



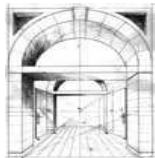
Projekt: e-PUAP - WKP

Zasady bezpieczeństwa ePUAP

 **infovide**
Architekci strategii informacyjnych

ZASADY BEZPIECZEŃSTWA ePUAP

e-PUAP - WKP



Projekt: e-PUAP - WKP

Zasady bezpieczeństwa ePUAP

Autor	Michał Tabor, Przemysław Momot (TI Consulting)
Klient	Ministerstwo Spraw Wewnętrznych i Administracji
Wersja dokumentu	1.02
Liczba stron	71

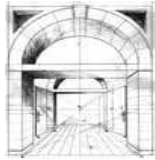
Historia zmian

Wersja	Data	Kto	Opis zmian
1.01	2006-07-28	Przemysław Momot	Zmiany wprowadzone po uzgodnieniach wewnętrznych
1.02	2006-08-23	Michał Tabor	Wersja zawierająca poprawki edytorskie



Spis treści

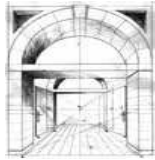
1	WSTĘP	5
1.1	CEL DOKUMENTU	5
1.2	ŹRÓDŁA INFORMACJI.....	6
1.3	ZASTOSOWANE SKRÓTY I POJĘCIA.....	8
2	ZASADY BEZPIECZEŃSTWA WEDŁUG KATEGORII BEZPIECZEŃSTWA.....	9
2.1	OGÓLNE ZASADY BEZPIECZEŃSTWA ORGANIZACJI.....	9
2.2	ZASADY BEZPIECZEŃSTWA W ZAKRESIE ZAUFANEGO SYSTEMU.....	17
3	ZAPEWNIENIE INTEGRALNOŚCI I NIEZAPRZECZALNOŚCI DOKUMENTÓW.....	30
3.1	PODSTAWOWA CHARAKTERYSTYKA	31
3.2	WERYFIKACJA POCZĄTKOWA.....	31
3.3	POBIERANIE CERTYFIKATÓW DO WERYFIKACJI.....	32
3.4	POBIERANIE INFORMACJI O STATUSIE CERTYFIKATÓW DO WERYFIKACJI.....	33
3.5	SPRAWDZENIE ELEMENTU SIGNINGTIME.....	33
3.6	SPRAWDZENIE ELEMENTU SIGNINGCERTIFICATE.....	33
3.7	SPRAWDZENIE ELEMENTÓW COMPLETECERTIFICATEREFS.....	34
3.8	SPRAWDZENIE ELEMENTÓW COMPLETEREVOCATIONREFS.....	35
3.9	SPRAWDZENIE ELEMENTÓW CERTIFICATEVALUES.....	36
3.10	SPRAWDZENIE ELEMENTÓW REVOCATIONVALUES.....	37
3.11	WERYFIKOWANIE ŻETONÓW ZNACZNIKA CZASU.....	37
4	NIEZAPRZECZALNOŚĆ ZDARZEŃ.....	39
4.1	ZDARZENIA JAKIE POWINNY BYĆ REJESTROWANE.....	39
4.2	ZASADY PROWADZENIA DZIENNIKÓW ZDARZEŃ	41
5	METODOLOGIA DOWODOWA - ZASADY.....	44
5.1	DOKUMENTOWANIE PRZEBIEGU.....	44
5.2	DOWODZENIE ZACHODZĄCYCH ZDARZEŃ	45
6	METODY UWIERZYTELNIANIA I AUTORYZACJI UŻYTKOWNIKÓW.....	46
6.1	PODZIAŁ UŻYTKOWNIKÓW ZE WZGLĘDU NA RODZAJ DOSTĘPU.....	46
6.2	SPOSOBY IDENTYFIKACJI.....	46
6.3	PROFILE UŻYTKOWNIKÓW.....	50
6.4	SINGLE SIGN-ON.....	50
6.5	SPOSOBY UZYSKANIA DOSTĘPU.....	51
6.6	WYMAGANIA DLA SYSTEMU E-PUAP	51
7	BEZPIECZNA SYNCHRONIZACJA CZASU.....	53
8	ZASADY BEZPIECZEŃSTWA TRANSMISJI DANYCH.....	59
9	ZASADY ANALIZY RYZYKA W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI.....	61



Projekt: e-PUAP - WKP

Zasady bezpieczeństwa ePUAP

9.1	IDENTYFIKACJA AKTYWÓW.....	62
9.2	WYCENA AKTYWÓW.	63
9.3	IDENTYFIKACJA ZAGROŻEŃ I PODATNOŚCI.....	63
9.4	METODA ANALIZY RYZYKA.....	64
9.5	ZAGROŻENIA ZWIĄZANE Z E-PUAP – WSTĘPNA ANALIZA.....	65



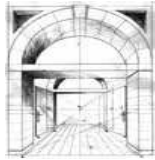
1 Wstęp

1.1 Cel dokumentu

Celem opracowania niniejszego dokumentu jest przedstawienie propozycji zasad bezpieczeństwa opartych o aktualnie obowiązujące akty prawne, normy i najlepsze praktyki w kontekście Programu Wrota Polski i platformy e-PUAP. W ramach dokumentu wykonano:

- Przygotowanie zasad bezpieczeństwa w układzie warstwowym (tj. wg podejścia dziedzinowego, określenie reguł dotyczących bezpieczeństwa, np. bezpieczeństwo fizyczne, sieciowe, logiczne, osobowe itd.) dla systemu zintegrowanego zarządzania dokumentami w ramach projektu e-PUAP
- Opracowanie metod, procedur i wymagań dla e-PUAP, zapewniających integralność i autentyczność dokumentów w postaci elektronicznej
- Opracowanie metod i wymagań dla e-PUAP zapewnienia niezaprzeczalności zdarzeń, znaczników czasu i potwierdzeń dostarczenia
- Opracowanie metodologii dowodowej i audytowej dla przeprowadzonych operacji
- Przygotowanie procedur uwierzytelniania i autoryzacji użytkowników do systemu oraz realizacji technologii jednokrotnego logowania
- Przygotowanie założeń do zapewnienia bezpiecznej synchronizacji czasu i niezaprzeczalności wystawionych znaczników czasu
- Przygotowanie zasad bezpieczeństwa transmisji danych
- Wstępną analizę ryzyka w zakresie bezpieczeństwa informacji

Zalecenia opisane w niniejszym dokumencie będą wymagały uszczegółowienia podczas dalszych prac projektowych – po ustaleniu architektury systemu oraz w fazie implementacji wykonywanej przez realizującego system.



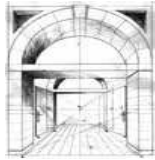
1.2 Źródła informacji

Akty prawne obowiązujące

- Ustawa z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne Dz. U. z dnia 20 kwietnia 2005 r.;
 - Rozporządzenie Rady Ministrów z dnia 11 października 2005 w sprawie minimalnych wymagań dla systemów teleinformatycznych. Dz.U.05.212.1766;
 - Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno – technicznych doręczania dokumentów elektronicznych podmiotom publicznym. Dz.U.05.200.1651;
- Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego Dz.U.00.98.1071 z póź. zm.;
- Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U.01.130.1450).
 - Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urzędów służących do składania i weryfikacji podpisu elektronicznego. (Dz.U.02.128.1094).
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. (Dz.U.02.144.1204) z późniejszymi zmianami
- Ustawa z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz. U. z dnia 4 lutego 2004 r.)
 - Rozporządzenie Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 19 marca 2004 w sprawie sposobów rozpowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL).

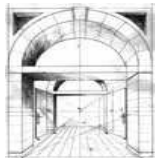
Akty prawne projektowane

- Projekt Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie struktury i sposobu sporządzania pism w formie dokumentów elektronicznych oraz warunków organizacyjno – technicznych ich doręczania.
- Projekt Ustawy o zmianie ustawy o podpisie elektronicznym przygotowywany w Ministerstwie Spraw Wewnętrznych i Administracji



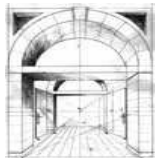
Standardy

- CEN - CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.
- CEN - CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic module for CSP Signing Operation – Protection Profile (MCSO-PP).
- CEN - CWA 14169 Secure Signature-Creation Devices “EAL 4+”
- CEN - CWA 14170 Security Requirements for Signature Creation Applications
- CEN - CWA 14171 General Guidelines for Electronic Signature Verification
- CEN - CWA 14172-8 EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes
- ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES).
- ETSI TS 101 733 CMS Advanced Digital Signature – CadES
- ETSI TS 102 023 Policy requirements for time-stamping authorities
- RSA PKCS#7 – Cryptographic Message Syntax
- W3C - Specyfikacja XML 1.1 <http://www.w3.org/TR/xml11/>
- W3C - Specyfikacja XMLdSig <http://www.w3.org/TR/xmlldsig-core/>
- W3C - Specyfikacja XSLT <http://www.w3.org/TR/xslt/>
- ISO/IEC 17799:2005 Information technology — Security techniques — Code of practice for information security management
- ISO/IEC TR 13335-3:1998, Guidelines for the Management of IT Security. Part 3: Techniques for the Management of IT Security
- PD 3002 Guide to BS 7799 Risk Assessment, British Standard
- RFC 1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis.
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol(TSP).
- PN-ISO/IEC 18014-1:2005 Technika informatyczna -- Techniki zabezpieczeń -- Usługi znacznika czasu -- Część 1: Struktura.
- PN-ISO/IEC 18014:2005 Technika informatyczna -- Techniki zabezpieczeń -- Usługi znacznika czasu -- Część 2: Mechanizmy tworzenia tokenów niezależnych.



1.3 Zastosowane skróty i pojęcia

Nazwa	Objaśnienie
NTP	Network Time Protocol Protokół umożliwiający synchronizację czasu pomiędzy urządzeniami w sieciach teleinformatycznych.
DS/NTP	Datum Secure/ Network Time Protocol Protokół umożliwiający synchronizację czasu pomiędzy urządzeniami w sieciach teleinformatycznych w sposób zabezpieczony kryptograficznie.
Zaufany system	System realizujący usługi certyfikacyjne – wydawanie certyfikatów, znakowanie czasem, potwierdzanie ważności certyfikatów, a także usługi elektronicznego potwierdzenia danych z wykorzystaniem wiarygodnego czasu
System teleinformatyczny	Oprogramowanie i urządzenia komputerowe realizujące lub wspomagające realizację usług publicznych, obsługiwane lub wykorzystywane przez organy administracji



2 Zasady bezpieczeństwa według kategorii bezpieczeństwa.

2.1 Ogólne zasady bezpieczeństwa organizacji

Poniższy opis wprowadza zasady bezpieczeństwa organizacji systemu e-PUAP, które należy wziąć pod uwagę przy projektowaniu architektury systemu. W wyniku ewaluacji proponowanej architektury rozwiązania powinny powstać zalecenia implementacyjne dla systemu.

Podstawą dla niniejszego opracowania był standard ISO 17799:2005, który wyróżnia trzydzieści dziewięć głównych kategorii bezpieczeństwa. Kategorie te można pogrupować w jedenaście grup.

2.1.1 Polityka bezpieczeństwa

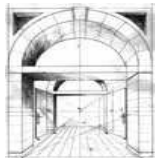
1. Polityka bezpieczeństwa informacji

Powinien powstać czytelny i zrozumiały dokument polityki bezpieczeństwa zgodny z celami i wymaganiami biznesowymi, przepisami prawa i regulacjami wewnętrznymi. Dokument taki powinien być podany do wiadomości wszystkich pracowników i stron trzecich. Powinno się dokonywać przeglądu polityki bezpieczeństwa w regularnych i zaplanowanych odstępach czasowych w celu zapewnienia przydatności, zgodności, skuteczności i aktualności dokumentu.

2.1.2 Organizacja bezpieczeństwa informacji

1. Organizacja wewnętrzna

W organizacji należy ustanowić strukturę organizacyjną, której zadaniem jest inicjowanie i kontrola zadań związanych z bezpieczeństwem informacji. W strukturze powinien być przewidziany interdyscyplinarny komitet sterujący, którego zadaniem jest zapewnienie spójności działań związanych z bezpieczeństwem w całej organizacji.



Wszystkie stanowiska w organizacji powinny mieć jasno zdefiniowane zakresy obowiązków i odpowiedzialności w dziedzinie bezpieczeństwa.

Wszelkie nowe środki służące do przetwarzania informacji powinny być autoryzowane przez kierownictwo organizacji.

Wszyscy osoby/organizacje, które mają kontakt z informacjami organizacji powinni mieć podpisane stosowne umowy o zachowaniu poufności. W celu przeciwdziałania zagrożeniom w organizacji powinny być utrzymywane kontakty z właściwymi organami władzy oraz innymi organizacjami, które są aktywnie zaangażowane w problematykę ochrony informacji.

Proces zarządzania bezpieczeństwem w organizacji powinien być poddawany przeglądom przez niezależnych ekspertów.

2. Strony zewnętrzne

Należy opracować zasady dostępu stron trzecich, zarówno dostawców, usługodawców jak i klientów do systemów przetwarzania informacji. Przed określeniem zasad należy zidentyfikować wszystkie możliwe ryzyka związane z dostępem stron trzecich. Wszędzie gdzie to możliwe powinny zostać podpisane stosowne umowy

2.1.3 Zarządzanie aktywami

1. Odpowiedzialność za aktywa

W celu utrzymania odpowiedniego poziomu ochrony aktywów organizacji należy sporządzić dokładny ich rejestr i do każdego z aktywów przypisać osobę, która będzie miała nad nim kierowniczą odpowiedzialność. Powinno się również określić zasady dopuszczalnego korzystania z aktywów i informacji w nich zawartych.

2. Klasyfikacja informacji

Informacje powinny być sklasyfikowane pod względem, wartości, wymagań prawnych, wrażliwości i krytyczności dla organizacji. Informacje, jeżeli to możliwe powinny być oznaczone w sposób właściwy dla danej klasy. Każda klasa informacji powinna mieć określony sposób postępowania z nią.

2.1.4 Bezpieczeństwo zasobów ludzkich

1. Przed zatrudnieniem

Powinny zostać określone wymagania bezpieczeństwa dla każdego stanowiska pracy zarówno dla pracowników, wykonawców jak i użytkowników reprezentujących stronę trzecią. Wszyscy kandydaci do zatrudnienia powinni być sprawdzeni zwłaszcza, jeżeli nabór dotyczy stanowisk wrażliwych. Zasady i warunki zatrudnienia powinny być szczegółowo opisane w umowie zawieranej pomiędzy organizacją a zatrudnianym.



2. Podczas zatrudnienia

Pracownicy, wykonawcy oraz użytkownicy reprezentujący stronę trzecia powinni być właściwie wdrożeni i przeszkoleni, aby byli świadomi zagrożeń, obowiązków i odpowiedzialności prawnej. Powinien być również wdrożony proces postępowania dyscyplinarnego związanego z naruszeniem bezpieczeństwa.

3. Zakończenie lub zmiana zatrudnienia

Powinien powstać proces przekazywania obowiązków i odpowiedzialności po ustaniu stosunku pracy pracownika, wykonawcy lub użytkownika reprezentującego stronę trzecią. Z chwilą ustania stosunku pracy powinny być odbierane wszelkie prawa dostępu.

2.1.5 Bezpieczeństwo fizyczne i środowiskowe

1. Obszary bezpieczne

Krytyczne lub wrażliwe środki przetwarzania informacji powinny być umieszczane w obszarach bezpiecznych, chronionych precyzyjnie określoną fizyczną granicą przez odpowiedni dobrane bariery i odpowiedni zabezpieczone wejścia. Powinny one chronić systemy i informacje w nich zawarte przed nieuprawnionym dostępem oraz szkodliwym wpływem środowiska oraz zakłóceniami. Powinny być opracowane szczegółowe zasady przebywania i pracy w obszarach bezpiecznych.

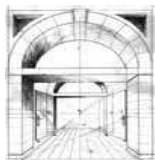
2. Bezpieczeństwo sprzętu

Sprzęt służący do przetwarzania informacji powinien być rozlokowany i chroniony w taki sposób aby zredukować ryzyka związane z zagrożeniami środowiskowymi oraz nieautoryzowanym dostępem. Powinien mieć on zapewnione systemy wsparcia w celu zabezpieczenia przed awariami (zasilacze awaryjne, klimatyzatory, itp.). Okablowanie służące do przesyłania danych powinno być zabezpieczone przed uszkodzeniem lub przejęciem. Środki przetwarzania informacji powinny być konserwowane przez odpowiedni przeszkolony personel. Powinny być opracowane szczegółowe zasady wnoszenia mienia poza siedzibę organizacji.

2.1.6 Zarządzanie systemami i sieciami

1. Procedury eksploatacyjne i zakresy odpowiedzialności

Powinny być wdrożone procedury związane z zarządzaniem i eksploatacją środków przetwarzania informacji, procedury powinny przewidywać również przypisanie odpowiedzialności. Procedury powinny zawierać dokumentowanie czynności eksploatacyjnych, zarządzanie i kontrolowanie zmian w środkach przetwarzania



informacji.

Obowiązki personelu powinny być rozdzielone w taki sposób aby uniemożliwić nadużycia w systemach przetwarzania informacji. Systemy testowe i rozwojowe powinny być odseparowane od systemów eksploatacyjnych.

2. Zarządzanie usługami dostarczonymi przez strony trzecie

Wszelkie usługi oraz dostawy powinny być szczegółowo regulowane odpowiednimi umowami, w których powinny się znaleźć uzgodnione zabezpieczenia, definicje usług i poziomy dostaw. Wykonanie tych umów powinno być regularnie monitorowane i audytowane. Powinna być również opracowana procedura zarządzania zmianami w usługach stron trzecich.

