Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Christoph Rensing, Hasan,
Martin Karsten, Burkhard Stiller

A Survey on AAA Mechanisms, Protocols, and Architectures and a Policy-based Approach beyond: A^x

TIK-Report
Nr. 111, May 2001

Institut für Technische Informatik und Kommunikationsnetze
Computer Engineering and Networks Laboratory

Christoph Rensing, Hasan, Martin Karsten, Burkhard Stiller:
A Survey on AAA Mechanisms, Protocols, and Architectures and a Policy-based Approach beyond: A^x
May 2001
Version 1
TIK-Report Nr. 111

Computer Engineering and Networks Laboratory,
Swiss Federal Institute of Technology (ETH) Zurich

Institut für Technische Informatik und Kommunikationsnetze,
Eidgenössische Technische Hochschule Zürich

Gloriastrasse 35, ETH-Zentrum, CH-8092 Zürich, Switzerland

A Survey on AAA Mechanisms, Protocols, and Architectures and a Policy-based Approach beyond: A^x

Christoph Rensing[*], Hasan[+], Martin Karsten[*], Burkhard Stiller[+]

[+] Computer Engineering and Networks Laboratory TIK, Swiss Federal Institute of Technology, ETH Zürich, Switzerland
[*] KOM - Industrial Process and System Communications, Darmstadt University of Technology, Germany
E-Mail: [hasan|stiller]@tik.ee.ethz.ch, [Christoph.Rensing|Martin.Karsten]@kom.tu-darmstadt.de[1]

Abstract

AAA, the Authentication, Authorization, and Accounting approach for dial-up connectivity of mobile users and devices has reached a status of maturity, however, limited to a dedicated set of minor scenarios. While the commercialization of the Internet has lead to a large variety of business models based on Internet technology, the demand for standardized and efficient solutions in support of reliable, secure, open, and flexible remote service accesses has increased. In addition to the traditional AAA approach, emerging support services, such as policy support, charging, pricing, and auditing for Internet services, are required essentially to offer as a service provider a viable set of distributed data communication and content services.

As discussed in this work, the existing work on a AAA Architecture still considers dedicated cases and lacks a scenario-independent and generic approach. Therefore, the approach termed A^x Architecture*, is proposed to enable a generic and integrated way of dealing in a policy-based manner with these support services, which a public service provider must offer for mobile as well as fixed users. This generic A^x Architecture is motivated by indicating basic areas of concern, discussing existing protocols, mechanisms, and data types, and the development of the architecture's scope and major modules required for A^x. Driven by business model needs, but focussed on the technical design and implementation only, this proposed work enables business cases as a top level policy, charging as an economic policy, and QoS support for end-to-end services in the Internet.*

Keywords: *Internet, AAA, Policy, Charging, Service Provider, Services Modelling, Quality-of-Service, Protocols.*

1 Introduction and Motivation

Communications in a mobile world are on their way to reach a high penetration in today's Internet Protocol (IP)-based networks. The Internet offers a public and private communication platform to enable a variety of services, for business users and private users. As soon as these services will be commercialized the need for access control, authorization, and charging drove technology developments accordingly.

Since the basic IP access can be seen as a commodity and simple services already are self-evident, service providers need to differentiate themselves across a wide range of content and more sophisticated services. This trend is clearly visible in the Internet today, as the variety of business models outline, *e.g.*, connectivity services and portals like AOL, Yahoo!, or bluewin, peer-to-peer application services like Napster, Gnutella, or Freenet, personal communication services like hotmail or content delivery services like AKAMAI. However, service providers in the Internet need to ensure that they receive a payback for their investments in technology for communications, servers, and content. This statement defines the instantiation of the most abstract, but crucial business policy of the provider to be followed in the market. Of utmost important is the answer to the question: What is the current state of the Internet communication environment economically or market-driven? Certainly, only service providers with well-developed connectivity and content models do have a chance, once technology is in place.

Besides these economic and market-driven aspects the underlying communication technology requires a close-up investigation. What is the state of the Internet technically in support of this environment? Existing Internet protocols for the transport of user data or payload, signaling protocol discussions in support of an end-to-end quality assurance, as well as service provisioning and deployment approaches are manifold. In addition, firewalls and further network devices have to be configured to ensure a negotiable degree of security for users, customers, and communications. The heterogenity in these components, the functionality in networking devices and hosts is another characteristic of existing Internet technology. However, today communication quality guarantees can be granted only in a homogeneous technology and administrative domain. For these reasons, the network of the near future to be considered will be a multi-service network, the multi-service Internet, consisting of multiple domains, operating in an inter-domain fashion, and offering access services, transport services, application services, and content.

To support mobile users in the Internet, adaptive network architectures and management of systems depending on monitoring the activity in this system are required. While customized user services, dynamic user behavior, and user as well as device mobility increase, the importance of access control, authorization, and security considerations arises significantly.

Especially for dial-up or PPP (Point-to-point Protocol) connections *Authentication*, *Authorization* and *Accounting* (AAA) solutions exist in form of protocols and implementations, which integrate these AAA tasks. These tasks are commonly referred to as AAA systems. Presently, extensions to theses systems for other access scenarios like roaming or mobile users and access control extensions to communication protocols like Mobile IP are under discussion in the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). Besides these protocol and data type parts, policies can be used as a mean for describing management goals and for the general management of networks.

1. The portion of work performed by Christoph Rensing was done mainly during his stay as an academic guest at ETH Zürich, TIK, Switzerland.

Such a policy approach is also under discussion in IETF and IRTF to be applied for the management of AAA systems.

To enable a particular understanding of major observations and their implications for a suitable Internet-based A^x, covering major extensions with respect to generic policy support, charging, pricing, and auditing of Internet services, the proposed architecture solution is illustrated using a concrete application scenario.

1.1 Application Scenario

To motivate the variety of services and access regulations for public and private communication means, a realistic communication scenario is introduced. It enables the reader to combine technological, organizational, and economic questions in an integrated fashion.

The father of a family is a technical IT consultant. Most of the time he is traveling for business and at a single day he is in his company's office. While traveling he accesses data from his office to handle his E-Mail and further business applications. For this purpose he uses a wireless Wide Area Network (WAN) access provided by a telecommunication company or the IP access of a customer's network. The protocol applied is preferably Mobile IP, if supported inside the customer's network. Additionally, he performs further studies using different web-based training offers at home on weekends. He pays for this courses by credit card. Some of these courses includes videos, which he wants to view in a reliable quality. To achieve this, he utilizes a Quality-of-Service (QoS)-enabled transport service from his provider.

His son is enrolled in different courses at a virtual business school to achieve his MBA (Master of Business Administration) in finance. From the business school he receives a user-identifier (ID), which he applies to register at the school's web server. This web server offers chat-rooms for enrolled students and also the possibility to do exams electronically. In free time the son trades with an on-line broker and reads business news from a specialized News on Demand (NoD) server.

These accesses to the Internet are implemented as shown in Figure 1. From home an Asymmetric Digital Subscriber Line (ADSL) access is used. In the office a local IP network exists, which is based on Wireless LAN (Local Area Network) being connected to an Internet Service Provider (ISP) over a switched link. The mobile access to the wireless WAN is realized using a pre-paid card and possibly different technologies like GSM (Global System for Mobile Communications) or EDGE (Enhanced Data Rate for GSM Evolution).

This scenario exemplifies the complexity of access control consisting of authentication and authorization. It is necessary to restrict connectivity to IP networks themselves, to transport services with QoS guarantees, and to provide content. Decisions on authorization may be influenced by technical (*e.g.*, remaining bandwidth), confidentiality, and financial aspects (creditworthiness). Also it can be seen that access control can be based on different identity types like personal user-IDs, IDs of hardware devices, or anonymous IDs. Access control has to be done for different access technologies and, especially for mobile users, by service entities which have no contract with users requesting a service.

In this scenario most services are charged, the telecommunication connection and the IP access depending on connection time, the transport depending on QoS parameters, and e-learning courses and news depending on content. Therefore, accounting is a must and it includes more than simply metering the time a user is connected to the IP network.

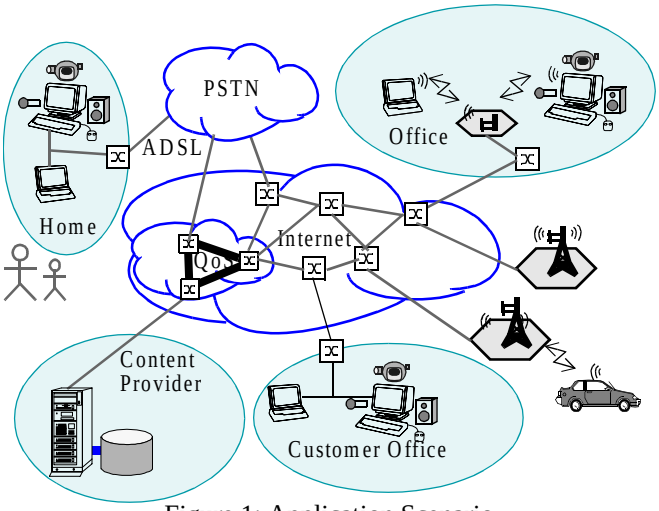

Figure 1: Application Scenario

This scenario shows in addition that different evolutions are leading to an increased complexity of network management in general and of AAA tasks in particular. Furthermore, it has to be investigated which additions to the traditional AAA approach are necessary. These additions are concerned with additional components for auditing and charging and pricing and billing tasks also. Therefore, future extensions of the AAA Architecture and services in this work are referred to as *A^x*, which includes auditing capabilities, policy support, billing, and pricing functionality. These A^x services are not completely independent from each other, due to various relations and feedback signals, which will be discussed in Section 4.1.2 in closer details. To meet those requirements, mainly resulting from the increasing complexity, major dependencies and future extensions to AAA of which the authors argue on their usefulness, are to be integrated in an overall view. Therefore, a generic A^x services architecture is proposed.

