

ROAMOPS Working Group
INTERNET-DRAFT
Category: Best Current Practice
<[draft-ietf-roamops-cert-01.txt](#)>
1 April 1999

Bernard Aboba
Microsoft

Certificate-Based roaming

1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. 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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

To view the list Internet-Draft Shadow Directories, see
<http://www.ietf.org/shadow.html>.

The distribution of this memo is unlimited. It is filed as <[draft-ietf-roamops-cert-01.txt](#)>, and expires October 1, 1999. Please send comments to the authors.

2. Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

3. Abstract

This document describes how scalable, secure roaming can be supported based on public key certificates, the Extensible Authentication Protocol (EAP), and the RADIUS protocol. The practices described in this document eliminate the use of intermediate proxies, improving scalability and security. They are compliant with the evaluation criteria described in [RFC 2477](#).

INTERNET-DRAFT

Certificate-Based Roaming

1 April 1999

[4.](#) Introduction

As noted in [\[1\]](#), existing roaming implementations have largely been based on the concept of proxy chaining, where packets are forwarded between the NAS and home server through a series of proxies.

As described in [\[8\]](#), roaming implementations based on proxy chaining typically provide only hop-by-hop authentication and integrity protection. These security weaknesses make proxy-based roaming vulnerable to attack as well as susceptible to misconfiguration. Security threats, described in [\[8\]](#) include theft of service as well as misuse of hidden attributes (such as PAP passwords) by untrusted proxies. Misconfiguration issues include policy implementation and attribute editing, support for RADIUS extensions as described in [\[12\]](#), shared secret maintenance and routing.

Note that providing end-to-end security within a proxying scheme further increases the complexity of the system and introduces its own set of issues. For example, in order to allow the end systems to verify message authenticity and integrity, a keyed MAC such as that described in [\[6\]](#) can be used. Alternatively, the packet may be digitally signed. Signing each packet in a AAA exchange is computationally intensive, particularly if EAP authentication is involved. On the other hand, a keyed MAC requires an automated key-exchange mechanism in order to permit deployment on a large scale, and introduces complications with respect to policy implementation.

In order to implement policy, it is necessary to permit a proxy to send an Accept-Reject to the NAS in cases where an Access-Accept has been sent by the home server. As described in [\[8\]](#), the home server is notified of this by having the proxy send an Accounting-Request to the home server with Acct-Status=Proxy-Stop. However, with end-to-end security, such policies cannot be implemented, since the NAS cannot accept an Access-Reject that is not authenticated by the end-system (home server). Similarly, the home accounting server cannot accept a non-authenticated Accounting-Request from the proxy, notifying it of the policy action.

In addition to security and policy issues, there are performance problems with proxy-based roaming. The introduction of proxy forwarding

multiplies the number of packets that must be sent in order to authenticate and authorize the user, increasing login time and increasing the likelihood of a timeout. This problem is particularly severe when EAP authentication is used.

For these reasons, as noted in [8], proxy-based roaming is not appropriate for wide-scale use on the Internet.

This document describes an alternative to proxy-based roaming which is based on the use of public key certificates and EAP authentication. Since public key authentication allows the local RADIUS server to verify the identity of the client without the need to proxy the authentication, the use of proxies is eliminated while still permitting the local proxy to implement policy. The result is that certificate-based roaming is simpler and easier to implement operationally than proxy-based roaming, as well as being more secure. As a result, certificate-based roaming is able to meet the criteria outlined in [2] without requiring the development of a new AAA protocol.

In order to implement the practices described in this document, the NAS MUST support EAP, described in [9], as well as RADIUS extensions, described in [12]. The local RADIUS server MUST support EAP and RADIUS extensions as well as a public-key authentication authentication method such as EAP-TLS, described in [11]. The client MUST support EAP as well as a public-key authentication method such as EAP-TLS. While there is no requirement that the home server implement EAP, EAP-TLS or even RADIUS, it is necessary for the local RADIUS server to determine that the certificate presented by the client remains valid. As a result, the entities involved in the trust chain MUST provide Certificate Revocation Lists (CRLs).

