

Education Sector Authentication & Authorisation (ESAA) Overview

VERSION: 1.0 (December 2009)

© Ministry of Education, 2009

Table of Contents

- 1. What is ESAA?..... 2
- 2. Why is ESAA Necessary?..... 3
- 3. How Does ESAA Work? 3
- 4. What Are Trust Levels? 4
- 5. Why Does ESAA Need Evidence of Identity?..... 6
- 6. What Are The Benefits of ESAA? 6

1. What is ESAA?

ESAA stands for the *Education Sector Authentication and Authorisation* service, and is an identity and access management system developed by the Ministry of Education for use by the entire Education Sector. It is a **role based access control identity management** system.

In this document we will address the high level principles behind ESAA, what ESAA is, and how it benefits its users. This document is not intended as a detailed technical overview – merely to introduce *identity management* and how ESAA fulfils the Education Sector and the application user's needs in this area.

Identity management is process of collecting, validating, recording, and maintaining user data. In this case the process allows users to access protected web applications. The data collected about users depends upon the security requirement of the application being used; this is discussed later in the document. ESAA stores details of the individuals who can access the protected systems, by using *roles* that the user is assigned. The roles are labels that are used by the protected applications to know what that user is allowed to access and do. ESAA validates who the user is, whenever they try to access the protected application, by use of credentials (most commonly username and password).

ESAA is used to store the details of the people within the Education Sector, who are granted permission to be “users” of the protected applications, each set of user details is said to be an **identity**. When a person is registered with ESAA their details are recorded and they are assigned the necessary roles, chosen by the application owner. ESAA is used by the applications to ensure each user:

- Is who they claim. This is called **authentication**;
- Can only see and modify information that they are allowed. This is call **authorisation**.

ESAA provides the information required that applications need to make access decisions by:

1. Recording a person's details when they register;
2. Facilitating the logon process;
3. Passing details of roles to the application;
4. Allowing users to maintain their information.

ESAA only manages authentication and authorisation; the applications themselves make the decisions based upon the information ESAA provides. This has the benefit of allowing each user to use many applications without having to enter their username and password every time a new application is accessed. This is called **single sign-on** and it is a very useful part of ESAA.

ESAA is being implemented by the participating agencies on an application by application basis. More applications will use ESAA as they are developed or existing applications are modified. Currently there are a number of older applications using ESAA as a common logon service (i.e. using the same username and password) and many applications are planned to be modified for full single sign-on use in the future.

2. Why is ESAA Necessary?

Increasingly people across the Education Sector require access to information to do their jobs. A large share of the data used is held on computers and requires protection from malicious or accidental access attempts. ESAA is one means by which information can be protected. With usernames and passwords ESAA attempts to prevent the wrong people accessing information they are not meant to see. Other stronger authentication credentials (such as a security token, digital certificate, fingerprint or voice recognition) can also be added.

