

Birds of a Feather meeting: Proposal for a Common Global Access Management System

TNC 2011, Thursday 19 May 2011, 1400-1730 CEST

Attendees

Miroslav Baranko, SANET
Licia Florio, TERENA
Brian Gilmore, University of Edinburgh (BG)
Maja Gorecka-Wolniewicz, PIONIER
David Groep, Nikhef / BiG Grid
Sam Hartman, Painless Security LLC (SH)
Luke Howard, PADL Software Pty Ltd
Josh Howlett, JANET(UK) (JH)
Mehdi Hached, RENATER
Henry Hughes, JANET(UK) (HH)
David Kelsey, STFC (DK)
Daniel Kouřil, CESNET
Janne Lauros, CSC
Rhys Smith, University of Cardiff (RS) (Scribe)
Milan Sova, CESNET (MS)
Martin Stanislav, SANET
Sat Mandri, University of Auckland / NZ Access Federation (SM)
André Marins, RNP
Karen O'Donoghue
Mark O'Leary, JANET(UK)
Jiří Pavlík, CESNET / eduID.cz
Dubravko Penezic, SRCE
Chris Phillips, CANARIE (CP)
Alex Reid, AARNet / Australian Access Federation
Hardi Teder, EENet
Stefan Winter, RESTENA (SW)
Tomasz Wolniewicz, PIONIER (TW)
Kazu Yamaji, NII


This list is not believed to be entirely complete. SW and BG left the BoF early owing to travel plans.

Background

The goal of this BoF was to discuss the paper by JH titled "A Proposal for a Common Global Access Management System for Education & Research", with the intent of establishing the level of interest within the TERENA community. This paper can be found at the following URL:

<http://webmedia.company.ja.net/edlabblogs/developmenteye/2011/05/10/proposal-for-a-common-global-access-management-system/>

The slides that were presented by JH during this meeting can be found at the back of these minutes; thumbnails of these slides are provided throughout the text as a convenience to the reader. Parties that are interested in following this work are encouraged to subscribe to cgams-announce@jiscmail.ac.uk.



A Proposal for a Common Global Access Management System for Education & Research

TERENA Networking Conference 2011, Prague.

JH welcomed the BoF and asked how many attendees had read the proposal. Approximately $\frac{1}{3}$ of the attendees indicated that they had.

JH stressed that this was not a talk about the Moonshot technology, but the possible application of the technology to establish an access management system. The goal of the BoF was to establish whether there the community had any interest in exploring this further.

JH postulated that the success of eduroam largely owes itself to the emphasis on establishing international collaboration on a common operational infrastructure and policies from the very start. Achieving a similar level of integration of identity federations, in systems such as eduGAIN, has proved much harder because the identity federations spent a long time evolving in isolation, often adapting to particular national requirements that are not matched elsewhere. JH claimed that following the eduroam model of building consensus internationally is a desirable first step.

JH walked through the “Introduction” section of the slide-set.

<h2 style="text-align: center;">Introduction</h2>	<h2 style="text-align: center;">Access management as a strategic requirements</h2> <p>The emergence of access management as a strategic requirement for the education and research community is a relatively new phenomenon. Traditionally, ICT services have been organised, delivered and consumed within individual organisations. Where services were delivered externally, or consumed from external sources, it was generally possible to engineer <i>ad hoc</i> approaches that, while technically unsophisticated, satisfied the business requirement.</p>
<h2 style="text-align: center;">Motivation – reduce complexity</h2> <p>Viewed independently, these services provide a consistent experience to their customers. However, these services use a variety of different security technologies. Customers of these services, and the organisations that deliver them, must necessarily maintain expertise and infrastructure for each technology. This technical redundancy imposes costs on those organisations that must deliver and consume these technologies, and complexity for their users who must learn to use them.</p>	<h2 style="text-align: center;">Motivation – extend scope</h2> <p>Despite the diversity of available technical approaches, there are still many applications and services that cannot be used effectively between organisations because no appropriate technical mechanism exists. This lack of inter-organisational functionality imposes a tremendous opportunity cost by preventing these applications and services from enjoying the benefits of inter-organisational operation.</p>
<h2 style="text-align: center;">A common & global system</h2> <p>There appears to be growing consensus that these issues are becoming increasingly acute. The purpose of this paper is to outline a <i>common</i> and <i>global</i> access management system that may comprehensively address these:</p> <ul style="list-style-type: none"> • A <i>common system</i>, meaning that is an appropriate solution for a broad range of application and service technologies. • A <i>global system</i>, meaning that it is accessible and usable for diverse, geographically or otherwise, user and service provider communities. 	<h2 style="text-align: center;">Questions 1 & 2</h2> <ul style="list-style-type: none"> • Does the community require a common and global access management system? • If not, why?