3. Planowanie i odbiór systemów

W celu dostarczenia systemu o odpowiedniej pojemności i wydajności należy dokonać szczegółowej analizy potrzeb, a po wdrożeniu systemu monitorować i planować przyszłą pojemność i wydajność aby uniknąć ryzyka przeciążenia. Powinno się opracować i wdrożyć odpowiednią procedurę doboru kryteriów odbioru oraz testów odbiorczych.

4. Ochrona przed kodem złośliwym i kodem mobilnym

Powinno się wprowadzić zabezpieczenia i przedsięwziąć środki ostrożności w celu zabezpieczenia systemów przed złośliwym kodem. W przypadku kodu mobilnego systemy powinny być tak skonfigurowane aby uniemożliwić uruchomienie nieautoryzowanego kodu mobilnego.

5. Kopie zapasowe

Powinno się wprowadzić procedury tworzenia, odtwarzania i testowania kopii zapasowych.

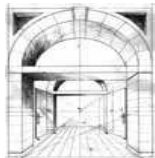
6. Zarządzanie bezpieczeństwem sieci

Sieci powinny być odpowiednio nadzorowane i zarządzane w celu utrzymania bezpieczeństwa systemów aplikacji sieciowych przed zagrożeniami. Elementy bezpieczeństwa i parametry poziomu usług powinny być zawarte w umowach z dostawcami usług.

W przypadku przesyłania informacji przez sieci publiczne powinny być wdrożone zabezpieczenia właściwe do realizacji tego celu.

7. Obsługa nośników

Powinno być wdrożone właściwe procedury postępowania z nośnikami wymiennymi, zabezpieczające przed nieautoryzowanym ujawnieniem, modyfikacją, usunięciem lub



zniszczeniem danych. Wykorzystane nośniki powinny być niszczone w sposób bezpieczny i pewny. Procedury postępowania z nośnikami powinny być dostosowane do klasyfikacji informacji na nich zawartej.

8. Wymiana informacji

Wymiana informacji wewnątrz organizacji jak i z każdym podmiotem zewnętrznym powinna być sformalizowana i oparta na odpowiedniej polityce, umowach i stosownych przepisach prawa. Nośniki fizyczne służące do wymiany informacji powinny być właściwie zabezpieczone przed nieupoważnionym dostępem, niewłaściwym użyciem lub uszkodzeniem podczas transportu. Wiadomości elektroniczne służące do wymiany informacji powinny być zabezpieczone zgodnie z klasyfikacją informacji w nich zawartej.

9. Usługi handlu elektronicznego

Informacje przesyłane w sieciach publicznych powinny być chronione przed nieautoryzowanym ujawnieniem lub modyfikacją. Transakcje dokonywane on-line powinny być zabezpieczone przed niekompletnością transmisji, nieautoryzowanymi zmianami, ujawnieniem, kopiowaniem lub powtórzeniem. Informacje publicznie dostępne powinny być chronione przed nieuprawnioną modyfikacją.

10. Monitorowanie

W celu wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji systemy powinny być monitorowane, a wszelkie zdarzenia związane z bezpieczeństwem informacji powinny być rejestrowane w odpowiednich dziennikach systemowych. Zapisy dzienników powinny być regularnie przeglądane przez odpowiednio przeszkolone osoby. Informacje zawarte w dziennikach powinny być chronione przed manipulacją i nieautoryzowanym dostępem. W celu łatwej korelacji zdarzeń zegary systemów powinny być synchronizowane.

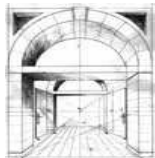
2.1.7 Kontrola dostępu

1. Wymagania biznesowe wobec kontroli dostępu

Dostęp do informacji, środków przetwarzania informacji i procesów biznesowych powinien być kontrolowany w oparciu o potrzeby i wymagania biznesowe.

2. Zarządzanie dostępem użytkowników

Procedury przyznawania i odbierania praw powinny obejmować cały okres życia korzystania użytkownika z systemu, od początkowej rejestracji nowych użytkowników do wyrejestrowania użytkowników, których dostęp do systemów nie jest już



wymagany. Przyznawanie i korzystanie z przywilejów powinno być ograniczone do niezbędnego minimum i kontrolowane oraz podlegać regularnym przeglądom.

3. Odpowiedzialność użytkowników

Użytkownicy powinni być świadomi swojej roli i odpowiedzialności w procesie utrzymania bezpieczeństwa systemów i informacji.

4. Kontrola dostępu do sieci

Kontrola dostępu do sieci powinna obejmować dostęp zarówno do wewnętrznych jak i zewnętrznych usług sieciowych. Jako zabezpieczenia powinno się stosować odpowiednie i odpowiednio zabezpieczone interfejsy pomiędzy siecią organizacji a sieciami stron trzecich i sieciami publicznym, odpowiednich mechanizmów uwierzytelnienia użytkowników i urzędów oraz kontroli dostępu użytkowników do usług informatycznych. Połączenia sieciowe powinny być monitorowane, a zdarzenia rejestrowane.

5. Kontrola dostępu do systemów operacyjnych

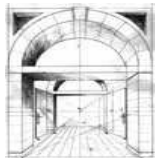
Dostęp do systemów operacyjnych powinien być ograniczony wyłącznie do użytkowników uwierzytelnionych przy pomocy odpowiednich środków uwierzytelnienia i autoryzowanych. Nieudane jak i udane próby dostępu oraz użycie przywilejów powinno być rejestrowane. Dla aplikacji i sesji wrażliwych powinien być ograniczony czas połączeń i nieaktywności.

6. Kontrola dostępu do aplikacji i informacji

Dostęp logiczny do informacji niepublicznych i aplikacji powinien być ograniczony wyłącznie do autoryzowanych użytkowników. Dostęp użytkowników i personelu obsługi technicznej do informacji oraz funkcji aplikacji powinien być ograniczony zgodnie ze zdefiniowaną polityką dostępu, która powinna bazować na potrzebach biznesowych. Systemy zawierające i przetwarzające informacje wrażliwe powinny mieć izolowane fizycznie lub logicznie środowiska przetwarzania.

7. Przetwarzanie mobilne i praca na odległość

Powinna zostać opracowana odpowiednia polityka dotycząca pracy na odległość i przetwarzania mobilnego. Powinny być zastosowane zabezpieczenia zgodne z przeprowadzoną analizą ryzyka dla tego typu pracy.



2.1.8 Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

1. Wymagania bezpieczeństwa systemów informacyjnych

Powinny powstać wymagania bezpieczeństwa dla nowych systemów oraz uaktualnień eksploatowanych systemów. Wymagania te powinny odzwierciedlać wartość biznesową aktywów oraz oszacować potencjalne szkody wynikające z braku zabezpieczeń. Ze względów ekonomicznych wymagania powinny być określone już w fazie projektowej.

2. Poprawne przetwarzanie w aplikacjach

Zabezpieczenia powinny być zaprojektowane jako część aplikacji w celu zapewnienia poprawności przetwarzania. Zabezpieczenia powinny obejmować weryfikację danych wejściowych i wyjściowych oraz wewnętrznego przetwarzania. Jeżeli wymagania bezpieczeństwa i analiza ryzyka stwierdza, że zabezpieczenia wewnętrzne są niewystarczające, to należy zastosować dodatkowe zewnętrzne zabezpieczenia.

3. Zabezpieczenia kryptograficzne

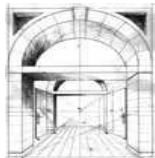
W celu zapewnienia poufności, niezaprzeczalności i integralności informacji należy wprowadzić odpowiednie mechanizmy kryptograficzne. Stosowanie zabezpieczeń kryptograficznych wymaga opracowania odpowiedniej polityki korzystania z nich oraz odpowiedniej polityki zarządzania kluczami.

4. Bezpieczeństwo plików systemowych

Pliki systemowe powinny być chronione przed nieuprawnionym dostępem i przypadkowym uszkodzeniem. Powinny być opracowane procedury instalacji i kontroli oprogramowania w eksploatowanych systemach.

5. Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej

Wszelkie zmiany w aplikacjach i systemach informatycznych powinny być kontrolowane i rejestrowane przy pomocy odpowiednich procedur. Po dokonaniu zmian powinien się odbyć przegląd techniczny i testowanie aplikacji biznesowych aby zapewnić, że zastosowane zmiany nie mają wpływu na bezpieczeństwo i poprawność ich działania. Wszelkie zmiany w oprogramowaniu powinny być ograniczone do niezbędnego minimum. Jeżeli prace rozwojowe zostały zlecone stronie trzeciej, to powinny być stale nadzorowane i monitorowane.



6. Zarządzanie podatnościami technicznymi

Podatności techniczne powinny być monitorowane w zależności od posiadanych aktywów. Zarządzanie podatnościami powinno być skuteczne i systematyczne.

2.1.9 Zarządzanie incydentami związanymi z bezpieczeństwem informacji

1. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości

Powinny być opracowane i wdrożone procedury zgłaszania i eskalowania zdarzeń związanych z naruszeniem bezpieczeństwa. Wszyscy pracownicy, przedstawiciele stron trzecich, klienci powinni być zobowiązani do niezwłocznego zgłaszania zauważonych incydentów.

2. Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami

Powinna zostać opracowana procedura obsługi zdarzeń związanych z incydentami naruszenia bezpieczeństwa. Procedura powinna być obsługiwana przez odpowiedzialny i kompetentny zespół ekspertów. Powinien być wdrożony proces ciągłego zarządzania incydentami. Incydenty powinny polegać ocenie w celu zmniejszenia częstości i rozmiaru szkód oraz kosztów związanych z ich wystąpieniem. Ocena incydentów może wskazać na konieczność udoskonalenia systemu zabezpieczeń przez dodanie nowych zabezpieczeń lub uaktualnienie istniejących. Należy gromadzić materiał dowodowy dotyczący incydentów.

2.1.10 Zarządzanie ciągłością działania

1. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania

W celu ochrony działalności biznesowej przed awariami i katastrofami należy opracować proces zarządzania ciągłością działania. Proces powinien zostać opracowany na podstawie wymagań biznesowych, z których wynikną priorytety niezbędnych działań. Plany ciągłości działania powinny być regularnie przeglądane i testowane w celu zapewnienia ich efektywności i aktualności.

2.1.11 Zgodność

1. Zgodność z przepisami prawnymi

Powinien zostać wdrożony proces mający na celu zapewnienie zgodności działalności



z przepisami prawa, zobowiązań ustawowych, regulacji wewnętrznych, umów i wymagań bezpieczeństwa.

2. Zgodność z politykami bezpieczeństwa i normami oraz zgodność techniczna

Wszystkie procedury stosowane w organizacji powinny być zgodne z politykami bezpieczeństwa oraz odpowiednimi normami.

3. Rozważania dotyczące audytu systemów informacyjnych

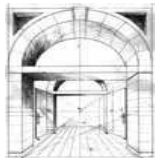
Podczas przeprowadzania audytu eksploatowane systemy i narzędzia audytu powinny być odpowiedni zabezpieczone w celu zminimalizowania zakłóceń z niego wynikających lub na niego wpływających. Audyty powinny być starannie uzgadniane i planowane. Narzędzia audytu powinny być zabezpieczone przed nadużyciami.

2.2 Zasady bezpieczeństwa w zakresie zaufanego systemu

System ePUAP będzie w ramach realizacji zadań wykorzystywał systemy zaufane, czyli takie, których działanie będzie mogło stanowić dowód w sporach. W szczególności będą to moduły ePUAP realizujące usługi certyfikacyjne tj. znakowanie czasem, usługę udostępniania zaufanego czasu, usługę OCSP, możliwe, że usługi certyfikacyjne polegające na wydawaniu certyfikatów zwykłych. Do zaufanych usług należy archiwizacja podpisów oraz wydanie poświadczenia przedłożenia zgodnie z rozporządzeniem (Dz.U.05.200.1651). Część z wymienionych usług zaufanego systemu może być realizowana przez zewnętrzne systemy (np. centrów certyfikacji) udostępniane w usłudze outsourcingowej.

Zaufany system stanowiący moduł systemu e-PUAP będzie wydawał lub wykorzystywał certyfikaty do weryfikacji: poświadczenia przedłożenia, poświadczenia doręczenia, OCSP i TSA oraz wszystkich poświadczeń danych. Dodatkowo system może wydawać certyfikaty. Na tym etapie projektu nie rozstrzygnięto czy będą one wykorzystywane czy nie. Przedstawione poniżej zasady bezpieczeństwa powinny być jednakowe dla całej zaufanej infrastruktury pracującej w e-PUAP, czyli zarówno systemy wewnętrzne e-PUAP jak i systemy zewnętrzne realizujące usługi zaufanego systemu powinny spełniać wymienione poniżej zasady.

Zestawienie wymagań zostało stworzone na podstawie norm i standardów określonych Decyzją Komisji Europejskiej z dnia 14 lipca 2002 (2003/511/EC). Wymienione tam standardy zostały opracowane dla systemów przeznaczonych do zarządzania certyfikatami: ich wydawania i zarządzania cyklem ich życia, co będzie, co najwyżej pomocniczą funkcjonalnością systemu ePUAP, jednakże ze względu na wagę realizowanych przez system zadań zalecane jest, aby urządzenia i aplikacje realizujące znakowanie czasem, wystawianie poświadczeń i inne zaufane usługi spełniały zapisy tych standardów w



zakresie wymagań ogólnych, wymagań odnośnie bezpiecznych urządzeń do składania podpisów i poświadczeń elektronicznych oraz generowania i dystrybucji znaczników czasu.

2.2.1 Zarządzanie systemami i bezpieczeństwem.

1. System teleinformatyczny powinien umożliwić zarządzanie rozdziałem zakresów obowiązków i odpowiedzialności personelu go obsługującego.
2. System powinien umożliwić podział i zarządzanie prawami dla następujących funkcji personelu:

Oficerowie bezpieczeństwa: odpowiedzialni za administrowanie wdrożonymi politykami bezpieczeństwa i procedurami

Inspektorzy ośrodka rejestracji: Odpowiedzialni za akceptację wniosków certyfikacyjnych użytkowników końcowych (wydawanie/odwoływanie/zawieszanie certyfikatów).

Administratorzy systemów: pracownicy posiadający uprawnienia do instalacji, konfiguracji i eksploatacji zaufanych systemów, ale z kontrolowanym dostępem do konfiguracji związanych z bezpieczeństwem.

Operatorzy systemów: pracownicy odpowiedzialni za codzienne utrzymanie zaufanych systemów, posiadający uprawnienia do archiwizacji i odtwarzania systemów.

Audytorzy systemów: pracownicy odpowiedzialni do przeglądania archiwów i zapisów w dziennikach zaufanych systemów.

3. System powinien umożliwić powiązanie użytkowników systemu z pełnionymi przez nich funkcjami.

2.2.2 Zarządzanie utrzymaniem.

1. Wraz z systemem powinny zostać dostarczone:

- * Podręcznik instalacyjny
- * Podręcznik administratora
- * Podręcznik użytkownika

Dokumentacja systemu powinna umożliwiać poprawne i bezpieczne utrzymywanie systemu, umiejscowienie systemu redukujące ryzyko jego awarii, zabezpieczenie systemu przed wirusami i złośliwym kodem w celu zapewnienia integralności systemów i bezpieczeństwa przetwarzanych informacji.



2.2.3 Ciągłość działania.

1. System powinien być odporny na przerwanie działania w wyniku wystąpienia awarii w pojedynczym module systemu i zapewniać nieprzerwane działanie systemów, które świadczą następujące usługi:

- * Wydawanie certyfikatów
- * Unieważnianie certyfikatów
- * Informowanie o statusie certyfikatów

System powinien zapewniać dostępność usługi unieważniania i informowania o statusie certyfikatów na poziomie 99,9%.

2. W przypadku wystąpienia katastrofy system powinien umożliwiać kontynuowanie działania przy użyciu systemu zapasowego. Maksymalny czas wznowienia usługi powinien być określony polityką certyfikacji.
3. Przełączenie z systemu głównego na awaryjny nie powinno powodować wzrostu ryzyka utraty zaufania do nieakceptowalnego poziomu.

2.2.4 Synchronizacja czasu

Wystawianie certyfikatów i późniejsze nimi zarządzanie związane jest z czasem, dlatego wymaga się, aby zaufane systemy były odpowiednio synchronizowane do standardowego źródła czasu. Wymóg ten jest niezależny od wymogów znakowania czasem, które mogą być stosowane przez dostawcę usług certyfikacyjnych.

1. System zapewnia synchronizację czasu z podaną dokładnością. Zaleca się, aby do przy synchronizacji było wykorzystywane zaufane źródło czasu.

2.2.5 Uwierzytelnienie użytkownika.

1. System zapewnia identyfikację tożsamości użytkownika i jego uwierzytelnienie przed jakimkolwiek umożliwieniem podjęcia działań.
2. System wymusza powtórne uwierzytelnienie po wylogowaniu się z systemu.
3. System zapewnia, że dane uwierzytelniające są unikalne i niepowtarzalne



2.2.6 Uwierzytelnienie zakończone niepowodzeniem.

1. System zapewnia ograniczenie liczby dozwolonych prób uwierzytelnienia, które zakończą się niepowodzeniem.

2.2.7 Weryfikacja sekretów.

1. System powinien zapewnić mechanizmy wymuszające ustalony poziom bezpieczeństwa stosowanych haseł.

2.2.8 Wymagania bezpieczeństwa.

1. System powinien zapewnić możliwość kontroli i ograniczenia dostępu do funkcji dedykowanych danemu systemowi lub użytkownikowi.
2. System powinien zapewnić zabezpieczenie dostępu do informacji wrażliwych (tj. kluczy prywatnych i haseł)

2.2.9 Generowanie kluczy.

1. System powinien wykorzystywać do generowania i przechowywania kluczy do podpisywania certyfikatów bezpieczne urządzenie kryptograficzne (HSM).
2. Bezpieczne urządzenie kryptograficzne, powinno być ocenione i certyfikowane zgodnie z następującymi wymaganiami:

- * Urządzenie powinno zapewnić poufność i integralność kluczy podczas ich całego czasu życia.
- * Urządzenie powinno zapewnić identyfikację i uwierzytelnienie użytkowników.
- * Urządzenie powinno ograniczać dostęp do swoich usług, w zależności od użytkownika i jego przywilejów przypisanych do tych usług.
- * Urządzenie powinno wykonywać serię testów sprawdzających poprawność jego pracy a w przypadku wykrycia błędów przełączyć się w stan bezpieczny.
- * Urządzenie powinno wykrywać próby sabotażu i w przypadku wykrycia takiej próby przełączyć się w stan bezpieczny.
- * Urządzenie powinno tworzyć zapisy zdarzeń dla każdej zmiany związanej z bezpieczeństwem.
- * Dopuszcza się, aby urządzenie umożliwiło wykonie kopii zapasowej klucza oraz jego odtworzenie, ale powinien zapewnić poufność i integralność kopii bezpieczeństwa i wymaga conajmniej dwuosobowego tworzenia kopii zapasowej i odtwarzania. Ocena powinna być przeprowadzona zgodnie z [CEN CMCSO-PP: CWA 14167-2 Cryptographic Module for CSP Signing Operations - ProtectionProfile] lub innym standardem, zawierającym porównywalny poziom wymagań.



