanism for password based login with protocols like RADIUS [RFC2865]. Two mechanisms used in WPA2-Enterprise areas are EAP-TTLSv0 and EAP-PEAPv0. Unfortunately, the specification of EAP-TLS does not specify how the EAP-TLS peer can verify that the certificate presented by the server is valid apart from the Key Usage identifiers and user set configuration parameters.

The configuration parameters include especially the information about the trust anchor and the expected domain.

In contrast to the usage of X509v3 certificates in other contexts, such as HTTPS, in EAP-TLS the expected name can not be distinguished...
from the context of the communication. This requires users to configure their supplicants accordingly. Especially in large setups with private devices this has led to insecure configurations with insufficient or even wrong name checks. Some security considerations for EAP-TLS in deployment in eduroam have been named in [RFC7593], Section 7.1.

The same basic security considerations apply for the certificate based login methods as they apply for password based methods, but are not that critical, since an attacker can not gain knowledge of the supplicant’s private key with an attack based on insufficient server certificate validation done by the peer.

The aim of the extension introduced in this document is to give EAP-TLS peers an option to check the certificate of the EAP-TLS server against parameters implicitly defined by the communication context.

2. Definitions

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Terminology

Readers are expected to be familiar with the terms and concepts used in EAP [RFC3748] and EAP-TLS [RFC5216].

In particular, this document frequently uses the following terms:

EAP-TLS server: The entity that authenticates the clients and is termination point of the EAP-TLS tunnel.

peer or supplicant: The client that authenticates to the server in order to gain access to the protected resource.

EAP Identity: The Identity sent by the peer in the first (unencrypted) EAP Identity Response as specified in [RFC3748] Section 5.1.
3. Syntax

TODO
There shall be a ASN.1 module in Appendix A

The EAP Parameter extension has the following format:

id-pe-eapparameter OBJECT IDENTIFIER ::= { id-pe XX }

EAPParameterValues ::= SEQUENCE {
  EAPParameterType OBJECT IDENTIFIER,
  EAPParameterValue OCTET STRING
}

EAPParameter ::= SEQUENCE OF (1..MAX) EAPParameterValues

The extnValue of the id-pe-eapparameter extension is the ASN.1 DER encoding of the EAPParameter structure.

The EAP Parameter extension MAY be marked as critical. Certificate Authorities SHOULD allow both, critical and not critical, in their application process for a certificate with this extension, so applicants can choose. Making the extension critical may not be desirable in the early future after the release of this RFC, but, when marked critical, it will help forcing users to update their devices, which might be, at least in the authors opinion, a good idea. This makes use of the specification of the handling of critical extensions, specified in [RFC5280]: Any supplicant not understanding a critical extension MUST reject the certificate if it does not understand this extension.

4. EAP Parameter Types

This RFC specifies several EAP Parameter Types. Other parameter types MAY be specified in the future. The handling of new parameters is described in Section 4.4

4.1. Realm Suffix types

The Realm Suffix types can be used to bind the certificate to a specific realm. It is either a realm separated by ‘@’ (EAPPARAMETERBASEOID.1) or a realm separated by ‘%’ (EAPPARAMETERBASEOID.2)

TODO: Reference to NAI [RFC7542] for Realms. Maybe even remove the ‘%’ seperated realm, since I have not found any usage. This is only here because it is in a default configuration file of FreeRADIUS
4.1.1. Syntax

The EAPParameterValue for these types is a DER-encoded UTF8String containing the full realm of the outer username. This is supposed to be a FQDN. It MAY not be a FQDN for testing purposes but MUST NOT contain the separator character, depending on the Suffix type. The value MAY contain one asterisk to indicate a wildcard validity for all realms under a specific domain. The asterisk MUST be the first character and MUST be followed by a dot. A certificate containing only an asterisk and a dot MUST NOT be issued by a trusted certificate authority.

4.1.2. Validation

To verify the supplicant will compare the sent EAP Identity with the realm contained in the EAPParameterValue. If the EAPParameterValue is not in a valid format, the supplicant MUST reject the certificate and SHOULD send a fatal bad_certificate alert (see [RFC5246], [RFC8446]). If the value contains an asterisk, the realm part should be matched as the dnsName of subjectAltName attribute would be matched.

