Przewodnik dla Partnerów: Zasady Zapewnienia Bezpieczeństwa i Integralności Procesów Certyfikacyjnych

Wprowadzenie

Jako Urząd Certyfikacji (CA) oraz dostawca usług zaufania, dążymy do utrzymania wysokich standardów bezpieczeństwa i zaufania.

Ten przewodnik jest skierowany do naszych partnerów. Partnerzy odgrywają kluczową rolę w zbieraniu dokumentów weryfikacyjnych, przesyłaniu ich za pośrednictwem API lub portalu CertManager oraz umożliwianiu wydawania certyfikatów za pośrednictwem sub-rootów (subCA) z marką partnera.

Celem tego przewodnika jest zapewnienie integralności i bezpieczeństwa procesu przesyłania dowodów weryfikacyjnych oraz zarządzania cyklem życia certyfikatu.

Nasi partnerzy wchodzą w interakcje z operacjami związanymi z cyklem życia certyfikatów za pomocą wyznaczonego API lub konta w portalu CertManager zarządzanym przez Certum.

Bezpieczne zbieranie dowodów weryfikacyjnych dla różnych typów weryfikacji

1. Minimalizacja danych

- Zbieraj tylko niezbędne dowody weryfikacyjne wymagane do wydania certyfikatu. Unikaj zbierania zbędnych lub wrażliwych informacji, aby zapewnić zgodność z normami ochrony danych.

2. Bezpieczne metody zbierania

- Używaj szyfrowanych kanałów (takich jak HTTPS, chronione hasłem i szyfrowane konta klientów, szyfrowane formularze, szyfrowane wiadomości e-mail oraz załączniki chronione hasłem) do zbierania dowodów weryfikacyjnych od użytkowników końcowych, aby zapewnić ochronę wrażliwych danych.
- Podpisuj całą korespondencję e-mailową wysyłaną do klientów za pomocą certyfikatu S/MIME, aby zapewnić jej integralność.

3. Kontrola dostępu

- Ogranicz dostęp do dowodów weryfikacyjnych tylko do upoważnionych osób. Wymagaj stosowania uwierzytelniania wieloskładnikowego (MFA), aby zwiększyć bezpieczeństwo i zredukować ryzyko nieautoryzowanego dostępu.

4. Integralność danych

- Wdrażaj środki zapewniające, że dowody weryfikacyjne nie zostaną zmienione podczas zbierania. Obejmuje to zarówno środki techniczne, jak i nadzór nad procesem.

5. Weryfikacja subskrybenta

- Podczas weryfikacji danych subskrybenta należy bezwzględnie przestrzegać obowiązujących standardów. Partnerzy nie powinni przekazywać dokumentów, które budzą wątpliwości lub nie spełniają wymagań Certum. Ponadto, wszelkie przypadki podejrzenia nadużycia w procesie weryfikacji – nawet jeśli zostaną wykryte po wydaniu certyfikatu – muszą zostać niezwłocznie zgłoszone do Certum.

Bezpieczne przesyłanie dokumentów weryfikacyjnych do Certum

1. Bezpieczeństwo API

- Korzystaj wyłącznie z wyznaczonego API lub portalu CertManager do przesyłania dokumentów weryfikacyjnych. Przesyłanie materiałów weryfikacyjnych może odbywać się również za pośrednictwem poczty elektronicznej, w takim przypadku upewnij się, że wiadomości e-mail są szyfrowane i/lub załączniki są zabezpieczone hasłem.

2. Przesyłanie przez API/ CertManager

- Podczas przesyłania dokumentów bezpośrednio przez portal CertManager, upewnij się, że są one powiązane wyłącznie z odpowiednim zamówieniem certyfikatu. Nie przesyłaj dokumentów niezwiązanych z danym zamówieniem.

3. Regularne audyty

- Przeprowadzaj regularne audyty logów z przesyłania dowodów, aby wykryć i zapobiec wszelkim nieautoryzowanym przesyłaniom dokumentów lub nieprawidłowościom w procesie.

4. Reakcja na incydenty

- Miej jasno określony plan reakcji na incydenty w przypadku jakichkolwiek nieprawidłowości lub naruszeń procesu przesyłania dokumentów. W przypadku wykrycia nieprawidłowości, niezwłocznie powiadom nas o tym w celu zbadania i rozwiązania problemu.

Najlepsze praktyki w zakresie korzystania z API operacji cyklu życia certyfikatów

1. Limitowanie liczby żądań

- Zwróć uwagę na limity liczby żądań na API, aby uniknąć przypadkowych zakłóceń w usługach i zapewnić płynne działanie procesów.

2. Monitorowanie i logowanie

- Wdroż ciągłe monitorowanie aktywności w API. Prowadź szczegółowe logi wszystkich interakcji i regularnie je przeglądaj pod kątem podejrzanej lub nieautoryzowanej aktywności.
- Regularnie zbieraj informacje o pracownikach posiadających dane dostępowe do CertManagera i okresowo je weryfikuj. W przypadku zakończenia współpracy z pracownikiem lub zmiany jego roli – niezwłocznie cofnij dostęp.
- Uwierzytelniaj wyłącznie adresy IP urządzeń, nad którymi masz pełną kontrolę i które spełniają wysokie standardy bezpieczeństwa systemowego w kontekście połączeń z API. Okresowo monitoruj listę uwierzytelnionych adresów IP i zgłaszaj usunięcie tych, które nie powinny już mieć dostępu do API.