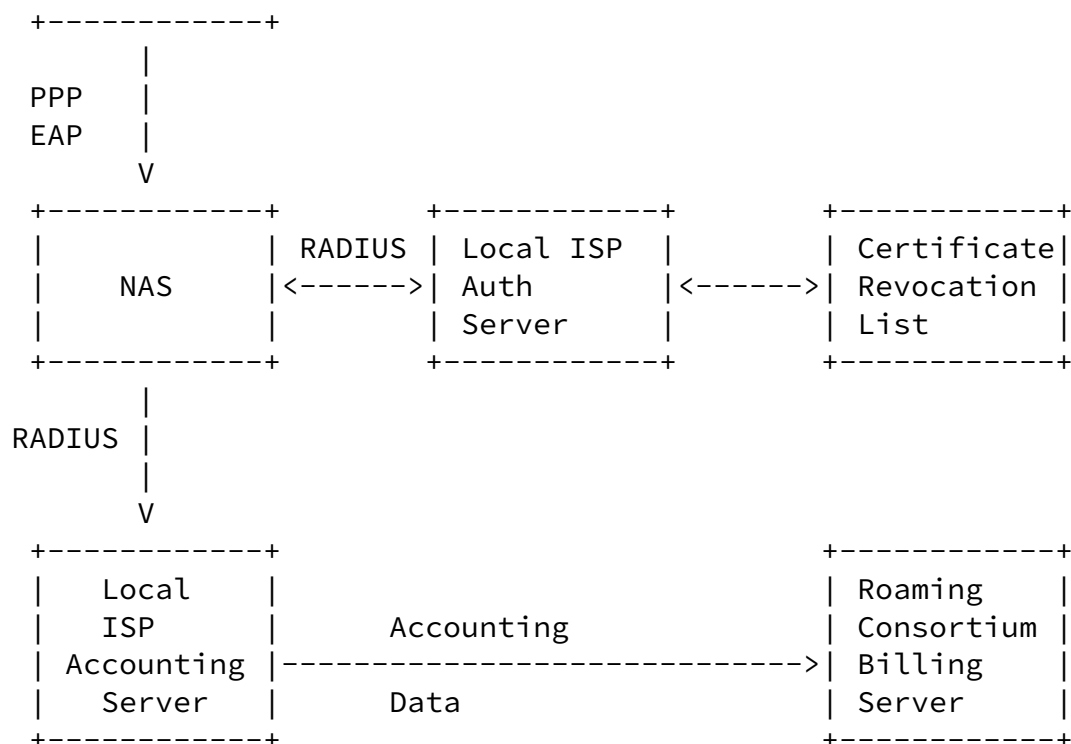
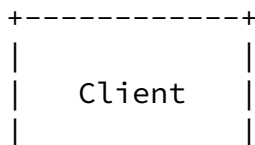
[5.](#) Requirements language

In this document, the key words "MAY", "MUST", "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [7].

[6.](#) Overview

In certificate-based roaming, the client authenticates to the NAS using a public-key certificate-based authentication protocol running over EAP, such as EAP-TLS, described in [11]. In order to permit the NAS to handle a variety of authentication protocols without understanding the details, in EAP [9] the NAS acts as a "pass through" device, forwarding EAP packets between the client and the local ISP RADIUS server, using the RADIUS extensions documented in [12].

A diagram of the authentication, authorization and accounting process is shown below:



Through use of certificate-based authentication, it is possible for the local ISP RADIUS server to verify the user's identity without the need to proxy the authentication to the home server. The use of public key certificates makes this possible, since the local ISP server is capable of verifying that the user has access to the private key corresponding

to the public key included on the user's certificate. Note however, that as part of the authentication process, the local ISP server will need to check for revocation of the certificates in the trust chain. Depending on the trust model, one or more Certificate Revocation List (CRL) servers may be contacted. These may include CRL server within the home domain or that of the roaming consortium.

Since the home server is not involved in the RADIUS authentication/authorization conversation, the authorization attributes are determined by the local ISP, based on information provided in the authentication process. For example, the local ISP could determine the authorization profile based on the realm included in the Network Access Identifier (NAI) described in [3], or based on the Certifying Authority (CA) included in the user certificate. Today, the most frequently provided roaming service is PPP access to the Internet, so that realm or CA-based authorization is adequate in most cases. Note that per-user authorizations can be supported within certificate-based roaming without requiring the local RADIUS server to proxy the request back to the home server. This can be accomplished via use of attribute certificates.