3. System teleinformatyczny powinien umożliwić przechowywanie kluczy infrastruktury i kluczy kontrolnych w sprzętowych modułach kryptograficznych lub komponentach technicznych
4. System powinien umożliwiać generowanie kluczy zgodnie z wymaganiami normy ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

2.2.10 Dystrybucja kluczy.

1. System zapewnia ochronę kluczy prywatnych i tajnych tak, aby nie były one dystrybuowane w postaci jawnej.
2. System zapewnia, że klucze publiczne przed certyfikacją są zabezpieczone przed przechwyceniem i manipulacją.
3. System powinien zapewnić dystrybucję kluczy wg określonej metody.
4. System powinien zapewnić, że klucze publiczne związane z kluczami do podpisywania certyfikatów lub kluczami certyfikacyjnymi są dystrybuowane w sposób zapewniający integralność i autentyczność tych kluczy oraz parametrów z nimi związanych.
5. Jeżeli system tworzy certyfikat samopodpisany, to spełnia on następujące cechy:
 1. Podpis poświadczający certyfikat powinien być weryfikowany przy użyciu danych znajdujących się wewnątrz certyfikatu.
 2. Pola certyfikatu: podmiot i wystawca powinny być identyczne.
6. Skrót certyfikatu samopodpisanego powinien być utworzony przy użyciu algorytmów zdefiniowanych w ETSI SR 002 176

2.2.11 Użycie kluczy.

1. Rozwiązanie powinno zapewniać kontrolowanie dostępu do urządzeń kryptograficznych wykorzystywanych do podpisywania certyfikatów oraz generowania kluczy infrastruktury i kluczy kontrolnych.
2. System powinien zapewniać dostarczanie odseparowanych kluczy służących do realizacji funkcji niezaprzeczalności od kluczy służących do realizacji innych celów np. szyfrowania.
System powinien zapewniać umieszczenie w certyfikacie rozszerzenia "key usage"
3. System powinien zapewniać weryfikację ważności certyfikatów kluczy infrastruktury i kluczy kontrolnych przed udzieleniem im zaufania. System powinien dokonać weryfikacji list unieważnionych certyfikatów i urzędów certyfikacji.



2.2.12 Wymiana kluczy.

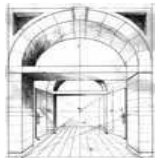
1. System powinien umożliwiać regularną wymianę kluczy infrastruktury i kluczy kontrolnych.
2. System powinien zapewniać bezpieczeństwo wymiany kluczy infrastruktury i kluczy kontrolnych.

2.2.13 Niszczenie kluczy.

1. System powinien umożliwiać zniszczenie kluczy służących do podpisywania certyfikatów po upływie ich ważności.
2. System powinien umożliwiać zniszczenie kluczy służących do przechowywania kluczy tajnych lub prywatnych.
3. System powinien umożliwiać skuteczne zamazanie zapisów sekretów przechowywanych jawnym tekstem i kluczy prywatnych przechowywanych w sposób sprzętowy i programowy.
4. System powinien umożliwiać skuteczne wymazywanie kluczy programowych (przechowywanych w software).

2.2.14 Przechowywanie, wykonywanie kopii bezpieczeństwa i odtwarzanie kluczy.

1. System powinien umożliwiać przechowywanie kluczy prywatnych i tajnych w sposób zapewniający ich bezpieczeństwo przed ujawnieniem.
2. Klucze służące do podpisywania certyfikatów powinny być przechowywane w bezpiecznym urządzeniu kryptograficznym (HSM) spełniającym warunki określone w wymaganiach dla generowania kluczy
3. Prywatne i tajne klucze kontrolne powinny być przechowywane w sprzętowych urządzeniach kryptograficznych
4. System powinien umożliwiać, że jeżeli jakkolwiek klucz prywatny/tajny przechowywany w bezpiecznym urządzeniu kryptograficznym, będzie eksportowany z tego urządzenia, powinien być zabezpieczony przez to urządzenie w sposób gwarantujący jego poufność już przed momentem składowania klucza na zewnątrz urządzenia. Jakiegokolwiek dane wrażliwe, związane z kluczem, nigdy nie powinny być przechowywane w sposób niezabezpieczony. Wszędzie tam, gdzie klucze prywatne/tajne są zabezpieczone przy pomocy szyfrowania, powinny zostać spełnione wymagania kryptograficzne określone w ETSI SR 002 176



5. System powinien zapewnić, że wykonanie kopii bezpieczeństwa, przechowywania i odtwarzania kluczy służących do podpisywania certyfikatów, kluczy infrastruktury i kluczy kontrolnych będzie wykonywane tylko przez osoby upoważnione (np.. Oficera bezpieczeństwa)
6. System powinien zapewnić, że wykonanie kopii bezpieczeństwa, przechowywania i odtwarzania kluczy służących do podpisywania certyfikatów będzie wykonywane pod kontrolą co najmniej dwóch osób.
7. System nie powinien umożliwiać wykonanie kopii bezpieczeństwa kluczy służących do składania podpisu elektronicznego.

2.2.15 Archiwizowanie kluczy.

1. System nie może umożliwiać wykonania kopii archiwizacyjnej kluczy służących do składania podpisu elektronicznego.

2.2.16 Generowanie zapisów dzienników zdarzeń.

1. System powinien rejestrować następujące zdarzenia:
 - * Ważne zdarzenia środowiskowe zaufanych systemów, zdarzenia związane z zarządzaniem kluczami i certyfikatami.
 - * Uruchamianie i zamykanie funkcji zapisu zdarzeń.
 - * Zmiany parametrów zapisu zdarzeń.
 - * Działań podjętych w wyniku awarii nośników służących do zapisywania dzienników zdarzeń.Wszystkie próby uzyskania dostępu do zaufanych systemów powinny być rejestrowane.

2.2.17 Zapewnienie dostępności zapisów dzienników zdarzeń.

1. System powinien prowadzić dzienniki zdarzeń i zapewnić wystarczającą ilość miejsca na nośnikach danych do zapisywania zdarzeń.
2. System powinien zapewniać, że dzienniki zdarzeń nie będą automatycznie nadpisywane.



2.2.18 Parametry zapisywane w dziennikach zdarzeń.

1. Wszystkie zapisy w dziennikach zdarzeń powinny zawierać następujące parametry:
 - * data i czas zdarzenia;
 - * rodzaj zdarzenia;
 - * tożsamość jednostki odpowiedzialnej za działanie;
 - * informację o sukcesie lub porażce zdarzenia.

2.2.19 Tworzenie raportów na podstawie dzienników zdarzeń.

1. System powinien zapewnić możliwość przeszukiwania zapisów dzienników zdarzeń na podstawie czasu i daty zdarzenia, rodzaju zdarzenia i/lub tożsamości użytkownika.
2. System powinien umożliwić prezentowanie dzienników zdarzeń w sposób umożliwiający użytkownikowi właściwą interpretację informacji.

2.2.20 Ograniczanie dostępu do dzienników zdarzeń.

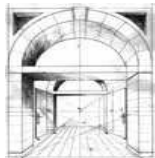
1. Zaufany system powinien zabronić wszystkim użytkownikom dostępu do odczytu zapisów dzienników zdarzeń, z wyjątkiem tych użytkowników, którym zostało przydzielone wyraźne prawo odczytu zapisów dzienników zdarzeń.
2. System powinien nie dopuszczać do modyfikacji zapisów dzienników zdarzeń

2.2.21 Alarmowanie.

1. Zaufany system powinien podnosić alarm po wykryciu potencjalnego naruszenia bezpieczeństwa.

2.2.22 Zapewnienie integralności zapisów dzienników zdarzeń.

1. System informatyczny powinien zapewniać integralność zapisów dzienników zdarzeń przez zastosowanie podpisu cyfrowego, funkcji skrótu lub kodu uwierzytelniającego dla każdego wpisu w dzienniku obliczonego na podstawie całego dziennika zdarzeń lub na podstawie aktualnego zapisu i wyniku



kryptograficznego poprzedniego zapisu. System powinien zapewnić możliwość sprawdzenia integralności danych zapisanych w dziennikach.

2.2.23 Zapewnienie źródła czasu dla dzienników zdarzeń.

1. Zapisy dzienników zdarzeń powinny zawierać czas z zaufanego źródła.

2.2.24 Tworzenie danych archiwalnych

1. System powinien umożliwiać tworzenie archiwów na nośnikach odpowiednich do przechowywania i następnie przetwarzania w celach dowodowych.
2. System powinien umożliwiać archiwizowanie następujących obiektów:
 - * wszystkie certyfikaty;
 - * wszystkie listy odwołanych urzędów certyfikacji i listy certyfikatów unieważnionych;
 - * wszystkie dzienniki zdarzeń.
3. Każdy zapis archiwalny powinien zawierać czas wykonania archiwizacji.
4. Archiwum nie powinno zawierać krytycznych parametrów bezpieczeństwa w niezabezpieczonej postaci.

2.2.25 Wybiórcze przeszukiwanie.

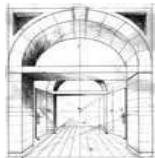
1. System powinien umożliwiać przeszukiwanie archiwaliów na podstawie ich rodzajów.

2.2.26 Integralność zarchiwizowanych danych.

1. Rozwiązanie powinno zapewniać zabezpieczenie archiwaliów przed modyfikacją.

2.2.27 Tworzenie kopii zapasowych.

1. System powinien być wyposażony w mechanizm tworzenia kopii zapasowych.



2. Dane zapisywane w kopii bezpieczeństwa powinny być wystarczające do odtworzenia stanu systemu.
3. Użytkownik posiadający odpowiednie uprawnienia powinien mieć możliwość wykonania kopii zapasowej na żądanie.

2.2.28 Integralność i poufność informacji zawartych w kopiach bezpieczeństwa.

1. Kopie zapasowe powinny być zabezpieczone przed modyfikacją.
2. System powinien zapewniać przechowywanie wyłącznie w postaci zaszyfrowanej krytycznych parametrów bezpieczeństwa i informacji poufnych.

2.2.29 Odtwarzanie.

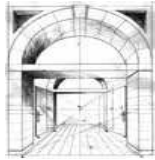
1. System powinien posiadać funkcję odtwarzania stanu systemu z kopii zapasowej.
2. System powinien Użytkownikowi posiadającemu odpowiednie uprawnienia dać możliwość odtworzenia systemu na żądanie.

2.2.30 Zabezpieczenie wiadomości.

1. Wszystkie wiadomości generowane przez jakąkolwiek usługę podstawową powinny:
 - * Być zabezpieczone przy użyciu kluczy infrastruktury skojarzonych z daną usługą.
 - * Zawierać czas, w którym nadawca wygenerował wiadomość.
 - * Zawierać zabezpieczenie przed atakami powtórzeniowymi.

2.2.31 Dane informacji o statusie certyfikatu.

1. System powinien zapewniać, że dane przesyłane okresowo lub w czasie rzeczywistym do usługi powinny pochodzić wyłącznie z zaufanych usług unieważniania.



2.2.32 Poprawność żądania.

1. Urząd znakowania czasem może sprawdzać pochodzenia żądania przed sprawdzeniem jego poprawności. Rozwiązaniem może być mechanizm uwierzytelnienia źródła.
2. Urząd znakowania czasem powinien zapewnić, że żądanie znakowania czasu wykorzystuje algorytm do tworzenia skrótu, który jest określony i zatwierdzony w ETSI SR 002 176

2.2.33 Tworzenie parametru czasu.

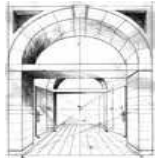
1. Źródło zaufanego czasu dla urzędu znakowania czasem powinno być synchronizowane do czasu UTC z tolerancją określoną w polityce np. do 1 sekundy. Dopuszcza się, aby było to, to samo źródło, co w wymaganiu 2.2.4.
2. Zegar urzędu znakowania czasem powinien być synchronizowany z UTC przy wykorzystaniu mechanizmu powszechnie uznanego za niezawodny.

2.2.34 Wytwarzanie znaku czasowego.

1. Numer seryjny tokena znacznika czasu powinien być unikalny dla każdego tokena znacznika czasu, wystawionego przez urząd znakowania czasem.
2. Token znacznika czasu powinien zawierać dokładność źródła czasu, jeżeli jest dokładniejsze niż wymagania polityki urzędu znakowania czasem.
3. Token znacznika czasu powinien zawierać wskaźnik polityki na podstawie której został wykonany.

2.2.35 Obliczanie tokena znacznika czasu

1. Klucze do podpisywania urzędu znakowania czasem powinny być wygenerowane i przechowywane w bezpiecznym urządzeniu kryptograficznym.
2. Bezpieczne urządzenie kryptograficzne, powinno być ocenione i certyfikowane zgodnie z następującymi wymaganiami:
 - * Urządzenie powinno zapewnić poufność i integralność kluczy podczas ich całego czasu życia.
 - * Urządzenie powinno zapewnić identyfikację i uwierzytelnienie użytkowników.
 - * Urządzenie powinno ograniczać dostęp do swoich usług, w zależności od użytkownika i jego przywilejów przypisanych do tych usług.



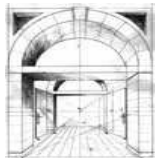
- * Urządzenie powinno wykonywać serię testów sprawdzających poprawność jego pracy a w przypadku wykrycia błędów przełączyć się w stan bezpieczny.
 - * Urządzenie powinno wykrywać próby sabotażu i w przypadku wykrycia takiej próby przełączyć się w stan bezpieczny.
 - * Urządzenie powinno tworzyć zapisy zdarzeń dla każdej zmiany związanej z bezpieczeństwem.
 - * Dopuszcza się, aby urządzenie umożliwiło wykonie kopii zapasowej klucza oraz jego odtworzenie, ale powinien zapewnić poufność i integralność kopii bezpieczeństwa i wymaga conajmniej dwuosobowego tworzenia kopii zapasowej i odtwarzania.
- Ocena powinna być przeprowadzona zgodnie z [CEN CMCSO-PP : CWA 14167-2 Cryptographic Module for CSP Signing Operations – Protection Profile] lub innym standardem, zawierającym porównywalny poziom wymagań.
3. Klucze kontrolne urzędu znakowania czasem powinny być przechowywane w sprzętowym urządzeniu kryptograficznym.
 4. Klucze do podpisywania urzędu znakowania czasem powinny być używane wyłącznie do podpisywania tokenów znakowania czasem.
 5. Urząd znakowania czasem powinien zapewnić, że odpowiedź zawierająca token znakowania czasem posiada tą samą datę jaka znajdowała się w żądaniu.
 6. Algorytmy i klucze do podpisywania, wykorzystywane przez urząd znakowania czasem, powinny, być zgodne z ETSI SR 002 176.

2.2.36 Dziennik zdarzeń urzędu znakowania czasem.

1. System zapewnia rejestrowanie następujących zdarzeń:
 - * Wszystkie zdarzenia związane z żądaniem odnowienia certyfikatu lub klucza urzędu znakowania czasem.
 - * Wszystkie zdarzenia związane z zarządzaniem cyklem życia kluczy do podpisu, urzędu znakowania czasem.
 - * Wszystkie awarie (włącznie z odchyleniem czasu poza wyznaczoną tolerancję) związane ze źródłami zaufanego czasu.

2.2.37 Przygotowanie urządzenia do składania podpisu.

1. Urządzenia do składania podpisu powinny być dostarczane w sposób umożliwiający zapewnienie autentyczności pochodzenia od oryginalnego dostawcy.

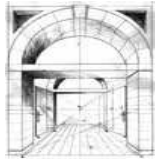


2. Jeżeli system realizuje przygotowanie urządzenia do składania podpisu, to powinno ono być realizowane w bezpiecznym środowisku.
3. Inicjalizacja, formatowanie i tworzenie struktury plików powinno ustawić bezpieczne wartości, parametry i warunki kontroli dostępu tworząc bezpieczną konfigurację urządzenia do składania podpisu, taką, która nie będzie mogła być niewłaściwie użyta.
4. Bezpieczne urządzenie do składania podpisu powinno być ocenione i certyfikowane zgodnie z CWA 14169 Secure Signature Creation Devices EAL4+ lub innym odpowiednim standardem.

Wybrany standard powinien określać wymagania dla wewnętrznego Signature-Creation Data/Signature-Verification Data Generation, SVD Export, kontrolę dostępu do bezpiecznego urządzenia do składania podpisu, personalizacji i tworzenia podpisu.

