Współczesne Problemy Systemów Czasu Rzeczywistego, Rozdział 31, str. 349-359, Warszawa 2004

BEZPIECZEŃSTWO E-URZĘDU – CENTRUM CERTYFIKACJI

Bogdan Księżopolski[1], Zbigniew Kotulski[2]

[1]Instytut Fizyki, Uniwersytet Marii Curie-Skłodowskiej
Pl. M. Curie-Skłodowskiej 1,20-031 Lublin, Polska
e-mail: bogdan@kft.umcs.lublin.pl
[2]Instytut Podstawowych Problemów Techniki PAN
Ul. Świętokrzyska 21, 00-049 Warszawa, Polska
e-mail: zkotulsk@ippt.gov.pl

Abstract

Celem niniejszej pracy jest zaprezentowanie elementów bezpieczeństwa e-urzędu ze szczególną uwagą na Centrum Certyfikacji. Przedstawione zostaną normy, które opisują wymagania jakie muszą zostać spełnione żeby infrastruktura e-urządu mogła być uważana za bezpieczną. Normy opisują zarówno architekturę sieciową urzędu jaki i moduły kryptograficzne, używane np. do realizacji poszczególnych kroków protokołu kryptograficznego na których to zazwyczaj opiera się cała komunikacja wewnątrz e-urzędu. Zaprezentowano również konkretne moduły kryptograficzne, które spełniają aktualne wymagania bezpieczeństwa. W pracy przedstawiono wymogi jakie powinny spełniać elementy składowe Centrum Certyfikacji czyli Centrum Autoryzacji (CA) oraz Centrum Znakowania Czasem (TSA), ze szczególnym rozważeniem modułów kryptograficznych. Analizę przeprowadzono dla zaufanej trzeciej strony składnika protokołu kryptograficznego realizującego elektroniczny przetarg[2].

1 WSTĘP

W społeczeństwie informacyjnym administracja publiczna zmienia klasyczną formę przekazywania informacji na formę elektroniczną. Korzyści płynące ze stosowania drogi elektronicznej są znaczne, oszczędzamy w ten sposób czas, znacznie usprawniamy przepływ dokumentów, obniżamy koszty. Aktualnie prowadzone są badania nad różnymi sferami administracji publicznej [1], tworzone są projekty wspierające takie inicjatywy (eTEN,IDAII), niektóre projekty zostały już częściowo wprowadzone, chociażby w ZUS.
Istotnym elementem o którym nie można zapomnieć jest ochrona informacji do których mają dostęp systemy elektroniczne administracji publicznej. Bezpieczeństwo takich systemów jest zagadnieniem bardzo złożonym, składającym się z wielu elementów, między innymi, bezpiecznej architektury sieciowej, systemów zabezpieczeń infrastruktury sieciowej oraz konkretnych systemów, protokołów kryptograficznych, ustalonych obowiązków dla personelu itd. Aktualnie tworzone są różne architektury, modele [13] gwarantujące założony wcześniej poziom bezpieczeństwa.
Wymienione zagadnienia dotyczące bezpieczeństwa opisywane są przez

Współczesne Problemy Systemów Czasu Rzeczywistego, Rozdział 31, str. 349-359, Warszawa 2004

międzynarodowe organizacje do spraw standardów (ISO,IEC,ETSI), które tworzą odpowiednie normy formalno-prawne. Stosowanie wspomnianych norm pozwala nam założyć, że stworzona w ten sposób infrastruktura jest odpowiednio zabezpieczona przed atakami oraz różnymi nadużyciami. Normy nie określają nam konkretnych zastosowań tylko wymagania jakie muszą być spełnione. W pracy przedstawiono konkretne rozwiązania, spełniające aktualnie istniejące normy.
Bezpieczeństwo rozwiązań w obrębie e-urzędu zależy od konkretnego projektu, nie mniej jednak jesteśmy wstanie przedstawić pewne ogólne zagadnienia. W pracy zaprezentowano analizę elementów bezpieczeństwa, protokołu kryptograficznego realizującego elektroniczną formę przetargu.