Level	*Control Path*	*Data Path*
Content	RTSP	news, streaming video
Application	HTTP, H.245, SIP	video conferencing, IP-telephony, Java applets
Transport	RSVP, RTCP, ICMP	TCP, UDP, RTP
Connectivity	DHCP	Sonet/SDH, DWDM

Figure 2: Generic Structure of Partitioning

Covering the set of protocols suitable for the scenario in Figure 1, Figure 2 exemplarily depicts some available protocols for signaling as well as data transport in an IP-based environment to enable a clear separation of concerns. This partitioning includes protocols like HTTP (Hyper Text Transfer Protocol) or ICMP (Internet Control Message Protocol), application classes such as video conferencing or streaming video, or mechanisms like Java applets, always depending on the use within the scenario.

1.2 The Big Picture and Objective

The work on Authentication, Authorization, and Accounting (AAA) has reached a status, where a selected number of mechanisms and algorithms are understood and proposals for supporting protocols as well as extensions have been made. Often this work is performed in isolation for shortened tasks and limited scenarios, like connectivity control through a Network Access Server (NAS) or content delivery control through a billing system.

However, the structured description of involved components and entities as well as the identification of interaction schemes between these components is a hard problem independent of existing technology (fixed or wireless networks) or Internet protocols (such as IP, Differentiated Services, or Mobile IPv6). Therefore, this work applies - based on the survey on state of the art in the area of AAA - for a future overall view a generic structure of four horizontal levels, where applicable. The lowest level 1 is concerned with Internet connectivity, level 2 with transport, level 3 with application issues, and level 4 with content issues. Besides these partition into levels a vertical segmentation in the signaling and data path is done as depicted in Figure 2 exemplarily above. The horizontal partitioning defines service classes with similar characteristics and similar AAA requirements also. On connectivity level an authentication based on a hardware device can be done, on content level a personal authorization is often necessary. The vertical partitioning helps to identify, at which point support services are necessary and where not. Authentication and authorization has to be done during signalling mostly, whereas accounting has to be performed on data path informations if it is volume based for instance. The overall partitioning defines protocols, application classes, policies, and mechanisms as Abstract Objects (AO), which are considered separately on purpose in the enhanced context of AAA with respect to their service characteristics, value, or security requirements.

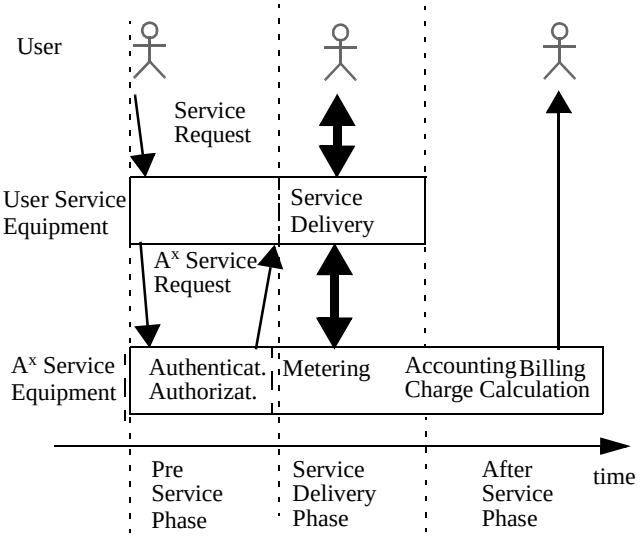

Figure 3: Service Interaction

The objective of this approach is, to define A^x services in the most generic way and to build an A^x architecture enabling services to be used in support of different user services on different levels in different scenarios. Therefore, it is suggested to logically separate user services and A^x services from the corresponding equipment which provides those services. A^x services are provided to user service equipment in different phases, as they are shown in the logical view of Figure 3 in a simplified form. First, during a service invocation or negotiation phase, a user requests a user service. This request is authorized from the Service Equipment (SE) delivering A^x services, which may be based on authentication. During the service delivery the service usage is metered based on the applied policy and mechanisms. Accounting and charge calculation as well as billing tasks, are performed after or during the service execution. Only the A^x service equipment is responsible for the delivery of those A^x services.

1.3 Outline

This work contrasts the generic policy paradigm, its application in the field of AAA, and its potential extension. Based on the terminology definition in Section 2, Section 3 identifies and briefly discusses major problems areas. Section 4 focusses on existing AAA work, covering mechanisms, policies, and protocols as separate entities. Section 5 describes the AAA Architecture proposed currently by the IRTF. Based on these investigations, Section 6 proposes a general A^x Architecture for enhanced AAA functionalities and a policy-based network management. The discussion in Section 7 complements the work, summarizes, and draws key conclusions.

2 Terminology

In the following basic terms are defined in alphabetic order, which are significant for the following singular understanding and use of terminology.

- *AAA Services*
  AAA Services are services related to authentication, authorization and accounting. They contrast to the user services in the sense that they are valuable for the provider of user services, to achieve his business goals, and not for the user in a direct way.
- *AAA Service Equipment*
  The AAA service equipment is the equipment of maybe different service providers which is used to provide AAA services.
- *A^x Services*
  A^x Services define the extended AAA services by policy support, auditing, charging, pricing, and billing.
- *Accounting*
  Accounting is the collection and aggregation of information (accounting records) in relation to a customer's service utilization. It is expressed in metered resource consumption, *e.g.*, for the end-system, applications, middleware, calls, or any type of connections. The data can be used for capacity and trend analysis or auditing.
- *Auditing*
  Auditing is the verification of the correctness of any process regarding the service delivery. Auditing is done by an independent real-time monitoring or examination of

logged system data in order to test for correctness of operational procedures and to detect breaches in security. Auditing of accounting records is the base for an after-usage proof of consumed resources and for customer charges.

- *Authentication*
  Authentication is the verification of the identity of a subject performing an action. The identity can be personal, logical, like a user ID and password, bound to an infrastructure like an IP-Address, or bound to a device, like a Medium Access Control (MAC) address or the International Mobile Subscriber Identity stored in the SIM (Subscriber Identification Module) Card. The subject of authentication can be a service user or a service provider.
- *Authorization*
  Authorization is the verification of whether a subject is allowed to perform an action on an object, *e.g.*, access to or use of some objects.
- *Billing*
  Billing is defined as the process of collecting charging records, summarizing their charging content, and delivering a bill or invoice including an optional list of detailed charges (itemization) to a user.
- *Charge Calculation*
  Charge Calculation covers the complete calculation of a price for a given accounting record and its consolidation into a charging record, while mapping technical values into monetary units. Therefore, charge calculation applies a given tariff to the data accounted for.
- *Charging*
  The overall term charging is utilized as a summary word for the overall process of metering resources, accounting their details, setting appropriate prices, calculating charges, and providing a fine-grained set of details required for billing. Note, that billing as such is not included in this definition. Charging is considered as a dedicated policy to enable a provider to gain revenue for a given network and service offer.
- *Metering*
  The task of metering determines the collection of data on the usage of resources within end-systems (hosts) or intermediate systems (routers) on a technical level, including QoS, management, and networking parameters.
- *Network Policy*
  Network policies are derived from management goals and define the desired behavior of (and relationship between) different entities in the network by actions to be performed from entities. These entities refer to users, applications, network elements, and service providers.
- *Service*
  A service defines a set of capabilities offered by a service provider to a customer. Service equipment, controlled by the provider, generates the service for the user. The pure connectivity service offers an access to the Internet, incorporating layer 1 and 2 of communication protocols. Transport services provide the pure transport of IP packets, covering layer 3 and 4 of communication protocols. This may include QoS-enabled services supported by mechanisms in layers 1-4 for the differentiation of packets. Application services are those services which are build upon transport services, comprising WWW (World-Wide Web) including applets or directory services like Napster or Microsoft's NetMeeting ILS. They include communication services for personal communication as well, like video conferencing or Voice-over-IP (VoIP). Finally, content services include content-driven offers, like News-on-Demand (NoD) or Video-on-Demand (VoD). Note that each of these services is related exactly to one of the levels as introduced in Figure 2.
- *Service Provider*
  Service providers are defined in the context of the multi-service Internet on every level, noting different roles. In a competitive market situation multiple of these roles may be combined by a single provider. Therefore, as a provider of IP-based services the Connectivity Service Provider (CSP) offers connectivity and pure IP access to an IP-Router. The connectivity can be achieved via different technologies and infrastructures, such leased from a telecommunication provider (cellular or switched phone) or physically from the CSP himself (switched lines). A Transport Service Provider (TSP) provides transport services with varying qualities or value-added enrichments, including routing. An Application Service Provider (ASP) offers application services, which may be bundled. An ASP can be a software developer selling his product pre-configured according to users demand via the Internet, but also offering additional on-line services, like directory services. Finally, the Content Provider (CP) has to manage content and information which is delivered and transported to users.
- *User Services*
  User services are services which are valuable for the end user in a direct way. It is the general term for connectivity, transport, application, and content services.
- *User Service Equipment*
  The user service equipment is the equipment of the service provider which is used to provide any type of user services.

3 Problem Areas

Besides the definition and specification of a generic set of A^x services, which deals with architectural and systems-related areas, the particular A^x application to roaming and mobile users in the context of Mobile IPv6 is essential. Finally, performance issues of a potential implementation of the architecture are critical with respect to a practical and scalable solution.

3.1 Problems Building Generic A^x Services

The scenario discussion above highlighted major components and functions existing in a scenario where A^x services are employed. To achieve the objectives defined in Section 1.2, many problem areas have to be considered. These are related to the general definition of the generic architecture including logical functions. They concern the design and implementation of the architecture implying sig-

nificant use cases for such an A^x service, including mobile and inter-domain scenarios.

