

Terena TF-AACE

AAI - Terminology - ver 1.0



■ AAI - Authentication and Authorisation Infrastructure

■ Background

An early interest in **Authentication**, verification of an asserted or claimed **Identity**, as a network service, had its background in the need Internet Service Providers has to charge for use of their networks. See for ex the development of Radius. To this driving force has by now been added the need to externalise authentication from applications and centralise it to keep the provisioning costs down. This need follows from the very clear trend that "every" student and/or employee are becoming (at least self-service) users of most of our IT systems. The same trend also motivates the corresponding effort to externalise **Authorisation**. If we just neglect this observation and instead continue with traditional internal **Identity** and **Privilege Management**, the increased number of users will lead to a steep increase in provisioning costs. There are also reasons to have increased concerns for the quality of the information in a situation where there are only manual routines for managing identities and privileges for an increasing number of users in an increasing number of systems.

The goal of these efforts thus is to replace the internal functions for authentication and authorisation with external network based **Authentication** and **Authorisation Services**. These **Infrastructural Network Services** belong to a type of software called **Middleware**. Together, often supported by an **Enterprise Directory**, they constitute an **Authentication and Authorisation Infrastructure (AAI)**.

For the user or **Principal**, this development means that the Principal has to acquire an **Electronic Identity** from an **Identity Provider** with authority to issue identities acceptable to the applications and content providers of interest to the Principal.

The rationale for the name Middleware is that it names something that is in between. In between architectural layers, like between the network layers and the application, or in between applications. This is a rather wide definition and this document is a compilation of a terminology for the narrower area around an Authentication and Authorisation Infrastructure. This document furthermore takes the application perspective of authentication and authorisation rather than the network or internet service provider perspective. First some of the basic terms are defined roughly in the order they were introduced in this section. This is followed by an alphabetic list of terms.

■ Basic terminology

First the definition of some basic terms, in the order they were introduced above. Most of the terms are not new but can also be found elsewhere. When the definition is almost the same as in some other glossary - the source is given in parenthesis. TF-AACE is given as the source when the term is introduced or redefined here.

Identity

The essence of an entity and often described by its characteristics. (Liberty Alliance)

Electronic Identity (eID)

The information about a registered entity, that the Identity Provider has chosen to represent the Identity of that entity. The eID includes a name or an identifier for the entity that is unique within the domain of the Identity Provider. (TF-AACE)

Authentication (Authn)

The process of using an Authentication Mechanism to verify or disprove a claimed Electronic Identity.

Authorisation (Authz)

Given an Authentication Assertion for an eID for the requesting Principal, the process of deciding if a request to perform an action on a resource shall be granted or not. (TF-AACE)

Identity Management

The process of creating, maintaining and asserting Electronic Identities. Identity Management is done by an Identity Provider.

Privilege Management

The process of creating, maintaining and releasing information concerning the privileges and responsibilities a Principal has in an organisation.

Authentication Service

An Infrastructural Network Service that authenticates registered Electronic Identities and produces Authentication Assertions.

Infrastructural Network Service

An Infrastructural Network Service, such as an Authentication or Authorisation Service, serves applications and content providers with common functionality that have been externalised from applications for efficiency and quality reasons. Infrastructural Network Services belong to a type of software called Middleware. (TF-AACE)

Authorisation Service

An Infrastructural Network Service that serves applications and content providers with Authorisation. The service replies with an Authorisation Assertion or a denial. (TF-AACE)

Middleware

The term has different meanings in different contexts but normally denotes specialised, rather high-level software that sits between applications or between the application layer and lower layers in a layered software architecture like a network or database architecture. (TF-AACE)

Authentication and Authorisation Infrastructure (AAI)

The Authentication and Authorisation Services, components for Identity and Privilege Management and the entities responsible for these services - constitute an Authentication and Authorisation Infrastructure (AAI). (TF-AACE)

Identity Provider

An entity in an AAI that performs Identity Management. (TF-AACE)

Principal

An entity who belongs to the organisation, is capable of making decisions, and to which authenticated actions are done on its behalf. A Principal may acquire an eID.