2 OPIS PROTOKOŁU E-PRZETARGU

2.1 OMÓWIENIE MODELU

Analizowany protokół e-przetargu składa się z czterech podprotokołów: *certyfikacji, zgłoszenia przetargu, zgłoszenia oferty oraz wyboru oferty.* W protokole bierze udział *n* oferentów (O_1, ... ,O_n), zaufana trzecia strona czyli *GAP* (Główna Agencja Przetargowa) oraz firma chcąca ogłosić przetarg *F.*
Pierwszym krokiem protokołu jest weryfikacja przez GAP, uczestników biorących udział w e-przetargu, czyli oferentów O_n oraz firmy F chcącej ogłosić przetarg (*podprotokół certyfikacji*). Kolejnym krokiem jest zgłoszenie, do GAP, przetargu przez zweryfikowaną firmę F. GAP publikuje warunki zgłoszonego przetargu, podając w nim wszelkie wymogi zgłoszone przez F *(podprotokół zgłoszenia przetargu).*W następnym kroku, osoba chcąca wziąć udział w przetargu, po wcześniejszej weryfikacji, przesyła swoją ofertę do GAP *(podprotokół zgłoszenia oferty).* Ostatni podprotokół wykonywany jest po upłynięciu czasu na zgłoszenie ofert, wówczas firma F oraz oferenci O_n, przesyłają do GAP, swoje części sekretu, potrzebne do odczytania ofert. Po odszyfrowaniu, zostaną one przesłane do firmy F, gdzie zostanie wybrana zwycięska oferta. W tym samym podprotokole, firma F wysyła informacje o wygranej ofercie do GAP, po czym zostanie ona opublikowana do publicznej wiadomości *(podprotokół wyboru oferty).*
Komunikacja pomiędzy uczestnikami protokołu jest bezpieczna. Uzyskujemy to dzięki zastosowani kryptografii z kluczem publicznym, gdzie każdy uczestnik protokołu posiada swój klucz prywatny (SK) oraz klucz publiczny (PK). Stosowane klucze nie są stałe, ich ważność kończy się wraz z ważnością numeru rejestracyjnego, uzyskanego w podprotokole certyfikacji.
Oferty przesłane przez oferentów O_n, są zaszyfrowane kluczem publicznym danego przetargu. Odczytać je możemy posiadając klucz prywatny, który to w podprotokole

zgłoszenia przetargu, zostaje podzielony na części za pomocą odpowiedniego progowego bezpiecznego schematu podz\iału sekretu. W protokole używamy również, generator liczb losowych (KG). Stosujemy go do tworzenie numerów identyfikacyjnych uczestników przetargu jak i numerów samych przetargów.
Przetarg kończy się po minięciu określonego czasu, do określenia tej chwili posłużmy się znacznikami czasu (T).

2.2 USŁUGI BEZPIECZEŃSTWA

W opisywanym protokole możemy wyodrębnić różne mechanizmy bezpieczeństwa, w głównej mierze wiążą się one z modułami kryptograficznymi. Możemy wskazać główne składniki.

Podpis cyfrowy

Dokumenty przesyłane pomiędzy uczestnikami są zawsze podpisywane cyfrowo. W ten sposób uzyskujemy *integralność danych*, ponieważ wiadomość podpisana cyfrowo nie może zostać zmieniona i jednoczesnym zachowaniem podpisu cyfrowego. Inną zaletą jest *niezaprzeczalność danych*, mianowicie osoba, która podpisała dany dokument nie może wyprzeć się tej czynności.

Szyfrowanie informacji

Przesyłana informacje są szyfrowane. Do tego celu można użyć różnych algorytmów szyfrujących, w opisywanym przypadku użyto modelu hybrydowego. Jednorazowe klucze sesyjne szyfrów symetrycznych są przesyłane za pomocą szyfru asymetrycznego, dzięki czemu możemy zapewnić *poufność danych* biorących udział w protokole.

Przyznawania Certyfikatów

Wszyscy uczestnicy elektronicznego przetargu, żeby wziąć w nim udział, muszą posiadać odpowiedni numer rejestracyjny. Takowe numery przyznawane są po wcześniejszej weryfikacji, za tą czynność odpowiedzialna jest zaufana trzecia strona (GAP). Przyznanie numeru rejestracyjnego jest równoważne z wygenerowaniem pary kluczy (klucz prywatny, klucz publiczny), które to będą niezbędne do tworzenia ważnych podpisów cyfrowych oraz przy użyciu modeli hybrydowych.

Znakowanie czasem

Część dokumentów biorących udział w protokole kryptograficznym, musi być jednoznacznie określona pod względem czasu ich utworzenia lub czasu przesłania. Do takich danych należy np. numer rejestracyjny, przesyłane oferty. Wykorzystujemy do tego znaczniki czasu, które generowane przez TSA.

