

MOONSHOT
Internet-Draft
Intended status: Standards Track
Expires: January 27, 2011

H. Tschofenig
Nokia Siemens Networks
July 26, 2010

Federated Authentication Beyond The Web: Problem Statement and
Requirements

draft-tschofenig-moonshot-ps-01.txt

Abstract

It is quite common that application developers and system architects are in need for authentication and authorization support in a distributed environment. At least three parties need to cooperate, namely the end host, the identity provider, and the relying party. At the end of the exchange the identity provider asserts identity information or certain attributes to the relying party without exposing the user's long-term secret to the relying party.

Although the problem sounds challenging and interesting, it is not new. In fact, various IETF groups have produced specifications to solve this problem, such as Kerberos, RADIUS, and Diameter. Outside the IETF various Single-Sign-On solution for HTTP-based applications have been developed as well.

The reader might therefore wonder about the need for new work given the existence of readily available solutions. This document tries to answer this question in a compact fashion. Note that the description in this document focuses on the scope of the new work as part of the "Federated Authentication Beyond The Web" BOF being proposed rather than what could be theoretically done.

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 <http://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."

Internet-Draft

Federated Auth. Beyond The Web: PS

July 2010

This Internet-Draft will expire on January 27, 2011.

Copyright Notice

Copyright (c) 2010 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 (<http://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 the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	4
2.	Terminology	7
3.	Assumptions and Requirements	8
4.	Security Considerations	10
5.	IANA Considerations	11
6.	Acknowledgments	12
7.	References	13
7.1.	Normative References	13
7.2.	Informative References	13
	Author's Address	14

1. Introduction

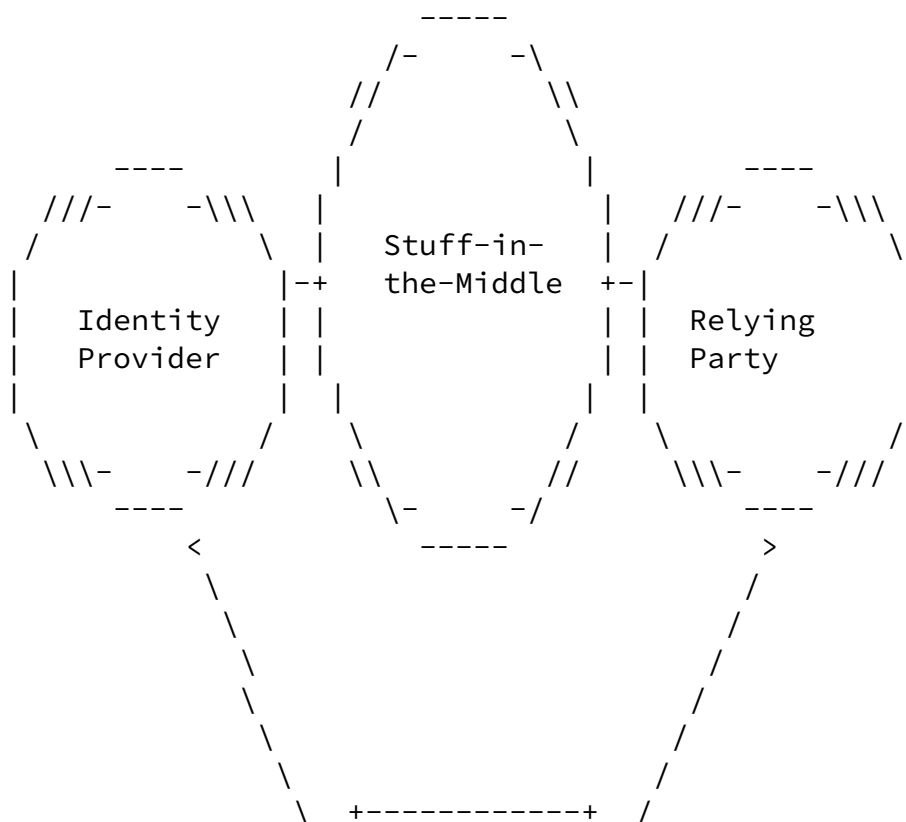
The typical setup for a three party protocol involves the End-host, the identity-provider and relying party as illustrated in Figure 1. It might be of surprise that there are actually four parties shown in Figure 1; we will address the invisible party in the middle a little bit later.

With three party protocols there are a number of different protocol variants possible, as the available crypto-literature shows. We will not discuss the different options in this document. What is relevant is that a real world entity is behind the end host and responsible for establishing some form of contract with the identity provider, even if it is only as weak as completing a web form and confirming the verification email. The outcome of this initial registration step is that credentials are made available to the identity provider and to the end host (or the user). It is important to highlight that in some scenarios there might indeed be a human behind the device denoted as end host and in other cases there is no human involved in the actual protocol execution.