JH posed the following questions to the BoF.

Q1 – Does the community require a common global access management system?

Yes – 20

No – 2

Abstain - 6

Q2 – If not, why not?

CP: It is necessary to contrast this proposal with other existing technologies (e.g. SAML & eduroam) and understand how this fits into that landscape before it's possible to answer that question.

HH: How this compares or relates with other technologies is not the point of the question. The question is at a higher level – is there actually a need or not? If there is, we can consider the technology options that might enable this (such as those mentioned).

SW: SAML & RADIUS federation together don't solve all problems. A single trust fabric that solved a range of federation problems is a desirable goal.

CP: Does system mean service?

JH: Yes


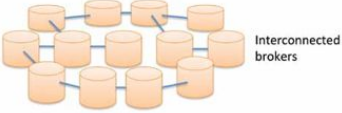
CP: Who gets to run it?

JH: We get to that later.

DK: Does this include both authentication and authorization?

JH: Yes.

JH walked through the “Vision” section of the slide-set.

<p>Vision</p>	<p>Vision</p> <p>This paper seeks the establishment of a common global access management system that is capable of supporting every service and application used by the education and research community.</p> <p>Figure 1 below provides a high-level depiction of this vision.</p>  <p>Figure 1</p>
<p>Vision</p>  <p>Interconnected brokers</p> <p>Figure 2</p> <p>The middle layer, illustrated in Figure 2 above, represents the access management infrastructure that mediates the users' access to these services and applications. This infrastructure consists of brokers, which mediate <i>vertically</i> between users and services, and an interconnection fabric which mediates <i>horizontally</i> between brokers.</p>	<p>Question 3 & 4</p> <ul style="list-style-type: none">• Does this vision resonate as a reasonable high-level framework for thinking about a common and global access management system?• If not, why?

JH posed the following questions to the BoF.

Q3 – Does this vision resonate as a reasonable high-level framework for thinking about a common and global access management system?

Yes or abstain: 28

No: 0

Q4 – If not, why not?

BG: It's too general to be particularly useful at the moment.

TW: It looks similar to what we tried to do in GN2 with bridging elements.

JH: Need to be careful to distinguish between the conceptualisation versus the implementation. The "Vision" diagram is not a technical model.

SW: Previous efforts to integrate RADIUS and SAML systems as in GN2 have been fiddling at the edges; this provides a more comprehensive approach.

SM: You're missing standards, audit, compliance of such a system, etc. None of this is technology specific.

JH: This is essential and probably represents the majority of the work that needs doing, although we can probably re-use many existing standards and policies; it's not been forgotten, more on this later.

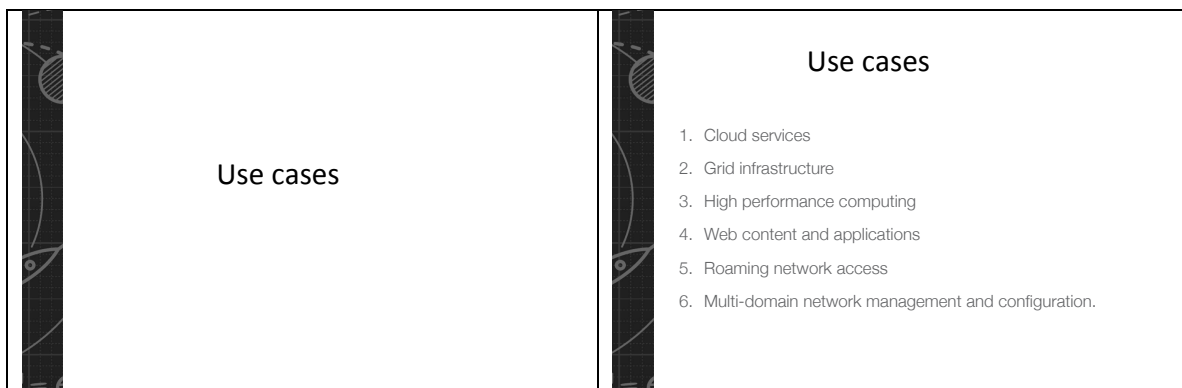
Unknown: Services see a single abstract layer due to brokers. How much do services have to rely on the integrity of the entire layer (with full amount of brokers and entities) to make reasonable decisions?

JH: You have to strike a balance of technical management of trust and business management of trust. We already have this problem in existing AMS; it's inherent in any federated system.