In certificate-based roaming, accounting services can be provided either via session records or in real time via RADIUS Accounting, described in

[5]. Note that since the home server is not involved in the authentication and authorization process, the local ISP MAY wish to provide the roaming consortia or home organization a means to audit the accounting information. One possible means of demonstrating the authenticity of the accounting data is to include credentials supplied by the user.

[6.1.](#) Authentication

[6.1.1.](#) Authentication conversation

As noted in [9], the EAP conversation between the client and NAS typically begins with the NAS sending an EAP-Request/Identity message to the client. The NAS then sends a RADIUS Access-Request to the local ISP RADIUS server, containing an EAP-Message attribute. Based on the Access-Request, the local ISP RADIUS server determines the EAP method to be

used, and sends an Access-Challenge containing an EAP-Response attribute to the NAS. Since certificate-based roaming does not involve proxies, the determination of the client's EAP type MUST be made based on the Network Access Identifier (NAI) supplied by the client, as described in [3]. For example, the local ISP RADIUS server MAY be configured to use a given EAP authentication type for all members of a given realm, or it MAY implement a default type. However, since the client certificate has not yet been presented to the local RADIUS server, information on the certificate such as the certificate authority, or other attributes cannot be taken into account in determining the EAP authentication method to be used to authenticate the client.

The EAP conversation between the local ISP RADIUS server and the client continues as described in [12] with the NAS serving as a passthrough device until the NAS receives an EAP-Success or EAP-Failure message.

In order to implement certificate-based roaming, the client MUST support a certificate-based EAP authentication method such as EAP-TLS, described in [11]. EAP-TLS, which is based on the TLS protocol described in [10], supports mutual authentication as well as key derivation. As a result, it permits the client to authenticate the RADIUS server as well as for the RADIUS server to authenticate the client. Note that since the client is not yet online, it is not possible for it to check for revocation of the server's certificate. However, the client MAY check for server certificate revocation after access has been granted. Since the RADIUS server has Internet connectivity, it MUST check whether the client's certificate has been revoked prior to granting access.

[6.1.2.](#) Trust models

In proxy-based roaming, the home server demonstrates willingness to pay by responding to the proxied Access-Request with an Access-Accept. In certificate-based roaming, the home server is not involved in the authentication/authorization conversation, so that another approach is needed.

In order for the local ISP to be willing to grant the client access to a Point of Presence (POP), it is necessary for a chain of trust to be established between the client and the local ISP. In the simplest case this can be accomplished by having the client present a certificate

signed by a trusted third party, such as a roaming association to which the local ISP belongs. Note that in order to verify that the client certificate remains valid, the local authentication server MUST check the Certificate Revocation List (CRL) maintained by the certificate authority. For the simple case, this implies that the roaming association would issue and revoke roaming certificates itself.

However, rather than dealing with end-users, the roaming association may prefer to only issue roaming certificates to participating ISPs or customers such as BIGCO. This allows the roaming association to delegate roaming certificate issuance and maintenance to other trusted entities. In this case, it is necessary for the client to submit a certificate chain, providing not only the roaming certificate issued by an ISP or company, but also the company or ISP roaming certificate issued by the roaming association. The combination of these roaming certificates then establishes the required chain of trust.

Note that the local ISP RADIUS server MUST check for revocation of each certificate presented in the certificate chain. Thus, the local ISP needs to check not only that the user certificate has not been revoked by the home ISP or company, but also that the home ISP or company's certificate has not been revoked by the roaming association.

[6.2.](#) Authorization and policy

Once the client has authenticated, it is necessary for the local RADIUS server to formulate the authorization attributes to be returned to the NAS. These attributes can be determined by information provided during the authentication, such from the NAI realm or the certificate authority, as well as by policy. For example, the local ISP could provide a default set of attributes for all non-local realms, or for all users whose chain of trust includes a given roaming association. It is also possible for the local RADIUS server to modify the attribute set based on policy, i.e. to return a smaller Session-Time when twenty or more users are logged in from a given realm.

