NUMER DOKUMENTU: 2022-0941
IDENTYFIKATOR KLASYFIKACJI:
3.2.3

Ramy zaufania

dotyczące szwedzkiej identyfikacji elektronicznej

Wersja z 04 października 2022 r.

1. Kontekst i cel

Ramy zaufania dotyczące szwedzkiej identyfikacji elektronicznej służą ustanowieniu wspólnych wymogów dla podmiotów wydających środki identyfikacji elektronicznej, które zostały poddane przeglądowi i zatwierdzone przez szwedzką Agencję Administracji Cyfrowej (DIGG). Wymogi podzielono na różne poziomy ochrony – nazywane poziomami bezpieczeństwa – które odpowiadają różnym stopniom bezpieczeństwa technicznego i operacyjnego po stronie wydawcy oraz różnym stopniom weryfikacji, czy osoba, której wydano dokument identyfikacji elektronicznej, rzeczywiście jest osobą, za którą się podaje.

Wymogi zawarte w niniejszych ramach zaufania mają zastosowanie do poziomów bezpieczeństwa 2–4, przy czym poziom 4 odpowiada najwyższemu poziomowi ochrony.

Zgodność interpretuje się w następujący sposób:

(a) w przypadku gdy poziom bezpieczeństwa nie jest określony, wymóg musi być spełniony na wszystkich poziomach, oraz

(b) w przypadku gdy poziom bezpieczeństwa jest określony, zgodność zapewnia się co najmniej na odpowiednim poziomie.

Nie uwzględnia się wymogów ustalonych dla poziomu niższego niż odpowiedni.

2. Organizacja i zarządzanie

Ogólne wymogi operacyjne

K2.1 Wydawcy szwedzkich środków identyfikacji elektronicznej (eID), którzy nie są organami publicznymi, działają jako zarejestrowane osoby prawne oraz zawierają i utrzymują ubezpieczenie wymagane do prowadzenia działalności.

K2.2 Wydawcy szwedzkich eID muszą mieć zarejestrowaną działalność, być w pełni operacyjni we wszystkich aspektach określonych w niniejszym dokumencie oraz dobrze zorientowani w wymogach prawnych nałożonych na nich jako wydawców szwedzkich eID.

K2.3 Wydawcy szwedzkich eID muszą być w stanie ponieść ryzyko odpowiedzialności za szkody i posiadać wystarczające środki finansowe na prowadzenie działalności przez co najmniej jeden rok.

Bezpieczeństwo informacji

K2.4 Wydawcy szwedzkich eID ustanawiają system zarządzania bezpieczeństwem informacji (ISMS) dla części ich działalności, na które mają wpływ ramy zaufania, oparty, w stosownych przypadkach, na normie ISO/IEC 27001 lub równoważnych zasadach zarządzania i kontroli prac w zakresie bezpieczeństwa informacji, w tym:

(a) Wszystkie procesy administracyjne i techniczne mające kluczowe znaczenie dla bezpieczeństwa muszą być udokumentowane i oparte na formalnych podstawach, w których role, obowiązki i uprawnienia są jasno określone.

(b) Wydawcy szwedzkich eID zapewniają, aby w każdym momencie dysponowali wystarczającymi zasobami ludzkimi w celu wypełniania swoich obowiązków.

(c) Wydawcy szwedzkich eID ustanawiają proces zarządzania ryzykiem, który w odpowiedni sposób, w sposób ciągły lub co najmniej raz na 12 miesięcy, analizuje zagrożenia i słabe punkty w działalności oraz który, poprzez wprowadzenie środków bezpieczeństwa, równoważy ryzyko do dopuszczalnego poziomu.

(d) Wydawcy szwedzkich eID ustanawiają proces zarządzania incydentami, który systematycznie zapewnia jakość usługi, formy dalszego zgłaszania oraz podejmowanie odpowiednich środków reaktywnych i zapobiegawczych w celu ograniczenia szkód wynikających z takich zdarzeń lub zapobieżenia im.

(e) Wydawcy szwedzkich eID ustanawiają i regularnie testują plan ciągłości działania, który spełnia wymogi dostępności przedsiębiorstwa dzięki możliwości przywrócenia krytycznych procesów w przypadku kryzysu lub poważnych incydentów.

(f) Wydawcy szwedzkich eID regularnie oceniają prace związane z bezpieczeństwem informacji i wprowadzają środki usprawniające w systemie zarządzania.

K2.5 Zakres i dojrzałość systemu zarządzania:

Poziom 4: System zarządzania bezpieczeństwem informacji musi być zgodny z normą SS-ISO/IEC 27001:2017 lub równoważnymi późniejszymi lub międzynarodowymi wersjami normy, a w ramach tego zakresu musi obejmować wszystkie wymogi nałożone na wydawców szwedzkich eID.

