Warunki Techniczne Polskiej Federacji Zarządzania Tożsamością
PIONIER.Id

1. Słowa kluczowe używane w tekście
   1.1. Słowa „MUSI”, „MOŻE”, „POWINIEN”, „NIE WOLNO” i ich odmiana, pisane wielkimi literami są używane zgodnie z definicją ich angielskich odpowiedników, określonych w RFC 2119 (http://www.ietf.org/rfc/rfc2119.txt).
2. Cel i Zakres
   2.1. Niniejszy dokument określa minimalne warunki techniczne dla wszystkich członków Polskiej Federacji Zarządzania Tożsamością PIONIER.Id. (dalej w skrócie „Federacja PIONIER.Id.”).
3. Rejestracja użytkowników końcowych i identyfikatory.
   3.1. Identyfikator przeznaczony dla użytkownika końcowego MUSI być powiązany z osobą fizyczną stowarzyszoną z podmiotem będącym Dostawcą Tożsamości w ramach Federacji PIONIER.Id.
   3.2. Proces rejestracji użytkowników MUSI być skonstruowany w sposób pozwalający na potwierdzenie faktu, że strona korzystająca z procesu rejestracji jest osobą fizyczną. Minimalnym dopuszczalnym poziomem potwierdzenia tego faktu jest zastosowanie metod opartych o tzw. CAPTCHA.
   3.3. Przy rejestracji POWINNO się stosować procedury zawierające element osobistego kontaktu między użytkownikiem końcowym a pracownikiem reprezentującym Dostawcę Tożsamości.
4. Przydzielanie identyfikatorów użytkownikom końcowym
   4.1. Każdy użytkownik końcowy MUSI być reprezentowany przez identyfikator, który MUSI być jednoznaczny w obrębie Dostawcy Tożsamości.
   4.2. Zakazane jest udostępnianie przez użytkowników ich identyfikatorów innym osobom .
   4.3. Dostawcy Tożsamości MUSZĄ stosować procedury zmniejszające ryzyko przejęcia identyfikatorów przez osoby nieuprawnione.
5. Identyfikacja stron komunikacji.
   5.1. Dostawcy Tożsamości oraz Dostawcy Usług są identyfikowani przez jednoznaczne identyfikatory przydzielane przez Operatora PIONIER.Id.
   5.2. Dostawcy Tożsamości oraz Dostawcy Usług zabezpieczają transmisję przy pomocy szyfrowania i podpisu elektronicznego.
   5.3. Klucze stosowane do zabezpieczenia transmisji NIE MOGĄ być słabsze (w rozumieniu rekomendacji NIST SP 800-57) niż 2048-bitowy klucz RSA i MUSZĄ być zmieniane nie rzadziej, niż co 3 lata.
6. Bezpieczeństwo procesu uwierzytelnienia.
   6.1. Transmisja danych chronionych (danych identyfikacyjnych, kluczy szyfrujących itp.) MUSI być zabezpieczona szyfrowaniem w sposób zgodny z wytycznymi dotyczącymi transmisji danych osobowych, o ile nie odbywa się w całości w ramach zabezpieczonej sieci wewnętrznej.
   6.2. Wszelkie protokoły uwierzytelniania używane podczas uwierzytelnienia stron MUSZĄ zawierać element potwierdzenia faktu posiadania dostępu do danych uwierzytelniających, np. w przypadku uwierzytelniania za pomocą hasła, użytkownik potwierdza ten fakt wprowadzając swoje hasło.
   6.3. Wszystkie klucze sesyjne MUSZĄ być generowane przy pomocy bezpiecznych metod kryptograficznych na podstawie wcześniejszego uwierzytelnienia.

6.4. Wszelkie zastosowane mechanizmy służące do uwierzytelnienia MUSZĄ być zabezpieczone przed typowymi atakami, np. przechwycenia, złamania, wyłudzenia haseł itp.