3. Obsługa błędów

- Opracuj jasne procedury obsługi błędów API. Szybko rozwiązuj wszelkie nieprawidłowości lub problemy i powiadamiaj nas o potrzebie pomocy, jeśli jest to konieczne.

Zachowanie bezpieczeństwa witryny internetowej i infrastruktury serwerowej

1. Prawidłowa konfiguracja serwera TLS

- Upewnij się, że Twój serwer obsługuje tylko silne szyfrowanie i protokoły kryptograficzne. Regularnie aktualizuj i łataj serwery, aby wyeliminować luki w zabezpieczeniach.

2. Zabezpieczanie systemu operacyjnego

- Ogranicz liczbę usług uruchamianych na serwerze. Stosuj łatki bezpieczeństwa w odpowiednim czasie i wykorzystuj narzędzia do zarządzania konfiguracją w celu wzmocnienia zabezpieczeń.

3. Zarządzanie lukami

- Regularnie skanuj witrynę i serwery w poszukiwaniu popularnych luk, na przykład, SQL Injection, Cross-Site Scripting (XSS) czy Cross-Site Request Forgery (CSRF) i inne, i niezwłocznie usuwaj wszelkie problemy.

4. Wymagania wobec haseł

- Upewnij się, że hasła są silne i trudne do odgadnięcia. Zalecaj stosowanie uwierzytelniania wieloskładnikowego (MFA), szczególnie w przypadku systemów krytycznych.

Wymagania bezpieczeństwa CA/B Forum i Systemów Certyfikacji

1. Kwartalne skany podatności

- Przeprowadzaj skany podatności co kwartał, aby zidentyfikować i usunąć potencjalne zagrożenia. Działaj szybko, aby rozwiązać zidentyfikowane problemy.

2. Coroczne testy penetracyjne

- Przeprowadzaj testy penetracyjne co najmniej raz do roku. Użyj tych testów, aby wykryć potencjalne słabości w infrastrukturze i praktykach zarządzania certyfikatami.

3. Zgodność z normami bezpieczeństwa

- Zapewnij zgodność z wymaganiami CA/B Forum Network and Certificate Systems Security Requirements. Jest to kluczowe dla utrzymania zaufania i integralności procesu wydawania certyfikatów i zarządzania cyklem ich życia.

Promowanie najlepszych praktyk w zakresie generowania, przechowywania i zarządzania kluczami przez użytkowników końcowych

1. Edukacja na temat generowania kluczy

- Zachęcaj użytkowników końcowych do korzystania z narzędzi zatwierdzonych przez CA do generowania kluczy i tworzenia CSR. Zapewnia to zgodność i bezpieczeństwo.

2. Długość klucza i algorytm

- Zalecaj użytkownikom końcowym stosowanie silnych algorytmów kryptograficznych i długości kluczy, nawet wyższych niż RSA 2048-bit, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa certyfikatów.

3. Bezpieczne przechowywanie kluczy prywatnych

- Doradź użytkownikom końcowym przechowywanie kluczy prywatnych w bezpieczny sposób, najlepiej w modułach sprzętowych (HSM) lub innych rozwiązaniach szyfrujących.

4. Rotacja kluczy i unieważnianie

- Zachęcaj do regularnej rotacji kluczy i unieważniania kluczy, które nie są już potrzebne lub zostały skompromitowane. Wdrażaj politykę szybkiego unieważniania kluczy w przypadku incydentów bezpieczeństwa.

5. Strategia reagowania na katastrofy

- Opracuj szczegółowy i skuteczny plan reagowania na incydenty w przypadku kompromitacji, utraty lub uszkodzenia klucza. Plan ten powinien zawierać jasne kroki dotyczące odzyskiwania kluczy lub minimalizowania związanego z tym ryzyka.

Zapewnienie komunikacji z użytkownikiem końcowym w zakresie statusu certyfikatu i kodów weryfikacyjnych

W sytuacjach, gdy partnerzy nie chcą, aby Certum wysyłało informacje lub wiadomości weryfikacyjne bezpośrednio do użytkowników końcowych, to na partnerach spoczywa obowiązek zapewnienia dostarczenia tych komunikatów za pośrednictwem alternatywnych, bezpiecznych kanałów. Brak terminowego i dokładnego przekazania informacji weryfikacyjnych może opóźnić wydanie certyfikatu lub negatywnie wpłynąć na doświadczenie użytkownika. Partnerzy muszą wdrożyć niezawodne mechanizmy umożliwiające:

- Powiadamianie użytkowników końcowych o statusie ich wniosku o certyfikat.
- Przekazywanie wymaganych linków do weryfikacji domeny.
- Zapewnienie, że metody dostarczania są bezpieczne, możliwe do śledzenia i zgodne z przepisami o ochronie danych.

Podsumowanie

Zaufanie do naszego Urzędu Certyfikacji oraz naszych partnerów jest kluczowe dla utrzymania integralności ekosystemu certyfikatów cyfrowych. Stosując się do tych najlepszych praktyk, przyczyniacie się do zabezpieczenia całego procesu wydawania certyfikatów, ochrony danych użytkowników końcowych oraz utrzymania zaufania do usług, które świadczymy.

Zachęcamy naszych partnerów do ścisłego przestrzegania przedstawionych zasad, które wspierają bezpieczeństwo i integralność operacji związanych z certyfikatami oraz zgodność z najlepszymi praktykami. W przypadku pytań lub potrzeby dodatkowych informacji prosimy o kontakt. Razem możemy utrzymać niezawodność i zaufanie do naszych usług cyfrowych.