3.1.1 Architecture-related Problems

- Definition and functional specification of logical modules
- Location and replication of logical modules in physical network components
- Dependency of authentication and authorization policy on business models expressed by payment and charging schemes
- Dependency of A^x services on terminal, user, and service mobility
- Dependency of A^x services on the kind of service (connectivity, transport, application service, content)
- Integration of auditing

3.1.2 Systems-related Problems

- Specification of protocol and component interactions
- Specification of data structures and data records for all A^x services
- Warranty of data privacy of all data in an inter-domain scenario
- Specification of a uniform user identifier
- Definition of technology-dependent (layer 2/layer 3) information available for any policy-related decision, including air interfaces, link-level, and network layer information
- Static trust model in an inter-domain multi-provider Internet
- Dynamic establishment of inter-domain trust relationships for all A^x services

3.2 Problems Applying Existing Services in Roaming Approaches and Mobile Scenarios

On a short term view it is also possible to extent existing AAA systems to support new requirements, particularly belonging to the implementation of mobility scenarios and roaming approaches, instead of building a new generic architecture. Existing AAA protocols, which will be presented in Section 4.3, and protocols supporting mobility like Mobile IP should be considered as the basis. These areas of concern are also revised in the project MobyDick (Mobility and Differentiated Services in a Future IP Network) [52]. These major problems will not be examined in depth at this stage, but should are considered a highly important problem area, which can be solved in a technology-dependent approach.

- Trust model in case of IPv6 and Mobile IP, covering security associations between the mobile node, AAAF (AAA Foreign), AAAH (AAA Home), and the HA (Home Agent)
- Integration/interaction of authentication/authorization issues with Mobile IPv6
- Definition of functionality and its location in AAAF, AAAH, HA, and the Packet Data Serving Node
- Warranty of data privacy in case of interdomain accounting and charging
- Impact of implementation of fast handovers for intra-domain, inter-domain and inter-technology handovers on authentication and authorization.
- Content of the accounting record depending on the scenario, the payment scheme, the mobility policy
- Type of credentials for mobile users/customers

Note that some of these issues have been solved for IPv4, but their use in a native IPv6 environment remains unsolved.

3.3 Performance Issues

Beyond these problems described, for each particular solution decision performance, scalability, and robustness issues have to be regarded in an integrated fashion.

- Scalability of the architecture and charging support with respect to thousands, even millions of users/customers
- Scalability of A^x components
- Strength and performance of authentication, authorization protocols, and auditing mechanisms
- Scalability of involved parties for authentication as well as authorization protocols and mechanisms like PKIs (Public Key Infrastructures)

4 Policies, Mechanisms, and Protocols for A^x

To offer services to customers, service providers have to manage distributed systems. This includes the configuration of networking devices (hardware) and the provision of various protocol mechanisms (software). Therefore, all existing AAA functions and their extensions can be seen as a provider-internal service. They cover policies, mechanisms, and protocols supported by exchanged or stored data record formats.

4.1 Policies

Policies define one possible approach to constrain communication in networks and to manage networks. The use of policies for network management in general has different advantages over, *e.g.*, manual (command line) configuration or management via the Simple Network Management Protocol (SNMP). Special evolutions as described in Section 1 can be handled by applying the policy paradigm to networks. The separation of a policy from an implementation enables dynamic changes to the management of systems and modifying the behavior of the system. It allows also for reusability of policies in different heterogeneous environments especially inside different administrative domains [63].

Since the beginning of the nineties it has been proposed to apply the policy paradigm in the area of network management [63]. The first major application of policies was access control in distributed systems. It is often termed “Role-based Access Control” [29], [61]. The first broader application of policies inside the Internet world is on QoS management in the Integrated Services and Differentiated Services architectures [9], [5], and [8].

These activities resulted in a more general work on network policies. The IETF policy framework working group is working on the definition of a policy terminology [75] and a network policy framework in general [38]. The IETF and the Distributed Management Task Force (DMTF) are concentrating on an object-oriented information model, the Common Information Model (CIM) [22] and extensions, the Policy Core Information Model [54]. These information models determine the base to represent policies of different types, like QoS or authorization policies.

Architectures for the use of policies are under discussion, too. Many architectural proposals use a common basic scheme with elements like Policy Decision Point (PDP), Policy Enforcement Point (PEP), and Policy Repository (PR) [49], [69], and [76]. In many proposals the PR is seen as a directory (cf. Section 5.3 for details). For an implementation COPS (Common Open Policy Service) [7] and a Policy Information Base (PIB) [17] have been proposed within the IETF (cf. Section 4.3).

Many languages for the specification of policies for different applications are proposed. They use either a natural language-like, syntactical or a formal logic-type of approach. The formal logic approach is often used for security policies [43], [57]. Mechanisms for consistency and conflict checks as well as for policy hierarchies have been an intensive topic of research. For network policies most languages use a syntactical approach [3], [18], [50], [56], [67], and [68]. There is also a proposal for an application area-independent language, called PONDER [20]. A survey on languages and policies in this area can be found in [67].

The IETF applies the policy paradigm on security as well. The IP security policy working group [36] is working on communication security policies, mainly for IPsec (IP Security) Architecture. This work started due to the restriction of IPsec protocols to exchange keying material and policy information only between end-points of a security association. The working group will define a data model as a representation of the policy core information model for IPsec policies, where most of the work is described in [44], including an architecture for policy management, a policy language, and a policy exchange protocol.

4.1.1 Application of Policies in the AAA Domain

For building a AAA infrastructure, a general approach based on policy rules is proposed by the IRTF AAAArch research group (cf. Section 5.3).

Concerning the scenario as described in the introduction (cf. Section 1.1), enhanced AAA services, A^x services become more and more important. A^x services are required essentially by providers to offer transport services as well as information services in a commercial environment. Therefore, A^x services can differ strongly, *e.g.*, on which accounting information is needed or which charging scheme shall be supported. In addition, the application of the policy-oriented paradigm in the area of A^x is productive to achieve those advantages specified above. A policy-based A^x services infrastructure offers the potential to separate service descriptions in form of policies from mechanisms and system-specific information. Furthermore, policies enable the construction of inter-domain A^x services applicable in the multi-domain Internet.

4.1.2 Relationships between Policies and Mechanisms

To explain the relationship of policy-based A^x services and their mechanisms implementing the service, a graphical representation is shown in Figure 4. It depicts dependencies between different policies. There exist two points of view: One starts at the top and follows to the bottom of the graph, defining the systematic view, where the upper level policy requires a set of mechanisms to be selected for its enforcement. *E.g.*, (1) the overall commercial policy of a service provider is enforced by billing, charging, and authorization mechanisms, or (2) the charging policy requires for enforcement an accounting mechanism. In addition, each of these mechanisms “owns” a policy themselves, determining which internal algorithm should be applied. *E.g.*, in case of the accounting mechanism, the accounting data record in use, such as the Call Data Record (CDR) or the Internet Protocol Data Record (IPDR) (cf. Section 4.4 below). Therefore, policies are not independent from each other.

The second point of view starts at the bottom and follows to the top of the graph defines the operational view. Accounting has to be done before charging, and authentication is a precondition for authentication-based authorization. Auditing is a support service. It is not necessary for service provisioning, but may be required due to legal and regulation reasons.

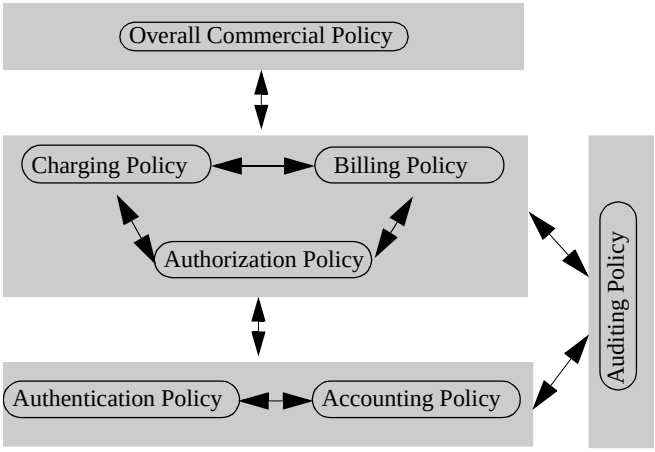

Figure 4: Model of A^x Policies

Section 4.2 discusses important mechanisms which can be part of policies for different services and how they enable the control of different mechanisms.

4.1.3 Relationship between Policies and Layers

Policies enable the application of actions, as defined in Section 2. Therefore, it is a key problem to identify parameters and values, which originate from the network, to base a policy decision on. These information and parameters in detail may originate from various layers of a communication network:

- Layer 2: Technology-related, *e.g.*, QoS on the link
- Layer 3: IP-oriented, *e.g.*, router statistics or network data
- Layer 4: Application-based, *e.g.*, ports or transport protocols

Depending on the network management model as well as the security and trust model, those layers of input parameters for policies are specified driven by available metering technology for QoS, topological information, or protocol information of data being in transit. According to Figure 4, a usage-based volume charging policy requires the metering technology for packets sent to be in place. The accounting policy in this case may restrict the metering to collect numbers for all bytes being transferred in a given time period. This is particular the case for the application scenario of Section 1.1, where the ADSL link to the home is provided with a transmission cap on the received data volume. For example, this policy is essential for the service provider to ensure that his backbone network will not be overloaded, or in case of additional requests, that this traffic is additionally charged for.

4.2 Mechanisms

To provide a complete overview, traditional AAA mechanisms and enhancements to them are presented at this stage separately.

4.2.1 Authentication

Authentication defines the verification of the identity of a subject. Authentication mechanisms can be classified as follows:

- *Knowledge*-based authentication founds on the knowledge of shared secrets, such as PINs (Personal Identification Number) and passwords.
- *Cryptography*-based authentication includes digital signatures, challenge-response mechanisms, and message authentication codes. The user owns a private key as a characteristics.
- Authentication based on *biometrics* uses inherent informations on subjects like fingerprint, voice, and eye characteristic.
- Authentication based on *secure tokens* binds the subject to some kind of ownership, e.g. the ownership of a smart card. It is combined mostly with cryptographic mechanisms to transfer the information on the token to the authenticator.
- *Digitized signatures*, including digital images of handwritten signatures and signature dynamics (i.e., measurements of the direction, pressure, speed, and other attributes of a handwritten signature) are not widely used so far.