Podział sekretu

W przedstawionym protokole, szczególnie istotnym elementem jest zachowanie poufności przesłanych ofert przez oferentów. Możemy to uzyskać dzięki zastosowaniu bezpiecznego schematu podziału sekretu. Klucz prywatny danego przetargu jest dzielony odpowiednim schematem progowym i jego części są rozsyłane między uczestników przetargu. Ponowne odtworzenie oferty wymaga zebrania, wcześniej wskazanej liczby, części sekretów.

Zaufana trzecia strona (Pełniąca rolę CA i TSA) - GAP

Wyżej wymienione usługi bezpieczeństwa uzależnione są w dużej mierze od Centrum Certyfikacji pełniącej rolę zaufanej trzeciej strony (TTP), która oferuje usługi kompletne, ujednolicające poziom bezpieczeństwa. W opisywanym przypadku rolę tą pełni *GAP,* która przydziela numery certyfikujące (CA), tworzy znaczniki czasu (TSA), dzieli sekret za pomocą różnych schematów podziału sekretu oraz może pełnić inne funkcje w których zaufanie jest kluczowym elementów. Analizując funkcje jakie pełni zaufana trzecia strona można stwierdzić, że jest to element krytyczny całej infrastruktury systemu.

3 CENTRUM CERTYFIKACJI – ELEMENT KRYTYCZNY INFRASTRUKTURY SYSTEMU

Bezpieczeństwo zaufanej trzeciej strony (TTP) możemy uzyskać stosując się do norm, które określają warunki jakie powinien spełniać dany system. W opisywanym przypadku, TTP pełni potrójną rolę, czyli Centrum Autoryzacji(CA), Centrum znakowania czasem (TSA) oraz dzieli dowolny sekret bezpiecznym schematem podziału sekretu. Specyfikacje dotycząca CA oraz TSA przedstawione przez Europejski Instytut do spraw standardów telekomunikacyjnych ETSI [3,4] są merytorycznie zbliżone. Zawarte tam wymogi można podzielić na trzy główne zagadnienia: *Zarządzanie kluczami, Zarządzanie certyfikatami, Zarządzanie samym urzędem.*

Zarządzanie kluczami

- generowanie kluczy
- przechowywanie kluczy, kopie oraz odtwarzanie kopii
- rozpowszechnianie publicznych kluczy
- użycie kluczy
- zakończenie „cyklu życia" kluczy
- sprzętowe urządzenia kryptograficzne

Zarządzanie certyfikatami

- rejestracja podmiotu
- uaktualnianie certyfikatów
- generowanie certyfikatów
- rozgłaszanie certyfikatów
- zawieszenie i odwoływanie certyfikatów

Zarządzanie urzędem

- zarządzanie bezpieczeństwem
- ochrona zasobów urzędu
- zabezpieczenia fizyczne oraz bezpieczeństwo całej infrastruktury
- zarządzenie procedurami urzędu

- bezpieczeństwo personelu
- zarządzanie dostępem do systemu
- stosowanie wiarygodnych systemów i aplikacji
- procedury awaryjne na wypadek nadużyć, ataków
- zakończenie działania urzędu
- archiwizacja danych dotyczących certyfikatów

Bezpieczne schematy podziału sekretu nie posiadają aktualnie norm ich opisujących, istnieją natomiast algorytmy [12] za pomocą, których możemy zrealizować wspomnianą operację.

4 ZAGADNIENIA KRYPTOGRAFICZNE

W przedstawianej pracy głównie chcemy skupić się na przedstawieniu modułów kryptograficznych, mieszczących się we wspomnianych normach. Wybór konkretnych algorytmów kryptograficznych oraz szczegółów związanych z ich zastosowaniem należy uzależnić od poziomu bezpieczeństwa jaki ma być zachowany w danym e-urzędzie. Takie założenia ustalamy podczas pierwotnej fazy tworzenia bezpiecznej infrastruktury czyli projektując konkretną politykę bezpieczeństwa.

4.1 POZIOMY BEZPIECZEŃSTWA

Poziomy bezpieczeństwa modułów kryptograficznych, opracowane przez organizacje ISO/IEC [6], zostały podzielone na cztery pułapy. W tej pracy przedstawiono część tych zagadnień, niezbędnych do realizacji e-przetargu.

