CENTAUR EST

Enigma Centaur to rodzina dojrzałych, rozwijanych od ponad 20 lat, produktów przeznaczonych do konstruowania systemów informatycznych, pozwalających na tworzenie i wykorzystywanie podpisu elektronicznego – czyli tzw. systemów infrastruktury klucza publicznego (z ang. PKI – Public Key Infrastructure).

Przeznaczenie

Centaur EST jest modułem systemu Centaur realizującym protokół EST (Enrollment over Secure Transport). EST umożliwia przekazywanie certyfikatów dla serwerów WWW, urządzeń końcowych i użytkowników, a także dla każdego innego rozwiązania, w którym używane są certyfikaty PKI. Głównym zastosowaniem EST jest automatyzacja procesów certyfikacji urządzeń sieciowych. EST jest następcą protokołu SCEP - jest łatwiejszy do wdrożenia na urządzeniach już posiadających stos HTTPS. EST używa protokołu HTTPS jako transportu i wykorzystuje TLS dla wielu swoich atrybutów bezpieczeństwa. Centaur EST implementuje zarówno podstawową wersję protokołu wyspecyfikowaną w RFC 7030 jak również rozszerzoną z RFC 8295. EST obecnie jest wspierany przez wiodących producentów sprzętu – takich jak np. CISCO, Aruba, IBM, Stormshield. EST standaryzuje uwierzytelniony proces wymiany żądań i odpowiedzi z CA, dzięki czemu jest bezpieczniejszy, a także szybszy i łatwiejszy dla zespołów IT do wdrażania certyfikatów w systemach i urządzeniach niż ręczne przekazywanie wymaganych informacji. EST obsługuje także zaawansowane algorytmy kryptograficzne oparte na krzywych eliptycznych (ECC, ECDSA), które obecnie są coraz częściej wykorzystywane w kryptografii, a nie są obsługiwane przez wcześniej użytkowany protokół SCEP.

Nie ma obecnie silniejszego, łatwiejszego w użyciu rozwiązania do uwierzytelniania i szyfrowania niż tożsamość cyfrowa zapewniana przez PKI. Barierą we wdrażaniu opartych o nie rozwiązań jest fakt, iż obciążone podstawowymi zadaniami zespoły IT nie mogą sobie pozwolić na ręczne wdrażanie certyfikatów i zarządzanie nimi, ponieważ jest to czasochłonne i wysoce podatne na błędy oraz może tworzyć niepotrzebne ryzyka. Niezależnie od tego, czy organizacja wdraża pojedynczy certyfikat SSL dla serwera internetowego, czy zarządza milionami certyfikatów we wszystkich punktach końcowych w sieci, urządzeniach mobilnych i tożsamościach użytkowników w organizacji, proces ręcznego udostępniania certyfikatu, od wystawienia do konfiguracji, a następnie wdrożenia, może zająć nawet kilka godzin. Przy niewłaściwej implementacji, gdzie brak zarządzania odwołanymi certyfikatami, a ich status nie jest na bieżąco sprawdzany - ręczne zarządzanie certyfikatami może narazić przedsiębiorstwa na ryzyko, że fakt wygaśnięcia certyfikatów zostanie przeoczony, co skutkować może nagłym wyłączeniem krytycznych systemów biznesowych i narażeniem na złośliwe ataki.

Biorąc pod uwagę wiele potencjalnych pułapek związanych z ręcznym zarządzaniem certyfikatami PKI, organizacje potrzebują standardowego certyfikatu automatyzacji zarządzania, takiego jak EST, aby upewnić się, że certyfikaty są prawidłowo konfigurowane i wdrażane na dużą skalę bez interwencji człowieka. Poziom automatyzacji zapewniany przez EST nie tylko pomaga zmniejszyć ryzyko, ale także pozwala administratorom IT oszczędzać czas.

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.

Oprócz funkcji rejestracji certyfikatu klient EST może odnowić lub ponownie wyznaczyć swój istniejący certyfikat, przesyłając żądanie ponownej rejestracji do Centaur EST.

Działanie systemu

W architekturze PKI Centaur EST znajduje się między klientem a urzędem certyfikacji Centaur CCK i wykonuje kilka funkcji tradycyjnie przypisywanych do roli urzędu rejestracji (RA). Jego zadaniem jest sprawdzenie, czy klienci EST powinni otrzymać certyfikat, którego zażądali, czy nie. Jeśli tak, przekazuje żądanie do urzędu certyfikacji i zwraca otrzymany certyfikat do klienta. Klient komunikuje się z serwerem EST, który nasłuchuje żądań na standardowej ścieżce URL. Klienci muszą tylko znać adres IP serwera, aby wysyłać żądania.

Miejsce instalacji systemu

Oprogramowanie można zainstalować na maszynach wirtualnych, lub na dedykowanym bezpiecznym komponencie sprzętowym instalowanym w szafie RACK.

Zalety Centaur EST w porównaniu do modułu SCEP

Bezpieczny transport danych

Wszystkie żądania i odpowiedzi klientów i serwerów są przesyłane za pośrednictwem protokołu TLS bez potrzeby uwierzytelniania wiadomości przez zakodowanie ich za pomocą wspólnego sekretu, tak jak to odbywa się przy zastosowaniu SCEP, lub hasła, tak jak odbywa się to przy użyciu protokołu Automated Certificate Management Environment (ACME).