An authentication policy describes whether authentication has to be done and which authentication mechanisms and algorithms (actions) should be used under which constraints.

4.2.2 Authorization

Authorization is defined as the verification of whether a subject is allowed to perform an action on an object or not. Authorization mechanisms can be categorized in two major classes:

- *Authentication-based* mechanisms require an authentication of the subject as precondition for the authorization. The information for the authorization decision is stored at object systems, such as in Access Control Lists (ACLs) of operating systems in the form “User S is allowed to perform action A on an object O”. Another example are database systems which enhance this basic lists by conditions based on attributes of the object. “User S is allowed to do action A on objects O, which fulfill the conditions C”.
- *Credential-based* mechanisms use credentials which are trustworthy information being hold by subjects of an authorization process. Credential-based mechanisms are widely accepted in E-Business, *e.g.*, in form of micro payments Millicent [33] or used in SPKI [27].

Authorization policies define those actions a subject is permitted to perform on an object. An authorization policy may be positive (permitting) or negative (prohibiting).

Formally, an authorization policy can be defined basically as follows:

a set O of objects
a set S of subjects
a set A of action types
Authorization rule: triple (s, o, a) where
$s \in S, o \in O, a \in A$
f: S x O x A -> (True, False)

“if f(s, o, a) = True”, the authorization decision is positive. If not, the subject did not achieve the authorization.

This basic definition is enhanced, to include constraints into the policy. These constraints can be current object states or universal conditions. This denotes, that the policy decision can depend on the value of attributes of the object or on universal conditions like time [63].

There exists obviously a great similarity between policies and mechanisms for authentication-based authorization. For credential-based mechanisms a credential has a similar form as a policy, whereby the set of objects has only one element which is the user (may be anonymized) who owns the credential.

4.2.3 Accounting

An accounting system takes two major tasks, to collect data from metering systems and to distribute data to users of accounting records. Therefore, two kinds of policies belong to the collection and distribution.

The user of accounting records can, depending on his objective, specify via an accounting policy, which information he needs at which time from the accounting system. This policy can be event triggered by internal events, the billing system request on an accounting record, or by external events like the end of month. Policies can be obligation-driven also: “if a new charging scheme is placed, new accounting informations has to be collected.”

For the collection task a metering policy describes which information has to be metered by a metering system and transported to the accounting system. These policies are event triggered by a signalling event unless static meters are used, which collect data for all flows in a fixed granularity [16]. Obviously, an accounting policy influences metering policies or is enforced through metering policies.

4.2.4 Charging

Charging includes the most entangled policy and mechanism at the same time. While a charging policy defines those tariffs and parameters which are applied by charging mechanisms, a charging mechanism provides the infrastructure to calculate final charges for service usage on accounted for information. Therefore, the term Charge Calculation is applied for the mechanism only [65]. Assuming that an overall commercial policy exists, a specific policy drives service providers to gain money and survive in the market. At this stage charging becomes a necessity and, in turn, billing. Therefore, charging is considered itself a policy. However, other service provider policies may exist, such as a government-driven social welfare. While policies determine descriptively which action to take or to react on an event, charging is considered as a dedicated policy to enable a provider to gain revenue for a given network and service offer. In addition, an internal task a provider must be engaged in is the pricing of resources and services. It forms the major input vector for the charge calculation and defines an intended market policy for charging Internet services.

4.2.5 Auditing

Auditing is defined as the independent examination of accounting records, or logged system data. The mechanisms used are dependent on the auditing goal. Auditing for an after usage proof of consumed resources and customers charges is performed by logging signed requests and session status records by the provider or by a trusted third party. Afterwards, evaluations may be necessary.

By applying this in a strong manner, event sequence tracking can be applied. Event sequence tracking or reconstruction is important particularly in the areas of financial transactions, where transactions must be irrefutable. Systems with irrefutable transactions provide non-repudiation service. Non-repudiation services generate, maintain, and validate irrefutable evidence of events in every transactions. The ISO (International Organization for Standardization) non-repudiation model is related to events of sending or receiving a message [39], [40], and [41]. Two types of non-repudiation services are distinguished: non-repudiation of origin (NRO) and non-repudiation of receipt (NRR). NRO gives the recipient the evidence that the sender has sent the specified message. NRR provides the sender the evidence that the recipient has received the specified message. Non-repudiation service comprises of four phases: evidence generation, evidence transfer and storage, evidence verification, and disputes resolution. There are two approaches in implementing non-repudiation services: with and without a trusted third party (TTP). Without the help of a TTP, secrets are released gradually. In early efforts, a TTP acted as a delivery agent to provide non-repudiation of submission (NRS) and non-repudiation of delivery (NRD). Current non-repudiation protocols reduced the involvement of TTPs to deal with keys only rather than with the content of transferred messages. A non-repudiation protocol is fair, if it provides the originator and the recipient with valid irrefutable evidence after completion of the protocol, without giving a party an advantage over the other party in any possible incomplete protocol run [77]. A fair non-repudiation protocol using an on-line TTP is proposed in [77]. In [78] the more secure and efficient fair non-repudiation protocol using an off-line TTP is presented.

A simple mechanism for auditing the correctness of logged system data is to compare log entries from cooperating servers. Auditing to detect security breaches is done using audit trails, which are an unbroken chronological log of activities and events containing information on who did what, when, where, and how. Actors or subjects involved in those activities or events can be users (human being), hardware (hosts, routers), or software (operating systems, applications). The examination can take the form of a real-time continuous or periodical monitoring of audit trail and immediate response or reaction, if some unexpected events or activities happen. Performing the examination off-line is possible, but may lose the chance to avoid security violations. Auditing policies in this sense describe which event and activities should be recorded in the audit trail and how the audit trail is checked.

Proving service request and access granting is a more general case, while proving service provisioning and service usage is usually application-dependent and sometimes hard to decide without human intervention. It is shown in [34] how non-repudiation methods are used to prove service request and access granting for a lease service.

4.3 Protocols

Different protocols in support of AAA on different levels exist. Those being discussed inside the IETF AAA working group and related ones are outlined.

4.3.1 Authentication Protocols at Connectivity Level

Authentication protocols are widely used in establishing a data-link layer connection, mostly a dial-up connection between an end-user’s host and the Network Access Server (NAS), but also for switched lines. In general, they allow a peer to transmit authentication information to the authenticator until the authenticator acknowledges the peer. In PPP PAP (Password Authentication Protocol) [46] the authentication is based on a pair of user name and password. PPP CHAP (Challenge Handshake Authentication Protocol) [62] supports a challenge response mechanism, which is controlled by the authenticator. In a challenge response mechanism the password does not have to be transmitted over the link. PPP EAP (Extensible Authentication Protocol) [6] supports authentication based on different mechanisms, identity- and challenge-based, but also using One Time Passwords or Generic Token Cards. These protocols are often integrated in the protocols at the transport level, which implement authentication-based authorization.

4.3.2 RADIUS

The RADIUS (Remote Authentication Dial In User Service) protocol [59] has been designed for transferring authentication, authorization, and some configuration data between a NAS, which is a RADIUS client, and a particular RADIUS server, which holds the information to authenticate and authorize a user. The RADIUS server itself can act as a client to other RADIUS servers. Originally, RADIUS has been defined to support dial-up connections and today it is being used in many more scenarios. RADIUS uses different

authentication protocols listed above. Extensions are defined in [58] for delivering accounting information to a RADIUS accounting server. There are major shortcomings in RADIUS, for which reasons it is not considered acceptable as a typical AAA protocol [12], [51].

4.3.3 Diameter

The Diameter protocol has been defined as a successor of RADIUS, which removes known RADIUS deficiencies. The scope of the protocol is limited to satisfy requirements of network access using different access technologies. Due to this it is not a generic AAA Protocol [12]. Diameter consist of a base protocol [13], which defines header formats and security extensions as well as a number of mandatory commands and AVPs (Attribute Value Pairs). The base protocol is a session-oriented protocol based on a peer-to-peer model. Diameter operates over SCTP (Stream Control Transmission Protocol) [64] as transport protocol, which is not widely used so far. Information is exchanged by means of AVPs.

Different extensions to the base protocol allow the usage of different access technologies, by defining special command codes and AVPs. The NASREQ (Network Access Server Requirements) extensions [15] cover the support of RADIUS authentication protocols, PPP EAP, and authorization needed by NAS-Services. Mobile IP extensions define AVPs to support Mobile IP across disparate administrative domains [14]. By this a Diameter server is able to authenticate, authorize, and collect accounting information for services requested by a mobile node. The accounting extension [4] defines a set of generic accounting AVPs that can be used for all services and supports real-time accounting. Each Diameter extension defines their own service specific accounting AVPs.

4.3.4 COPS

The COPS (Common Open Policy Service) protocol [7] is a protocol to exchange policy information between a policy Policy Decision Point (PDP) and the Policy Enforcement Points (PEP). It is a simple query and response protocol in a client/server model. PEPs are clients and PDP acts as server. COPS supports two common models for policy control: the outsourcing and the provisioning model.

COPS has been originally specified to allow authorization of Resource Reservation Protocol (RSVP) resource requests in networks supporting Integrated Services. But the protocol has been designed to be applicable in a much larger context. Policy Provisioning by COPS has been suggested in [17], independent of a special applications. COPS is considered acceptable as an AAA protocol for requirements defined in the AAA working group [51]. Therefore, additions are made in [25] to extend COPS from the client server model to a broker-based or proxy-based model supporting AAA.

4.3.5 SNMP

SNMPv3 (Simple Network Management Protocol Version 3) proposes a new management model. This model enables the design, development, and deployment of sophisticated management applications, also AAA applications. Especially accounting is supported by transferring accounting records to and storing them in a SNMP Management Information Base (MIB). But SNMP can not be accepted as a general AAA Protocol [51], since it is restricted to a low-frequency management information base access scheme.