CP: Does the vision imply a fully meshed environment? If not, what does vision say about how things are connected?

JH: The system should ideally support any topology, in whatever way the requirements dictate. Could be full mesh but unlikely.

JH walked through the "Use-cases" section of the slide-set.



Questions 5 & 6

- Are these use-cases adequately representative of the community's requirements?
- If not, why?

JH noted that a comprehensive discussion of these would consume substantial time, and so the list of use-cases (presented in the slide-set) is for illustrative purposes only; the CGAMS paper contains more detail.

JH posed the following questions to the BoF:

Q5 - Are these use-cases adequately representative of the community's requirements?

General reluctance to cast votes; consensus appeared to be that there wasn't sufficient information.

Q6 - If not, why not?

Unknown: Mobility (mobile devices) could be useful.

Unknown: Also emerging technologies.

Unknown: Some seem more technologies than use cases...


BG: Complex environment, cross relationships between (e.g. multiple affiliations).

Claim to solve but skated over how in the web use-case.

JH: Yes, additional clarity and detail is needed; this has been mentioned previously.

Unknown: - Also need a solution to (as defined by Sam) access management system administration (not just making decision but managing policy about who can do what, shared contacts, etc).

JH walked through the "Conceptual Model" section of the slide-set.

<p>Conceptual model</p>	<p>Actors</p> <ul style="list-style-type: none"> • Identity providers – sources of information for access management decisions. • Service providers – consumers of identity information, to make access management decisions. • Brokers – create clubs of identity and service providers, facilitating the transfer of useful identity information. • Inter-connect – creates a network of brokers, which facilitates the scalability of the system.
	<p>Questions 7 & 8</p> <ul style="list-style-type: none"> • Do these actors and interactions capture the requirements of the use-cases? • If not, why not?

SM: There may also be a requirement for a "gateway" actor that decreases the complexity of connecting sets of brokers together.

SH: Queried this requirement; not clear what a gateway does that is different from a broker?

Unknown: We should map eduroam and SAML federations to this general model, to test it.

JH: Need to consider these actors in their most general sense, not in specific technical senses (e.g., SAML) that we may be more familiar with. In this discussion we are still at the business level, not the protocol level.

JH posed the following questions to the BoF:

Q7 - Do these actors and interactions capture the requirements of the use-cases?

General reluctance to cast votes because of insufficient information on the use-cases.

Q8 - If not, why not?

As above, insufficient information.

JH walked through the "Proposed Implementation" section of the slide-set.

The following discussion started with the “Interconnect” slides.

<h2>Proposed implementation</h2>	<h2>Interconnect</h2> <p>The international RADIUS infrastructure is composed of RADIUS systems that are typically nationally organised, with the national research and education network usually acting as the National Roaming Operator. This role is very similar to that of a broker, using the nomenclature of the previous section. The interconnect, in this case, is the set of regional top-level RADIUS proxy servers that connects the national RADIUS systems.</p> <p>Although this infrastructure is essentially ready for an ABFAB-based system, some effort is nonetheless required to place the system on solid foundations. This work consists of the following:</p>
<h2>Interconnect</h2> <ul style="list-style-type: none">• Develop an interconnect policy.<ul style="list-style-type: none">◦ <i>How:</i> Building on the existing eduroam policy, develop an interconnect policy that addresses both network and application access management.◦ <i>Who:</i> The governance body, brokers, and other interested communities and stakeholders.◦ <i>Due:</i> April 2012.	

MS: Because of current (bad) credential management practices, reusing existing infrastructure may be a problem for higher assurance services.

JH: Yes, for some use cases. But campuses may be willing to make changes where they see the requirement from desirable services.

Unknown: Can't guarantee existing infrastructure will be there in 5-10 years time.

JH: As long as the business is there, and the B2B agreements, that's fine.

Infrastructure changes, nothing stands still.

Unknown: In many places SAML federation and eduroam federations are completely separate. This could complicate things.

JH: Yes, this approach is easier for some than others.

CP: Different LoAs will be necessary.

RS: Almost beyond scope of system, as long as the proposed technology supports this.

SH: Yes, but a governance body to establish policy and suchlike might also be necessarily a part of this.

JH moved onto the “Broker” slides.