2.2.38 Dostarczanie urządzenia do składania podpisu.

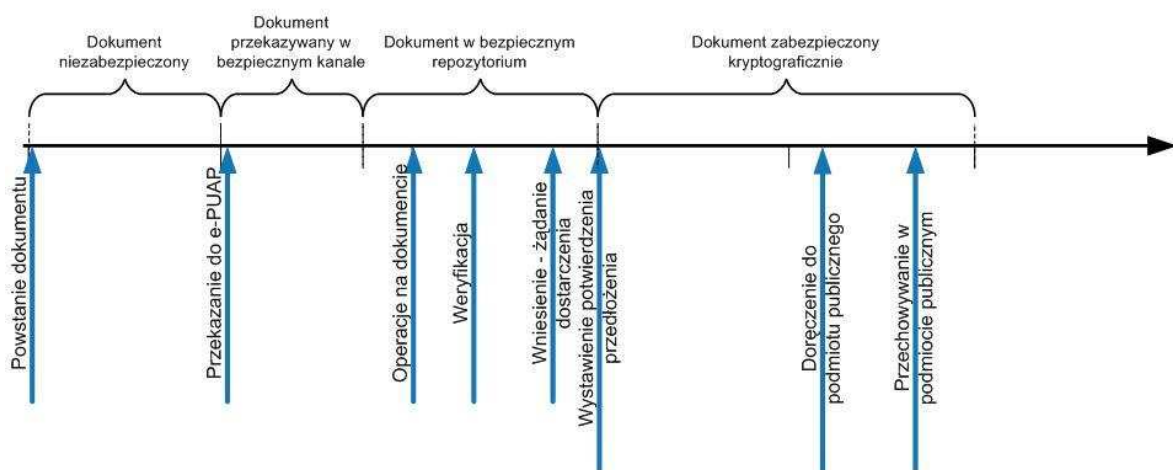
1. Konfiguracja systemu powinna umożliwiać bezpieczne dostarczenie urządzenia do składania podpisu do właściwego i uwierzytelnionego podmiotu.



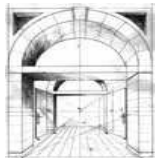
3 Zapewnienie integralności i niezaprzeczalności dokumentów

W systemie e-PUAP występują różnego rodzaju potwierdzenia opierające się na powszechnej technologii podpisu elektronicznego. W tym rozdziale został opisany mechanizm weryfikacji podpisu elektronicznego. Inne techniki związane np. z rejestracją logowań, prowadzeniem bezpiecznych repozytoriów (spełniających normy bezpieczeństwa informacji), mogą być niewystarczające do przeprowadzenia postępowania dowodowego w przed sądem, tak więc mogą być jedynie elementem pomocniczym przy sporządzaniu rejestrów z wykonanych czynności, nie są zalecane jako jedyny sposób zabezpieczenia informacji stosowany w systemie e-PUAP.

W systemie e-PUAP będą występowały dwa rodzaje dokumentów: podpisane i niepodpisane. Dokumentom podpisanym, integralność i niezaprzeczalność zapewnia podpis elektroniczny składany przez przygotowującego lub akceptującego dokument. Dla dokumentów niepodpisanych, mechanizm zapewnienia integralności i niezaprzeczalności jest trochę bardziej skomplikowane, został on przedstawiony na rysunku 1.



Rys. 3-1 Ochrona integralności dokumentów niepodpisanych



3.1 Podstawowa charakterystyka

Sprawdzenie niezaprzeczalności przekazywanych dokumentów polega na zweryfikowaniu podpisu elektronicznego, którym dokument został opatrzony. Niniejszy rozdział został przygotowany na podstawie zasad weryfikacji określonych standardem ETSI TS 101 903 XML Advanced Digital Electronic Signatures oraz normy CEN - CWA 14171 General Guidelines for Electronic Signature Verification.

W związku z tym, że rozwiązania prawne wskazują na oficjalne dokumenty w formacie XML oraz na format podpisu XML do stosowania w administracji państwowej, autorzy niniejszego opracowania przedstawili zasady zabezpieczenia niezaprzeczalności przekazywanych dokumentów oparte o format podpisu XAdES stanowiący rozszerzenie formatu XML Signature i oferujący archiwizację ważności podpisu elektronicznego.

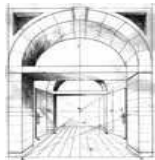
Zastosowanie poniższych zasad w stosunku do dokumentów elektronicznych, poświadczeń odbioru i przedłożenia umożliwi zapewnienie niezaprzeczalności tych dokumentów przez okres znacznie dłuższy niż ważność certyfikatu, którym jest weryfikowany podpis elektroniczny.

Proces weryfikacji podpisu elektronicznego dostarcza jednego z trzech statusów podpisu elektronicznego:

- **nieważny** oznacza, że albo format podpisu jest niepoprawny, albo wartości zawarte w podpisie nie przeszły pozytywnej weryfikacji (np. brak pozytywnej weryfikacji integralności podpisu elektronicznego, lub jeden z certyfikatów znajdujących się na ścieżce certyfikacyjnej jest niepoprawny lub odwołany);
- **niekompletnie zweryfikowany** oznacza, że zarówno format podpisu jest poprawny jak i proces weryfikacji podpisu nie zakończył negatywnie, jednak system weryfikujący nie znalazł wystarczającej ilości informacji do uznania podpisu za ważny, np. system nie mógł zweryfikować wszystkich certyfikatów na ścieżce certyfikacyjnej. ;
- **ważny** oznacza, że podpis przeszedł pozytywnie proces weryfikacji.

3.2 Weryfikacja początkowa.

W technologii XAdES sprawdzenie niezaprzeczalności dokumentów rozpoczyna się od sprawdzenia czy podpis, którym opatrzony jest dokument wykonany jest w formacie XAdES oraz od zidentyfikowania formy podpisu na podstawie właściwości zawartych w



strukturze podpisu. Struktury te muszą być zgodne z opisanymi w części normatywnej i załączniku B standardu ETSI TS 101 903 v 1.3.2 lub nowszej.

Początek procesu weryfikacji polega na sprawdzeniu referencji do certyfikatu podmiotu podpisującego. Referencja ta zapisana jest we właściwości *ds:SigningCertificate*. W przypadku braku tej właściwości należy sprawdzić czy referencja występuje w jednym z elementów właściwości *ds:KeyInfo*.

Następnie należy określić czy dołączenie właściwości jest bezpośrednie (wszystkie właściwości w granicach elementu *ds:Object* są zakopertowane przez element *ds:Signature*) czy pośrednie (określone przez obecność elementów *QualifyingPropertiesReference* w granicach elementu *ds:Object* są zakopertowane przez element *ds:Signature*) oraz czy dołączone są do dokumentu zgodnie ze standardem XAdES. Również ważnym elementem pozwalającym na zaliczenie podpisu elektronicznego jako podpisu XAdES jest wystąpienie wartości <http://uri.etsi.org/01903#SignedProperties> atrybutu *Type* w elemencie *ds:Reference* stanowiącym referencję *ds:Object*.

3.3 Pobieranie certyfikatów do weryfikacji.

Standard XAdES wymaga użycia pełnego zestawu certyfikatów wymaganych do przeprowadzenia weryfikacji podpisu elektronicznego. W konsekwencji system sprawdzający powinien wykorzystać właściwość *CertificateValues*, jeżeli występuje oraz właściwość *ds:KeyInfo* do pobrania wszystkich certyfikatów i na ich podstawie zbadać całą ścieżkę certyfikacji.

W przypadku braku właściwości *CertificateValues* powinna wystąpić właściwość *CompleteCertificateRefs* z której powinny zostać pobrane dane niezbędne do weryfikacji ścieżki certyfikacji. Brak obu tych wartości oznacza brak możliwości stwierdzenia poprawności podpisu zgodnie ze standardem.

Te same reguły dotyczące weryfikacji stosuje się do właściwości *AttrAuthoritiesCertValues* w odniesieniu do wartości certyfikatów służących urzędem do wystawiania certyfikatów atrybutów oraz ich wykorzystania w procesie weryfikacji certyfikatów atrybutów występujących we właściwości *SingerRole*.



3.4 Pobieranie informacji o statusie certyfikatów do weryfikacji.

Standard XAdES wymaga wykorzystania zawartości elementu *RevocationValues*, zawierającego wartości zawierające informacje o statusie certyfikatów wymaganych w procesie weryfikacji. W chwili obecnej jedynymi standaryzowanymi wartościami zawartości tego elementu są odpowiedzi CRL i OCSP. System weryfikujący powinien sprawdzić czy wartości te zawierają odpowiednie wartości dotyczące odwołanych certyfikatów, ich brak oznacza niemożliwość zweryfikowania podpisu. W przypadku braku elementu *RevocationValues* system powinien sprawdzić w analogiczny sposób wartości elementu *CompleteRevocationRefs*. Brak obu tych wartości oznacza brak możliwości stwierdzenia poprawności podpisu zgodnie ze standardem.

Te same reguły dotyczące weryfikacji stosuje się do właściwości *AttributeRevocationValues* w odniesieniu do wartości certyfikatów służących urzędom do wystawiania certyfikatów atrybutów oraz ich wykorzystania w procesie weryfikacji certyfikatów atrybutów występujących we właściwości *SingerRole*.

3.5 Sprawdzenie elementu SigningTime.

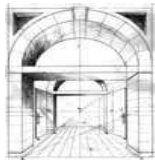
Własność określa czas, w którym złożono podpis elektroniczny.

Proces powinien sprawdzić czy czas rozpoczęcia procesu podpisywania jest wcześniejszy niż czas złożenia podpisu elektronicznego.

3.6 Sprawdzenie elementu SigningCertificate.

Klucz prywatny użytkownika może być wykorzystywany do różnych celów (np. do celów prywatnych lub do celów służbowych). Różne cele użycia klucza mogą być weryfikowane różnymi certyfikatami wystawianymi przez różne centra certyfikacji. Właściwość *SigningCertificate* jest niezbędna do precyzyjnego określenia, który z certyfikatów został użyty.

Jeżeli wśród danych związanych z podpisem elektronicznym występuje element *CertificateValues* system weryfikacji może wykorzystać zawartą w nim referencję do certyfikatu użytkownika, jeśli nie występuje referencja powinna być pobrana z elementu



ds:KeyInfo. W przypadku braku obu elementów nie ma możliwości dokonania weryfikacji zgodnie ze standardem.

Po uzyskaniu certyfikatu użytkownika system powinien sprawdzić go na podstawie referencji występujących w elemencie *ds:SigningCertificate*, jeżeli element występuje. Dla każdej wartości występującej w tym elemencie system powinien wykonać następujące czynności:

1. Porównać nazwę urzędu certyfikacji wydającego dany certyfikat oraz numer seryjny występujący w elemencie *IssuerSerial*. W tym celu system powinien utworzyć odpowiedni ciąg znaków związany z identyfikatorem wyróżniającym urząd certyfikacyjny, zgodnie z wytycznymi formatu XMLDSIG. W przypadku niemożności porównania referencji system powinien pobrać następną i tak do momentu natrafienia na zgodność a następnie przejść do wykonania następnej czynności.
2. Jeżeli element *ds:KeyInfo* zawiera element *ds:X509IssuerSerial* numer seryjny tam zawarty powinien być identyczny z numerem zawartym w *IssuerSerial* z elementu *SigningCertificate*.
3. Porównać zawartość elementu *ds:DigestValue* ze skrótem wyliczonym z certyfikatu przy pomocy algorytmu wymienionego w *ds:DigestMethod* po jego zakodowaniu metodą base64.

Jeżeli system nie znajdzie żadnej referencji zgodnej z certyfikatem wykorzystanym do podpisu, weryfikacja powinna być uznana za nieudaną.

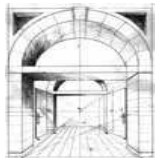
W przypadku gdy element *SigningCertificate* zawiera referencje do innych certyfikatów w ścieżce certyfikatów system powinien dokonać sprawdzenia ich wszystkich. Jeżeli w elemencie wystąpią referencje do certyfikatów nie znajdujących się w ścieżce certyfikacji lub w ścieżce znajdują się certyfikaty bez referencji, weryfikacja powinna być uznana za nieudaną.

3.7 Sprawdzenie elementów CompleteCertificateRefs

Element *CompleteCertificateRefs* zawiera sekwencję referencji do pełnego zestawu certyfikatów urzędów certyfikacji, umożliwiającą weryfikację ścieżki certyfikacyjnej od certyfikatu użytkownika do certyfikatu urzędu certyfikacji najwyższego poziomu.

Jeżeli występuje element *CompleteCertificateRefs* system powinien:

1. Uzyskać dostęp do wszystkich certyfikatów urzędów certyfikacji, które występują w ścieżce certyfikacji.
2. Dla każdego z wymienionych certyfikatów sprawdzić odpowiednie referencje, które stanowią wartości *IssuerSerial*, *ds:DigestMethod* i *ds:DigestValue*, zgodnie z metodą opisaną w podrozdziale „Sprawdzenie elementu *SigningCertificate*” punkt 1 i 3.



3. Sprawdzić, że nie ma referencji do innych certyfikatów niż występujące w ścieżce certyfikacji.

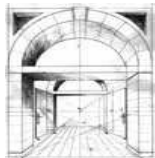
Reguły dla *AttributeCertificateRefs* są podobne, ale zamiast certyfikatów urzędów certyfikacji w ścieżce certyfikacji, sprawdzeniu poddane zostaną certyfikaty służące do wystawiania certyfikatów atrybutu, użyte do walidacji certyfikatu atrybutu zawartego w podpisie.

3.8 Sprawdzenie elementów CompleteRevocationRefs

Element *CompleteRevocationRefs* zawiera sekwencję referencji do pełnego zestawu danych umożliwiających sprawdzenie czy certyfikat użytkownika lub certyfikat, któregoś z urzędów certyfikacji znajdującego się na ścieżce certyfikacji nie został odwołany.

Sprawdzenie *CompleteRevocationRefs* wymaga od systemu uzyskania dostępu do informacji o statusie certyfikatów używanych do weryfikacji podpisu. Jeżeli występuje element *CompleteRevocationRefs* system powinien:

1. Jeżeli występuje element *RevocationValues*, system powinien sprawdzić czy zawiera odpowiednie informacje dotyczące odwołania dla wszystkich certyfikatów wymaganych do weryfikacji podpisu elektronicznego, a następnie porównać je z wartościami w *CompleteRevocationRefs*, zgodnie z krokiem 3.
2. Jeżeli nie występuje element *RevocationValues*, system powinien pobrać informacje dotyczące odwołań i sprawdzić czy są aktualne i odpowiednie dla wszystkich certyfikatów wymaganych do weryfikacji podpisu elektronicznego i porównać z odpowiednimi referencjami, zgodnie z krokiem 3.
3. Po pobraniu list CRL system powinien sprawdzić czy każda z nich odpowiada odpowiednim referencjom w *RevocationRefs*. W tym celu, dla każdej listy CRL:
 - Jeżeli nie występuje element *CRLRefs*, system nie powinien zweryfikować podpisu pozytywnie. Jeżeli występuje niepusta lista, system powinien pobrać pierwszy element *CRLRefs* i:
 - a. Sprawdzić, że ciąg znaków identyfikatora wyróżniającego listę CRL wygenerowany zgodnie z formatem XMLDSIG, jest taki sam jak wartość elementu *Issuer*.
 - b. Sprawdzić czy czas umieszczony w polu *thisUpdate* w liście CRL jest taki sam jak w elemencie *IssueTime*.
 - c. Jeżeli lista CRL zawiera rozszerzenie *cRLNumber*, system powinien sprawdzić czy jego wartość jest taka sama jak elementu *Number*.
 - d. W przypadku gdy powyższe kroki wykonane zostały pozytywnie, system powinien wyliczyć skrót listy CRL zgodnie z algorytmem wykazanym w *ds:DigestMethod* a wynik zakodować metodą *base64* i sprawdzić czy wyliczona wartość jest taka sama jak element *ds:DigestValue*.



- Jeżeli, jeden z powyższych kroków zakończy się negatywnie, należy powtórzyć proces dla następnego elementu CRLRef aż do pozytywnego wyniku lub końca listy. Jeżeli żadne sprawdzenie referencji nie zakończy się pozytywnie, system nie powinien zweryfikować podpisu pozytywnie.
4. Jeżeli system pobrał odpowiedzi OCSP, powinien sprawdzić czy każda odpowiedź OCSP jest zgodna z właściwą referencją w RevocationRefs. W tym celu system powinien:
- Jeżeli nie występuje element OCSPRefs, system nie powinien zweryfikować podpisu pozytywnie. Jeżeli występuje niepusta lista, system powinien pobrać pierwszy element OCSPRefs i:
 - a. Sprawdzić, że zawartość elementu ResponderID jest zgodna z zawartością pola responderID wewnątrz odpowiedzi OCSP. Jeżeli zawartość tego pola zawiera wskaźnik wyboru byName, należy sprawdzić czy ich format jest taki sam. Jeżeli zawartość tego pola zawiera wskaźnik wyboru byKey, ResponderID powinien zawierać zakodowany metodą base64 skrót klucza. W tym przypadku system powinien porównać tą wartość z wartością byKey.
 - b. Sprawdzić czy czas umieszczony w polu thisUpdate wewnątrz odpowiedzi OCSP jest taki sam jak w elemencie ProducedAt.
 - c. W przypadku gdy powyższe kroki wykonane zostały pozytywnie, system powinien wyliczyć skrót odpowiedzi OCSP zgodnie z algorytmem wykazanym w ds:DigestMethod a wynik zakodować metodą base64 i sprawdzić czy wyliczona wartość jest taka sama jak element ds:DigestValue.
 - Jeżeli, jeden z powyższych kroków zakończy się negatywnie, należy powtórzyć proces dla następnego elementu OCSPRef aż do pozytywnego wyniku lub końca listy. Jeżeli żadne sprawdzenie referencji nie zakończy się pozytywnie, system nie powinien zweryfikować podpisu pozytywnie.
5. Sprawdzić, że nie istnieje żaden element CRLRef posiadający referencje do innych list CRL niż te które zostały pobrane w krokach 1 i 2.
6. Sprawdzić, że nie istnieje żaden element OCSPRef posiadający referencje do innych odpowiedzi OCSP niż te które zostały pobrane w krokach 1 i 2.