Warunki podwykonawstwa

K2.6 Wydawca szwedzkich eID, który zlecił wykonanie jednego lub większej liczby procesów krytycznych dla bezpieczeństwa innej stronie, określa w umowie, za które procesy krytyczne odpowiada podwykonawca i jakie wymogi mają do nich zastosowanie, oraz wyjaśnia stosunek umowny w oświadczeniu wydawcy.

Identyfikowalność, usuwanie i przechowywanie dokumentów

K2.7 Wydawcy szwedzkich eID przechowują:

(a) dokumenty związane ze składaniem wniosków i dokumenty związane z wydawaniem, otrzymywaniem lub blokowaniem eID;

(b) umowy, dokumenty programowe i oświadczenia wydawcy oraz

(c) historię przetwarzania i inne dokumenty wymagane w celu udowodnienia zgodności z wymogami nałożonymi na wydawców szwedzkich eID i które umożliwiają podjęcie działań następczych wykazujących, że procesy i kontrole o krytycznym znaczeniu dla bezpieczeństwa zostały wdrożone i są skuteczne.

K2.8 Okres przechowywania nie może być krótszy niż pięć lat, a materiały muszą być dostępne w czytelnej formie przez cały ten okres, chyba że wymóg usunięcia uzasadniają względy prywatności, a jego podstawę prawną stanowią przepisy ustawowe lub wykonawcze.

Przegląd i działania następcze

K2.9 Wydawcy szwedzkich eID ustanawiają funkcję audytu wewnętrznego, która ma na celu okresowy przegląd działalności w zakresie wydawania. Audytor wewnętrzny jest niezależny w wykonywaniu swoich obowiązków w sposób zapewniający obiektywną i bezstronną kontrolę oraz posiada kompetencje i doświadczenie wymagane do wykonywania swoich obowiązków. Audytor wewnętrzny niezależnie planuje przeprowadzenie audytu i dokumentuje to w planie audytu obejmującym okres trzech lat. Elementy audytu są wybierane na podstawie analizy ryzyka i istotności i opierają się na opisach operacji przedłożonych przez wydawcę do Agencji Administracji Cyfrowej.

Poziomy 3 i 4: Audyt wewnętrzny przeprowadza się na podstawie przyjętych standardów audytu.

3. Bezpieczeństwo fizyczne, administracyjne i osobowe

K3.1 Centralne części operacji są fizycznie chronione przed uszkodzeniem w wyniku zdarzeń środowiskowych, nieuprawnionego dostępu lub innych zakłóceń zewnętrznych. Kontrolę dostępu stosuje się w taki sposób, aby dostęp do obszarów wrażliwych był ograniczony do upoważnionego personelu, nośniki informacji były bezpiecznie przechowywane i usuwane, a dostęp do tych obszarów chronionych podlegał stałemu monitorowaniu.

K3.2 Przed objęciem przez osobę którejkolwiek z ról określonych zgodnie z K2.4 lit. a) i mających szczególne znaczenie dla bezpieczeństwa wydawca szwedzkich eID przeprowadza weryfikację przeszłości w celu upewnienia się, że osobę tę można uznać za wiarygodną oraz że posiada ona kwalifikacje i przeszkolenie wymagane do bezpiecznego i pewnego wykonywania zadań wynikających z pełnionej funkcji.

K3.3 Wydawcy stosują procedury zapewniające, aby dostęp do danych gromadzonych i przechowywanych zgodnie z K2.7 miał wyłącznie specjalnie upoważniony personel.

K3.4 **Poziomy 3 i 4:** Wydawcy dopilnowują w całym łańcuchu procesu wydawania, aby rozdzielenie obowiązków było stosowane w taki sposób, by żadna pojedyncza osoba nie była w stanie uzyskać środka identyfikacji elektronicznej w imieniu innej osoby.

4. Bezpieczeństwo techniczne

K4.1 Wydawcy szwedzkich eID zapewniają, aby stosowane kontrole techniczne były wystarczające do osiągnięcia poziomu ochrony uznanego za niezbędny zważywszy na charakter, zakres i inne okoliczności prowadzenia działalności oraz aby kontrole te funkcjonowały i były skuteczne.

K4.2 Elektroniczne środki komunikacji wykorzystywane do przekazywania danych wrażliwych muszą być chronione przed przechwyceniem, manipulacją i ponownym odtworzeniem.