<table>
<tr><th></th><th>Poziom bezpieczeństwa 1</th><th>Poziom bezpieczeństwa 2</th><th>Poziom bezpieczeństwa 3</th><th>Poziom bezpieczeństwa 4</th></tr>
<tr><td>Specyfikacja modułów kryptograficznych</td><td colspan="4">Specyfikacja modułów kryptograficznych, kryptograficzne granice, potwierdzone algorytmy oraz kroki działania. Opis kryptograficznych modułów, czyli sprzętu, oprogramowania, autorskich komponentów. Polityka bezpieczeństwa modułów kryptograficznych.</td></tr>
<tr><td>Porty i interfejsy modułów kryptograficznych</td><td colspan="2">Wymagana i opcjonalne interfejsy. Specyfikacja wszystkich interfejsów i wszystkich portów wejścia/wyjścia danych.</td><td colspan="2">Niezabezpieczone porty wejścia/wyjścia danych oddzielone od innych portów.</td></tr>
<tr><td>Model możliwych stanów</td><td colspan="4">Specyfikacja modelu o określającego wszelkie możliwe stany. Stany żądane oraz opcjonalne. Diagram przejść pomiędzy stanami i specyfikacja poszczególnych stanów.</td></tr>
<tr><td rowspan="2">Zarządzanie kluczami kryptograficznymi</td><td colspan="4">Mechanizm zarządzania kluczem: generator liczb losowych, generator kluczy, ustanowienie kluczy, dystrybucja kluczy, wejście/wyjście kluczy, przechowywanie kluczy, anulowanie kluczy.</td></tr>
<tr><td colspan="2">Prywatny oraz publiczny klucz przekazywany drogą manualną, wejście/wyjście kluczy może być przekazywana w formie zaszyfrowanej jako całość</td><td colspan="2">Prywatny oraz publiczny klucz przekazywany drogą manualną,, wejście/wyjście kluczy powinno być w formie zaszyfrowanej za pomocą procedur podziału sekretu</td></tr>
</table>

Wewnętrzny Audyt	Testy: algorytmów kryptograficznych, integralności oprogramowania, funkcji krytycznych.

Tabela nr.1 Poziomy bezpieczeństwa.

4.2 ZAŁOŻENIA DLA E-PRZETARGU

Poziom bezpieczeństwa w konkretnym urzędzie jest uzależniony od pełnionych przez niego funkcji. W przypadku elektronicznego przetargu możemy mówić o najwyższym poziomie ochrony. Szczególną uwagą należy zwrócić na zaufaną trzecią stronę czyli „Główną Agencje Przetargową". Wspomniany element jest krytyczny dla całej infrastruktury dlatego powinien spełniać najwyższy czwarty poziom bezpieczeństwa.

4.2.1 SPECYFIKACJA MODUŁÓW KRYPTOGRAFICZNYCH – POTWIERDZONE ALGORYTMY

W elektronicznym przetargu używamy wielu mechanizmów kryptograficznych, chcąc zachować odpowiedni poziom bezpieczeństwa musimy stosować potwierdzone algorytmy kryptograficzne. Zaufana trzecia strona używa schematów hybrydowych do przesyłania informacji, podpisów cyfrowych do znakowania dokumentów, bezpiecznych schematów podziału sekretu do rozdzielenia kluczy prywatnych, funkcji skrótu do tworzenia certyfikatów.
Główna komunikacja między stronami uczestniczącymi w elektronicznym przetargu, w tym głównie z GAP, odbywa się za pomocą schematów hybrydowych. Do tego rodzaju szyfrowania używamy dwa rodzaje operacji, pierwsza, mechanizm enkapsulacji klucza (KEM) polega na bezpiecznym przekazaniu między stronami klucza oraz druga, mechanizm enkapsulacji danych (DEM) polega na szyfrowaniu za pomocą wcześniej przekazanego klucza.
Pierwsza operacja wykonywana jest za pomocą szyfrów asymetrycznych [9] przy użyciu różnych modeli [14]. Do tego rodzaju szyfrowania możemy zastosować szyfry RSA [7], ElGamal [8] oraz inne zbudowane na ich podstawie.
Druga operacja polega na szyfrowaniu danych wcześniej przesłanym kluczem, używamy do tego szyfrów symetrycznych [10]. W tej grupie szyfrów znajdują się szyfry o dwóch długościach kluczy 64-bitowym oraz 128-bitowym. Z grupy szyfrów 64-bitowych możemy wybrać np. szyfry DES, TDEA, natomiast z 128-bitowej np. AES, Camellia.
Zaufana trzecia strona, przesyłając dokumenty do innych uczestników przetargu, wcześniej je podpisując. Do tego celu możemy użyć np. wcześniej wspominanego algorytmu RSA lub DSA [11].
Schematy podziału sekretu aktualnie nie są opisywane przez stosowne normy, nie mniej jednak istnieją pewne modele, które realizują wspomniane zagadnienie. W przypadku elektronicznego przetargu możemy użyć automatyczny schemat podziału sekretu [12].