3.9 Sprawdzenie elementów CertificateValues

Element CertificateValues zawiera certyfikaty wszystkich urzędów certyfikacji znajdujących się na ścieżce certyfikacyjnej certyfikatu użytkownika.

Zgodnie z rozdziałem „Pobieranie certyfikatów do weryfikacji”, jeżeli występuje element CertificateValues system powinien sprawdzić wszystkie certyfikaty w nim zawarte jak również występujące w elemencie ds:KeyInfo, są to wszystkie certyfikaty wymagane do sprawdzenia ważności podpisu.



W przypadku istnienia specjalnych reguł akceptacji ważności podpisu XAdES system weryfikujący powinien mieć je uwzględnić.

3.10 Sprawdzenie elementów *RevocationValues*

Element *RevocationValues* zawiera dane umożliwiające sprawdzenie czy certyfikat użytkownika lub certyfikat, któregoś z urzędów certyfikacji znajdującego się na ścieżce certyfikacji nie został odwołany.

Zgodnie z rozdziałem „Pobieranie informacji o statusie certyfikatów do weryfikacji”, jeżeli występuje element *RevocationValues* system powinien sprawdzić czy są w nim wszystkie informacje dotyczące odwoływania certyfikatów, związane z certyfikatami wymaganymi do sprawdzenia ważności podpisu.

W przypadku istnienia specjalnych reguł akceptacji ważności podpisu XAdES system weryfikujący powinien mieć je uwzględnić.

3.11 Weryfikowanie żetonów znacznika czasu.

Żeton znacznika czasu wydany przez zaufany system jest wystarczającym dowodem zapewniającym, że podpis elektroniczny został złożony nie później, niż czas wskazany w znaczniku. Dzięki temu można stwierdzić, czy podpis został złożony (lub zweryfikowany) w okresie ważności certyfikatów stanowiących ścieżkę certyfikacyjną. W zależności od elementu, w którym znacznik czasu jest umieszczony, odnosi się on do różnych obiektów wchodzących w skład podpisanych danych.

3.11.1 Sprawdzenie elementu *AllDataObjectsTimeStamp*

Element zawiera znacznik czasu obliczony przed złożeniem podpisu elektronicznego na podstawie sekwencji utworzonej ze wszystkich elementów *ds:Reference*.



3.11.2 Sprawdzenie elementu *IndividualDataObjectsTimeStamp*

Element zawiera znacznik czasu obliczony przed złożeniem podpisu elektronicznego na podstawie sekwencji utworzonej ze wskazanych elementów *ds:Reference*.

3.11.3 Sprawdzenie elementu *SignatureTimeStamp*

Element zawiera znacznik czasu podpisu elektronicznego umieszczonego w elemencie *ds:SignatureValue*. Jest to kluczowy znacznik czasu w procesie ustalania jego ważności.

3.11.4 Sprawdzenie elementu *RefsOnlyTimeStamp*

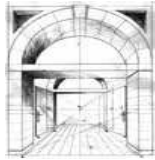
Element zawiera znacznik czasu obliczony dla wszystkich dołączonych danych do weryfikacji podpisu elektronicznego, umieszczonych w elementach *CompleteCertificateRefs*, *CompleteRevocationRefs*.

3.11.5 Sprawdzenie elementu *SigAndRefsTimeStamp*

Element zawiera znacznik czasu obliczony dla podpisu elektronicznego umieszczonego w elemencie *ds:SignatureValue*, znacznika czasu z elementu *SignatureTimeStamp* (jeśli występuje) oraz wszystkich dołączonych danych do weryfikacji podpisu elektronicznego, umieszczonych w elementach *CompleteCertificateRefs*, *CompleteRevocationRefs*.

3.11.6 Sprawdzenie elementu *ArchiveTimeStamp*

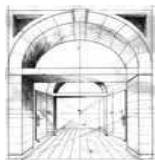
Element zawiera znacznik czasu obliczony dla wszystkich obiektów wchodzących w skład podpisu elektronicznego, dołączony podczas archiwizacji, w celu zagwarantowania przedłużonej ważności podpisu elektronicznego w związku z utratą ważności wcześniej dołączonych znaczników czasu, kompromitacji kluczy wykorzystywanych przy ich tworzeniu lub niewystarczającej siły stosowanych algorytmów kryptograficznych lub funkcji skrótu w przyszłości. Kolejne archiwalne znaczniki czasu (z zastosowaniem silniejszych algorytmów kryptograficznych) mogą być sukcesywnie dołączane w przyszłości.



4 Niezaprzeczalność zdarzeń

4.1 Zdarzenia jakie powinny być rejestrowane

Lp.	Zdarzenie	Opis
Zdarzenia operacyjne		
1.	Wydanie urzędowego poświadczenia odbioru (poświadczenie przedłożenia).	Poświadczenie jest realizowane przez system zbudowany zgodnie z rozporządzeniem Dz.U.05.200.1651 i stanowi dowód wniesienie pisma do podmiotu publicznego. Rejestrowanie informacji związanych z wydaniem poświadczenia stanowi podstawowy dowód w rozstrzyganiu sporów związanych z czasem i zawartością potwierdzenia.
2.	Otrzymanie urzędowego poświadczenia odbioru (poświadczenia doręczenia).	Poświadczenie jest realizowane przez adresata pisma z rozporządzeniem w sprawie struktury i sposobu sporządzania pism Przyjęcie przez system ePUAP podpisanego potwierdzenia jest warunkiem doręczenia dokumentu. Rejestrowanie informacji związanych z weryfikacją zawartości potwierdzenia, podpisami, zawartym czasem będzie jest podstawowym dowodem w sprawach związanych z brakiem skuteczności doręczenia.
3.	Wystawienie awizo.	Wystawienie awizo – czyli przesłanie informacji do urzędu administracji informującej o oczekującym piśmie do doręczenia ma zasadnicze znaczenie w zakresie ustalenia 7 dniowego okresu na skuteczne doręczenie dokumentu elektronicznego. Rejestrowanie tego zdarzenia ma znaczenie w sprawach związanych z ustalaniem powodu uniemożliwienia doręczenia w postaci elektronicznej.
4.	Doręczenie pisma.	Doręczenie pisma następuje po weryfikacji urzędowego poświadczenia odbioru i stanowi zakończenie procesu doręczania. Mimo że skuteczność doręczenia jest związana z podpisaniem poświadczenia odbioru to operacje związane z samym



Zasady bezpieczeństwa ePUAP

		dostarczeniem dokumentu do obywatela wymagają zarejestrowania. Niezależnie od tego system powinien umożliwiać wielokrotne dostarczenie dokumentu, dla którego zostało podpisane poświadczenie odbioru.
5.	Wniesienie podania.	System przyjmujący dokument od obywatela lub firmy dokonuje wydania urzędowego poświadczenia odbioru. Jednakże w celach dowodowych związanych ze skargami, że system przyjął dokument i nie wydał urzędowego poświadczenia odbioru należy rejestrować fakt wniesienia podania oraz dane umożliwiające ustalenie, dlaczego nie zostało wydane poświadczenie.
6.	Uwierzytelnienie w systemie.	Udane i nieudane próby uwierzytelnienia się w systemie przez użytkowników wraz z dokładnym czasem zdarzenia.
7.	Weryfikacja dokumentu.	Weryfikacja dokumentu, to weryfikacja zgodności z wzorcem dokumentu oraz ważności złożonych podpisów. Status weryfikacji stanowi o możliwości skutecznego złożenia podania. Operacje oraz wszystkie decyzje związane z weryfikacją dokumentu wymagają rejestrowania zdarzeń.
8.	Zarchiwizowanie ważności podpisu pod dokumentem.	Zebranie informacji niezbędnych do wykazania, że podpis był ważny w momencie jego weryfikacji oraz zarchiwizowanie ich
Zdarzenia administracyjne		
9.	Rejestrowanie w systemie (dodanie nowego użytkownika).	Zdarzenia te są ważne ze względu na spełnienie zasad bezpieczeństwa systemu i kontroli prawidłowości działania.
10.	Archiwizowanie, odtwarzanie i weryfikacja danych.	
11.	Czynności administracyjne.	
12.	Dodawanie, modyfikowanie i usuwanie wzorców XML.	
13.	Dodawanie modyfikowanie i usuwanie wzorców workflow	
14.	Dodawanie, modyfikowanie i usuwanie aplikacji, ich składników i składników systemu operacyjnego	
Wystąpienie błędu		
15.	Błędy systemowe.	Ze względu na wykrywanie potencjalnych problemów i ich źródeł oraz podjęcia działań naprawczych.
16.	Błędy komunikacyjne.	
17.	Błędy aplikacji	



4.2 Zasady prowadzenia dzienników zdarzeń

4.2.1 Dziennik audytu

Dzienniki audytu powinny być tworzenie i przechowywanie przez czas określony w politykach bezpieczeństwa zgodnie z normami i wymaganiami prawnymi. Jako zasadę należy przyjąć określony obowiązującym prawem czas przechowywania dokumentów, których dotyczą zapisy zawarte w dziennikach. Dzienniki te powinny rejestrować działania użytkowników oraz zdarzenia związane z bezpieczeństwem informacji dla potrzeb przyszłych postępowań wyjaśniających oraz monitorowania kontroli dostępu.

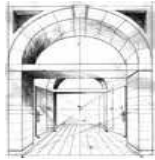
W zależności od potrzeb powinny zawierać:

1. identyfikator użytkownika;
2. datę, czas
3. szczegóły ważnych zdarzeń, np. rozpoczęcia i zakończenia pracy w systemie;
4. szczegóły operacji wykonywanych przez użytkowników systemu;
5. jeśli to możliwe, identyfikator lub lokalizację terminala;
6. rejestr pomyślnych i odrzuconych prób dostępu do systemu;
7. rejestr pomyślnych i odrzuconych prób dostępu do danych i innych zasobów;
8. zmiany konfiguracji systemu;
9. informacje o korzystaniu z przywilejów;
10. informacje o korzystaniu z narzędzi systemowych i aplikacji;
11. używane pliki wraz ze sposobem użycia;
12. adresy sieciowe i protokoły;
13. alarmy podniesione przez system kontroli dostępu;
14. aktywacje i dezaktywacje systemów ochrony, takich jak oprogramowanie antywirusowe i systemy wczesnego wykrywania włamań.

Dzienniki zdarzeń mogą zawierać szczegółowe i poufne dane osobowe. Zaleca się stosowanie odpowiednich mechanizmów ochrony danych osobowych zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Tam gdzie to możliwe, nie należy przydzielać administratorom systemów uprawnień do kasowania lub dezaktywacji dzienników zawierających zapisy o własnych działaniach.

4.2.2 Dzienniki monitorowania użycia systemu

Zapisy dzienników monitorowania i użycia systemu są potrzebne do zapewnienia, że użytkownicy wykonują tylko te działania, do których zostali autoryzowani. Należy rozważyć następujące obszary monitorowania i tworzenia zapisów dzienników użycia środków przetwarzania informacji:



1. autoryzowany dostęp, z uwzględnieniem takich szczegółów, jak:
 - a. identyfikator użytkownika;
 - b. data i czas ważnych zdarzeń;
 - c. typ zdarzenia;
 - d. użyte pliki;
 - e. użyte środki/aplikacje;
2. wszystkie uprzywilejowane operacje, takie jak:
 - a. korzystanie z uprzywilejowanych kont;
 - b. zatrzymanie i uruchomienie systemu;
 - c. podłączenie lub odłączenie urządzeń wejściowych lub wyjściowych;
3. nieautoryzowane próby dostępu, takie jak:
 - a. pomyślne lub odrzucone działania użytkownika;
 - b. pomyślne lub odrzucone działania związane z danymi lub innymi zasobami;
 - c. naruszenia polityki dostępu oraz powiadomienia z bram lub zapór sieciowych;
 - d. alarmy z własnych systemów wczesnego wykrywania intruzów;
4. alarmy systemowe lub błędy takie jak:
 - a. alarmy lub wiadomości z konsoli zarządzającej;
 - b. wyjątki zapisane w dzienniku systemowym;
 - c. alarmy systemu zarządzania siecią;
 - d. alarmy podniesione przez system kontroli dostępu;
5. zmiany, lub próby zmian, ustawień bezpieczeństwa i zabezpieczeń systemu.

Zapisy dzienników działań monitorujących powinny być regularnie przeglądane. Częstość przeglądów zapisów powinna zależeć od rozpatrywanych ryzyk, które powinny uwzględniać następujące czynniki:

1. krytyczność procesów aplikacyjnych;
2. wartość, wrażliwość oraz krytyczność informacji;
3. doświadczenia z przeszłości dotyczące infiltracji i niewłaściwego użycia systemu oraz częstość wykorzystywania podatności;
4. zasięg połączeń między systemami (szczególnie połączeń z sieciami publicznymi);
5. dezaktywację podsystemu logowania.

4.2.3 Dzienniki administratora i operatora

Administratorzy i operatorzy jako osoby uprzywilejowane mają duży wpływ na funkcjonowanie systemu oraz dostęp do dużej części danych systemowych i danych przetwarzanych w systemie. W celu wyeliminowania możliwości nadużyć powinno się rejestrować działania administratorów i operatorów systemów. Dzienniki te powinny być regularnie przeglądane przez niezależne komórki organizacyjne nie związane z utrzymaniem systemu. Dzienniki administratora i operatora powinny zawierać:



1. czas zajścia zdarzenia (sukcesu lub niepowodzenia);
2. informację na temat zdarzenia (np. użyte pliki) lub niepowodzenia (np. wystąpił błąd i podjęto działania korygujące);
3. jakie konto użyto i który z administratorów lub operatorów brał udział;
4. użyte procesy.

4.2.4 Dzienniki i rejestry błędów

Pojawianie się błędów w systemie może powodować problemy w podsystemach przetwarzania danych, podsystemach komunikacyjnych i innych. Powinno się rejestrować błędy zgłaszane przez użytkowników oraz programy systemowe. Dzienniki błędów powinny być przeglądane przez kompetentny personel, aby zapewnić, że pojawiające się problemy zostały rozwiązane w sposób skuteczny oraz że nie naruszono żadnych zabezpieczeń, a podjęte działania były w pełni autoryzowane.

4.2.5 Zalecenia dla dzienników zdarzeń

Zapisy dzienników zdarzeń mogą być wykorzystane do przeprowadzenia dokładnej analizy na potrzeby przyszłych postępowań wyjaśniających, prowadzenia śledztw lub jako dowody sądowe. W związku z tym powinny być odpowiednio zabezpieczone zgodnie z następującymi wymaganiami:

1. *Synchronizacja zegarów*
Zegary wszystkich stosownych podsystemów powinny być zsynchronizowane z dokładnym i zaufanym źródłem czasu co umożliwi precyzyjną korelację zdarzeń.
2. *Ochrona informacji zawartej w dziennikach*
Zmiany zapisów dzienników powinny być niemożliwe a dzienniki nieusuwalne. Dzienniki powinny być archiwizowane w celu gromadzenia i przechowywania materiału dowodowego.
3. *Informacje stanowiące materiał dowodowy dla procesów administracyjnych powinny być automatycznie wysyłane do dedykowanych systemów rejestrów zdarzeń (serwerów logów) o restrykcyjnych warunkach dostępu.*
4. *Wydajność systemu*
Prowadzenie dzienników zdarzeń może wpływać na wydajność systemu. System powinien być zaprojektowany tak aby przewidywał nadmiarowość środków przetwarzania kompensujący potrzeby podsystemu rejestrowania.



5 Metodologia dowodowa - zasady

Praca systemów informatycznych oraz świadczenie usług elektronicznych niesie za sobą wiele ryzyk. Najważniejsze z nich to ryzyka związane z niewłaściwym użyciem systemu, awariami oraz umyślnym lub nieumyślnym naruszeniem zapisów prawnych.

Narzędziem pomocnym we właściwym reagowaniu na wszelkiego rodzaju incydenty są prowadzone w systemach zapisy dzienników. Wszystkie zdarzenia powinny być rejestrowane zgodnie z polityką bezpieczeństwa systemu oraz politykami bezpieczeństwa dla poszczególnych usług.

5.1 Dokumentowanie przebiegu

Wszystkie operacje wykonywane przez użytkownika powinny być rejestrowane. W szczególności rejestracji podlegają następujące zdarzenia:

- Uwierzytelnienie użytkownika (nadawcy i odbiorcy dokumentu)
- Podpisanie dokumentu
- Wysłanie dokumentu
- Realizacja wydania poświadczenia przedłożenia / realizacja poświadczenia doręczenia
- Weryfikacja poświadczenia doręczenia
- Przekazanie poświadczenia przedłożenia
- Weryfikacja dokumentu
- Nawiązanie komunikacji z systemem docelowym
- Przeniesienie dokumentu do systemu docelowego
- Doręczenie
- Komunikacja z systemem zewnętrznej instytucji finansowej
- Wystawienie Elektronicznego Numeru Usługi¹
- Wystawienie Elektronicznego Potwierdzenia Opłaty²
- Uzyskanie Elektronicznego Potwierdzenia Opłaty

¹ Elektroniczny Numer Usługi został opisany w dokumencie „Algorytm wnoszenia opłat skarbowych”.

² Elektroniczne Potwierdzenie Opłaty zostało opisane w dokumencie „Algorytm wnoszenia opłat skarbowych”.



Zdarzenia powinny zawierać informacje opisane w zasadach w rozdziale 4 Niezaprzeczalność zdarzeń:

- identyfikator użytkownika;
- datę, czas;
- szczegóły zdarzenia;
- jeśli to możliwe, identyfikator lub lokalizację terminala;
- rejestr pomyślnych i odrzuconych prób dostępu do systemu;
- rejestr pomyślnych i odrzuconych prób dostępu do danych i innych zasobów;
- informacje o korzystaniu z przywilejów;
- informacje o korzystaniu z narzędzi systemowych i aplikacji;
- używane pliki wraz ze sposobem użycia;
- adresy sieciowe i protokoły;
- aktywacje i dezaktywacje systemów ochrony, takich jak oprogramowanie antywirusowe i systemy wczesnego wykrywania włamań.