Autoryzacja podmiotów pozyskujących certyfikaty

W przypadku EST żądanie podpisania certyfikatu (CSR) może być powiązane ze ściśle określonym zaufanym podmiotem żądającym, który jest uwierzytelniany za pomocą protokołu TLS. Za pomocą SCEP żądanie CSR jest uwierzytelniane przy użyciu wspólnego sekretu między klientem a urzędem certyfikacji, co stwarza zagrożenie bezpieczeństwa w przypadku utraty lub ujawnienia wspólnego sekretu.

Generowanie klucza po stronie serwera

Generowanie klucza po stronie serwera jest konieczne w przypadku środowisk urządzeń, które nie mają możliwości generowania losowego klucza prywatnego. SCEP obsługuje tylko generowanie klucza prywatnego na kliencie, podczas gdy EST umożliwia serwerowi generowanie klucza prywatnego.

Automatyczne odnawianie certyfikatu

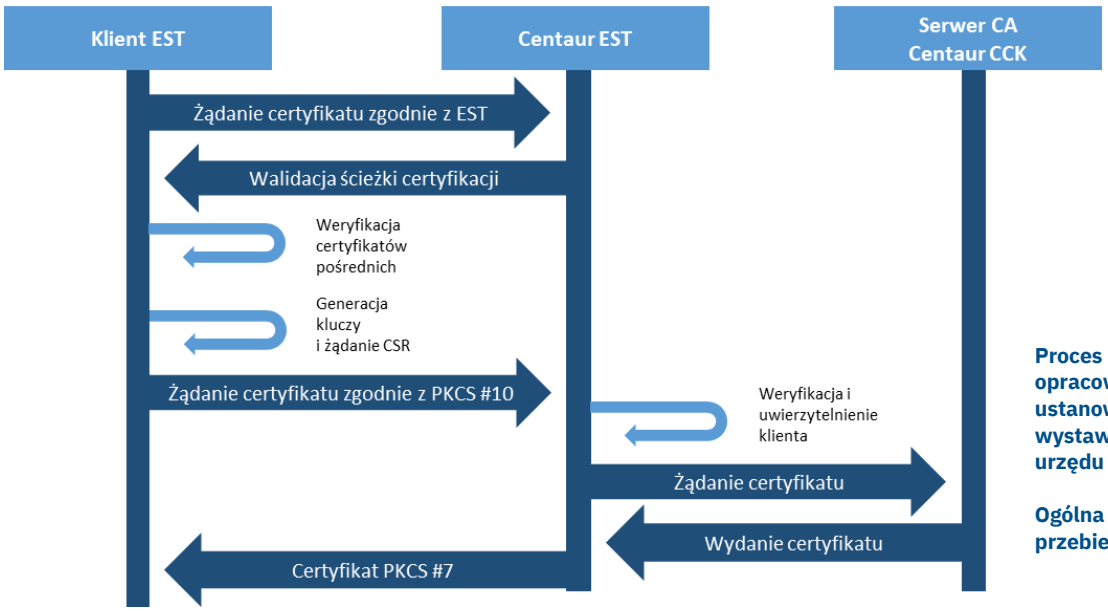
EST został opracowany w celu obsługi automatycznej recertyfikacji. Chociaż niedawno przesłana wersja robocza aktualizacji SCEP wprowadza komunikaty o odnowieniu, SCEP wcześniej nie obsługiwał recertyfikacji. W rezultacie wiele istniejących wdrożeń SCEP wymaga od zespołów IT dokonywania istotnych aktualizacji systemów administracyjnych w celu obsługi automatycznego odnawiania certyfikatów.

Odwołane certyfikaty

SCEP obsługuje tylko sprawdzanie statusu certyfikatów w oparciu o listy CRL. Przy wykorzystaniu EST obsługiwany jest protokół OCSP (Online Certificate Status Protocol) co umożliwia natychmiastowe i każdorazowe sprawdzanie statusu używanych przez urządzenia certyfikatów kluczy.

Obsługa zaawansowanych algorytmów

EST obsługuje algorytmy ECC i ECDSA, których SCEP nie obsługuje.



Proces rejestracji EST został opracowany tak, aby ułatwić ustanowienie automatycznego wystawiania certyfikatów z zaufanego urzędu certyfikacji.

Ogólna interakcja klient/serwer przebiega zgodnie ze schematem.

- Klient inicjuje sesję HTTP zabezpieczoną TLS z serwerem EST i weryfikuje certyfikat oferowany przez serwer.
- Klient żąda i weryfikuje ścieżkę certyfikacji z serwera, w tym wszelkie certyfikaty pośrednie, które znajdują się między urzędem Root CA i Centaur EST, i przechowuje certyfikat główny.
- Klient generuje klucz i CSR, a następnie żądanie certyfikatu PKCS #10 i wysyła je do Centaur EST.
- Centaur EST żąda i odbiera certyfikat wystawiony z urzędu certyfikacji, a następnie zwraca podpisany certyfikat do klienta w formacie PKCS #7 w celu przechowywania na urządzeniu klienckim.