

**Zagrożenia związane z korzystaniem z usługi zawierania umów członkowskich z Amplico OFE i/lub MetLife Amplico DFE, zmiany danych i składania oświadczeń/zawiadomień oraz usługi PTEnet świadczonej drogą elektroniczną oraz zastosowane sposoby ochrony przed nimi.**

1. Zagrożenia związane z transmisją danych przez sieć Internet:

- a) Czy dane, które przesyłam, np. wypełniając formularz na stronie WWW i korzystając z usługi elektronicznej mogą być podsłuchane przez osoby postronne?

Użytkownik Internetu musi liczyć się z faktem możliwości podsłuchania przesyłanych i niezabezpieczonych przez niego danych (nie tylko zawartych formularzach) przez osoby postronne. W odpowiedzi na to zagrożenie powstał protokół SSL (Secure Sockets Layer), dzięki któremu przesyłana informacja jest wymieniana między dostawcą i odbiorcą usługi w sposób zaszyfrowany. Usługodawca musi umożliwić korzystanie z tego protokołu na swoim serwerze, a użytkownik, aby móc korzystać z tego protokołu, musi włączyć jego obsługę w przeglądarce internetowej. Np. w Microsoft Internet Explor w wersji 8 należy z menu wybrać NARZĘDZIA/OPCJE INTERNETOWE/zakładka ZAAWANSOWANE/przewinąć zawartość okna suwakiem pionowym w dół/zaznaczyć kratki przy UŻYJ SSL 3.0 oraz przy UŻYJ TLS 1.0), a następnie nacisnąć przycisk ZASTOSUJ i zamknąć okno. Od tej chwili przeglądarka będzie obsługiwać protokół SSL w wersji trzeciej.

Jeżeli usługodawca potwierdza swą wiarygodność w niezależnej firmie certyfikującej, użytkownik może sprawdzić w certyfikacie, kto wystawił certyfikat, dla kogo, jego czas ważności i stan. W takim przypadku użytkownik może być pewny, że serwer, z którym się połączył jest serwerem, z którym się chciał połączyć. Certyfikat można sprawdzić otwierając właściwości strony WWW i klikając na przycisk CERTYFIKATY (w Internet Explorer w wersji 8).

b) Zagrożenie dla autentyczności, integralności i niezaprzeczalności podpisanego dokumentu w formie elektronicznej podczas korzystania z możliwości podpisywania dokumentów podpisem elektronicznym:

Korzystając z usług świadczonych drogą elektroniczną, obydwu stronom (usługodawca i usługobiorca) zależy na potwierdzeniu tożsamości drugiej strony. Ważne jest również, aby podpisywany przez nie dokument w drodze między nimi (np.: przez sieć Internet) nie zmieniał treści oraz aby po podpisaniu dokumentu strona podpisująca nie mogła oświadczyć, że treść dokumentu została zmieniona lub, że nie był on wcale wysłany.

Dzięki zastosowaniu mechanizmu podpisu elektronicznego, któremu ustawa z dnia 18 września 2001 r. o podpisie elektronicznym nadała moc równoważną z podpisem złożonym ręcznie na dokumentach, możliwe jest zawieranie umów bez obecności stron w jednym czasie i miejscu. Mechanizm podpisu elektronicznego, używający kwalifikowanego certyfikatu, pozwala stwierdzić w niezaprzeczalny sposób, czy treść dokumentu została "po drodze" zmieniona czy nie, czy dokument podpisano ważnym certyfikatem i kto jest jego właścicielem. Ponieważ certyfikat kwalifikowany jest wydawany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, który ma obowiązek sprawdzenia tożsamości osoby ubiegającej się o certyfikat, a także poinformowania tej osoby o warunkach uzyskania i używania certyfikatu oraz o ograniczeniach jego użycia, podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem podpisujący dokument jest dowodem, że został on złożony przez osobę określoną w certyfikacie.

Podpis elektroniczny zapewnia więc autentyczność, integralność i niezaprzeczalność podpisanego dokumentu.

- c) Czy osoby postronne mogą oglądać dane udostępnione w usłudze tylko dla mnie?

Nie, ponieważ dane dotyczące usługobiorcy są zabezpieczone dodatkowym unikalnym identyfikatorem i hasłem, a cała transmisja danych między stronami jest szyfrowana przy użyciu protokołu SSL.

d) ActiveX - mechanizm umożliwiający tworzenie i przesyłanie przez sieć wykonywalnego kodu.

Pozwala na tworzenie między innymi interaktywnych aplikacji i multimedialnych elementów stron WWW. Pozwala na wykonanie operacji na komputerze klienta. Dlatego też odwiedzając witryny internetowe, których nie znamy, warto ustawić przeglądarkę internetową w ten sposób, aby wyświetlała komunikat z pytaniem o zezwolenie na uruchomienie oprogramowania takiego jak formanty ActiveX i dodatki (plug-ins). Np. w Microsoft Internet Explorerze w wersji 8 z menu należy wybrać: NARZĘDZIA/OPCJE INTERNETOWE/zakładka ZABEZPIECZENIA/INTERNET/POZIOM

NIESTANDARDOWY/ Formanty ActiveX i dodatki plugin/ zaznaczyć MONITUJ we wszystkich zakładkach dotyczących pobierania i uruchamiania formantów ActiveX i plug-inów.

## 2. Zabezpieczenie własnego komputera.

- a) Należy na bieżąco aktualizować system operacyjny i używane oprogramowanie. Producenci udostępniają odpowiednie poprawki i uaktualnienia.
- b) Należy zabezpieczyć swój komputer przed wirusami instalując oprogramowanie antywirusowe.
- c) Warto zainstalować personalny firewall, który zabezpieczy komputer przed próbami włamań.
- d) Należy robić kopie zapasowe ważnych danych i przechowywać je na osobnych nośnikach (np.: CDR, CD-RW, taśmy, dyski lub prendrive USB).

## 3. Oprogramowanie lub dane niebędące składnikiem treści usługi wprowadzane przez usługodawcę do systemu teleinformatycznego, którym posługuje się usługobiorca.

- a) cookies - mechanizm umożliwiający usługodawcy np.: odróżnianie osób odwiedzających serwer lub personalizację odwiedzanego serwisu. W naszym przypadku służą do technicznego wsparcia działania formularza. Cookies są informacjami, które serwer zostawia na komputerze klienta. Każdy serwer zostawiający cookies może odczytać tylko informacje, które sam zostawił.
- b) ActiveX - mechanizm umożliwiający tworzenie i przesyłanie przez sieć wykonywalnego kodu. Pozwala na tworzenie, między innymi, interaktywnych aplikacji i multimedialnych elementów stron WWW.

## 4. Przydatne przykładowe adresy stron WWW :

<http://www.microsoft.com/poland>  
<http://windowsupdate.microsoft.com>  
<http://www.mks.com.pl>  
<http://www.symantec.com>  
<http://www.mcafee.pl>  
<http://www.cert.pl>