W zależności od rodzaju zdarzenia lub złożonej przez użytkowników reklamacji, do analizy lub dowodzenia zdarzeń i sporów wykorzystywany będzie różny zestaw zapisów (zestawy te są wyszczególnione w dokumentach dotyczących właściwych usług).

5.2 Dowodzenie zachodzących zdarzeń

Ważnym elementem wymiany dokumentów pomiędzy przedsiębiorcami i obywatelami a jednostkami administracji publicznej jak i pomiędzy jednostkami administracji publicznej stanowiącymi spory zarówno w postępowaniu administracyjnym jak i późniejszym dowodowym. Spory będą rozstrzygane na drodze instancyjnej i dotyczyć będą między innymi przekroczenia terminów, nie załatwienia sprawy w terminie oraz zaskarżania rozstrzygnięć do sądów administracyjnych.

Rodzaje sporów, zestawy rejestrowanych zdarzeń niezbędnych do ich wyjaśnienia oraz sposoby rozstrzygania sporów opisane są szczegółowo w dokumentach zawierających algorytmy usług:

- „Algorytm doręczania pism i wezwań” – w zakresie doręczania.
- „Algorytm przekazywania dokumentów przez firmę i obywatela” – w zakresie wnoszenia podań.
- „Wnoszenie opłat skarbowych” – w zakresie opłat skarbowych.



6 Metody uwierzytelniania i autoryzacji użytkowników.

6.1 Podział użytkowników ze względu na rodzaj dostępu.

Proponujemy następujący podział użytkowników:

- A. użytkownicy z dostępem do informacji – użytkownicy korzystający wyłącznie z informacji zawartych w systemie ePUAP.
- B. użytkownicy z dostępem jednorazowym – użytkownicy, którzy uzyskują dostęp do systemu ePUAP w celu jednorazowego przesłania dokumentu i wskazania jednostki administracji właściwej do załatwienia sprawy.
- C. użytkownicy stali - użytkownicy, którzy wykorzystują ePUAP do załatwiania wszystkich możliwych spraw z urzędami administracji państwowej oraz urzędnicy administracji państwowej.
- D. Administratorzy – użytkownicy, którzy mają uprawnienia do modyfikacji konfiguracji urządzeń i systemów oraz repozytoriów informacji.

6.2 Sposoby identyfikacji

Proponujemy następujące sposoby identyfikacji:

1. Identyfikacja kanału zwrotnego
2. Uwierzytelnienie hasłem statycznym
3. Uwierzytelnienie hasłem jednokrotnym
4. Uwierzytelnienie metodami kryptograficznymi

Identyfikacja kanału zwrotnego.

Mechanizm umożliwiający ustalenie kanału do otrzymania potwierdzenia przedłożenia.



Kanał taki nie wprowadza żadnych mechanizmów bezpieczeństwa służy jedynie do wskazania adresu zwrotnego dla potwierdzenia przedłożenia. W procesie składania dokumentu użytkownik zobowiązany jest do wprowadzenia adresu poczty elektronicznej pod który ma być wysłane potwierdzenie przedłożenia. Portal powinien zapewnić mechanizm zabezpieczający kanał zwrotny. Takim mechanizmem jest nadanie i przekazanie użytkownikowi numeru sprawy i/lub instalacja odpowiedniego cookie w przeglądarce użytkownika. Użytkownik posiadając numer sprawy i/lub cookie powinien mieć możliwość uzyskania kopi potwierdzenia przedłożenia, gdyby z przyczyn od niego niezależnych potwierdzenie to nie dotarło do wskazanej na wstępie skrzynki.

Uwierzytelnienie hasłem statycznym.

Informacja uwierzytelniająca składa się z identyfikatora i hasła (metoda stosowana od dawna w systemach komputerowych). Użytkownik uzyskuje dostęp do systemu po weryfikacji przez system podanego identyfikatora i hasła. Hasło używane jest wielokrotnie. Umożliwia też korzystanie z jednego konta przez kilku użytkowników, nie zapewnia jednak rozliczalności użytkowników i poufności hasła.

Uwierzytelnienie hasłem jednokrotnym.

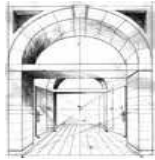
Użytkownik wysyła do systemu identyfikator i hasło. Hasło składa się z dwóch części:
- odpowiedniej sekwencji znaków generowanej przez odpowiednie urządzenie (token)
- PIN'u znanego użytkownikowi.

System po otrzymaniu takiego zestawu informacji sprawdza czy identyfikator użytkownika, skojarzony jest z użytym tokenem i PIN'em. Jeżeli informacja uwierzytelniająca jest poprawna użytkownik uzyskuje dostęp do systemu. Bezpieczeństwo systemu polega na rozdzieleniu informacji uwierzytelniającej na dwie części: „coś co wiesz” – PIN oraz „coś co masz” – token. Sekwencja znaków generowana przez token, może być wykorzystana tylko raz co zabezpiecza przed podejrzeniem lub podsłuchaniem hasła.

Uwierzytelnienie metodami kryptograficznymi.

Uwierzytelnienie polega na założeniu, że osoba która dokonuje jakiś czynności przy użyciu klucza prywatnego skojarzonego z kluczem publicznym zawartym w certyfikacie (logująca się do stron www lub podpisująca wiadomość) jest prawie na pewno osobą, która widnieje w certyfikacie. Stopień pewności zależy od klasy certyfikatu oraz urzędu certyfikacji który wydał dany certyfikat. Metoda ta zapewnia rozliczalność i umożliwia korzystanie wielu użytkowników z jednego konta.

Tabela 1 przedstawia sugerowane stosowanie metod uwierzytelnienia w zależności od profilu użytkownika.



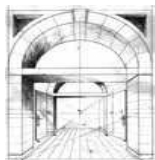
	Brak uwierzytelnienia	Identyfikacja kanału zwrotnego	Uwierzytelnienie hasłem statycznym	Uwierzytelnienie hasłem jednokrotnym	Uwierzytelnienie metodami kryptograficznymi
Użytkownicy z dostępem do informacji	X				
Użytkownicy z dostępem jednorazowym		X			
Użytkownicy z dostępem stałym			X	X	X
Administratorzy*			X	X	X

* Sposób uwierzytelnienia administratorów powinien być dobrany tak, aby zapewnić maksymalną siłę uwierzytelnienia, jaką umożliwia urządzenie lub system, aby w połączeniu z dziennikami zdarzeń umożliwiły maksymalną rozliczalność podejmowanych działań.

Tabela 1. Matryca powiązań pomiędzy możliwymi typami użytkowników i metodami identyfikacji.

Tabela 2 przedstawia wady i zalety poszczególnych metod uwierzytelnienia oraz zalecenia, jakimi powinien się kierować wykonawca systemu podczas projektowania.

	Wady	Zalety	Zalecenia
Uwierzytelnienie hasłem statycznym	Niski poziom poufności hasła. Niski poziom uwierzytelnienia. Brak mechanizmów niezaprzeczalności informacji.	Tanie	Możliwe do stosowania do usług nie wymagających dużego poziomu poufności i autentyczności osoby logującej się do systemu, np. monitorowanie spraw, listy dyskusyjne, czaty.



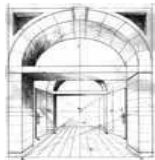
Zasady bezpieczeństwa ePUAP

Uwierzytelnienie hasłem jednokrotnym	Drogi system do obsługi haseł jednokrotnych. Brak mechanizmów niezaprzeczalności informacji.	Wysoki poziom uwierzytelnienia	W związku z wadami proponujemy nie stosować tego rozwiązania.
Uwierzytelnienie metodami kryptograficznymi	W przypadku zastosowania komercyjnych urzędów certyfikacji podnosi koszty korzystania z portalu	Tani system do obsługi uwierzytelnienia. Wysoki poziom uwierzytelnienia. Wysoki poziom niezaprzeczalności. Wysoki poziom poufności informacji.	Jest to najbardziej uniwersalny sposób uwierzytelnienia (możliwy do zastosowania zarówno w kanałach HTTP, SMTP jak i innych). Certyfikaty i klucze wykorzystywane w procesie uwierzytelnienia mogą być również zastosowane do innych celów jak np. podpisywanie dokumentów, do których nie istnieje wymóg stosowania bezpiecznego podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem.

Tabela 2. Zestawienie wad i zalet mechanizmów uwierzytelnienia

Sposób uwierzytelniania powinien być dostosowany do wymagań usługi. Użytkownik może korzystać z wielu sposobów uwierzytelnienia, jednak w zależności od siły uwierzytelnienia może otrzymywać różne profile usług.

Procedury uwierzytelnienia, identyfikacji, kontroli dostępu, obsługi dzienników zdarzeń oraz innych działań powinny być zgodne z zaleceniami normy ISO/IEC 17799:2005.



6.3 Profile użytkowników.

W zależności od rodzajów wykorzystywanych usług użytkowników można umieścić w następujących profilach (każdy „silniejszy” profil zawiera również profile „słabsze”):

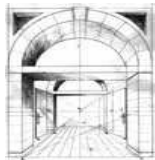
- Profil dla usług niezabezpieczonych (brak uwierzytelnienia) – informacje publicznie dostępne, otwarte czaty, skrzynka podawcza do wysyłania pism z poświadczeniem przedłożenia, bez elektronicznej formy załatwienia sprawy (wymaga podania adresu skrzynki pocztowej do wysłania potwierdzenia przedłożenia).
- Profil dla usług zabezpieczonych hasłem statycznym – zamknięte czaty i fora dyskusyjne, możliwość monitorowania postępu załatwienia spraw elektronicznych. Zakładanie kont użytkowników w ramach własnej jednostki organizacyjnej na poziomie tego profilu usług.
- Profil dla usług zabezpieczonych certyfikatem niekwalifikowanym (wystawianym bez konieczności osobistego stawienia się w centrum certyfikacji – w dalszej części opracowania zwanym „otrzymanym zdalnie”) – Zakładanie kont użytkowników w ramach własnej jednostki organizacyjnej na poziomie tego profilu usług.
- Profil dla usług zabezpieczonych certyfikatem niekwalifikowanym (wystawianym po osobistym stawieniu się w centrum certyfikacji – w dalszej części opracowania zwanym „otrzymanym osobiście”) – podpisywanie dokumentów nie wymagających bezpiecznego podpisu weryfikowanego kwalifikowanym certyfikatem. Zakładanie kont użytkowników w ramach własnej jednostki organizacyjnej w dowolnym profilu usług.

Oddzielny profil powinien być dedykowany administratorom systemów dziedzinowych korzystających z usługi single sign-on. Uwierzytelnienie powinno odbywać się przy pomocy najsilniejszej, zastosowanej w ePUAP, metody uwierzytelnienia.

6.4 Single sign-on

Dodatkowym rozszerzeniem systemu uwierzytelnienia użytkownika może być usługa single sign-on. Usługa ta może być dedykowana serwerom dziedzinowym, które mogą udostępniać zasoby użytkownikom uwierzytelnionym przez ePUAP bez konieczności dodatkowego uwierzytelniania. System single sign-on składa się z trzech głównych elementów:

- a. serwera do zarządzania tożsamością użytkowników,
- b. oprogramowania klienckiego dla użytkownika,
- c. oprogramowania klienckiego dla systemów końcowych.



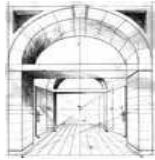
System single sign-on powinien zapewniać zarządzanie przez administratorów dziedzinowych, którzy będą decydowali o tym, jakich użytkowników dopuścić do informacji w ich systemach dziedzinowych. System powinien zapewnić rozliczalność administratora.

6.5 Sposoby uzyskania dostępu.

- Dostęp na wniosek podpisany bezpiecznym podpisem elektronicznym.
- Uzyskanie rejestracji jednostki organizacyjnej w systemie ePUAP oraz otrzymanie identyfikatora i hasła – hasło i identyfikator przesyłane są w specjalnej kopercie przez odpowiedniego pracownika ePUAP na elektroniczny lub pisemny wniosek użytkownika pod wskazany w KRS, KEP, REGON, lub innym rejestrze adres. Po otrzymaniu identyfikatora i hasła użytkownik powinien niezwłocznie zmienić hasło.
- Uzyskanie rejestracji jednostki organizacyjnej w systemie ePUAP oraz otrzymanie identyfikatora powiązanego z certyfikatem (otrzymanym zdalnie) wskazanym we wniosku – identyfikator przesyłane jest w specjalnej kopercie przez odpowiedniego pracownika ePUAP na elektroniczny lub pisemny wniosek użytkownika pod wskazany w KRS, KEP, REGON, lub innym rejestrze adres.
- Użytkownik uzyskuje rejestrację jednostki organizacyjnej w systemie ePUAP oraz identyfikator powiązany z certyfikatem (otrzymanym osobiście) po osobistym stawieniu się w biurze ePUAP po uprzednim uzyskaniu certyfikatu z wybranego przez siebie, z ograniczeniem do listy wskazanej przez ePUAP, centrum certyfikacji.
- Dostęp poprzez certyfikaty wydawane przez różne urzędy certyfikacji, które e-PUAP będzie wskazywał jako zaufane.
- Dostęp i uprawnienia kolejnych użytkowników mogą być konfigurowane przez użytkownika pierwotnego.

6.6 Wymagania dla systemu e-PUAP

- System powinien obsługiwać wszystkie wymienione metody uwierzytelnienia.
- System powinien udostępniać profile usług w zależności od metody uwierzytelnienia.
- Użytkownicy powinni mieć możliwość korzystania ze wszystkich metod uwierzytelnienia.
- System powinien umożliwiać zarządzanie kontami użytkowników w ramach jednostki organizacyjnej przez administratora tej jednostki.
- System powinien umożliwiać współpracę z komercyjnymi urzędami certyfikacji.
- System powinien posiadać listę zaufanych urzędów certyfikacji i listę klas certyfikatów związanych z odpowiednimi profilami usług.
- System powinien umożliwić korzystanie z własnego centrum certyfikacji.



Zasady bezpieczeństwa ePUAP

- System powinien zapewnić monitorowanie nadużyć przy zakładaniu kont metodami zdalnymi.
- System single sign-on powinien zapewnić wsparcie dla użytkowników komunikujących się poprzez interfejs www, oraz wsparcie dla jak największej liczby systemów operacyjnych, które zapewni wsparcie dla systemów dziedzinowych. Istotnym zagadnieniem jest ustalenie jednolitego standardu usługi jednokrotnego logowania (single sign-on) realizowanego przez e-PUAP a wykorzystywanego przez systemy dziedzinowe i systemy podmiotów publicznych.



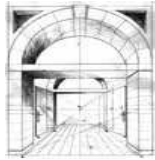
7 Bezpieczna synchronizacja czasu

Zadania powierzone portalowi ePUAP wymagają użycia zaufanego czasu, czyli czasu pochodzącego z umocowanego prawem źródła czasu w Polsce. Pojęcie używania zaufanego czasu oznacza możliwość niepodważalnego (niezaprzeczalnego) wykazania, iż czas wskazany w ramach poszczególnych transakcji i interakcji składników systemu ePUAP jest czasem zgodnym z czasem obowiązującym z założoną dokładnością oraz gdzie możliwe jest udowodnienie autentyczności i zgodności z przyjętym wzorcem tego czasu używanego przez systemy portalu ePUAP. Szczególnie ważne jest zapewnienie możliwości weryfikacji wstecznej prawidłowości użytego w transakcjach czasu - należy zagwarantować wartość dowodową parametru czasu w opisach poszczególnych zdarzeń gospodarczych. Określenie czasu wszystkich wykonywanych czynności, rejestrowanie zdarzeń oraz znakowanie czasem będzie kluczowym zadaniem portalu. Operacje te muszą być wykonywane w sposób bezpieczny, który zapewni niezaprzeczalność, integralność danych i weryfikowalny stempel czasowy oraz weryfikowalne informacje na temat pochodzenia wartości czasu użytego w tych stemplach czasowych. Zadaniem stemplowania urzędowym czasem nie jest tylko zapewnienie dokładnego czasu, ale również zapewnienie, iż jest/był to czas pochodzący z obowiązującego w Polsce źródła czasu wzorcowego i/lub? Możliwa jest pełna weryfikacja zgodności tego czasu z czasem wzorcowym.

Zaufany czas jest niezbędny do realizacji następujących usług: poświadczenie przedłożenia, poświadczenie odbioru, usługi weryfikacji ważności certyfikatu i usługi archiwizacji ważności certyfikatu.

Zaufany czas – jest to czas, który posiada kryptograficzne potwierdzenie wiarygodnego źródła pochodzenia a jego sfałszowanie będzie widoczne zarówno w początkowym momencie użycia jak i w przyszłości.

W chwili obecnej na terenie Rzeczypospolitej istnieje oficjalne źródło zaufanego czasu, lecz nie istnieje system wiarygodnej i weryfikowalnej jego dystrybucji od tego źródła do poszczególnych dokumentów i transakcji wymagających oznaczenia tym właśnie czasem. Praktycznie stosowany model dystrybucji zaufanego czasu nie polega na jego faktycznej dystrybucji ale na synchronizacji serwerów czasu niższego poziomu z czasem wzorcowym oraz realizacji mechanizmu okresowej weryfikacji dokładności tej synchronizacji w celu potwierdzenia jakości czasu podawanego przez serwery niższego poziomu czyli dokładności tej synchronizacji. Taka okresowa kontrola jest procesem niezależnym od samego procesu zapewnienia jakości synchronizacji źródeł czasu.



Rolą procesu kontrolnego jest wydawanie zabezpieczonych podpisem elektronicznym świadectw zgodności czasu podawanego przez serwery niższych warstw (operacyjne serwery zaufanego czasu) z czasem wzorcowym - zaufanym źródłem czasu.