<h3 style="text-align: center;">Broker</h3> <p>The brokers, at least initially, would probably be largely represented by eduoam's National Roaming Operators (NRO) which are typically, but not exclusively, the national research and education networks. However, other bodies could assume the role of broker for non-eduroam applications for a particular constituency.</p> <p>The interconnect's policy may impose modifications to the policies and practices of brokers</p>	<h3 style="text-align: center;">Broker</h3> <ul style="list-style-type: none"> • Consider, and react to, the implications of the interconnect policy. <ul style="list-style-type: none"> ◦ <i>How</i>: analyse the impact on existing policies, and potentially modify them. In particular, there may be significant efficiency savings to be made by re-using (insofar as possible) an existing national identity federation's framework to avoid duplication. SWAMID, the Swedish Higher Education identity federation, provides an excellent model for this that brokers are encouraged to consider. A substantial majority of education and research identity federations are also NROs, and so this approach would deliver a synthesis of policy, satisfying both network and applications access management, for their customers. ◦ <i>Who</i>: any broker that wishes to participate. ◦ <i>Due</i>: prior to any operational changes.
<h3 style="text-align: center;">Broker</h3> <ul style="list-style-type: none"> • Make any modifications to existing technical and business processes where necessary. <ul style="list-style-type: none"> ◦ <i>How</i>: determined by results of the policy analysis. ◦ <i>Who</i>: the broker, probably in co-ordination with their customers and user communities. ◦ <i>Due</i>: prior to connection to the interconnect. 	

CP: Who could be brokers? Governments? School boards? Anyone?

JH: Yes. Likely to be community based, but interconnect should be able to connect these communities. Should be able to discriminate between actors in system based on policy.

CP: There will be a price for autonomy - if anyone can be a broker. Federation operators can bring aggregation to the picture and help reduce this "price".

JH: Different communities may have different policies, including about connectivity.

JH moved onto the "IdPs and SPs" slide.

<h3 style="text-align: center;">Identity & Service Providers</h3> <ul style="list-style-type: none"> • Consider, and react to, the implications of their broker's policies. <ul style="list-style-type: none"> ◦ <i>How</i>: analyse the impact on existing policies, and potentially modify them. ◦ <i>Who</i>: all providers, probably with the guidance of their broker. ◦ <i>Due</i>: prior to any changes to operational practices. • Make any modifications to existing operational practices where necessary. <ul style="list-style-type: none"> ◦ <i>How</i>: determined by results of the policy analysis. ◦ <i>Who</i>: all providers that intend to participate. ◦ <i>Due</i>: prior to connection to their broker. • Connect to a broker. <ul style="list-style-type: none"> ◦ <i>How</i>: deploy ABFAB-conformant software (see Appendix III for more information). ◦ <i>Who</i>: any provider that intends to participate, probably with the guidance of their broker. ◦ <i>Due</i>: prior to any operational use. 	<h3 style="text-align: center;">Questions 9 & 10</h3> <ul style="list-style-type: none"> • Is this implementation approach reasonable? • If not, why not?
---	---

CP: Stewardship of this ecosystem is going to be responsibility of whom?

JH: Good question.

SH: Steward per "club"/community

CP: So there is no global stewardship, like the internet. Will be driven by economics - do I set up links directly or go through a broker?

JH: Definitely need a steward for each community. Open question as to whether the interconnect has/needs one.

Unknown: Potential problem if assuming one interconnect will emerge. We assumed that would happen with PKI.

JH posed the following questions to the BoF:

Q9 - Is this implementation approach reasonable?

CP: Do we have sufficient clarity to answer this question given the overall vision is still vague?

KO: Not sure we understand the question enough to be able to answer.

There following some discussion about the question – it was agreed to narrow it down to "as an initial direction".

Yes – 23

No – 0

Abstain – 3

Q10 – If not, why not?

No responses.

JH walked through the “Proposed Roadmap” section of the slide-set.

<p style="text-align: center;">Proposed Roadmap</p> <ol style="list-style-type: none">1. Solicit feedback to this proposal.2. Establish a mailing list to obtain feedback, and for general discussion of the proposal.3. Create a wiki to collect and structure the feedback.4. Identify alternative implementation strategies (to that described in section 7).5. Develop a consensus strategy, based on this feedback.6. Organise a workshop to seek consensus on an implementation strategy.	<p style="text-align: center;">Questions 11 & 12</p> <ul style="list-style-type: none">• Is this roadmap reasonable?• If not, why not?
---	--

JH: Suggest we have a repeat of this meeting in 6-9 months to see if we've made progress in between; focus on getting some initial stakes in the ground.

CP: Also need to use feedback from today to refine roadmap, increase clarity on existing stuff (especially including use cases), etc.

JH: Do we need a mailing list?

Room: General agreement.

JH: Do we need a shared space like a wiki?

Room: General agreement.

JH: Next meeting in about 6-8 months somewhere?

Room: General agreement.

JH thanked the BoF for their participation.