4.2.2 PORTY I INTERFEJSY MODUŁÓW KRYPTOGRAFICZNYCH

Informacje przekazywane między uczestnikami e-przetargu początkowo są szyfrowana a następnie poprzez fizyczne porty oraz logiczne interfejsy kierowane są do miejsca przeznaczenia. Porty oraz interfejsy, do których kierowane są informacje powinny być jasno określone, zarówno dla danych wchodzących jak i wychodzących. Ponad to, zgodnie z najwyższym poziomem bezpieczeństwa musimy stworzyć dwa niezależne połączenia fizyczne oraz logiczne, którymi przesyłane będą dane. W jednym kanale będą przesyłane wszelkie informacje jako tekst jawny, natomiast w drugim wyłączenie dane zaszyfrowane.

4.2.3 MODEL MOŻLIWYCH STANÓW

Operacje wykonywane przy użyciu modułów kryptograficznych powinny być opisane za pomocą szczegółowego, kompletnego modelu opisującego wszystkie możliwe stany w jakich może znaleźć się TTP. Model powinien zawierać następujące elementy:

- Wszelkie możliwe stany, poprawne jak i błędne modułów kryptograficznych
- Opis transakcji pomiędzy poszczególnymi stanami
- Możliwe stany danych wejściowych, które powodują transakcje pomiędzy stanami
- Możliwe stany danych wyjściowych, które zostały spowodowane wcześniejszymi transakcjami

W przypadku e-przetargu główne stany uczestników przetargu zostały opisane we wspominanym protokole kryptograficznym. Stany pośrednie należy również opisać ale takową czynność najlepiej wykonać podczas procesu implementacji całej architektury gdyż wiele elementów zależy od konkretnych wyborów i rozwiązań.

4.2.4 ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI

Proces zarządzania kluczami kryptograficznymi składa się z cyklu, który składa się z elementów, które zostały wyszczególnione podczas opisywania poziomów bezpieczeństwa. W e-przetargu używane elementy kryptograficzne muszą spełniać najwyższy poziom bezpieczeństwa.

Generator liczb losowych, używany jest do generowania ciągów pseudolosowych, które wykorzystywane są do innych modułów kryptograficznych. W opisywanym przypadku warto zastosować potwierdzone generatory, spełniające odpowiednie normy [15]. Takowym generatorem może być np. BBS (Blum-Blum-Shub), który posiada mocne teoretyczne podstawy pseudolosowości generowanych przez niego ciągów. Dane wychodzące z generatora liczb losowych powinny być weryfikowane za pomocą testu ciągłości, którego opis zostanie przedstawiony w dalszej części pracy.

Generator kluczy, jest zazwyczaj integralnym elementem modułów kryptograficznych. Do ich generowania używamy wcześniej wspomnianych generatorów liczb losowych, również w tym elemencie powinniśmy wybrać ich zaufane wersje.

Współczesne Problemy Systemów Czasu Rzeczywistego, Rozdział 31, str. 349-359, Warszawa 2004

Ustanowienie kluczy, może być wykonane za pomocą metod automatycznych, manualnych lub przy wykorzystaniu obydwóch metod. W przypadku elektronicznego przetargu istotnym elementem jest ograniczenie wykonywanych operacji dlatego zaleca się wykorzystanie jedynie metod automatycznych. Metody kryptograficzne realizujące założenia opierają się głównie na wykorzystaniu asymetrycznych mechanizmów, szczegóły opisane są przez określone normy [16].
Wejście/wyjście kluczy. Klucze kryptograficzne są zarówno wprowadzane jak i wyprowadzane z modułów kryptograficznych. Klucze prywatne oraz publiczne przekazywane automatycznie wcześniej są szyfrowane przy użyciu sprawdzonych algorytmów. Dla zwiększenia bezpieczeństwa proces transportu kluczy może zostać poprzedzony dodatkową autoryzacja za pomocą metod manualnych (np. smard cards/tokens).
Przechowywanie kluczy. Kryptograficzne klucze używane przez moduły kryptograficzne powinny być przechowywane również w innym bezpiecznym miejscu. W przypadku e-przetargu, powinniśmy zadbać o wysoki stopień bezpieczeństwa, dlatego klucze nie powinny być przechowywane jako tekst jawny tylko w formie zaszyfrowanej. Do przechowywanych kluczy nie może mieć dostęp nikt oprócz upoważnionych osób.
Anulowanie kluczy. Moduły kryptograficzne, powinny posiadać możliwość wymazywania wszystkich używanych przez siebie kluczy.

