This document contains a “best effort” translation of its Polish original. It is provided for information only. The only legally binding document is the original in Polish.

Polish Identity Federation PIONIER.Id Technical Terms

1. The key words used in the text
   1.1. "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in this chapter are to be interpreted as described in RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt)
2. Purpose and Scope
   2.1. This document defines the lowest common level of technical requirements for all members of the Polish Identity Federation PIONIER.Id (further called PIONIER.Id Federation)
3. User registration and credentials
   3.1. End User identifier MUST be issued to a physical person affiliated to a PIONIER.Id Federation Identity Provider.
   3.2. The registration procedure MUST be constructed so as to be able to establish that the interacting subject is a human. Using CAPTCHAs or relying on an identity proofing process that uses CAPTCHAs (or a technical control of comparable reliability) is a minimally acceptable way of controlling this.
   3.3. It is RECOMMENDED that registration procedure contains an element of a face-to-face contact between the End User and an employee representing the Identity Provider.
4. Credentials issuance
   4.1. Each End User MUST be represented by an identifier ("username") which MUST be unique for the Identity Provider.
   4.2. End Users MUST NOT share their credentials with other persons.
   4.3. Identity Providers MUST take measures reducing the risk of credentials theft.
5. Identification of the communication parties
   5.1. Identity Providers and Service Providers are identified by unique identifiers assigned by the PIONIER.Id Operator.
   5.2. Identity Providers and Service Providers secure the transmission by encryption and electronic signature
   5.3. Keys used to secure transmission MUST NOT be weaker (in the sense of NIST SP 800-57) than a 2048 bit RSA key and MUST be changed at least every 3 years.
6. Security of the Authentication process
   6.1. Transmission of protected data (identifiers, encryption keys etc.) MUST be secured by encryption in a way complying with Personal Data Protection regulations, unless the transmission is restricted to a secured internal network.
   6.2. Any authentication protocols used when authenticating subjects MUST require a proof-of-possession step for subject credentials. For regular passwords this involves validating that the user knows her/his password.
   6.3. Any session tokens MUST be generated by safe cryptographic methods and based on earlier authentication.

6.4. Authentication mechanisms MUST be protected against common attacks such as man-in-the-middle attacks, eaves-dropper attacks and off-line password guessing.

7. Technical requirements
   7.1. The servers and other infrastructure involved in the operation of identity providers or relying parties MUST be maintained according to best practice.
8. Technical requirements of the SAML WebSSO implementation
   8.1. The service is based upon SAML V2.0 Web Browser SSO Profile (http://docs.oasisopen.org/security/saml/v2.0/saml-profiles-2.0-os.pdf) – a standard d that enables Identity Providers and Relying parties to create and use web Single Sign on services using SAML.
   8.2. All SAML metadata MUST fulfil the SAML V2.0 Metadata Interoperability Profile Version 1.0.
   8.3. All entities (service providers and identity providers) SHOULD fulfil either the Interoperable SAML 2.0 Profile or the ShibbolethSAML 1.1 Profile. Interoperable SAML 2.0 Profile is RECOMMENDED.
   8.4. All SAML attributes SHOULD be represented using the urn:oasis:names:tc:SAML:2.0:attrname-format:uri NameFormat.
   8.5. All SAML attribute Names SHOULD be represented using either the urn:oid or urn:mace:dir:attribute-def namespace.
   8.6. All SAML Identity Providers SHOULD implement the Shibboleth Scope Extension.
   8.7. If the Shibboleth Scope Extension is implemented by an Identity Provider then it MUST be declared in the metadata as defined in the Shibboleth Metadata Schema. The Scope value MUST be a string equal to a domain owned by the organisation that owns the Identity Provider.
   8.8. All SAML Service Providers SHOULD implement the Shibboleth Scope extension.
9. Identity Assertion
   9.1. Authentication Response supplied by the Identity Provider MUST contain a permanent identifier of the subject. This identifier MAY be specific to a singly Service Provider.
   9.2. The permanent identifier used SHOULD be one of the recommended in chapter 7 of Interoperable SAML 2.0 Profile. It is RECOMMENDED that permanent identifier should hide End User's true identity.
   9.3. The Identity Provider MAY supply a true End User's identity, however this option should be carefully analysed taking into account Personal Data Protection law, acceptability and necessity with respect to a given Service Provider.
10. Logs
    10.1. Identity Providers MUST keep logs of all identity assertions
    10.2. Information kept MUST be sufficient for unique identification of End Users
    10.3. All relevant logs MUST be created with synchronisation to a reliable NTP time source
    10.4. The minimum log retention is 6 months
    10.5. Authentication logs must and properly secured and released only to authorized authorities
    10.6. Bilateral agreements with Service Providers MAY specify additional conditions on log contend and/or retention.