4.3.6 Further Protocols

In addition, further protocols can be used for authentication and authorization; some protocols being application-independent, like DHCP and DNS, and some being integrated into an application to authorize the use of this application. The following list can not be complete, but it shows that AAA tasks is not performed at the connectivity and transport level only.

- *DHCP*
  The Dynamic Host Configuration Protocol (DHCP) [23] provides no methods to authenticate clients requesting configurations. In [24] mechanisms of authentication of the source and contents of DHCP messages are added, which allows for the authorization of clients also.
- *DNS*
  Reverse Domain Name System (DNS) lookups on source IP addresses can be used for access control. The DNS name assigned to the IP address is used in order to perform access management. This needs a secure DNS system itself, maybe as defined in [26], and requires that all hosts owning DNS names are enlisted in internal tables, which is often not the case especially when using DHCP.
- *LDAP*
  LDAP (Light-weight Directory Access Protocol) can be used to publish different information, policy information in general as well as access control information, for instance in form of Access Control Lists (ACLs). Since access to LDAP information can be authenticated [74] LDAP can be regarded as a protocol supporting AAA.
- *HTTP Authentication*
  Part of the Hypertext Transfer Protocol (HTTP/1.1) [30] is a framework for a basic access authentication scheme. [31] specifies a basic and a digest authentication scheme. Applying these mechanisms, the access to Web pages can be authorized.
- *Secure Socket Layer*
  The Secure Socket Layer (SSL) protocol is located on top of the transport layer and offers applications using protocols like HTTP, File Transfer Protocol (FTP), or Post Office Protocol (POP) to authenticate the server and client and to build a secure connection providing confidentiality, integrity and authenticity. SSL 3.0 is part of Transport Layer Security (TLS) [21].
- *Secure Shell*
  Secure Shell (SSH) is a client-server application which offers the authentication of users and machines establishing a terminal connection between client and server using TCP/IP (Transmission Control Protocol/IP). It is used for encrypted remote logins instead of insecure rlogin or telnet applications.
- *Credit Card Systems*
  Typing in the credit card number in an HTML (Hyper Text Markup Language) form to buy access to content in the WWW and transferring this number via HTTP

defines in principle an authorization approach used for content services.

4.3.7 Overview

These protocols described show a variable degree of suitability for generic AAA purposes. As depicted in Figure 5, they can be arranged according to the levels introduced in Figure 2, where the signaling and data path are considered in an integrated fashion. Figure 5 does not depict the implementation view, but clearly indicates those levels at which a user service may be offered by applying the respective protocol. Therefore, the Abstract Objects mentioned above are instantiated particularly to AAA protocols, each of which providing a highly specialized service.

AAA Protocols

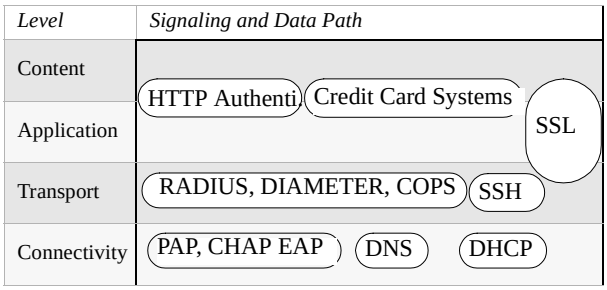

Figure 5: AAA Protocols

4.4 Standards for Data Records

The above mentioned Call Detail Records (CDR) [42] and Internet Protocol Detail Records (IPDR) [19] are two examples for accounting records as agreed upon data structures. In addition, RADIUS Accounting Records (RAC), the DIAMETER attributes, and Real-time Flow Measurement (RTFM) architecture are important. The recently published informal RFC (Request for Comments) on accounting attributes and record formats [11] summarizes existing IETF and ITU-T work and discusses advantages as well as drawbacks in closer detail.

While CDRs [42] are sometimes termed Call Detail Reporting, Call Data Records, or Station Message Detail Record (SMDR), they are the most commonly known records for call-specific data, originating from telephony-based telecommunication systems and developed over many years in an environment with quite static services portfolios. Such a record defines the fundamental unit of data to be exchanged in the circuit-switched voice world. It contains data about each call made, *e.g.*, dialed digits, the phone number dialed from, call direction, service type, associated inverse multiplexing session and port, date, time, off-hook time, on-hook time, determining how long the call lasted, and a circuit identifier. Virtually all telephony switches, Private Branch Exchanges (PBX), and ATM (Asynchronous Transfer Mode) switches [60] produce CDRs. However, each switch product tends to produce CDRs in different formats, which means that data fields of each record may appear in a different order from one switch to another. Therefore, performance-intensive software needs to convert various CDR formats into a standard format usable by a charging system. Because the network provider may charge for bandwidth on an as-used basis, the CDR can be used to understand and manage bandwidth usage. However, they are different in that an SMDR is focused on the station (terminal) and the CDR is focused on the call itself. Therefore, the two terms should not be used interchangeably, since the formats of the records will be different. Usually, a single device, say a PBX, will produce one or the other, not both.

To cope with networking characteristics of the Internet, mainly the packet-switched characteristic compared to the telephone network's circuit-switched system, a corresponding data specification is required. In addition, the Internet market trend to develop and deploy new services frequently arises a second dimension of complexity for an "Internet CDR". Therefore, the initiative "IPDR.org" decided to develop a basic framework for a usage specification, called Internet Protocol Detail Record, allowing different companies to develop dedicated code within the framework, supporting interoperability and the usefulness of the specification [19]. It refers (1) to a functional operation, where an NDM (Network Data Management) function collects data from devices and services in a provider's network, and (2) to usage, the type of data, which shows an open, extensible, and flexible record format (the IPDR record) for exchanging usage information of essential parameters of IP-related transactions. A repository for defined IPDRs is envisioned, including the variety of services, such as e-mail services as well as real-time services. The framework will provide the foundation for the development of open, carrier-grade Internet services enabling next-generation IP networks to operate efficiently and cost effectively.

While RADIUS a.o. deals with start, stop, and activity data including various accounting, tunneling, and general attributes, Diameter being part of the AAA Architecture (cf. Section 5) inherits all of them and defines a secure protocol to transfer these accounting attributes. Finally, the RTFM architecture supports flow measurements via RTFM meter readers, which read data from MIBs to be stored in RTFM attributes, such as source and destination information as well as packets and byte counts.

Additional data formats are available, however, mainly with respect to a particular protocol as mentioned above or an application. DNS and DHCP maintain customer profile data, which form a type of standardized data format. Additionally, LDAP offers mechanisms with transfer capabilities for customer profile data. However, these data formats are not generally exploited for the purpose of accounting or other AAA tasks.

5 The IRTF AAA Architecture

The IRTF research group AAAArch aims at the definition of an architecture and model for inter-organizational AAA. To achieve this, they apply a policy-based approach. This group's work shall be in conformance to the work of the IETF policy framework group. Within the IETF a policy is defined as an aggregation of policy rules, made up of conditions and of policy actions [54].

5.1 AAA Components

The Rule-based Engine (RBE) is a central component, which evaluates policy conditions to take a policy decision

and executes a policy action depending on the outcome. Policies are stored in Policy Repositories (PR). In the IRTF research group the main focus is on authorization policies for service requests and accounting policies belonging to a requested service. The enforcement of policy actions has to be done by different components, depending on the kind of action. Most actions, belonging to a requested service have to be done by the Service Equipment (SE), which covers all kinds of network elements itself. Other actions belonging to support services, especially accounting, are done by AAA servers separated or integrated into the service equipment [47].

5.2 AAA Services

The foundation of this AAA Architecture is the assumption of a multi-domain Internet topology. In each administrative domain resides at least one AAA server. Distributed AAA servers offer authorization and accounting services. The authorization service is defined as the process of achieving an authorization decision to grant or deny a user's request for services or resources. An implied request is transformed into an authorized session by setting up the service equipment and logging the session's state. Accounting services record relevant accounting information obeying the authorization's decision and the ongoing resource use of the authorized session.

Authentication of users is not a generic part of these services. It may be done by a AAA server based on the user authentication information which can be part of the AAA request. Future extensions of the AAA servers are envisioned and discussed in the IRTF RG also.

To generate the AAA Services secure trust relationships between different AAA servers are necessary. By contract, the user establishes a trust relationship with one dedicated service provider, his User Home Organization (UHO). This UHO operates a AAA server, as all service providers do including the Foreign Organization, from where the user requests a service. For existing trust relationships between service providers' AAA servers the chain can be solved and the Foreign Organization can trust the user [72]. Therefore, authentication between peer AAA servers is also part of services [47].

5.3 AAA Architecture and Protocols

All components discussed above are structured in a AAA Architecture as shown in Figure 6. The RBE resides inside a AAA server. The AAA server receives service requests from the Service Equipment (SE) via an Application-specific Module (ASM) or form other AAA servers. On one hand, a request received by the AAA server is inspected by AAA servers considering policies stored in the PR. To evaluate policy conditions, it may be necessary to consult other AAA servers or the status of the service equipment. This is done firstly by sending requests to other AAA servers and secondly via an ASM. ASMs are needed additionally to enforce policy actions. Therefore, ASMs configure the Service Equipment and provision a service. On the other hand, policy actions are taken by the AAA server itself. It holds session states, records accounting data, and logs actions [47], [48].