4.1.3. CA Requirements

A trusted CA MUST validate that the applicant is authorized to request certificates under the domain represented by the realm. CAs SHOULD rely additionally on the CAA issuewild DNS value and SHOULD NOT issue a certificate with this extension if the CAA value forbids wildcard certificates.

4.2. Identity

The Identity Parameter Type can be used to bind the server certificate to use with a specific EAP Identity.

4.2.1. Syntax

The EAPParameterValue for this type is a DER-encoded UTF8String containing the full EAP Identity.

The value MAY contain up to two asterisks, one for the local part of the Identity, one for the realm. This can be used to allow EAP-Identities with variable parts. If two asterisks are used, the
certificate extension MUST also contain an EAPParameter for
verification of the Realm (e.g. Realm Suffix, separated by ‘@’)

The asterisk for the realm part follows the same rules as described
in the Realm suffix type.

The asterisk for the local part MAY be at any position.

4.2.2. Validation

To verify this parameter the supplicant has to verify the sent EAP
Identity and the parameter value in the certificate match. The
supplicant SHOULD do this with a case insensitive comparison.

TODO: Here should also be a description how to deal with asterisks.

4.2.3. CA Requirements

The CA requirements for this type depend on the used Identity format.

If the Identity is in a format that would also allow Realm Suffix
Types (e.g. separated by @ or %) for the domain part the same CA
Requirements as for the defined Realm Suffix Types apply. CAs SHOULD
allow the local part to be chosen by the certificate requestor inside
normal parameters.

Globally trusted CAs MUST NOT issue certificates with the Identity
EAP Parameter Type if it does not contain a Realm or the Realm can
not be mapped to a DNS name.

4.3. Login Medium

EAPPARAMETERBASEOID.4

TODO
This is intended to limit the validity of the certificate to e.g.
802.1x authentication

4.3.1. Syntax

4.3.2. Validation

4.3.3. CA Requirements
4.4. Handling of future EAP Parameter Types

TODO

5. IANA Considerations

TODO: Here the IANA considerations should be updated. The decimal id of the id-pe-eapparameter will be registered once the draft has reached a state where proof of concept implementations can be made.

On approval, IANA shall add in the SMI Security for PKIX Certificate Extension (1.3.6.1.5.5.7.1) registry the following entry:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>XX</td>
<td>id-pe-eapparameter</td>
<td>{this RFC}</td>
</tr>
</tbody>
</table>

Additionally the IANA shall install a new registry for PKIX Certificate Extension EAP Parameter Types for the parameter types with the following initial content:

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Realm Suffix, separated by '@'</td>
<td>{this RFC}</td>
</tr>
<tr>
<td>2</td>
<td>Realm Suffix, separated by '%'</td>
<td>{this RFC}</td>
</tr>
<tr>
<td>3</td>
<td>Identity</td>
<td>{this RFC}</td>
</tr>
<tr>
<td>4</td>
<td>Login Medium</td>
<td>{this RFC}</td>
</tr>
</tbody>
</table>

TODO: Here there may be also defined Realm Prefix Types (e.g. WINDOWS-NET/username). Obviously this can’t be issued by a globally trusted CA, but might be issued by a company CA.

Further EAP Parameter Types may be registered in future. New registration requests MUST include a detailed description how peers should validate the given parameter and a detailed description for Certificate Authorities how they must verify the authorization of a certificate request with this parameter.
6. Security Considerations

TODO
There will be security considerations. There are security considerations which lead to this draft.

Here might be a reference to [RFC4334]. It specifies X509v3 extensions to help the supplicant to choose the client certificate used for login based on connection parameters such as SSID or Login Medium.

7. References

7.1. Normative References


7.2. Informative References


Appendix A. ASN.1 Modular

This is obviously also an open TODO

Acknowledgements

There will be acknowledgements. I haven’t done the work all by myself and a lot of people should and will be listed here for supporting me in all my work.

Carsten Bormann, ...

Author’s Address

Jan-Frederik Rieckers
Universitaet Bremen
Bibliothekstr. 5
Bremen 28359
Germany

Email: rieckers@uni-bremen.de