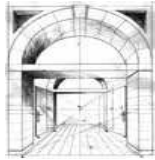
Zależnie od potrzeb dystrybucyjnych zaufanego czasu możliwe jest utworzenie hierarchicznej struktury dystrybucji czasu zaufanego przez tworzenie warstw serwerów będących pod kontrolą serwerów warstwy wyższej aż do serwerów wzorcowych Root w Głównym Urzędzie Miar.

Proponujemy dwa możliwe rozwiązania procesu pobierania/synchronizacji z czasem wzorcowym, które wymagają jednak wydania odpowiednich ustaw i rozporządzeń:

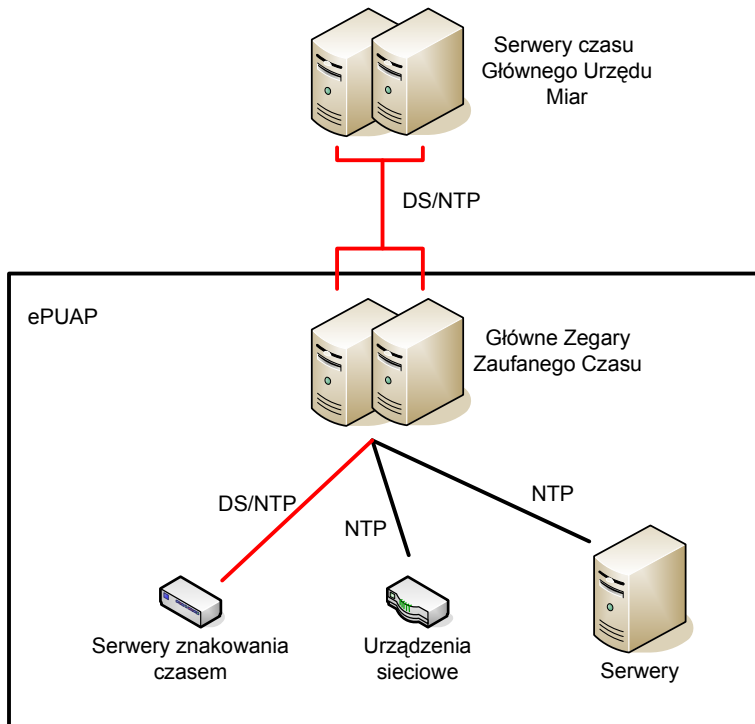
1. Utworzenie serwera źródła zaufanego czasu w Głównym Urzędzie Miar, z którego będzie pobierany zaufany czas zgodnie z rysunkiem 2. W tym przypadku mogą być konieczne zmiany prawne wprowadzające regulacje zobowiązujące GUM do stosowania protokołu DS/NTP.
2. Utworzenie odpowiedniej struktury źródła zaufanego czasu w ramach projektu ePUAP zgodnie z rysunkiem 3, który synchronizowałby swój czas z czasem urzędowym z Głównego Urzędu Miar za pośrednictwem sieci rozległych.

Ponieważ najwyższy poziom dokładności procesu synchronizacji można osiągnąć stosując integrację wzorca czasu z serwerami czasu zaufanego wykluczającą połączenia sieciowe, najwygodniej będzie umieścić serwery zaufanego czasu wzorcowego (serwery Root) w miejscu instalacji wzorca czasu należącego do GUM.

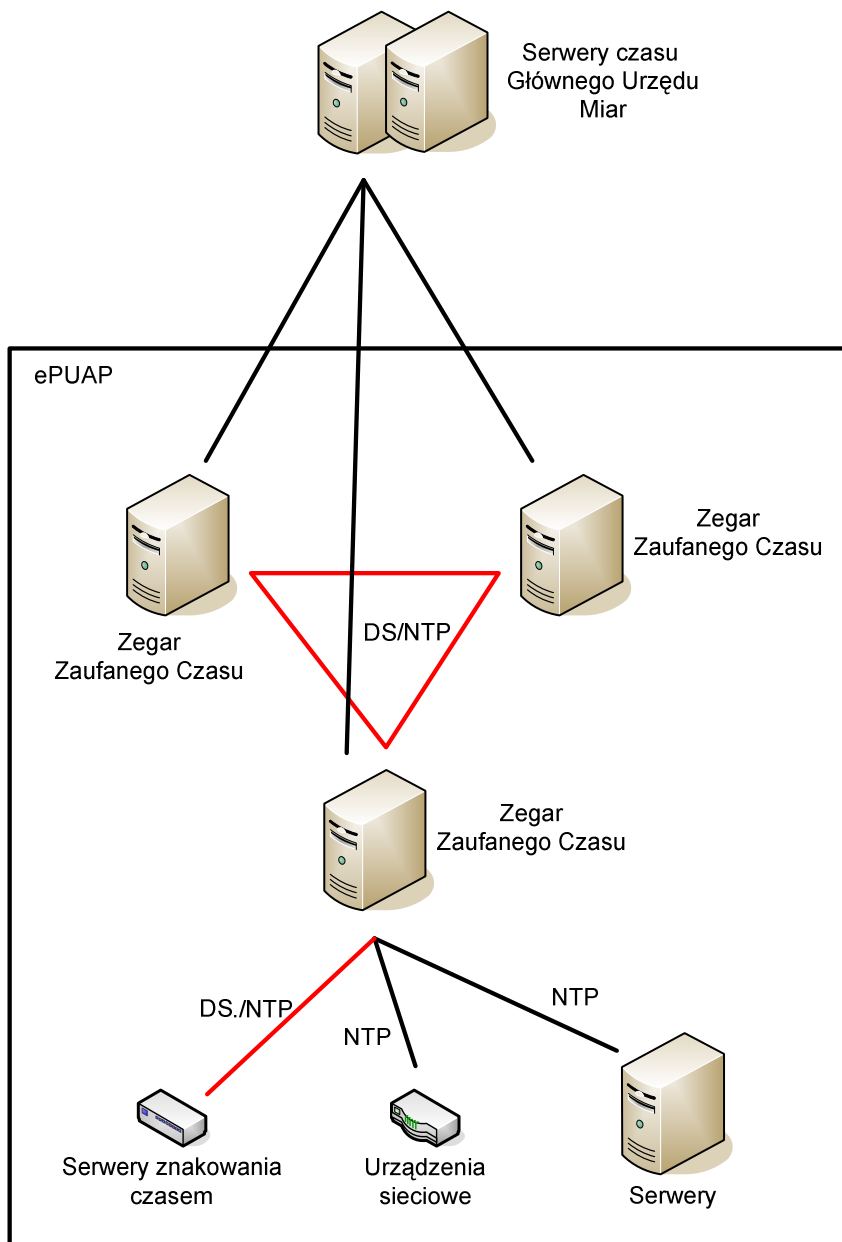
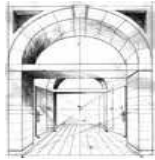
Niezależnie od sposobu realizacji zagadnienia dystrybucji lub synchronizacji wartości czasu wzorcowego, zapewnienie jego zaufanego charakteru wymaga realizacji procesu kontrolno/legalizacyjnego weryfikującego dokładność operacyjnie wykorzystywanego czasu niższych warstw. Obecnie na rynku znany jest protokół DS/NTP zaprojektowany właśnie do realizacji zadania kryptograficznie zabezpieczonego procesu kontroli/legalizacji zegarów czasu zaufanego. Może być zastosowany inny protokół niż DS/NTP, dający ten sam poziom bezpieczeństwa. Proponowany system docelowy powinien obejmować również proces generowania i dystrybucji niepodważalnych dowodów legalizacyjnych dla serwerów bezpośrednio podających wzorcowy czas w ramach systemu ePUAP, np dla serwerów oznaczania czasem, które generując stempel czasu dla realizowanej transakcji będą każdorazowo dołączały do tego stempla dowód legalizacyjny potwierdzający kryptograficznie (z użyciem podpisu elektronicznego) jakość zastosowanego czasu i jego zgodność z wzorcowym czasem zaufanym pochodzącym z GUM.



Kolorem czerwonym oznaczono czas uwierzytelniony metodami kryptograficznymi



Rysunek 2. Infrastruktura zaufanego czasu dla portalu ePUAP pobieranego z GUM.



Rysunek 3. Własna infrastruktura zaufanego w portalu ePUAP z pobraniem czasu urzędowego z GUM

W przypadku wariantu przedstawionego na rysunku 3 występuje pewien konflikt uprawnień gdyż system ePUAP posiada serwer Root zaufanego czasu w PL, legalizując serwery operacyjne niższego poziomu (np. serwery stemplowania czasem) potwierdzając ich zgodność z czasem wzorcowym. Jednak obecnie czasem wzorcowym w Polsce jest tylko czas podawany przez GUM. W wariantcie tym występuje obszar kolizji uprawnień, co do sposobu synchronizacji zegarów zaufanego czasu z zegarami czasu wzorcowego w GUM, dokładności tego procesu a co najważniejsze audytowalności jakości tej synchronizacji i kompletnej weryfikowalności tego procesu w przyszłości (dowodowość).



Rozwiązanie przedstawione na rysunku 3 jest mniej bezpieczne gdyż nie zabezpiecza przed atakiem na serwery GUM. Dodatkowym zabezpieczeniem powinno być wykorzystanie innego źródła czasu np. połączenia telefonicznego z GUM lub zegarów synchronizowanych przez GPS lub metodą radiodyfuzyjną.

Na podstawie Rozporządzenia Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 19 marca 2004 w sprawie sposobów rozpowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL) jedynym urzędem upoważnionym do dystrybucji urzędowego czasu na terenie Rzeczypospolitej jest Główny Urząd Miar.

Główny Urząd Miar zobowiązany jest do rozpowszechniania sygnałów czasu trzema sposobami:

- a. Całodobowo za pośrednictwem sieci Internet z dwóch serwerów czasu o adresach: tempus1.gum.gov.pl i tempus2.gum.gov.pl z zastosowaniem protokołu transmisyjnego NTP.
- b. Całodobowo za pośrednictwem sieci telekomunikacyjnej z wykorzystaniem modemu telefonicznego numer (0-prefiks-22) 6548872 i zastosowaniem kodu sygnałów czasu European Telephone Time Code.
- c. Metodą radiodyfuzyjną za pośrednictwem jednostek radiofonii publicznej, co każdą pełną godzinę.

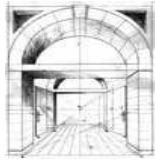
Portal powinien zostać wyposażony w serwer czasu zaufanego umożliwiający bezpieczną dystrybucję dokładnego czasu do wszystkich urządzeń i systemów portalu. Serwer ten powinien synchronizować się z serwerami czasu wzorcowego w GUM za pomocą metod pozwalających na uzyskanie właściwego poziomu zgodności czasu serwowanego lokalnie w systemach ePUAP z czasem wzorcowym w GUM. Jednym z możliwych rozwiązań jest użycie protokołu NTP. Zalecane jest jednak zastosowanie protokołu DS/NTP lub równoważnego w celu zapewnienia weryfikowalnych danych audytowych i zapewnienia realizacji zadań legalizacyjnych dla serwera czasu zaufanego w systemie ePUAP.

Serwer czasu zaufanego w ramach ePUAP powinien podawać czas zgodny z czasem wzorcowym w GUM (UTC-PL) z dokładnością 10ms.

System dystrybucji zaufanego czasu powinien umożliwić urządzeniom do znakowania czasem dokładność czasu do 100 ms. Dokładność czasu umieszczanego w znaczniku czasu powinna w zależności od obciążenia systemu wynosić od 100 do 200 ms. Zakładane poziomy realizują założenia ustawowe synchronizacji czasu do jednej sekundy zgodnie z § 31 Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.

Warstwy czasu:

Źródła czasu podzielone są na szesnaście warstw od 0 do 15.



STRATUM0 – źródło czasu np. rezonator cezowy lub rubidowy.

STRATUM1 – serwer warstwy root, dokładność 1 ms.

STRATUM2 – serwer synchronizowany do serwera STRATUM1, dokładność 10-100ms.

STRATUMx – serwer synchronizowany do serwera STRATUM x-1, dokładność zmniejsza się 10-100ms na każdą warstwę.

Wymagania

- W przypadku realizacji źródła zaufanego czasu w GUM, istniejące źródła czasu urzędowego powinno zostać wyposażone w sprzęt i oprogramowanie wspomagające kryptografię klucza publicznego i realizujące zdania audytowalnej i weryfikowalnej dystrybucji zaufanego czasu wraz z legalizacją (kalibracją) serwerów zaufanego czasu w ePUAP. ePUAP powinien być wyposażony w dwa zegary (STRATUM2), które będą się synchronizowały z zegarami w GUM i będą stanowić wzorzec zaufanego czasu dla urządzeń znakowania czasem i innych urządzeń.
- W przypadku realizacji źródła zaufanego czasu w ePUAP, system powinien zostać wyposażony w trzy zegary STRATUM0 i połączone ze sobą trzy zegary STRATUM1.
- Wszystkie serwery czasu zaufanego powinny posiadać własne, stabilne źródła czasu oparte na rezonatorze atomowym lub równoważnym synchronizowane z czasem zegarów wyższych warstw oraz czasem serwerów tej samej warstwy.
- Zegary STRATUM1 powinny obsługiwać protokół DS/NTP i wykorzystywać kryptografię klucza publicznego.
- Urządzenia stemplujące czasem, synchronizujące się do źródeł zaufanego czasu powinny mieć możliwość udostępniania certyfikowanych przez serwer czasu zaufanego informacji potwierdzających zgodność używanego przez nie czasu z czasem wzorcowym.



8 Zasady bezpieczeństwa transmisji danych

Bezpieczeństwo komunikacji polega na zapewnieniu pewnego, niezawodnego i poufnego kanału przesyłania danych pomiędzy dwoma komunikującymi się stronami. Komunikacja może odbywać się na dwa sposoby. Przy pomocy łączy dedykowanych, które są dość kosztowne, jednak zapewniają żądaną prędkość transmisji oraz niezawodność ze względu na redundancję sieci operatora. Drugą możliwością przesyłania danych są sieci publiczne. Są one tanie, jednak stanowią duże zagrożenie dla poufności informacji oraz zazwyczaj nie zapewniają niezawodnego kanału i nie zapewniają stałej przepustowości. W celu zapewnienia optymalnego rozwiązania można łączyć ze sobą różne techniki, należy przy tym kierować się następującymi zasadami:

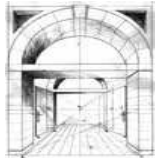
Niezawodności transmisji – wszędzie tam, gdzie wymagana jest wysoka dostępność systemów i usług należy zastosować redundancję łączy lub wykorzystać łącza dzierżawione, które mają zapewnioną wewnętrzną redundancję w sieci operatora.

Właściwa przepustowość łączy – należy zapewnić właściwą przepustowość łączy na podstawie szacowanego wolumenu transmisji danych.

Poufność – zapewnienie, że dane nie będą mogły być odczytane przez nieuprawnione osoby. Może to być uzyskane za pomocą odpowiednich metod kryptograficznych, np. szyfrowania. Przy dużym wolumenie transmisji należy zastosować odpowiednie rozwiązania sprzętowe.

Integralność – zapewnienie, że dane nie mogą zostać zmienione w sposób zamierzony lub przypadkowy podczas przesyłania. Uzyskuje się to przy pomocy odpowiednich mechanizmów kryptograficznych, np. sum kontrolnych.

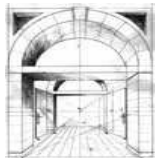
Uwierzytelnienie stron – zapewnienie wiarygodnego uwierzytelnienia stron komunikacji. Do uwierzytelnienia stron stosuje się odpowiednie mechanizmy kryptograficzne, które w zależności od przyjętego rozwiązania wykorzystują certyfikaty cyfrowe, lub współdzielony sekret.



Kontrola dostępu – zapewnienie, że tylko autoryzowani użytkownicy uzyskują dostęp do właściwych zasobów i usług.

Należy pamiętać że żadne rozwiązanie nie zapewnia absolutnego bezpieczeństwa. Wybór właściwego rozwiązania powinien być poprzedzony analizą ryzyka i analizą potrzeb biznesowych.

Szczegółowe rozwiązania przedstawione zostały w dokumencie „Zasady przepływu, przechowywania i archiwizowania dokumentów.”



9 Zasady analizy ryzyka w zakresie bezpieczeństwa informacji.

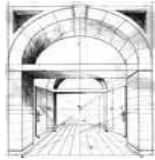
Celem szacowania ryzyka jest zidentyfikowanie i ocena ryzyka, na jakie narażone są systemy informacyjne i ich aktywa oraz znalezienie odpowiednich mechanizmów zarządzania bezpieczeństwem. Szacowanie oparte jest na wartości aktywów i poziomach wymagań bezpieczeństwa z uwzględnieniem istniejących i planowanych mechanizmów zabezpieczeń. Na obecnym etapie projektu e-PUAP nie jest możliwe przeprowadzenie ryzyka ze względu na brak podstawowych informacji takich jak aktywa i ich wycena. W świetle powyższego przedstawione zostaną podstawy analizy ryzyka, które mają za zadanie zwrócić uwagę na analizę ryzyka w fazie projektowania. Niniejsze opracowanie przygotowano na podstawie zasad opisanych w dokumencie PD 3002 - Guide to BS 7799 Risk Assessment.

Proces szacowania ryzyka składa się z następujących etapów:

- Identyfikacja i wycena aktywów;
- Identyfikacja warunków bezpieczeństwa: zagrożeń, podatności, wymagań prawnych i biznesowych oraz innych niezbędnych firmie;
- Określenie prawdopodobieństwa wystąpienia zagrożeń i podatności oraz ważności wymagań prawnych i biznesowych;
- Wyznaczenie ryzyka na podstawie kroków przedstawionych powyżej;
- Wybór odpowiedniej metody ograniczania ryzyka;
- Wybór odpowiednich mechanizmów zarządzania w celu redukcji ryzyka do akceptowalnego poziomu.