4.2.5 WEWNĘTRZNY AUDYT

Moduły kryptograficzne powinny być weryfikowane za pomocą testów, których poprawność wskazuje na zachowanie odpowiedniego poziomu bezpieczeństwa. Normy zalecają używania dwóch rodzajów testów.
Pierwszy test, test inicjalizujący, jest przeprowadzany po uruchomieniu całego systemu, który sprawdza integralność systemu oraz jego poprawne funkcjonowanie.
Drugi rodzaj, test warunkowy, jest przeprowadzony gdy moduły kryptograficzne wykonują pewne określone czynności np. generują klucze kryptograficzne.
Test inicjalizujący. Dla e-przetargu test inicjalizujący powinien zawierać testy a*lgorytmów kryptograficznych ,integracji oprogramowania* oraz *krytycznych funkcji.*
Test *algorytmów kryptograficznych* przeprowadzana jest za pomocą metody *znanej odpowiedzi* czyli na wejście algorytmu przekazujemy dane, które po przejściu przez algorytm dają pewną wartość, która to jest przez nas znana. Porównując takowe wyniki możemy stwierdzić poprawność danego algorytmu. W przypadku e-przetargu powinniśmy sprawdzić wszelkie kryptograficzne funkcje np. funkcje szyfrujące, funkcje deszyfrujące, funkcje biorące udział w autoryzacji, generator liczb losowych itd.
Test *integracji oprogramowania* polega na sprawdzeniu autentyczności oraz integralności używanego oprogramowania. W przypadku e-przetargu do tego celu można wykorzystać algorytm podpisu cyfrowego, który zweryfikuje autentyczność oprogramowania.
Test krytycznych funkcji obejmuje pozostałe operacje, które związane są z bezpiecznym

funkcjonowaniem modułów kryptograficznych. Krytyczne elementy są uzależnione od konkretnych projektów, w przypadku e-przetagu takimi elementami są na przykład składniki wchodzące w skład bezpiecznego schematu podziału sekretu.

Test warunkowy. Testy warunkowe są wykonywane gdy dowolna operacja kryptograficzna tego zażąda, mogą to być testy z*wartości par kluczy publiczny-prywatny* (kryptografia asymetryczna)*,obciążenia oprogramowania, ciągłości generatora liczb losowych.*

Testy z*wartości par kluczy publiczny-prywatny* jest wykonywany podczas operacji KEM, szyfrowana jest wówczas znana wiadomość kluczem publicznym, następnie deszyfrowany jest utworzony szyfrogram za pomocą klucza prywatnego i wówczas porównywane są otrzymane wartości. Innym warunkiem wykonania opisywanego testu jest weryfikacja podpisu cyfrowego np. przez centrum autoryzacji.

Test *obciążenia oprogramowania* wykonywany jest gdy oprogramowanie wchodzące w skład modułów kryptograficznych jest mocno obciążone. Przeprowadzana jest wówczas autoryzacja takowego oprogramowania np. za pomocą algorytmów podpisu cyfrowego.

Test *ciągłości generatora liczb losowych* jest wykonywany gdy moduły kryptograficzne potrzebują wykorzystania generatorów liczb losowych. Podczas inicjalizowania systemu, generator liczb losowych tworzy blok złożony z N bitów gdzie $N > 16$, który następnie służy jako wzorzec dla kolejnych generowanych ciągów. Każdorazowo gdy wykorzystywany jest generator liczb losowych przeprowadzona jest wspomniana weryfikacja poprawności ciągów.