Note that without attribute certificates it is not possible to support per-user authorizations. For example, if Bob and Jane have certificates signed by the same CA, and if it is desired to treat bob@bigco.com and jane@bigco.com differently, then this cannot be accomplished based solely on the NAI and the certifying authority. Some other information

must be brought into play. Since in certificate-based roaming proxying back to the home server is not acceptable, the required input is supplied as part of the user's certificate.

6.3. Accounting

Once the client has been authenticated and authorized, the local ISP will be interested in obtaining compensation for the use of network resources. In order to accomplish this, the local ISP can use either real-time or batch accounting.

When batch accounting is used, the local ISP will transmit session record batches to the settlement agent. In real-time accounting, an Accounting-Request is sent to the settlement agent. As discussed in [8], the settlement agent MAY respond to the request directly, or MAY proxy it to other parties on the roaming relationship path.

Note that with certificate-based roaming, the situation differs from the proxy approach in that the systems along the roaming relationship path have not previously participated in a proxied authentication/authorization conversation prior to receiving accounting data.

This has several implications. Firstly, the systems receiving the accounting data do not have a means to correlate the accounting information received with a previous authentication event. In the proxy approach, the use of a unique session-ID allows accounting records to be matched up with the corresponding authentication/authorization request. While in certificate-based roaming the local ISP will have contacted the relevant Certificate Revocation List (CRL) servers in order to check for certificate revocation, no session-ID is generated in this conversation that would allow linking to the relevant accounting record.

Secondly, using the session-ID, in proxy roaming a home server receiving an accounting record is able to link this back to an authentication conversation in which the user credentials were verified. As a result, barring replay attacks, it is possible to audit whether the accounting data corresponds to an Access-Accept sent by the home server. This provides some degree of protection against fraudulent submission of accounting data on non-existent sessions.

To provide equivalent protection in certificate-based roaming, it is necessary for the local ISP to supply user credentials in the accounting data. This permits parties on the roaming relationship path to verify that a valid authentication occurred. In the case of EAP-TLS, this can be accomplished by including the Nonce sent by the server, along with the signed response sent by the client, using the private key. Given these two pieces of information, and access to the client certificate, it is possible for a third party to verify that the client was authenticated.

[7. RFC 2477](#) Compliance

Certificate-based roaming complies with the evaluation criteria specified in [RFC 2477](#).

Connection Management

Certificate-based roaming supports PPP, as well as IP and non-IP protocols.

Identification

Certificate-based roaming supports the NAI as described in [\[3\]](#).

Authentication types

Certificate-based roaming is based on EAP and certificate-based authentication protocols such as EAP-TLS. PAP and CHAP are not supported.

Scalability

Certificate-based roaming is sufficiently scalable to allow the formation of roaming associations with thousands of ISP members.

RADIUS Support

Certificate-based roaming is compatible with RADIUS-enabled devices implementing EAP [\[9\]](#) and RADIUS extensions [\[12\]](#).

NAS Configuration/Authorization

Since in certificate-based roaming authorization parameters are determined by the local RADIUS server, a wide range of authorization profiles and policies may be implemented.

Address assignment/routing

Certificate-based roaming supports dynamic address assignment. Static address assignment may also be supported via layer 2 or layer 3 tunneling.

INTERNET-DRAFT

Certificate-Based Roaming

1 April 1999

Layer 2 tunneling protocols

Certificate-based roaming is compatible with layer-2 tunneling. Note that without attribute certificates, per-user tunneling cannot be supported. Thus compulsory tunnels may only be brought up based on information obtained in the authentication, i.e. realm or CA-based tunneling.

Layer 3 tunneling protocols

Certificate-based roaming is compatible with Mobile IP.

Security analysis

Certificate-based roaming addresses fraud prevention and detection issues through inclusion of credentials within the accounting packet.

Hop by hop security

Certificate-based roaming supports hop-by-hop integrity protection and confidentiality via use of IPSEC.

End-to-end security

As certificate-based roaming does not involve proxies, the authentication conversation occurs solely between the local NAS and the RADIUS server. As a result, policy implementation is supported while eliminating attacks by rogue proxies.

