UNIVERSITY OF AMSTERDAM

Multi-Domain Authorization for e-Infrastructures

L.H.M. Gommans

Summary

In this thesis we show what is needed to build a generic multi-domain authorization system. When placed in e-Infrastructure context, such system is capable of allowing scientific applications to access combinations of infrastructure components. These components are delivered as a chain by multiple service providers. The research emerged from the notion that automatic creation of service chains will need an authorisation system. A multi-domain authorization system allows different service providers to work together when automatically delivering service chains, whilst retaining the ability to define own access policies. Maintaining autonomy amongst Service Providers is an essential requirement. To allow authorization transaction to happen, involved parties must trust each other. To be trusted in a chain, each service provider must know that any policy rule it executes is correct. Such trust emerges from a common set of rules that may need to be enforced depending on the risk involved.

In our research to the question what is needed to build a multi-domain authorization system, we recognized that the question must be approached from at least two viewpoints:

- **The engineering viewpoint**, where different authorization transaction scenario's must be supported by different functions and protocols.
- **The business viewpoint**, where fulfilment of service agreements in mutual trust is key.

Our research was performed in three phases over a period of 15 years. Phase one and two considers the engineering viewpoint. The third phase considers the business viewpoint along with the engineering viewpoint.

The engineering viewpoint.

From the engineering viewpoint we asked ourselves questions like: "What generic authorization functions can be distinguished?", "How do they interact?", "What concepts are expected to work best in multi-domain scenarios?" and "How can these concepts be applied?"

In our research, performed in phase one within the context of the Internet Engineering Task Force, we proposed an Authorization Framework and Generic AAA Architecture to describe and handle authorization transactions. The Framework recognizes a number of fundamental authorization sequence models. The Architecture describes functional elements that can generically handle authorization transactions across multiple domains. Using a number of example scenarios we motivated that our proposal could be generically applicable. We also recognized a number requirements for a design.

Phase two of our research focussed on the question how the Authorization Framework and Generic AAA Architecture concepts can be applied to perform multi-domain authorization.

The inherent research orientation of National Research and Education Networks, and the need for these autonomous organisations to collaborate in order to provide dedicated network connections at global scale, legitimized our research questions to be placed in this context. We transformed our research questions into more specific questions like "What generic concepts work best for classes of applications that use multi-domain network resources?" and subsequently "How can these concepts be applied to optical networking?". This phase of our research explores and demonstrates the use of two of our Framework sequence models and its combination, using tokens, to authorize the use of multi-domain network segments.

We first hypothesized that the "Agent" model (whereby a request is first send to the authority and subsequently the authority provisions the connection) would be most suitable. Based on experiments with this model we concluded that this model, when applied to multi-domain scenario's, would be potentially too slow to handle requests. By separating the request for a connection from signalling the fact an application wants to use a connection, we concluded that a combination of the agent model with a model whereby the authority issues a token that can be used to access the connection at the desired moment (so called "push" model) is a more suitable alternative. With experiments we have demonstrated that this combined (so called "token") model can be implemented in different ways in network environments. We show that a simple token, that within a domain only refers to a meaning of a token (the meaning of a token can be different for each domain) allows a domain to preserve its autonomy as much as possible. The token can point in each domain to something that must be

done correctly. Each domain will determine what the correct thing is that should be done. As such, phase two validates that the functionalities, described by our Generic AAA Architecture, can handle such scenarios.

The business viewpoint.

In phase three of our research we ask the question "*What is needed to arrange trust when authorizing e-infrastructure resources?*" We already saw in phase one that *trust relationships are necessary for authorization transactions to take place.* Based on a study of existing examples from the payment world and the educational roaming world, we created a framework describing the organisation of "Service Provider Groups". This framework makes the often implicit assumed ways explicit of how rules and agreements are transformed in to policies that determine what the *correct things* are that must be done to achieve the desired trust in the operation of a system.

We foresee that our models are in particular applicable to scenario's where chains of electronic services are created automatically and offered as a single service to users. Currently we increasing see the appearance of such chained services that are built using Cloud type services and services that are built via so called Application Programming Interfaces (API's). Joining these autonomous service raises the question who is going to act as party that takes liability for an offered service chain as a whole. Same as in our studied example from the Credit Card world, it takes a parties such as MasterCard to take liability for handling authorization transactions in collaboration with banks as autonomous service providers. When thinking about what is needed to build an authorization system in such context, this research contributes by recognizing the necessary functional elements, both on technical and business side, by using a number of frameworks and a technical architecture that has been validated for its applicability.