7. Wymagania techniczne
   7.1. Serwery i inne elementy infrastruktury związane z utrzymaniem i eksploatacją usług przez Dostawców Tożsamości i Dostawców Usług muszą być administrowane i zarządzane z zastosowaniem tzw. „najlepszych praktyk".
8. Warunki techniczne implementacji usługi SAML WebSSO
   8.1. Usługa jest Oparta o profil SAML V2.0 Web Browser SSO Profile (http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf) – standard umożliwiający Dostawcom Tożsamości oraz Dostawcom Usług tworzenie i użytkowanie stron za pomocą techniki jednorazowego logowania do usług z wykorzystaniem technologii SAML.
   8.2. Wszystkie metadane SAML MUSZĄ być zgodne ze standardem SAML v2.0 specyfikacja v 1.0.
   8.3. Wszystkie podmioty (zarówno Dostawcy Tożsamości jak i Dostawcy Usług) POWINNI spełniać specyfikację Interoperable SAML 2.0 Profile lub Shibboleth SAML 1.1 Profile. Interoperable SAML 2.0 Profile jest REKOMENDOWANY.
   8.4. Wszystkie nazwy atrybutów SAML POWINNY być zapisane w postaci zgodnej z urn:oasis:names:tc:SAML:2.0: attrname-format: Uri.
   8.5. Wszystkie nazwy atrybutów SAML POWINNY pochodzić z przestrzeni nazewnictwa urn:oid lub urn:mace:dir: attribute-def.
   8.6. Wszyscy Dostawcy Tożsamości POWINNI wdrożyć Shibboleth Scope Extension.
   8.7. Jeżeli Shibboleth Scope Extension jest wdrożone przez ***Dostawcę Tożsamości***, to MUSI być ono zadeklarowane w metadanych zgodnie z definicją Shibboleth Metadata Schema. Wartość Scope musi być ciągiem znaków zgodnym z nazwą domeny będącej własnością ***Dostawcy Tożsamości***.
   8.8. Wszyscy ***Dostawcy Usług*** POWINNI wdrożyć Shibboleth Scope Extension.
9. Potwierdzenie tożsamości
   9.1. ***Dostawcy Usług*** MOGĄ oczekiwać, że w ramach Authentication Response ***Dostawca Tożsamości*** przekaże identyfikator na stałe związany z ***Użytkownikiem końcowym***. Wartość takiego identyfikatora MOŻE być specyficzna dla danego ***Dostawcy Usługi***.
   9.2. Jako niezmienny identyfikator użytkownika końcowego POWINIEN być stosowany atrybut rekomendowany w części 7 profilu Interoperable SAML 2.0 Profile. REKOMENDOWANE jest stosowanie atrybutów niezdradzających rzeczywistej tożsamości Użytkownika końcowego.
   9.3. Dostawcza tożsamości MOŻE przekazywać identyfikator rzeczywisty, korzystanie z tej możliwości powinno być zawsze przeanalizowane pod względem zgodności z przepisami dotyczącymi Ochrony Danych Osobowych, dopuszczalności i niezbędności w odniesieniu do danego Dostawcy Usług.
10. Rejestracja zdarzeń
    10.1. Dostawcy Tożsamości MUSZĄ zapisywać dane na temat wszystkich wydanych potwierdzeń tożsamości.
    10.2. Logi systemowe MUSZĄ pozwalać na jednoznaczne zidentyfikowanie Użytkownika końcowego.
    10.3. Logi systemowe MUSZĄ być znakowane czasem synchronizowanym przy pomocy usługi NTP.
    10.4. Logi systemowe MUSZĄ być przechowywane przez okres co najmniej 6 miesięcy.
    10.5. Logi systemowe MUSZĄ podlegać ochronie i być udostępniane wyłącznie uprawnionym do tego organom.

10.6. Dwustronne umowy z Dostawcami usług MOGĄ nakładać dodatkowe zobowiązania dotyczące logów systemowych w zakresie ich treści i/lub okresu przechowywania.