Ryzyko (R) jest miarą narażenia systemu informatycznego na szkody. Ryzyko zdarzenia przynoszącego szkodę jest funkcją:

- **prawdopodobieństwa (P)** wystąpienia zagrożenia na skutek istniejącej podatności systemu, z uwzględnieniem istniejących i planowanych mechanizmów zabezpieczeń;
- potencjalnego **kosztu naprawy szkody (K)** powstałej w wyniku zdarzenia, tzn. szacowanej wartości odtworzeniowej aktywów systemu informacyjnego utraconych na skutek wystąpienia danego zagrożenia.



Ryzyko danego zdarzenia można wyrazić jako iloczyn dwóch argumentów:

$$R = P * K$$

Ryzyko jest więc kategorią, którą można zmierzyć. Aby to zrobić, wystarczy określić wartości P i K. Jest to niestety bardzo trudne, szczególnie w przypadku określenia prawdopodobieństwa wystąpienia zagrożenia. W związku z tym stosuje się prostsze i bardziej efektywne ekonomicznie metody szacowania ryzyka.

W wielu metodach analizy ryzyka dla oszacowania wartości ryzyka wykorzystuje się względne, jakościowe skale wartościowania. Dotyczy to zarówno wagi zdarzeń, jak i prawdopodobieństwa ich wystąpienia. W ten sposób ryzyko rozpatruje się w kategoriach wartościowania jakościowego, umożliwiając porównywanie ryzyka różnych typów i porządkowanie ich zgodnie z potrzebami biznesowymi.

9.1 Identyfikacja aktywów.

Aktywa to wszystko, co ma wartość i jest użyteczne dla instytucji, jej operacji biznesowych oraz dla zapewnienia ciągłości działania. Dlatego też aktywa potrzebują odpowiednich zabezpieczeń, aby zapewnić instytucji warunki do poprawnej działalności i zachowania ciągłości biznesowej. W trakcie inwentaryzacji należy upewnić się, że żaden aktyw nie zostanie pominięty ani zapomniany.

Każdy aktyw powinien być odpowiednio zidentyfikowany i sklasyfikowany, a jego wartość z punktu widzenia firmy wyceniona. Powinien mieć także przypisaną osobę odpowiedzialną. Przykłady aktywów:

- **Aktywa informacyjne:** zasoby danych i pliki z danymi, dokumentacje systemów, instrukcje użytkownika, materiały szkoleniowe, procedury eksploatacyjne i wsparcia, plany utrzymania ciągłości działania, plany awaryjne, zarchiwizowane informacje itp.
- **Papierowe dokumenty:** kontrakty, informatory, dokumentacja firmowa, dokumenty finansowe itp.
- **Oprogramowanie:** aplikacyjne, systemowe, programy narzędziowe i użytkowe, itp.
- **Aktywa fizyczne:** sprzęt komputerowy (procesory, monitory, laptopy, modemy), sprzęt komunikacyjny (routery, centrale abonenckie, telefaxy, automatyczne sekretarki), nośniki magnetyczne (taśmy i dyski), inny sprzęt techniczny (zasilacze, klimatyzatory), meble, pomieszczenia itp.
- **Ludzie:** personel, klienci, dostawcy itp.
- **Wizerunek firmy.**



- **Usługi:** usługi obliczeniowe i telekomunikacyjne, inne usługi infrastruktury technicznej (ogrzewanie, oświetlenie, zasilanie, klimatyzacja) itp.

9.2 Wycena aktywów.

Wycena zidentyfikowanych aktywów odbywa się na podstawie ich przydatności do zaspokajania potrzeb biznesowych instytucji. Aby wybrać odpowiedni poziom bezpieczeństwa dla aktywów, należy określić ich wartość w odniesieniu do ich ważności dla biznesu lub ich potencjalną wartość, związaną z ich możliwościami wykorzystania dla celów biznesowych. Wartość ta wyraża się zazwyczaj w stosunku do potencjalnego wpływu niepożądanego incydentu, takiego jak: ujawnienie, modyfikacja, niedostępność lub zniszczenie informacji lub innych zasobów, na działalność biznesową. Incydenty te mogą prowadzić do strat finansowych, spadku dochodów, strat w rynku lub utratę dobrego wizerunku firmy.

Dane wejściowe do wyceny powinny dostarczyć osoby odpowiedzialne za dane aktywa lub informacje i oraz osoby z nich korzystające, gdyż tylko one są w stanie właściwie określić ich ważność w świetle przydatności dla firmy.

Przypisane wartości powinny być związane z kosztem nabycia i utrzymania aktywów oraz następstw utraty poufności, integralności i dostępności dla ciągłości interesów instytucji.

9.3 Identyfikacja zagrożeń i podatności

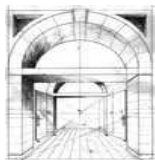
Dla wszystkich aktywów należy zidentyfikować zagrożenia, które mogą wywołać incydenty bezpieczeństwa (tzn. zdarzenia wpływające w sposób niekorzystny na działalność biznesową, np. przynoszące straty finansowe).

Podobnie dla wszystkich aktywów należy zidentyfikować ich podatności, które mogą być wykorzystane przez zagrożenia, co przynieść może wymierne straty dla firmy.

Przykład: Dokumenty papierowe są łatwopalne. Z tego względu są one podatne na zagrożenie pożarem. W przypadku pożaru dokumenty papierowe mogą łatwo ulec zniszczeniu.

W procesie szacowania ryzyka należy powiązać aktywa z kombinacją zagrożeń i podatności oraz określić stopień zagrożenia (tzn. niekorzystnych skutków zdarzenia związanego z zagrożeniem) i stopień podatności (tzn. jak bardzo dany aktyw jest podatny). Stopień zagrożenia określamy na podstawie skali {0; 1; 2}, która oznacza odpowiednio stopień nieznaczny, średni, wysoki. Przy określaniu stopni zagrożeń i podatności należy uwzględnić następujące czynniki:

1. niedostępność lub zniszczenie majątku,



2. nieupoważniona modyfikacja lub uszkodzenia sprzętu, pomieszczeń,
3. nieupoważniony dostęp, który powoduje straty wymierne (np. bezpośrednie lub pośrednie koszty) albo niewymierne (np. utratę dobrego imienia firmy, naruszenie prywatności),
4. ujawnienie danych, przechowywanych przetwarzanych lub przesyłanych,
5. fizyczne przerwanie funkcjonowania.

9.4 Metoda analizy ryzyka

Dalszą analizę ryzyka opiera się na predefiniowanej tablicy wartości ryzyka. Tabela predefiniowanych wartości ryzyka przedstawia się następująco:

Tabela 1. Tabela predefiniowanej wartości ryzyka.

Miara ryzyka	Skala wartości dla zagrożeń	0			1			2		
	Skala wartości dla podatności	0	1	2	0	1	2	0	1	2
Wartość aktywu	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

W oparciu o powyższą tabelę szacuje się ryzyko zdarzeń, związanych z zagrożeniami i podatnościami dla wszystkich zidentyfikowanych aktywów.

Analiza ryzyka będzie miała postać tabeli z następującymi kolumnami:

- Aktyw,
- Lista zdarzeń (kombinacja zagrożenie, podatność),
- Ryzyko związane z wystąpieniem zdarzenia (odczytane z Tabeli 1).

Na podstawie tak przeprowadzonej analizy należy dobrać odpowiednie zabezpieczenia w celu zminimalizowania ryzyka do określonego poziomu.

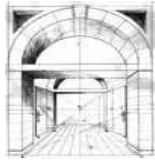


9.5 Zagrożenia związane z e-PUAP – wstępna analiza

Na obecnym etapie projektowym nie jest możliwe przeprowadzenie analizy ryzyka ze względu na brak wyceny kosztów jak również decyzji odnośnie postępowania z ryzykiem. Można natomiast wstępnie określić zagrożenia i konsekwencje zdarzeń związane z algorytmami przekazywania dokumentów jak i wnoszenia opłat skarbowych przy pomocy e-PUAP.

Zagrożenia związane z przekazywaniem pism do jednostek administracji państwowej:

Zagrożenie	Skutki wystąpienia zagrożenia	Możliwe zabezpieczenia
Brak dostępności usług	Krótkoterminowy brak dostępności usług nie stanowi poważnego zagrożenia. Natomiast długotrwały może skutkować zwiększoną ilością interesantów w urzędach, co z kolei może spowodować niemożliwość załatwienia spraw w określonym terminie. Brak dostępności usług na krótko przed upłynięciem doby.	Ośrodek zapasowy. Lokalna redundancja systemów. Informacja mówiąca, że dokumenty przyjęte po określonej godzinie (którą należy określić na podstawie czasu przełączania na ośrodek zapasowy) mogą być przyjęte z datą dnia następnego.
Brak dostępności usług poddostawców (np. centra certyfikacji, rejestry).	Konsekwencją wystąpienia incydentu związanego z zagrożeniem jest brak dostępności poszczególnych usług systemu ePUAP. W szczególności wystąpienie zagrożenia może uniemożliwić weryfikację podpisów elektronicznych, a co za tymi idzie skuteczną archiwizację podpisów.	Odpowiednie umowy SLA z poddostawcami oraz zapewnienie redundancji łącz.



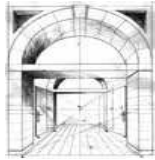
Zasady bezpieczeństwa ePUAP

Brak możliwości wystawienia poświadczenia przedłożenia.	Konsekwencją wystąpienia incydentu związanego z zagrożeniem jest niemożliwość uzyskania potwierdzenia doręczenia w określonym czasie przez nadawcę. Takie zagrożenie może mieć duży wpływ we wszystkich procesach, gdzie termin złożenia pisma wpływa na decyzję: np. termin złożenia oferty w przetargu publicznym.	Redundancja systemów służących do wystawiania poświadczenia przedłożenia.
Brak możliwości archiwizacji podpisu.	Konsekwencją wystąpienia incydentu związanego z zagrożeniem może być konieczność przesłania pisma do adresata bez dokonania archiwizacji podpisu zwłaszcza w przypadku przedłużającej się niedostępności tej usługi.	Redundancja systemów służących do archiwizacji podpisu. Funkcjonalność umożliwiająca przesłanie dokumentu bez archiwizacji podpisu i późniejsze jej uzupełnienie.
Naruszenie integralności dokumentu.	Wystąpienie incydentu uniemożliwia przekazanie dokumentu do jednostki administracji, powoduje to narażenie na konsekwencje prawne wynikające z nie wszczęcia sprawy w określonym terminie. W zależności od rodzaju sprawy i terminów konsekwencje mogą dotyczyć zarówno strony jak i administracji.	Zastosowanie funkcjonalności umożliwiającej powiadomianie strony o wystąpieniu incydentu.
Niedostarczenie pism do organów administracji państwowej w odpowiednim terminie	Narażenie na konsekwencje prawne wynikające z niewszczęcia sprawy w określonym terminie tym bardziej, że strona nadająca pismo otrzymuje urzędowe poświadczenie odbioru i dla niej sprawa jest w toku.	Zapewnienie redundancji łącz. Umowy SLA z poddostawcami. Redundancja systemów odpowiedzialnych za dostarczanie dokumentów.



Zasady bezpieczeństwa ePUAP

Utrata dokumentu przeznaczony do przekazania.	Narażenie na konsekwencje prawne wynikające z niewszczęcia sprawy w określonym terminie tym bardziej, że strona nadająca pismo otrzymuje urzędowe poświadczenie odbioru i dla niej sprawa jest w toku.	Redundancja systemów przechowywania dokumentów. Wykonywanie kopii bezpieczeństwa. Implementacja funkcjonalności śledzenia transakcji.
Utrata poświadczenia odbioru.	Brak możliwości dowodzenia w przypadku wystąpienia sporu.	Redundancja systemów przechowywania urzędowego poświadczenia odbioru. Wykonywanie kopii bezpieczeństwa.
Ekspozycja treści dokumentów (utrata poufności polegająca na uzyskaniu nieuprawnionego dostępu do dokumentów przez osoby trzecie).	Narażenie na konsekwencje prawne wynikające z faktu upublicznienia informacji prawnie chronionych.	Stosowanie zabezpieczeń zgodnych z normą ISO/IEC 17799:2005 opisanych w rozdziale 2.
Niewystawienie potwierdzenia dostarczenia dokumentu do organu administracji państwowej.	Brak możliwości dowodzenia w przypadku wystąpienia sporu.	Redundancja systemów wystawiania potwierżeń. Implementacja funkcjonalności monitowania.
Utrata potwierdzenia dostarczenia dokumentu do organu administracji państwowej.	Brak możliwości dowodzenia w przypadku wystąpienia sporu.	Redundancja systemów przechowywania potwierżeń. Wykonywanie kopii bezpieczeństwa.



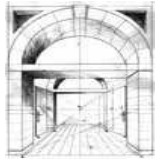
Zagrożenia związane z doręczaniem decyzji i wezwań

Zagrożenie	Skutki wystąpienia zagrożenia	Możliwe zabezpieczenia
Brak dostępności usług	Krótkoterminowy brak dostępności usług nie stanowi poważnego zagrożenia. Natomiast długotrwały może skutkować zwiększoną ilością interesantów w urzędach, co z kolei może spowodować niemożliwość załatwienia spraw w określonym terminie. Straty finansowe wynikające z przejścia na papierową obsługę dokumentów.	Ośrodek zapasowy. Lokalna redundancja systemów.
Brak dostępności usług poddostawców (np. centra certyfikacji, rejestry).	Konsekwencją wystąpienia incydentu związanego z zagrożeniem jest brak dostępności poszczególnych usług systemu ePUAP. W szczególności wystąpienie zagrożenia może uniemożliwić weryfikację podpisów elektronicznych, a co za tymi idzie skuteczną archiwizację podpisów.	Odpowiednie umowy SLA z poddostawcami oraz zapewnienie redundancji łącz.



Zasady bezpieczeństwa ePUAP

Brak możliwości przygotowania poświadczenia doręczenia.	Konsekwencją wystąpienia incydentu związanego z zagrożeniem jest niemożliwość doręczenia wezwania lub decyzji, co może spowodować konieczność zastosowania komunikacji papierowej. CO w konsekwencji spowoduje większe obciążenie urzędów. Straty finansowe wynikające z przejścia na papierową obsługę dokumentów.	Redundancja systemów służących do wystawiania poświadczenia przedłożenia.
Niedostarczenie awiza do strony.	Przejęcie na papierową obsługę doręczeń. Straty finansowe wynikające z przejścia na papierową obsługę dokumentów.	Implementacja funkcjonalności śledzenia transakcji.
Brak udostępnienia poświadczenia doręczenia.	Przejęcie na papierową obsługę doręczeń. Straty finansowe wynikające z przejścia na papierową obsługę dokumentów.	Redundancja systemów do udostępniania poświadczeń doręczenia.
Brak udostępnienia decyzji lub wezwania.	Narażenie strony na konsekwencje wynikające z niedotrzymania terminów.	Poinformowanie strony o możliwości wystąpienia zagrożenia i załączenie odpowiedniej instrukcji co do dalszego postępowania.
Utrata dokumentu przeznaczonego do doręczenia	Wszczęcie postępowania drogą papierową. Przy jednostkowych incydentach niskie konsekwencje, przy większej ilości incydentów wzmożony ruch w urzędach. Straty finansowe wynikające z przejścia na papierową obsługę dokumentów.	Redundancja systemów służących do przechowywania dokumentów. Wykonywanie kopii bezpieczeństwa.



Zasady bezpieczeństwa ePUAP

Utrata potwierdzenia doręczenia	Może spowodować ponowne wszczęcie tego samego postępowania drogą papierową. Brak możliwości dowodzenia w przypadku wystąpienia sporu.	Redundancja systemów przechowywania potwierżeń. Wykonywanie kopii bezpieczeństwa.
Niedostarczenie decyzji w terminie ustawowym.	Narażenie na konsekwencje prawne wynikające z faktu niedostarczenia decyzji w terminie ustawowym. Na tego typu zagrożenia narażony jest urząd, który nie posiada własnego systemu informatycznego i korzysta z e-PUAP wyłącznie przy pomocy przeglądarki www. Incydent wystąpi wtedy, gdy urzędnik regularnie nie przegląda stanu spraw realizowanych przez e-PUAP	Redundancja systemów dostarczania dokumentów. Redundancja łącz. Umowy SLA z poddostawcami.
Ekspozycja treści dokumentów (utrata poufności polegająca na uzyskaniu nieuprawnionego dostępu do dokumentów przez osoby trzecie).	Narażenie na konsekwencje prawne wynikające z faktu upublicznienia informacji prawnie chronionych.	Stosowanie zabezpieczeń zgodnych z normą ISO/IEC 17799:2005 opisanych w w rozdziale 2.



Zagrożenia związane z repozytoriami służącymi do przechowywania dokumentów dla gmin

Zagrożenie	Skutki wystąpienia zagrożenia	Możliwe zabezpieczenia
Utrata dostępności repozytoriów dla gmin.	Krótkoterminowy brak dostępności usług nie stanowi poważnego zagrożenia. Natomiast długotrwały może skutkować brakiem możliwości obsługi elektronicznej dokumentów oraz niemożliwość załatwienia spraw w określonym terminie.	Ośrodek zapasowy. Lokalna redundancja systemów.
Utrata dokumentów zawartych w repozytoriach.	Narażenie na konsekwencje wynikające z zawartych umów.	Ośrodek zapasowy. Lokalna redundancja systemów. Kopie bezpieczeństwa.
Ekspozycja treści dokumentów (utrata poufności polegająca na uzyskaniu nieuprawnionego dostępu do dokumentów przez osoby trzecie).	Narażenie na konsekwencje prawne wynikające z faktu upublicznienia informacji prawnie chronionych.	Stosowanie zabezpieczeń zgodnych z normą ISO/IEC 17799:2005 opisanych w rozdziale 2.

Wystąpienie jakiegokolwiek zdarzenia powinno skutkować uruchomieniem wewnętrznej procedury reakcji na incydent w celu szybkiej lokalizacji źródła zdarzenia, wyciągnięciem wniosków oraz podjęciem odpowiednich akcji naprawczych.