

Overview and Comparison of Inter-domain Authentication Protocols

Henk Eertink[♦], Arjan Peddemors[♦], Remco Poortinga[♦], Roy Arends[♦] and Klaas Wierenga[‡]

[♦]INCA Group, Telematica Instituut, Postbus 589, Enschede, The Netherlands
{Henk.Eertink, Arjan.Peddemors, Remco.Poortinga, Roy.Arends}@telin.nl

[‡]SURFnet, Postbus 19035, Utrecht, The Netherlands
Klaas.Wierenga@SURFnet.nl

Keywords Network Roaming, Authentication Infrastructure, Comparison, Dynamic Trust Establishment, RADIUS, Secure Domain Name System, DIAMETER

Extended Abstract

The RADIUS-based configuration currently widely used for the authentication of roaming network users that move between the networks managed by different authorities has a number of well known limitations and drawbacks [4]. This paper provides an overview and comparison of advanced roaming protocols that tackle all or most of these disadvantages. The results are used, within the context of the *GÉANT2 JRA5/EduRoam-NG* initiative, as input for the decisions on the roaming configuration that will replace the existing *EduRoam* [3] infrastructure.

Two of the most important aspects, given the *GÉANT2* requirements, are 1) the introduction of a mechanism for dynamic trust establishment and 2) improvements in scalability. These requirements typically translate into: the parties involved in an authentication or authorization action set up direct on-the-fly peer to peer connections for communication. In that case, no RADIUS [6] tree traversing as with the current *EduRoam* setup is necessary. Another important consideration is the compatibility with existing *EduRoam* configurations. The alternatives compared here are (see also below): DIAMETER [2], RadSec [5], RADIUS-DNSSEC [4], and RadDNSSEC. These all are capable of establishing dynamic peer to peer connections for authentication.

Connection setup between peers consists of *peer discovery* and *trust establishment*. The peer discovery step answers the question: which server handles authentication and authorization requests for the user's realm? The trust establishment confirms that the peer (or the user's realm) is part of the roaming domain. For the alternatives under consideration here, peer discovery is performed using the Domain Name System (DNS), either 'ordinary' DNS or (secured) DNSSEC [1]. For the confirmation of participation in the roaming domain, the alternatives either use a Public Key Infrastructure (PKI) or, again, DNS (in the form of DNSSEC).

The *DIAMETER* protocol is positioned as the successor of RADIUS. Contrary to RADIUS, the *DIAMETER* standard has various features that explicitly support inter-domain roaming. *DIAMETER* can support different kinds of 'roaming models': we focus mostly on the model with peer discovery through DNS and trust establishment based on the PKI.

RadSec is the name for a new, non-standard, implementation of the RADIATOR RADIUS server. The essential part of this approach is that the – dynamic – trust-establishment is done in a TLS key-exchange handshake based on PKI, and the RADIUS transport is changed from traditional UDP messages into a TLS connection. It incorporates some of the advantages of *DIAMETER* while maintaining easy integration with the installed base of RADIUS.

RADIUS-DNSSEC is based on using DNS both for peer-discovery and for trust establishment and RADIUS for authentication. The trust establishment for the interaction is based on the availability of a dedicated roaming domain secure DNS tree. All the participating servers trust this tree: all other trust during interaction is derived from this. This means that trust establishment is essentially the same as with the PKI based solutions *DIAMETER* and *RadSec*.

RadDNSSEC is mixing RadSec with RADIUS-DNSSEC. All peer interaction is as with RadSec, but PKI usage is replaced by DNSSEC usage. The difference with RADIUS-DNSSEC consists of the peer connections: these are over TCP/TLS instead of UDP.

The main properties of the alternatives are indicated in the table below.

<i>Alternative</i>	<i>Authentication Protocol</i>	<i>Peer Discovery</i>	<i>Trust Establishment</i>
DIAMETER	DIAMETER over TCP / TLS	DNS	PKI
RadSec	RADIUS over TCP/TLS	DNS	PKI
RADIUS-DNSSEC	RADIUS over UDP	DNSSEC	DNSSEC
RadDNSSEC	RADIUS over TCP/TLS	DNSSEC	DNSSEC

Next to the main properties, the comparison considers such aspects as support for multiple roaming agreements, insight in membership of organizations, deployments issues, ‘reasonable’ security, scalability, data integrity, etc. We conceived various architectures that support interoperability between these approaches, focussing on integrating DIAMETER and RADIUS by means of DIAMETER-RADIUS proxying (which has been defined in the DIAMETER standard).

Migration of the current eduroam infrastructure to a more loosely coupled authentication model is quite important. Therefore, our architectural work focusses on making the top-level part of the RADIUS hierarchy more dynamic. We worked out various interoperability scenarios between dynamic trust-establishment in parts of the authentication infrastructure while maintaining RADIUS trees towards the individual organizations. We found that the current standards actually support this quite well, but the currently available implementations do not support DIAMETER-RADIUS proxying yet.

We are currently evaluating an authentication infrastructure that consists of a combination of RadSec authentication mechanisms and traditional RADIUS-based authentication, using Radiator technology. RADIUS-hierarchies are used only when RadSec cannot be applied because a (intermediate) domain does not support RadSec, but only standard RADIUS. Tests are expected to be finalized early 2006.

The conclusion of this work is that the current state of the art in standardized authentication protocols is sufficiently rich to allow for interoperable solutions, both with respect to trust-establishment and with respect to discovery mechanisms. Current DIAMETER implementations, however, do not support RADIUS interoperability yet. However, this is being worked on. Solutions like RadSec (although proprietary) may very well fit this gap that currently exists because neither DIAMETER nor DNSSEC is widely deployed yet. Our test-setup shows that a combination of Radius hierarchies with RadSec is a feasible approach for federated authentication.

References

- [1] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, “*DNS Security Introduction and Requirements*”, IETF RFC 4033, March 2005
- [2] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, “*Diameter Base Protocol*”, IETF RFC 3588, Sept. 2003
- [3] EduRoam, <http://www.eduroam.org/>
- [4] H. Eertink, A. Peddemors, R. Arends, and K. Wierenga, “*Combining RADIUS with Secure DNS for Dynamic Trust Establishment between Domains*”, TERENA Networking Conference 2005 (TNC’05), June 2005; <http://www.terena.nl/conferences/2005/>
- [5] The Open Group, “*RadSec, a secure, reliable, RADIUS protocol*”, Whitepaper retrieved on 5/12/2005 from <http://www.open.com.au/radiator/radsec-whitepaper.pdf>
- [6] C. Rigney, S. Willens, A. Rubens, and W. Simpson, “*Remote Authentication Dial In User Service (RADIUS)*”, IETF RFC 2865, June 2000

Vitae

Henk Eertink is a senior researcher at Telematica Instituut. He leads a group that is focused on security issues, mobility management and context awareness.

Arjan Peddemors is a research engineer at the Telematica Instituut. His interests are in the area of mobile and pervasive computing, with a specific focus on mobility management and network resource awareness for mobile applications. He is currently working towards his PhD.

Remco Poortinga is an application engineer at Telematica Instituut. He has worked in national and European projects in the area of networking and middleware, accounting, mobility management, IPv6, multimedia IP-based streaming, interoperability, and context awareness.

Roy Arends is a network engineer at Telematica Instituut, and an active member in the DNSsec working groups of the IETF.

Klaas Wierenga is manager of Middleware Services at SURFnet. He is co-chair of the TERENA taskforce on Mobility (TF-Mobility) and active member of the Internet2 working group on network authentication (SALSA NetAuth).