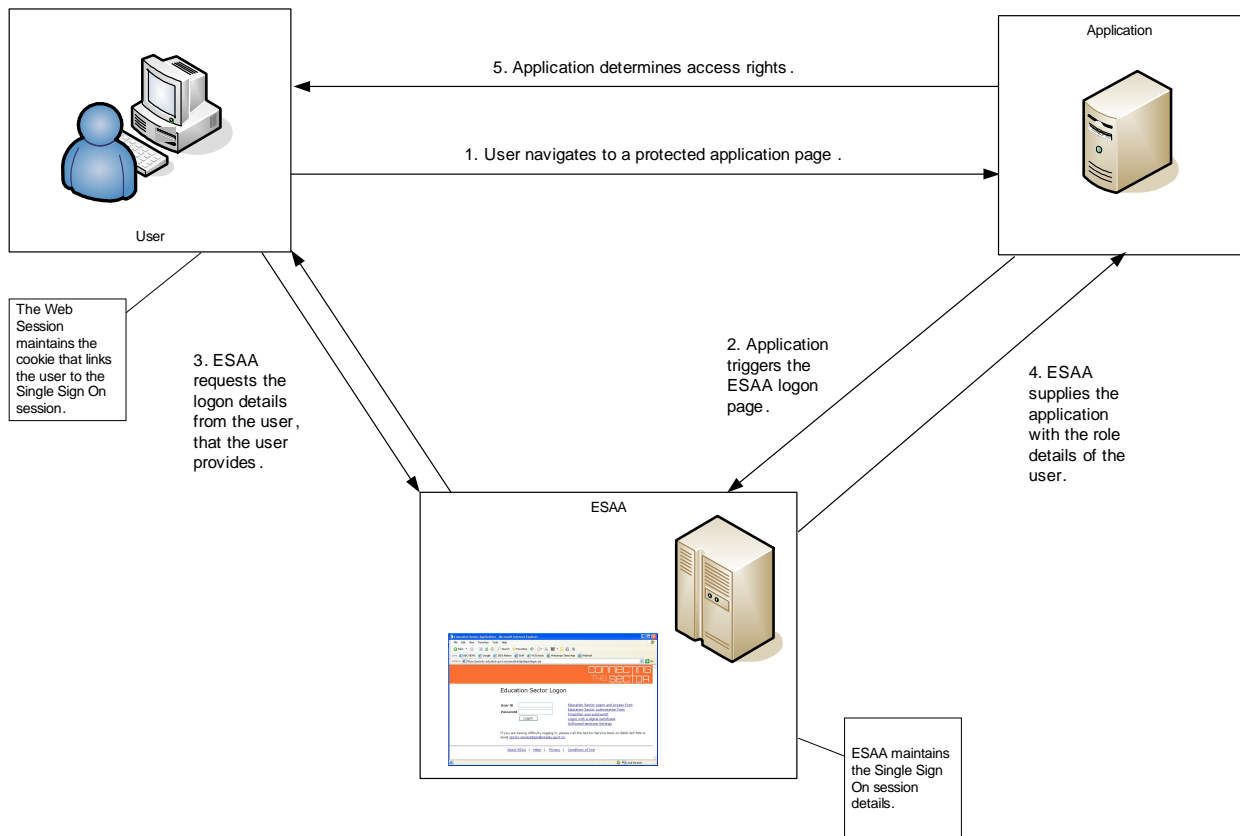
ESAA has been chosen by the Ministry of Education, Tertiary Education Commission (TEC), New Zealand Qualifications Authority (NZQA,) Career Services, Education Review Office (ERO), Teachers Council, and the National Library to be the identity management system for the Education Sector. This decision has been approved by the State Services Commission.

ESAA provides a service that would have to be provided in a piecemeal fashion by all the participating agencies. By having one system that all the users of education agency systems can access there are many benefits for agencies and users alike.

3. How Does ESAA Work?

The first step for ESAA is the collection of personal data; generally this occurs out of the system, except for self-registered users. The information is supplied by the user on their paper request form. Then their **evidence of identity** (EOI) is validated by an approved person (this is covered later). Once this data is captured it is entered into ESAA and the roles, requested as part of the registration process, are assigned. Then the user is issued with a username and password (and possibly a stronger authentication credential).

When a user attempts to access an ESAA protected website they enter their username and password. This way ESAA can identify who that user is, and then informs the application of the roles that the user holds. From this information the application is able to grant the appropriate access to the user. The following diagram illustrates the steps when someone wishes to access an ESAA protected application.



The user is also able to manage their details online:

- Change personal data, e.g. contact details.
- Challenge Response Questions – the questions and answers that provide an alternative means to prove they are the user they claim to be if they forget their password.
- Change their password – the password should be kept secure so frequent changes are enforced.
- Some applications will allow users to self-register. These are known as *pseudonymous* users. They do not have supply as much information when registering, and will only have access to lower risk applications.

