



Przeznaczenie systemu

PEM-HAERT Seal jest oprogramowaniem udostępniającym interfejs REST do opatrywania dokumentów pieczęcią elektroniczną, której klucze znajdują się na lokalnych urządzeniach HSM jak również w chmurze. PEM-HAERT Seal przeznaczony jest do integracji z systemami informatycznymi wykorzystującymi proces pieczętowania dokumentów.

Pieczęć elektroniczna jest specyficznym procesem, wykorzystującym mechanizmy podpisu elektronicznego do zapewnienia autentyczności i integralności dokumentów opatrywanych taką pieczęcią. O ile klasyczny podpis elektroniczny wykorzystywany jest przez konkretne osoby, pieczęć elektroniczna wykorzystywana jest przez podmioty posiadającą osobowość prawną. Z pieczęci mogą korzystać np. firmy, instytucje, urzędy, czy jednostki im podległe. Możliwe jest także wykorzystanie jej w ich oddziałach, delegaturach, filiach, przedstawicielstwach. W przypadku klasycznego podpisu elektronicznego podpisuje się konkretna osoba, znana z imienia i nazwiska, w przypadku zastosowania pieczęci elektronicznej podpisuje się konkretna instytucja – bez danych osobowych. Pieczęć elektroniczna nie jest więc alternatywą dla stosowania podpisu, stosujemy ją gdy ważne jest potwierdzenie prawdziwości wystawcy dokumentu oraz jego niezmięność zawartości. Można więc powiedzieć, że pieczęć elektroniczna jest odpowiednikiem stosowania tradycyjnej pieczętki firmowej, zapewniając jednocześnie dodatkowe korzyści.

Takie działanie systemu jest szczególnie przydatne, gdy instytucja wykorzystująca pieczęć nie chce, aby dane osobowe pracowników były uwidocznione w firmowej wymianie dokumentów elektronicznych. Typowym przykładem jest pracownik BOK wystawiający fakturę lub zamówienie i pieczętujący je kwalifikowaną pieczęcią firmową. Mimo iż nie mamy potwierdzenia tego, kto konkretnie w imieniu danej instytucji dokonał pieczętowania, możemy potwierdzić, że dokument pochodzi z odpowiedniej instytucji, i nie został zmieniony w sposób nieuprawniony.

Korzyści, jakie daje stosowanie pieczęci elektronicznej można podsumować w kilku punktach:

- Umożliwia automatyzację procesów wydawania dokumentów.
- Umożliwia usprawnienie istniejących procesów, opartych o podpis elektroniczny.
- Umożliwia masowe pieczętowanie dokumentów.
- Zapewnia uwierzytelnianie dokumentów pochodzących z danej instytucji.
- Zapewnia integralność, przez informację o ewentualnej modyfikacji dokumentu.



Komponenty systemu

Dedykowany komponent sprzętowy posiada następujące parametry:

- Wbudowany czytnik kart kryptograficznych.
- Wbudowany wyświetlacz led.
- Wbudowana klawiatura numeryczna.
- Pamięć RAM 32GB z możliwością rozszerzenia.
- Dysk twardy 1TB z możliwością rozszerzenia.



Działanie systemu

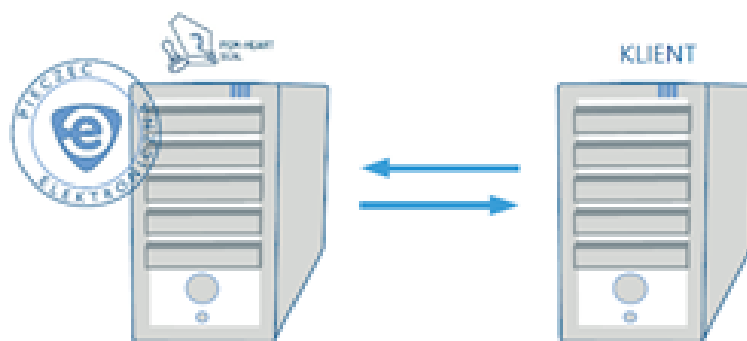
Zgodnie z obecnym stanem prawnym, możliwe jest stworzenie usług pieczętowania elektronicznego w dwóch modelach:

- Zaawansowana pieczęć elektroniczna
- Kwalifikowana pieczęć elektroniczna

Z technicznego punktu widzenia obie usługi realizowane są w oparciu o te same narzędzia, różnicę stanowi wykorzystanie w tej drugiej kwalifikowanych środków technicznych i kwalifikowanego certyfikatu kluczy służących do pieczętowania dokumentów. Oba modele usługi muszą posiadać funkcje zapewniające bezpieczeństwo. Po pierwsze muszą zapewniać unikalność osoby prawnej, która składa pieczęć i pozwalać na rozpoznanie tożsamości tej instytucji.

Muszą także zapewniać, że osoba lub podmiot pieczętująca dokument ma kontrolę nad danymi służącymi do jej składania. Kolejnym składnikiem takiej usługi jest to, że zmiany dokonywane na dokumencie opatrywanym pieczęcią muszą być rozpoznawalne.

System **PEM-HEART Seal** jest narzędziem umożliwiającym budowę usługi pieczęci zarówno dla modelu Zaawansowanego, jak i Kwalifikowanego, w zależności od decyzji instytucji, decydującej się na uruchomienie usługi pieczętowania. Jedna instalacja systemu umożliwia obsługę wielu pieczęci kwalifikowanych lub niekwalifikowanych.



PEM-HEART Seal udostępnia niezbędne interfejsy API, pozwalające integrować system z innymi aplikacjami. Dokumenty, które powinny zostać opatrzone pieczęcią mogą zostać przesłane do serwera na którym uruchomiono PEM-HEART Seal, gdzie opatrywane są pieczęcią elektroczną, a następnie odsyłane na odpowiedni zasób dyskowy lub do API zewnętrznego systemu. Istnieje również tryb działania systemu, w którym nie ma konieczności przesyłania całego dokumentu do serwera PEM-HEART Seal – w takim modelu wysyłany jest jedynie skrót kryptograficzny opieczętownianego dokumentu, wykonany z użyciem odpowiedniego oprogramowania. Skrót ten jest wystarczający do wykonania pieczęci – w takim wypadku system zapewnia także poufność danych – w tym sensie, że konkretne dane zawarte w pieczętowanym dokumencie nie są przesyłane do komponentu wykonującego proces pieczętowania.

W przypadku uruchomienia usługi w wariantcie chmurowym, ma to niebagatelne znaczenie. Oprogramowanie obsługuje następujące formaty podpisów elektronicznych: XAdES, PAdES, CAdES.

W skład **PEM-HEART Seal** wchodzi komponent serwerowy i aplikacja administracyjna. Oprogramowanie można zainstalować na maszynach wirtualnych, lub na dedykowanym bezpiecznym komponencie sprzętowym instalowanym w szafie RACK.