We assume that the identity provider and the relying party belong to different administrative domains. Very often there is some form of relationship between the identity provider and the relying party. This is particularly important when the relying party wants to use information obtained from the identity provider for authorization decisions and when the identity provider does not want to release information to every relying party (or only under certain conditions). While it is possible to have a bilateral agreement

between every identity provider and every relying party; on an Internet scale this setup does require some intermediary, the "stuff-in-the-middle". Please note that the lack of scalability is not caused by technical limitations but rather by business limitations since the agreements between identity providers and the relying parties are often business contracts that are financially motivated. The "stuff-in-the-middle" is a placeholder for technical interoperability as well as business practices and operational arrangements, many aspects are outside the scope of the IETF.

Agreed terminology for what is labeled as generically "stuff-in-the-middle" is unfortunately not available. Sometimes the term "identity federation", or "trust framework" are used. To make it worse, different terminology is used when looking at specific protocols.



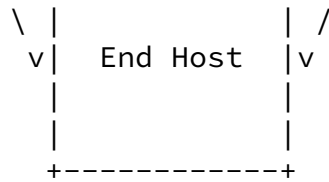


Figure 1: Three Party Authentication Framework

Designing new three party authentication and authorization protocols is hard and cryptographic flaws common in designs. Achieving widespread deployment is even more difficult. The HTTP-based Web has enjoyed a lot of attention from the industry with respect to this problem and some amount of success can be noticed even though many of the business aspects with the "stuff-in-the-middle" still has to be sorted out. This document does not focus on an HTTP-based environment and instead focuses on those protocols where HTTP is not used. Despite the increased excitement for layering every protocol on top of HTTP there are still a number of protocols available that do not use HTTP-based transports. Many of these protocols are lacking an authentication and authorization framework of the style shown in Figure 1.

Interestingly, for network access authentication the usage of the AAA framework with RADIUS [[RFC2865](#)] and Diameter [[RFC3588](#)] was quite successful from a deployment point of view. To map the terminology used in Figure 1 to the AAA framework the identity provider

corresponds to the AAA server, the relying party corresponds to the AAA client, and the "stuff-in-the-middle" are AAA proxies and relays (particularly if they are operated by third parties, such as AAA brokers and clearing houses). The front-end, i.e. the end host to AAA client communication, is in case of network access authentication offered by link layer protocols that forward authentication protocol exchanges back-and-forth.

Is it possible to design a system that builds on top of successful protocols to offer non-Web-based protocols with a solid starting point for authentication and authorization in a distributed system?

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

[3.](#) Assumptions and Requirements

Some requirements restrict the solution space more than others. In this particular case the main requirement is to re-use an existing infrastructure, namely the AAA framework. Briefly stated: The solution **MUST** make use of the AAA infrastructure (RADIUS and Diameter). Ideally, modifications at AAA servers **SHOULD** be kept at a minimum. Modifications to the AAA infrastructure that affect operational aspects **MUST NOT** be made.

The next requirement concerns security: The relying party **MUST NOT** get in possession of the long-term secret of the entity that is authenticated towards the AAA server. Since there is no single authentication mechanism that will be used everywhere there is another associated requirement: The authentication framework **MUST** allow for the flexible integration of authentication mechanisms.

Those who are familiar with the AAA framework might realize that the choices are limited. The standardized Extensible Authentication Protocol (EAP) framework [[RFC3748](#)] fits the above requirements and is widely deployed.

Assuming that this design decision is taken for granted the remaining work is with the integration of the AAA infrastructure into non-Web-based application protocols. Figure 2 illustrates it graphically.

The changes to the end host and the changes to the relying party SHOULD be kept at a minimum. A mechanism that can demonstrate deployment benefits (based on ease of update of existing software, low implementation effort, etc.) MUST be preferred. There MAY be a need to specify multiple mechanisms to support the range of different

deployment scenarios.

Tschofenig

Expires January 27, 2011

[Page 9]

Internet-Draft

Federated Auth. Beyond The Web: PS

July 2010

[4.](#) Security Considerations

This entire document is about security.

[5.](#) IANA Considerations

This document does not require actions by IANA.

[6.](#) Acknowledgments

The author would like to thank Sam Hartman for a discussion about all aspects of the "Federated Authentication Beyond The Web" effort when he was visiting MIT in June 2010.

I would like to thank Mayutan Arumaithurai and Klaas Wierenga for their feedback.

[7.](#) References

[7.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.
- [RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", [RFC 3588](#), September 2003.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.

- [RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", [RFC 3579](#), September 2003.
- [RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", [RFC 4072](#), August 2005.

[7.2.](#) Informative References

- [I-D.nir-tls-eap]
Nir, Y., Sheffer, Y., Tschofenig, H., and P. Gutmann, "TLS using EAP Authentication", [draft-nir-tls-eap-08](#) (work in progress), July 2010.
- [I-D.howlett-eap-gss]
Hartman, S. and J. Howlett, "A GSS-API Mechanism for the Extensible Authentication Protocol", [draft-howlett-eap-gss-00](#) (work in progress), March 2010.

Tschofenig Expires January 27, 2011 [Page 13]

Internet-Draft Federated Auth. Beyond The Web: PS July 2010

Author's Address

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: <http://www.tschofenig.priv.at>