4. What Are Trust Levels?

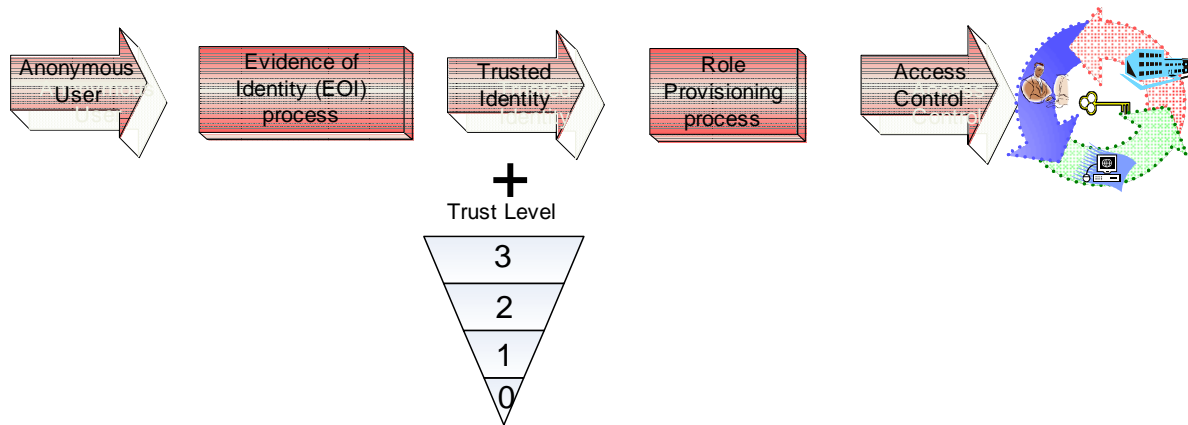
The **trust level** is a process to differentiate between the different risks that arise from data security being compromised. The concept of trust level is used to ensure that only users, who are known (trusted), have access to the most sensitive data. The underlying assumption is that *knowing who someone is minimises the risk of misuse*.

Trust is built into ESAA through the use of trust levels assigned to organisations, applications and users. The education sector has agreed to comply with strong security and privacy practices, by doing so trust is strengthened. This achieves the high standards needed for users to access information across the sector.

In order to authorise a new user access to an application and its associated information it is necessary to establish the:

- Trust level for application and information; and
- Roles appropriate to the rights and privileges existing within an application.

As a result applications, information and user roles will be assigned a trust level ranging from 0 (the lowest) to 3 (the highest).



A user or application remains un-trusted until they pass through the Evidence of Identity (EOI) process. EOI requirements will depend on the level of confidence needed to prove a person is who they claim to be. A trust level must be assigned to all registered users, applications, organisations and authorisers.

Only users with a level of trust that equals or exceeds the trust level of the application are able to access that application and the information it manages.

As ESAA use grows, ESAA will be able to develop **Circles of Trust** that will allow users to access applications and information anywhere inside the circle that they are allowed to enter.

To achieve this, a common approach and acceptance of consistent security and privacy practices is essential across all ESAA applications.

The ESAA solution is the chosen model moving forward. Through the implementation of Circles of Trust education sector employees, teachers, lecturers, principals, students and researchers will gain access to an ever growing pool of information that does not require them to logon again and again as they move from application to application.

Users will be able to access information with the knowledge that the information is secure and provided from trusted sources. Likewise users will be able to publish information secure in the knowledge that only authorised people will be able to view it and, if allowed, add and/or modify it.

5. Why Does ESAA Need Evidence of Identity?

When a user provides EOI they are verifying who they say they are. The type of EOI required depends on the type of trust level required for a particular role. This is explained to the user when they make their application request to ESAA.

Strong EOI requirements will need good proof of identity such as passports, or driver's license, or some similar document containing a photograph. Weaker EOI requirements are less restrictive and will not require a photograph. Pseudonymous users do not prove who they are, and hence need no EOI.

Users only have to provide their EOI once for all roles and applications that require that level of trust. If the user requires access to a higher trust application, then they will need to provide additional EOI as required.

6. What Are The Benefits of ESAA?

The New Zealand's ICT Strategic Framework for Education has the objective of *learning and research supported and enhanced by the smart use of ICT*. ESAA is a key system that will help to meet this objective.

- The use of one username and password removes the need for users to remember multiple passwords and usernames.
- Improved security by reducing the number of different passwords required to access applications across the education sector (users are less likely to write down their passwords).
- Regardless of where a user enters the system, ESAA will provide a secure, single sign-on for all education sector applications.
- Users will experience reduced time and inconvenience when completing transactions by using Single Sign-On (SSO).
- ESAA addresses the fundamental issue of authentication and authorisation allowing the application providers to concentrate on their core services.
- ESAA will enable a network of collaborative environments for learners, teachers, lecturers, researchers, education providers and agencies.

The Education Sector has a legal and ethical obligation to ensure that privacy of individuals and the quality and integrity of electronic information is not compromised. Maintaining privacy and security of electronic information is compounded by the complexity and variety of stakeholders and systems involved. Using a Circle of Trust will establish a virtual sector that shares privacy and security principles, rules and expectations.