Identity Assurance Profile

Document	TAAT Identity Assurance Profile
Identifier (OID)	1.3.6.1.4.1.19974.12.2.1.3
Version	1.3
Last modified	05.09.2012

1. Requirements for Identity Providers

Requirements that are only set for the user accounts sent to TAAT. Performance of the requirements in specific institutions must be described in the Identity Administration Report.

1.1. Authentication of End Users

1.1.1. A user account must refer to one specific natural person (End User).

1.1.2. End Users may be authenticated in information systems using an ID card, Mobile ID or a username and password, which are subject to the provisions of clauses 1.3-1.4.

1.2. Registration and identification of users

1.2.1. The personal data associated with a user account must come from a reliable source: data given by the person themselves or obtained from a register trusted by the Identity Provider (incl. SAIS), in which case the Identity Provider will be held responsible for the correctness of the data.

1.2.2. One of the following must be used to identify a person:

- a face-to-face meeting and presentation of ID;
- authentication with an ID card;
- Mobile ID;
- authentication via a bank.

1.2.3. Usernames and passwords may be given only to identified accountholders.

1.3. Requirements for user name

1.3.1. A username must be unique at all times.

1.3.2. Repeated use of usernames is permitted if the aforementioned requirement of uniqueness is guaranteed.

1.4. Requirements for passwords

1.4.1. A password must consist of at least six (preferably eight or more) characters and at least one of the following measures must be used:

- it contains both upper and lower case letters;
- it contains both letters and numbers;
- it contains special characters (punctuation marks).

1.4.2. Basis measures required to prevent others from guessing the password must be used (e.g. using one’s username or first name as the password is not permitted).

1.4.3. The password may not be preserved or typed in as plaintext.

1.5. Keeping data up to date

1.5.1. The Identity Provider is responsible for keeping the data associated with users up to date.

1.6. User account administration

1.6.1. The account of each End User must have a unique identifier throughout history.

1.6.2. Connection to the previous identifier must be ascertainable when the identifier is changed.

1.6.3. User data may be accessible only to employees whose duties include handling user accounts.

1.6.4. A user must be informed of the password confidentiality requirement.

1.6.5. If a password leak is ascertained, the Identity Provider must change the password or lock the account as soon as possible.

1.6.6. If a password or username is forgotten, the person must be identified according to the requirements in clause 1.2.2. in order to restore access. Only passwords that are used once or password change keys may be sent to users as plaintext.

1.7. Roles

1.7.1. Every active user account must be tied to at least one role that corresponds to its position in the institution.

1.7.2. If the person's role in the institution change or end (exmatriculation, expiry of employment contract, change of job tasks, etc.), the roles associated with their account must be renewed within 14 days.

2. Requirements for Service Providers

2.1. Preservation and use of data received via TAAT

2.1.1. A Service Provider has the right to preserve and use the data received via TAAT only for the provision of the services listed in the contract entered into with EENet.

2.1.2. If the Service Provider also uses a local authentication system, which enables access to data received via TAAT, the provisions of clauses 1.1., 1.3. and 1.4. will extend to such authentication system.

3. Requirements for all Federation Participants

3.1. Security

3.3.1. All data associated with End Users must be encrypted if they are sent across an open network, whilst the minimal strength of the keys used must be 2048 bit RSA or an equivalent standard.

3.3.2. Authentication mechanisms must be protected from common attacks such as interception, main in the middle attack, or guessing the password.

3.3.3. The used software and hardware must comply with modern security requirements, e.g. the security updated of manufacturers must be implemented as soon as possible.

3.3.4. Physical access to hardware that contains user data and their backups must only be permitted for employees whose job tasks include hardware or user data administration. Unauthorised persons are only allowed access at the responsibility of the aforementioned employees.

3.3.5. Written-off hardware and software that contain user data must be disposed of in a manner that excludes any data recovery.

3.3.6. All requirements for user data extend to logs containing such data.