The protocols used in this architecture include:

- (1) special AAA protocol, which is assumed to be standardized in the research group of the IRTF
- (2) particular API (Application Programming Interface) or the AAA protocol also
- (3) depending on the implementation of the PR, the LDAP or an API
- (4) an application-specific protocol

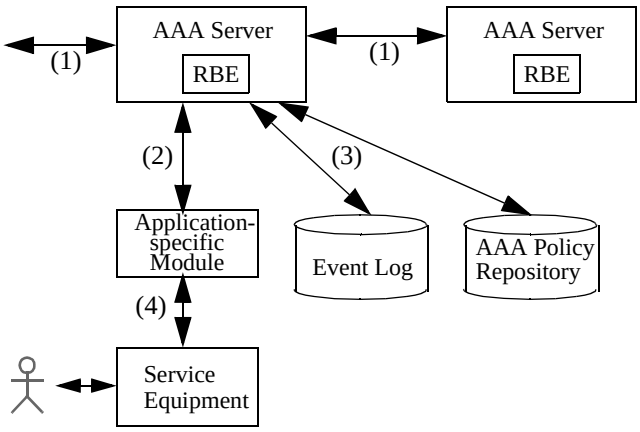

Figure 6: AAA Architecture

6 Proposed Generic A^x Architecture

In Section 3 key problem areas were listed to motivate the required extensions of the traditional AAA Architecture. Until today, they have been solved for highly specialized scenarios only. Due to the advantages discussed above, a policy-based approach defines an excellent starting point, but the IRTF's AAA Architecture can not solve all problems related to A^x services. There exist some major weaknesses presented below and the architecture is not completely generic:

- Functions of policy decision and policy enforcement are not separated clearly. The AAA server takes policy decisions on authorization, but also enforces accounting policies by performing accounting tasks.
- The extensibility to functions beyond AAA, as presented in Section 4.1.2 is complicated, since components are not defined in a generic way. Many enforcement functions are located in the AAA server itself or in the ASM.
- The usability of A^x services for applications and content level services is difficult, since AAA services are provisioned mainly for transport and connectivity level services. Especially accounting, auditing, or charging are not defined for these upper levels.
- The function of the ASM has not been defined completely. It seems to act as a place holder for those tasks, which can not be assigned otherwise.
- The inclusion of QoS-related support services has not been considered.

The appropriate desire is given by an architecture for generic A^x services, which can be used in all applications shown in the scenario in Section 1.1 and additional ones.

6.1 Approaching a Generic A^x Architecture

As a path leading toward such a generic architecture the following steps are proposed:

- Definition of network policies describing the behavior of A^x supporting elements separated for each A^x service and for each level as defined in Section 1.2.
- In-depth examination of dependencies between policies for different A^x services and also to an overall commercial policy, which by itself will not be part of the A^x architecture.
- Definition of basic logical modules which, on one hand, are necessary to enforce different policies and, on the other hand, support the policy management, like with PDPs or PRs. These logical modules define the design space of the architecture.
- Investigation of different implementation architectures which can be build out of these logical modules. These components of the architecture can implement one or more logical modules. They can be replicated and located in different domains. These instantiated architectures differ with respect to performance, scalability, and robustness as well as functionality.
- Definition of A^x protocols involved in that type of architecture and their interaction between components.
- Validation of instantiated architectures by mapping them to different complex multi-service multi-provider scenarios, like the one shown in Section 1.1.

6.2 Scope of a Generic, Policy-based A^x Architecture

The overall commercial policy, as mentioned in Section 4.1.2, is enforced on one hand using the Service Equipment providing those services requested from users and on the other hand from entities providing different A^x services. The behavior of each entity performing an A^x service can be described by a policy derived from the overall policy. The behavior of the Service Equipment, which is controlled by the service provider, can be described as whether and how a service is provided to a customer dependent on constraints and additionally by describing the internal behavior of the Service Equipment, depending on the state of the system. The first one can be derived also from an overall policy and represented as an authorization policy.

Due to these reasons and advantages described in Section 4.1.1 the policy paradigm is utilized to build an A^x service architecture. As the base of a generic A^x Architecture the common base scheme for policy-based architectures as shown below is applied.

Policies are edited via a policy management tool in general. This can be a simple editor, but also a full management tool which performs inconsistency- and conflict checking. Policies edited are distributed to the PR or directly to the PDP by configuration. PDPs take decisions, which means, they evaluate policies along with other data and potentially other policies. If a policy maps, the policy is sent to a PEP. Therefore, policies are translated in configuration data for the PEP. The corresponding architecture is depicted in Figure 7 which shows a scalable approach for multiple PDPs and PEPs in support of PRs.

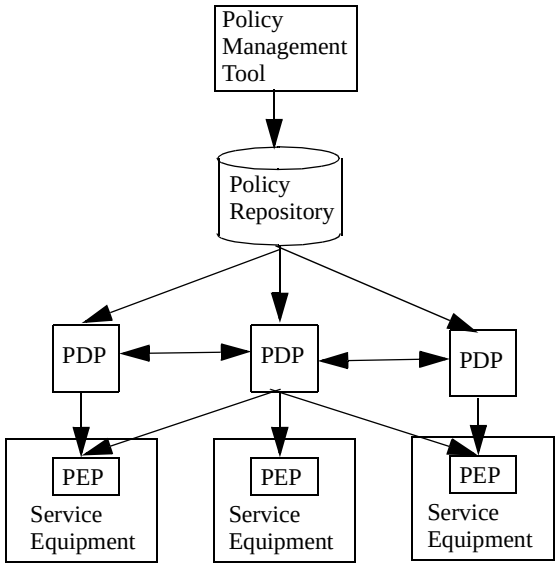

Figure 7: Policy-based Management Architecture

6.2.1 A^x Modules

Necessary modules of the A^x Architecture can be deduced from the base scheme. All different A^x policies have to be stored in a PR. This can be a single integrated one or many distributed ones. To evaluate policies, a PDP is used as a module. There can be one PDP for every of the different kinds of A^x policies or an integrated one. The instantiated design is dependent on those dependencies between different kind of policies. While the PDP is the major part of the A^x server, investigations on policy dependencies are for further work.

PEPs are also modules of the A^x Architecture. They are located in the Service Equipment, either the Service Equipment used to provide user-requested services or Service Equipment providing A^x services only by implementing the variety of mechanisms. To describe PEPs different policies and functions presented in Section 4 have to be considered.

Authorization policies are normally enforced by a decision with specified service parameters, whether or not a service is provided. This decision describes the behavior of the Service Equipment according to a user request.

Authentication policies are enforced by a special module, which owns necessary authentication information on identities to be authenticated, depending on the mechanism, and which implements various authentication mechanisms.

The PEP of a metering policy is located regularly in the Service Equipment for user-requested services or an extension of this, since it meters service provisioning. Appropriate data can be transmitted to an accounting module or can be stored inside or outside the Service Equipment itself.

For accounting and charging purposes PEPs are located in special modules, which are operating on metered data by aggregation and other mechanisms. Results of these operations are stored in accounting and charging databases.

The location of enforcement points of auditing policies is dependent on mechanisms described for auditing policies. For real-time auditing the enforcement is performed in all

modules provisioning services, covering user services as well as A^x services. For an after-usage-auditing a special auditing PEP is necessary.

Overall the following components have been identified:

- A^x PDPs as a major part of an A^x server
- A^x Policy Repository
- Authentication PEP module
- Authorization PEP module inside the Service Equipment
- Metering PEP module inside the Service Equipment
- Accounting and Charging PEPs with additional databases for accounting and charging records
- Auditing PEPs dependent on auditing policies located inside each other module or as an independent module

Additionally, a policy management tool is essential, which allows administrators to specify those A^x policies required.

Different modules have to be arranged in the generic architecture. By using the common base scheme, as shown in Figure 7, the proposed architecture can be drawn, where each A^x PEP is considered as an isolated module. After an in-depth examination of these dependencies, this can be adapted, mainly driven by dedicated performance and security issues as presented in Section 3.3. Furthermore, additional elements are required for the implementation of enforcement purposes, like event logs or session directories.

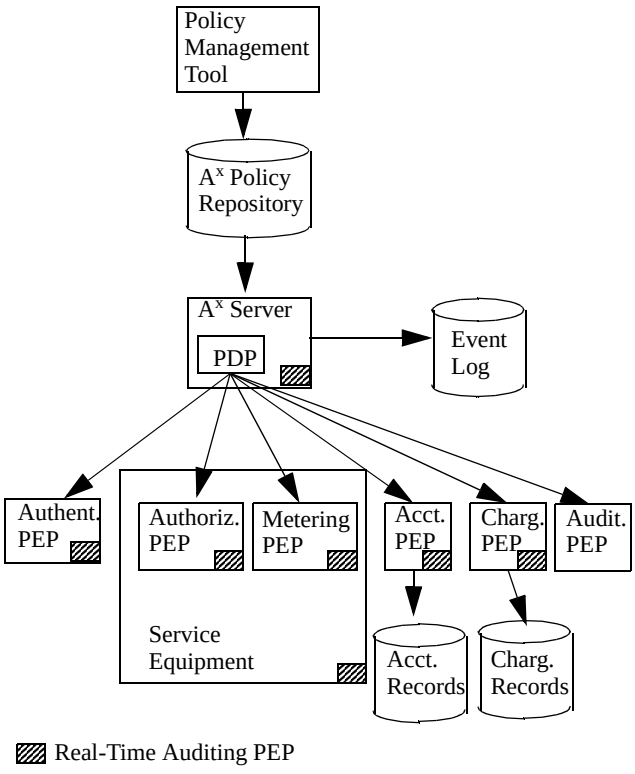

Figure 8: Generic A^x Service Architecture

Figure 8 shows the proposed architecture, while only major relations are depicted. *E.g.*, the accounting PEP requires metered data, originating from the metering PEP, or the auditing PEP inspects accounting or charging records accordingly.

6.2.2 A^x Services

A^x services are independent services which are provided for Service Equipment performing user-requested services or to other A^x servers. If an A^x service is requested from an A^x server, he requests necessary policies from the PR and takes the policy decision, depending on constraints. A^x services are performed by the A^x server through the enforcement of policies in the different PEPs.

For instance, if a user requests an application service, the application Service Equipment sends an A^x service request to the A^x server. This request has to specify the requested service as a minimum. Depending on the authentication policy, authentication information on the user are needed further on. The A^x server takes the policy decision and configures, if the request is authorized, the Service Equipment and, additionally, the other A^x PEPs in respect to these policies. There does not have to be an explicit response to the A^x service request, aside from the authorization enforcement. If the authorization succeeds, all other A^x services have to be enforced also. If this is impossible, the authorization decision has to take this into account. It has to be noted, as shown in Figure 3, that some services, like authentication and authorization, are delivered once, when the request is signalled. Other services like metering and real-time auditing happen continuously during the service delivery. Finally, others like accounting and charging can be performed afterwards. This has to be ensured in the signaling phase by configuration of PEPs.