■ Terminology

This terminology contains terms for such things as actors, components, services, and mechanisms in the area of Authentication and Authorisation Infrastructure. It is an evolving area and whence this is expected to be an evolving document, subject to change as the technology and its application evolve.

AA Middleware

Synonym for Infrastructural Network Service

AAI Federation

See Federated AAI

Access Control

The process of authorising access to a resource. (TF-AACE)

Assertion

A positive statement or declaration (of a successful Authentication or approved Authority). (Merriam-Webster)

Authentication (AuthN)

The process of using an Authentication Mechanism to verify or disprove a claimed Electronic Identity.

Authentication and Authorisation Infrastructure (AAI)

The Authentication and Authorisation Services, components for Identity and

Privilege Management and the entities responsible for these services - constitute an Authentication and Authorisation Infrastructure (AAI). (TF-AACE)

Authentication Assertion

A statement conveying information about a successful Authentication of an Electronic Identity. (TF-AACE)

Authentication Mechanism

A mechanism, such as username/password, used to verify or disprove a claimed Electronic Identity. (TF-AACE)

Authentication Service

An Infrastructural Network Service that authenticates registered Electronic Identities and produces Authentication Assertions.

Authentication Service Provider

An entity in an AAI that provides an Authentication Service.

Authentication Strength

A declaration made by an Authentication Service Provider, indicating the level of assurance any client can place in an Authentication Assertion it receives.

Authorisation (AuthZ)

Given an Authentication Assertion for an eID for the requesting Principal, the process of deciding if a request to perform an action on a resource shall be granted or not. (TF-AACE)

Authorisation Service

An Infrastructural Network Service that serves applications and content providers with Authorisation. The service replies with an Authorisation Assertion or a denial. (TF-AACE)

Authorisation Service Provider

An entity in an AAI that provides an Authorisation Service.

Electronic Identity (eID)

The information about a registered entity, that the Identity Provider has chosen to represent the Identity of that entity. The eID includes a name or another identifier for the entity that is unique within the domain of the Identity Provider. (TF-AACE)

Federated AAI

An AAI that supports multiple Identity and Privilege Providers, trusted by the members of the federation. (TF-AACE)

Federation

A Federation is a group of organisations, whose members have agreed to cooperate in an area such as operating an inter-organisational AAI - a Federated AAI or an AAI Federation. (TF-AACE)

Identity

The essence of an entity and often described by its characteristics. (Liberty Alliance)

Identity Federation

A Federated AAI containing multiple Identity Providers, trusted by the members of the federation. (TF-AACE)

Identity Management

The process of creating, maintaining and asserting Electronic Identities. Identity Management is done by an Identity Provider.

Identity Provider

An entity in an AAI that performs Identity Management. (TF-AACE)

Infrastructural Network Service (AA Middleware)

An Infrastructural Network Service, such as an Authentication or Authorisation Service, serves applications and content providers with common functionality that have been externalised from applications for efficiency and quality reasons. Infrastructural Network Services belong to a type of software called Middleware. (TF-AACE)

Middleware

The term has different meanings in different contexts but normally denotes specialised, rather high-level software that sits between applications or between the application layer and lower layers in a layered software architecture like a network or database architecture. (TF-AACE)

Principal

An entity who belongs to the organisation, is capable of making decisions, and to which authenticated actions are done on its behalf. A Principal may acquire an eID.

Privilege Management

The process of creating, maintaining and releasing information concerning the privileges and responsibilities a Principal has in an organisation.

Privilege Provider

An entity in an AAI that performs Privilege Management. (TF-AACE)

Provisioning

A measure taken beforehand to deal with a need or contingency. In this context the need for applications to have access to identity and privilege information about principals and resources. (Merriam-Webster)

Resource

Any information entity, application, IT-controlled physical equipment or service available through the Internet, whatever its nature and use. (TF-AACE)

Virtual Organisation

A group or association of users collaborating in a common experiment, project or other joint venture. A VO is formed as a selection of users belonging to different administrative domains. (eIRG)

/Torbjörn Wiberg, Umeå Universitet, 040630