5 PODSUMOWANIE

W pracy zaprezentowano szereg wymogów jakie powinna spełniać bezpieczna infrastruktura e-urzędu ze szczególnym uwzględnieniem modułów kryptograficznych. Rozważania prowadzono analizując elementy bezpieczeństwa protokołu kryptograficznego realizującego elektroniczny przetarg ze szczególnym uwzględnieniem elementów kryptograficznych. Zawarte w niej elementy są konieczne przy implementacji infrastruktury e-przetargu a ich zastosowanie gwarantuje spełnienie najwyższego stopnia bezpieczeństwa modułów kryptograficznych. Chcąc uzyskać najwyższy poziom bezpieczeństwa wszystkich elementów składowych danej infrastruktury e-urzędu należy przeprowadzić ich podobne rozumowanie. Implementacja dowolnego składnika infrastruktury e-urzędu na niższym poziomie niż pozostałe, automatycznie zmienia jego ogólny poziom bezpieczeństwa na poziom najniższego użytego elementu. Zachowanie wcześniej ustalonego poziomu bezpieczeństwa możemy uzyskać stosując się do wymogów określonych przez międzynarodowe organizacje do spraw standardów, kierując się wyznaczonymi przez nie normami.

6 BIBLIOGRAFIA

[1] Piotr Czarnecki. *Seminarium eGoverment w Polsce – teraźniejszość i przyszłość.*
[2] Bogdan Księżopolski, Zbigniew Kotulski. *Cryptographic protocol for electronic auctions with extended requirements.* Annales UMCS Informatica 2004.
[3] ETSI TS 102 023: Policy requirements for time-stamping authorities. 2003-01.
[4] ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates. 2002-04.
[5] ISO/IEC 17799: Information technology – Code of practice for information security management. 2000-12-01.
[6] ISO/IEC 19790: Security techniques – Security requirements for cryptographic modules. 2003-06-30.
[7] R.L.Rivest, A.Shamir, and L.M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120-126,1978.
[8] T.ElGamal. A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31:469-472, 1985.
[9] ISO/IEC 18033-2: Security techniques – Encryption algorithms – Part 2: Asymetric cipher. 2003-07-10.
[10] ISO/IEC 18033-3: Security techniques – Encryption algorithms – Part 3: Block cipher. 2003-12-29.
[11] ISO/IEC 14888-3: Security techniques – Digital signatures with appendix – Part 3: Certyficate-based mechanism. 2004-01-02.
[12] K. Kulesza, Z. Kotulski, On Automatic Secret Generation and Sharing for Karin-Greene - Hellman Scheme, in: J. Sołdek, L. Drobiazgiewicz, [ed.], *Artificial Intelligence and Security in Computing Systems*, Kluwer 2003, pp. 281-292. ISBN: 1-4020-7396-8.
[13] B. Hulsebosch, O. Massar, E.J.Godvolk, P.M. Pont, P.Postuma, A. Mahabier – T4D3:Security Architectures Virtual Heaven. 2001.12.21.
[14] Victor Shoup – Research Report: On formal Models for Secure Key Exchange – 1999.04.19.
[15] ISO/IEC 18031: Security techniques – Random bit generation – 2004-01-14.
[16] ISO/IEC 11770-3: Key management-Part 3: Mechanisms using asymmetric techniques. 1999-11-01.

Współczesne Problemy Systemów Czasu Rzeczywistego, Rozdział 31, str. 349-359, Warszawa 2004

Security of e-government – Center of Certifications

Bogdan Księżopolski[1], Zbigniew Kotulski[2]

[1]*Institute of Physics, M. Curie-Skłodowska University,*
Pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland
e-mail:bogdan@kft.umcs.lublin.pl
[2]*Institute of Fundamental Technological Research, Polish Academy of Science,*
ul. Świętokrzyska 21, 00-049 Warsaw, Poland
e-mail:zkotulsk@ippt.gov.pl

Abstract

The aim of presented work is to present the elements of safety of e-government with special attention on Center of Certification. We present norms, which describe requirements which have to be fulfilled in order to set infrastructure of e-government as safe. Norms describe both the network architecture of office as well as cryptographic modules, used for example for realization of individual steps of cryptographic protocols on which the whole communication inside e-government is based. We present also concrete cryptographic modules, which fulfill the current requirements of safety. We present requirements which the component elements of the Center of Certification, that is the Center of Authorization (CA) as well as the Time Stamping Authority (TSA), should fulfill, with special considering of the cryptographic modules. The analysis was conducted for the trustworthy third person, the component of cryptographic protocol realizing the electronic auction[2].