Different protocols are needed to implement this proposed architecture. To request a service from a user, a special protocol is needed. It is necessary to define an interface, like LDAP, between the PR and the A^x server. Different interfaces between the A^x server and different PEPs are necessary as well.

7 Summary and Conclusions

Based on a real world scenario this work motivated the future necessity of A^x services in a commercial-driven Internet, where many problems identified restrict the design and implementation of A^x services. To solve these problems of A^x services for todays and future user services a generic approach has been proposed. Therefore, user services on different levels and A^x services have been separated clearly. Applying the theoretical policy paradigm to describe different A^x services and the behavior of the according Service Equipment is defined. Based on these consideration the existing policy architecture base scheme has been adapted to the A^x environment to define a generic A^x architecture.

Assuming an implementation of this architecture, including major mechanisms and protocols, all user services shown in the application scenario of Section 1.1 are able to use A^x services under the following preconditions. (1) In each administrative domain an A^x server, which determines the PDP, has to be located, (2) trust relationships between service provider's PDPs have to be established, and (3) the provider's overall commercial policy has to be described in a uniform way. The adaptation of the scenario, including the

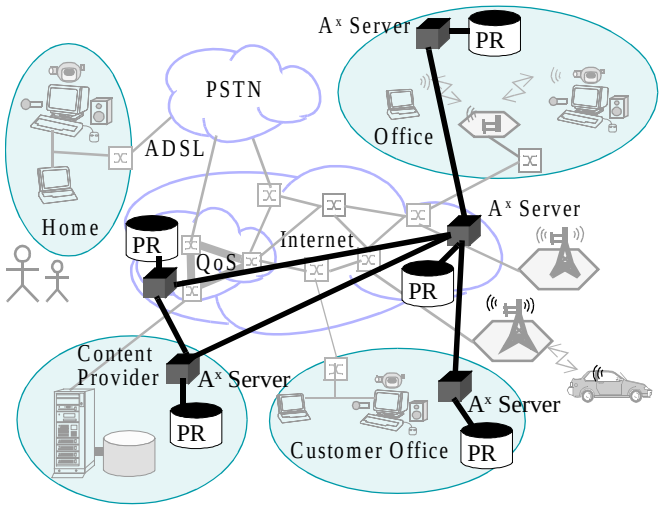

Figure 9: Ax Service Application Scenario

infrastructure of newly distributed Ax servers, is shown in Figure 9.

Future work is concerned with the analysis of dependencies between different Ax policies and the overall policy. In particular, implications on authentication and authorization policy are of interest. In addition, the detailed investigation of QoS support plans by this Ax Architecture is under consideration, enabling a homogeneous and integrated approach. Furthermore, the presented higher-level draft architecture will be extended to a complete model of a generic Ax Architecture, including a proposed Ax protocol, Ax data types, and Ax message sequence charts, which will enable the functional prove of this model's value in different major scenarios.

Acknowledgments

This work has been performed partially in the framework of the EU IST project Mobility and Differentiated Services in a Future IP Network (MobyDick, IST-2000-25394), where ETH Zürich has been funded by the Swiss Bundesministerium für Bildung und Wissenschaft, Bern under grant No. 00.0275. In addition, the authors like to acknowledge many fruitful discussions with P. Kurtansky, T. V. Prabhakar, and J. Pandey on the design of the generic Ax Architecture.

References

[1] B. Aboba, J. Arkko, D. Harrington: *Introduction to Accounting Management*; IETF, RFC 2975, October 2000.

[2] B. Aboba, P. Calhoun, S. Glass, T. Hiller, P. McCann, H. Shiino, P. Walsh, C. Perkins, B. Patil, D. Mitton, S. Manning, M. Beadles, X. Chen, S. Sivalingham, A. Hamed, M. Muson, S. Jacobs, B. Lim, B. Hirschman, R. Hsu, H. Koo, M. Lipford, E. Campbell, Y. Xu, S. Baba, E. Jaques: *Criteria for Evaluating AAA Protocols for Network Access;* IETF, RFC 2989, November 2000.

[3] C. Alaettinoglu, C. Villamizar, E. Gerich, D. Kessens, D. Meyer, T. Bates, D. Karrenberg, M. Terpstra: *Routing Policy Specification Language (RSPL)*; IETF, RFC 2622, June 1999.

[4] J. Arkko, P. Calhoun, P. Patel, G. Zorn: *Diameter Accounting Extension*; Internet Draft, work in progress, draft-ietf-aaa-diameter-accounting-01.txt, March 2001

[5] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss. *An Architecture for Differentiated Services;* IETF, RFC 2475, December 1998.

[6] L. Blunk, J. Vollbrecht: *PPP Extensible Authentication Protocol (EAP)*; IETF, RFC 2284, March 1998.

[7] J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry: *The COPS (Common Open Policy Service) Protocol;* IETF RFC 2748, January 2000.

[8] R. Braden, D. Clark, S. Shenker: *Integrated Services in the Internet Architecture: An Overview;* IETF, RFC 1633, June 1994.

[9] B. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin: *Resource Reservation Protocol (RSVP) Version 1 Functional Specification*; IETF, RFC 2205, September 1997.

[10] N. Brownlee: *Traffic Flow Measurement: Experiences with NeTraMet;* IETF, RFC 2123, March 1997.

[11] N. Brownlee, A. Blount: *Accounting Attributes and Record Formats;* IETF, RFC 2924, September 2000.

[12] P. Calhoun, G. Zorn, P. Pan, H. Akhtar: *Diameter Framework Document*; Internet Draft, work in progress, draft-ietf-aaa-diameter-framework-01.txt, March 2001.

[13] P. Calhoun, A. Rubens, H. Akhtar, E. Guttman: *Diameter Base Protocol*; Internet Draft, work in progress, draft-ietf-aaa-diameter-01.txt, March 2001.

[14] P. Calhoun, C. Perkins: *Diameter Mobile IP Extensions*; Internet Draft, work in progress, draft-ietf-aaa-diameter-mobileip-01.txt, March 2001.

[15] P. Calhoun, W. Bulley, A. Rubens, J. Haag: *Diameter NASREQ Extension*; Internet Draft, work in progress, draft-ietf-aaa-diameter-nasreq-01.txt, March 2001

[16] G. Carle, S. Zander, T. Zseby: *Policy-based Accounting*, Internet Draft, work in progress, draft-irtf-aaaarch-pol-acct-02.txt, March 2001.

[17] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, A. Smith: *COPS Usage for Policy Provisioning (COPS-PR);* IETF, RFC 3084, March 2001.

[18] D. Clark: *Policy Routing in Internet Protocols*; IETF, RFC 1102, May 1989.

[19] S. A. Cotton (edt.): *Network Data Management – Usage (NDM-U) for IP-Based Services;* IPDR Specification Version 1.1, June 2000.

[20] N. Damianou, N. Dulay, E. Lupu, M. Sloman: *The Ponder Policy Specification Language*; POLICY 2001, Lecture Notes on Computer Science, Springer, Berlin, Germany, Vol. 1995, January 2001, pp 18-38.

[21] T. Dierks, C. Allen: *The TLS Protocol Version 1.0*; IETF, RFC 2246, January 1999.

[22] Distributed Management Task Force, Inc. (DMTF): *Common Information Model (CIM) Specification, version 2.2*, June 14, 1999. URL: http://www.dmtf.org.

[23] R. Droms: *Dynamic Host Configuration Protocol*; IETF, RFC 2131, March 1997.

[24] R. Droms, W. Arbaugh: *Authentication for DHCP Messages*; Internet Draft, work in progress, draft-ietf-dhc-authentication-16.txt, January 2001.

[25] D. Durham, H. Khosravi, W. Weiss, A. Doria: *COPS Usage for AAA*; Internet Draft, work in progress, Draft-durham-aaa-cops-ext-00.txt, May 2000.

[26] D. Eastlake: *Domain Name System Security Extensions*; IETF, RFC 2535, March 1999.

[27] C.M. Ellison, B. Frant, B. Lampson, R. Rivest, B.M. Thomas und T. Ylonen: *SPKI Certificate Theory*; IETF, Internet Draft, work in progress, November 1998.

[28] S. Farrell, J. Vollbrecht, P. Calhoun, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: *AAA Authorization Requirements;* IETF, RFC 2906, August 2000.

[29] D. Ferraiolo, R. Kuhn: *Role based access controls*; 15th NIST-NCSC National Computer Security Conference, Baltimore Maryland, U.S.A., 1992, pp. 554-563.

[30] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee: *Hypertext Transfer Protocol - HTTP/1.1*; IETF, RFC 2616, June 1999.

[31] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart: *HTTP Authentication: Basic and Digest Access Authentication*; IETF, RFC 261**7**, June 1999.

[32] S. Glass, T. Hiller, S. Jacobs, C. Perkins: *Mobile IP Authentication, Authorization, and Accounting Requirements;* IETF, RFC 2977, October 2000.

[33] S. Glassman, M. Manasse, M. Abadi, P. Gauthier und P. Sobalvarro: *The MilliCent protocol for inexpensive electronic commerce*. 4th International World Wide Web Conference Proceedings, Boston, USA, December 1995, pp 603-618.

[34] P. Hasselmeyer, M.Schumacher, M. Voß: *Pay As You Go - Associating Costs With Jini Leases;* 4th International Enterprise Distributed Object Computing Conference (EDOC 2000), Makuhari, Japan, IEEE Publishing, September 2000, pp. 48-57.

[35] M. Hitchesn, V. Varadharajan: *Tower: A Language for Role Based Access Control*; POLICY 2001, Lecture Notes on Computer Science, Springer, Berlin, Germany, Vol. 1995, January 2001, pp 88-106.