[8. Security issues](#)

The following security threats have been identified in roaming systems:

- Rogue proxies
- Theft of passwords
- Theft of accounting data
- Replay attacks
- Connection hijacking
- Fraudulent accounting

Certificate-based roaming reduces or eliminates each of these threats.

[8.1. Rogue proxies](#)

In certificate-based roaming, authentication and authorization terminates at the local ISP RADIUS server. As a result, the risk of rogue proxies is eliminated.

INTERNET-DRAFT

Certificate-Based Roaming

1 April 1999

[8.2.](#) Theft of passwords or keys

Since certificate-based roaming only supports certificate-based authentication without proxies, in no circumstance will the local ISP proxy have access to PAP passwords.

While a key is generated as part of the EAP-TLS authentication, this can be communicated between the local RADIUS server and the NAS without passing through a proxy. In order to protect the key, IPSEC ESP SHOULD be used between the RADIUS server and the NAS.

[8.3.](#) Integrity and confidentiality of accounting data

Since certificate-based roaming does not involve proxies, integrity and confidentiality of accounting data can be provided via IPSEC.

[8.4.](#) Connection hijacking

Since certificate-based roaming avoids proxying of authentication and authorization, the risk of connection hijacking is reduced.

[8.5.](#) Fraudulent accounting and replay attacks

In order to prevent the local ISP from requesting payment for non-existent sessions, it is desirable for the accounting record to include proof of authentication. This can be provided by including the credentials supplied by the client within the accounting record. For example, in the case of EAP-TLS, the accounting record can include the Nonce supplied by the server, as well as the signature returned by the client that proves the client's possession of the private key corresponding to the client certificate.

Since the Nonce will vary with each authentication, it is not possible for the local ISP to replay the authentication. This therefore limits the local ISP's ability to fraudulently claim payment for non-existent sessions.

Through use of a signed Nonce, certificate-based roaming prevents accounting for non-existent sessions. Note that as with proxy roaming, no protection is provided against submission of exaggerated session times for actual sessions.

9. References

- [1] Aboba, B., Lu J., Alsop J., Ding J., and W. Wang, "Review of Roaming Implementations", [RFC 2194](#), September 1997.
- [2] Aboba, B., and G. Zorn, "Criteria for Evaluating Roaming Protocols", [RFC 2477](#), January 1999.
- [3] Aboba, B., and M. Beadles, "The Network Access Identifier", [RFC 2486](#), January 1999.
- [4] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April, 1997.
- [5] Rigney, C., "RADIUS Accounting", [RFC 2139](#), April 1997.
- [6] Rivest, R., Dusse, S., "The MD5 Message-Digest Algorithm", [RFC 1321](#), April 1992.
- [7] Bradner, S., "Key words for use in RFCs to Indicate Requirement

Levels", [BCP 14](#), [RFC 2119](#), March 1997.

- [8] Aboba, B., Vollbrecht, J.R., "Proxy Chaining and Policy Implementation in Roaming", Internet draft (work in progress), [draft-ietf-roamops-auth-10.txt](#), February 1998.
- [9] Blunk, L., Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", [RFC 2284](#), March 1998.
- [10] Dierks, T., Allen, C., "The TLS Protocol Version 1.0", [RFC 2246](#), November 1998.
- [11] Aboba, B., Simon, D., "PPP EAP TLS Authentication Protocol", [draft-ietf-pppext-eaptls-05.txt](#), Internet Draft (work in progress), January 1999.

Aboba

Standards Track

[Page 11]

INTERNET-DRAFT

Certificate-Based Roaming

1 April 1999

- [12] Rigney, C., Willens, S., Calhoun, P., "RADIUS Extensions", [draft-ietf-radius-ext-03.txt](#), Internet Draft (work in progress), January 1999.

[10.](#) Acknowledgments

Thanks to Ashwin Palekar of Microsoft for useful discussions of this problem space.

[11.](#) Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 206-936-6605
EMail: bernarda@microsoft.com

12. Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.
This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English. The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns. This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."

13. Expiration Date

This memo is filed as <[draft-ietf-roamops-cert-01.txt](#)>, and expires October 1, 1999.