[36] Internet Engineering Task Force: *IP Security Policy (ipsp) Working Group:* URL: http://www.ietf.org/html.charters/ipsp-charter.html, April 2001.

[37] Internet Engineering Task Force: *Policy Framework (policy) Working Group*: URL: http://www.ietf.org/html.charters/policy-charter.html, April 2001.

[38] Internet Research Task Force: *AAA Architecture Research Group*; URL http://www.phys.uu.nl/~wwwfi/aaaarch/, April 2001.

[39] ISO/IEC 13888-1: *Information Technology - Security techniques - Non-repudiation - Part 1: General*; ISO/IEC, 1997.

[40] ISO/IEC 13888-2: *Information Technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques*; ISO/IEC, 1998.

[41] ISO/IEC 13888-3: *Information Technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques*; ISO/IEC, 1997.

[42] ITU-T Q.825: *Specification of TMN Applications at the Q3 Interface: Call Detail Recording;* Recommendation Q.825, Geneva Switzerland, 1998.

[43] S. Jajodia, P. Samarati, V.S. Subrahmanian: *A Logical Language for Expressing Authorizations*; IEEE Symposium on Security and Privacy, Oakland, USA, May 1997, pp 31- 42.

[44] J. Jason, L. Rafalow, E. Vyncke: *IPsec Configuration Policy Model*, Internet Draft, work in progress, draft-ietf-ipsp-config-policy-model-02.txt, March 2001.

[45] M. Khalil. H. Akhtar, K. Pillai, E. Qaddoura: *AAA Interface for IPv6 Handoff;* Internet Draft, work in progress, draft-mkhalil-mobileip-ipv6-handoff-00.txt, October 2000.

[46] B. Lloyd, W. Simpson: *PPP Authentication Protocols*; IETF, RFC 1334, October 1992.

[47] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence: *Generic AAA Architecture;* IETF, RFC 2903, August 2000.

[48] C. de Laat: *Structure of a Generic AAA Server;* IETF, Internet Draft, work in progress, draft-irtf-aaaarch-generic-struct-00.txt, February 2001.

[49] H. Mahon, Y. Bernet, S. Herzog: *Requirements for a Policy Managed System*; IETF, Internet Draft, work in progress, draft-ietf-policy-req-01.txt, October 1999

[50] D. Meyer, J. Schmitz, C. Orange, M. Prior, C. Alaettinoglu: *Using RSPL in Practice*; IETF, RFC 2650, August 1999.

[51] D. Mitton, M. St. Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens, B. Wolff: *Authentication, Authorization, and Accounting: Protocol Evaluation;* IETF, Informational Draft, work in progress, January 2001.

[52] *MobyDick - Mobility and Differentiated Services in a Future IP Network;* European Union 5th Framework Program IST, IST-2000-25394, URL: http://www.ist-mobydick.org, April 2001.

[53] J. Moffett, M. Sloman: *Policy Hierarchies for Distributed Systems Management*, IEEE Journal on Selected Areas in Communications, Vol. 11, No. 9, December 1993, pp 1404-1414.

[54] B. Moore, E. Ellesson, J. Strassner, A. Westerinen: *Policy Core Information Model - Version 1 Specification*; IETF, RFC 3060, February 2001.

[55] K. Nichols, V. Jacobson, L. Zhang: A *Two-bit Differentiated Services Architecture for the Internet;* IETF, RFC 2638, July 1999.

[56] M. Nossik, F. Welfeld, M. Richardson: *PAX PDL - A Non-Procedural Packet Description Language;* http://www.solidum.com/papers/paxpdel/pax-pdl-00.html, September 1998.

[57] R. Ortalo: *A Flexible Method for Information System Security Policy Specificatio;* 5th European Symposium on Research in Computer Security (ESORICS 98), Louvain-la-Neuve, Belgium, Springer-Verlag, Heidelberg, Germany, 1998.

[58] C. Rigney: *RADIUS Accounting*, IETF, RFC 2139, April 1997.

[59] C. Rigney, A. Rubens, W. Simpson, S. Woolens: *Remote Authentication Dial-In User Service (RADIUS);* IETF, RFC 2138, April 1997.

[60] F. C. Röhmer: *Charging Information Management and its Technical Implication in a Liberalized Broadband Telecommunications Environment;* SI Informatik/Informatique, Switzerland, No. 3, 1999, pp 37-38.

[61] R. Sandhu, E. J. Coyne, H. L. Feinstein: *Role-based Access Control Models*, IEEE Computer, Vol. 29, No. 2, February 1996, pp 38-47.

[62] W. Simpson: *PPP Challenge Handshake Authentication Protocol*; IETF, RFC 1994, August 1996.

[63] M. Sloman: *Policy Driven Management For Distributed Systems*, Plenum Press Journal of Network and Systems Management, Vol. 2, No. 4, December 1994, pp 333-336.

[64] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, V. Paxson: *Stream Control Transmission Protocol*; IETF, RFC 2960, October 2000.

[65] B. Stiller, J. Gerke, P. Reichl, P. Flury: *Management of Differentiated Service Usage by the Cumulus Pricing Scheme and a Generic Internet Charging System;* 7th IEEE/IFIP Symposium on Integrated Network Management (IM 2001), Seattle, Washington, U.S.A., May 14-17, 2001, pp 93-106.

[66] I. Stoica, H. Zhang: *Providing Guaranteed Services Without Per-flow Management;* ACM Computer Communication Review (SIGCOMM'99), Vol. 29, No. 4, October 1999, pp 81-94.

[67] G. Stone, G. Xie: *Network Policy Languages: A Survey and a New Approach*; IEEE Network, Vol. 15, No. 1, January 2001, pp 10-21.

[68] J. Strassner, S. Schleimer: *Policy Framework Definition Language*; IETF, Internet Draft, work in progress, draft-ietf-policy-framework-pfdl-00.txt, November 1998.

[69] J. Strassner, E. Elleson, B. Moore: *Policy Framework Core Information Model*; IETF, Internet Draft, work in progress, draft-ietf-policy-core-schema-02.txt, February 1999.

[70] B. Teitelbaum, P. Chimento: *QBone Bandwidth Broker Work Group*. URL: http://qbone.ctit.utwente.nl/BBroker/, August 2000

[71] D. Verma: *Supporting Service Level Agreements on IP Networks;* Macmillan Technology Series, Indianapolis, Indiana, U.S.A., 1999.

[72] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: *AAA Authorization Framework;* IETF, RFC 2904, August 2000.

[73] J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: *AAA Authorization Application Examples;* IETF, RFC 2905, August 2000.

[74] M. Wahl, H. Alvestrand, J. Hodges, R. Morgan: *Authentication Methods for LDAP*; IETF, RFC 2829, May 2000.

[75] A. Westerinen, J. Schnizlein, J. Strassner, Mark Scherling, Bob Quinn, Shai Herzog, An-Ni Huynh, Mark Carlson, Jay Perry, Steve Waldbusser: *Terminology*; IETF, Internet Draft, work in progress, draft-ietf-policy-terminology-03.txt, April 2001.

[76] R. Yavatkar, D. Pendarakis, R. Guerin: *A Framework for a Policy-based Admission Control;* IETF, RFC 2573, January 2000.

[77] J. Zhou, D. Gollmann: *A Fair Non-repudiation Protocol*; IEEE Symposium on Security and Privacy, Oakland, California, May 1996.

[78] J. Zhou, R. H. Deng, F. Bao: *Evolution of Fair Non-repudiation with TTP*; Australasian Conference on Information Security and Privacy, University of Wollongong, Australia, April 1999, pp. 258-269.

8 Abbreviations

AAA	Authentication Authorization Accounting
AAAF	AAA Foreign
AAAH	AAA Home
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface
ASM	Application-specific Module
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
AVP	Attribute Value Pair
CDR	Call Data Record
CHAP	Challenge Handshake Authentication Protocol
CIM	Common Information Model
COPS	Common Open Policy Service
CP	Content Provider
CSP	Content Service Provider
DHCP	Dynamic Host Configuration Protocol
DMTF	Distributed Management Task Force
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data Rate for GSM Evolution
ETH	Eidgenössische Technische Hochschule
EU	European Union
GSM	Global System for Mobile Communications
HA	Home Agent
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
ID	Identity
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDR	Internet Protocol Data Record
IPSec	IP Security
IRTF	Internet Research Task Force
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Information Society Technologies
KOM	Fachgebiet KOM
LAN	Local Area Network
LDAP	Light-weight Directory Access Protocol
MAC	Medium Access Control
MBA	Master of Business Administration
MIB	Management Information Base
MobyDick	Mobility and Differentiated Services in a Future IP Network
MPLS	Multi-Packet Label Switching
NAS	Network Access Server
NASREQ	Network Access Server Requirements
NDM	Network Access Server Requirements
NoD	News on Demand
NRD	Non-repudiation of Delivery
NRO	Non-repudiation of Origin
NRR	Non-repudiation of Receipt
NRS	Non-repudiation of Submission
PAP	Password Authentication Protocol
PBX	Private Branch Exchanges
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PIB	Policy Information Base
PPP	Point-to-point Protocol
PR	Policy Repository
QoS	Quality of Service
RAC	RADIUS Accounting Records
RADIUS	Remote Authentication Dial-In User Service
RBE	Rule Based Engine
RFC	Request for Comments
RSVP	Resource Reservation Protocol
RTFM	Real-time Flow Measurement
SCTP	Stream Control Transmission Protocol
SE	Service Equipment
SIM	Subscriber Identification Module
SMDR	Station Message Detail Record
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TIK	Institut für Technische Informatik und Kommunikationsnetze
TLS	Transport Layer Security
TSP	Transport Service Provider
TTP	Trusted Third Party
UHO	User Home Organization
VoD	Video on Demand
VoIP	Voice over IP
WAN	Wide Area Network
WWW	World Wide Web