K4.3 Wrażliwy kryptograficzny materiał klucza wykorzystywany do wydawania eID, identyfikacji posiadaczy i wydawania certyfikatów tożsamości jest chroniony w taki sposób, aby:

(a) dostęp był ograniczony, pod względem logicznym i fizycznym, do ról i aplikacji, które są ściśle niezbędne;

(b) materiał klucza nigdy nie był przechowywany w postaci zwykłego tekstu na trwałych nośnikach danych;

(c) materiał klucza był chroniony za pomocą kryptograficznego modułu sprzętowego z aktywnymi mechanizmami bezpieczeństwa, które przeciwdziałają zarówno fizycznym, jak i logicznym próbom naruszenia bezpieczeństwa materiału klucza;

(d) mechanizmy bezpieczeństwa służące ochronie materiału klucza były przejrzyste i oparte na uznanych i ugruntowanych standardach oraz

(e) **Poziomy 3 i 4:** danymi aktywacyjnymi do ochrony materiału klucza zarządza się za pomocą kontroli wieloosobowej.

K4.4 Wydawcy dysponują udokumentowanymi procedurami zapewniającymi utrzymanie wymaganego poziomu ochrony w odpowiednim środowisku informatycznym w miarę upływu czasu i w związku ze zmianami, w tym regularnymi ocenami podatności oraz odpowiednią gotowością do sprostania zmieniającym się poziomom ryzyka i występującym incydentom.

5. Zgłoszenie, identyfikacja i rejestracja

Informacje o warunkach

K5.1 Wydawcy szwedzkich eID przekazują informacje na temat umów, warunków i zasad, a także powiązane informacje oraz wszelkie ograniczenia dotyczące korzystania z usługi użytkownikom połączonym, dostawcom usług elektronicznych i innym osobom, które mogą polegać na usłudze wydawcy.

K5.2 Wydawca szwedzkich eID wyraźnie odnosi się do warunków i opracowuje procedury w taki sposób, aby warunki te były przekazywane wnioskodawcy w procesie wydawania.

K5.3 Wydawcy szwedzkich eID przedstawiają deklarację wydawcy zawierającą:

(a) tożsamość i dane kontaktowe wydawcy;

(b) krótki opis usług i rozwiązań zapewnianych przez wydawcę, w tym stosowanych metod składania wniosków, wydawania i blokowania;

(c) warunki związane ze świadczoną usługą, w tym obowiązki użytkownika w zakresie ochrony jego eID, obowiązki i odpowiedzialność wydawcy, wszelkie udzielone gwarancje oraz deklarowaną dostępność;

(d) informacje na temat przetwarzania danych osobowych i sposobu, w jaki jest ono realizowane oraz

(e) ustalenia dotyczące zmiany warunków lub innych postanowień dotyczących świadczonej usługi, w tym kroków, jakie należy podjąć w celu zaprzestania świadczenia usługi w kontrolowany sposób.

K5.4 **Poziomy 3 i 4:** Na wniosek Agencji Administracji Cyfrowej (DIGG) lub innej umawiającej się strony, która korzysta z usług świadczonych przez wydawcę, emitenci szwedzkich eID przekazują informacje na temat własności przedsiębiorstwa oraz sposobu zarządzania nim.

K5.5 Wydawca szwedzkich eID, który zaprzestaje działalności, stosuje wcześniej ustalony plan zaprzestania świadczenia usługi. Plan obejmuje poinformowanie wszystkich użytkowników usługi i DIGG. Wydawca przechowuje ponadto materiały archiwalne dostępne zgodnie z K2.7 i K2.8 po zaprzestaniu świadczenia usługi.

Składanie wniosków

K5.6 Szwedzki eID może zostać wydany wyłącznie na wniosek wnioskodawcy lub w ramach innej równoważnej procedury akceptacji i dopiero po poinformowaniu wnioskodawcy o warunkach, na jakich jest wydawany, oraz o odpowiedzialności, jaka zostanie na niego nałożona.

Wydanie środka identyfikacji elektronicznej, który zastępuje lub uzupełnia ważny lub niedawno zablokowany dokument eID wydany wcześniej przez tego samego wydawcę, może jednak nastąpić bez procedury uprzedniego składania wniosku.

K5.7 Wniosek o wydanie szwedzkiego eID musi być powiązany z osobistym numerem identyfikacyjnym lub numerem koordynacyjnym, a także z informacjami, które są niezbędne wydawcy do wydania takiego eID.

Ustalenie tożsamości wnioskodawcy

K5.8 Wydawcy szwedzkich eID muszą zweryfikować, czy informacje związane z wnioskiem są kompletne i odpowiadają informacjom zarejestrowanym w rejestrze urzędowym.

K5.9 W przypadku gdy informacje, które mają zostać sprawdzone w rejestrze urzędowym, są oznaczone jako poufne („tożsamość chroniona"), niezbędne kontrole mogą zostać przeprowadzone za pomocą innych równoważnych środków.

K5.10 Identyfikacja wnioskodawcy podczas wizyty bezpośredniej:

Wydawcy szwedzkich eID mogą zweryfikować tożsamość wnioskodawcy podczas wizyty osobistej, w taki sam sposób jak przy wydawaniu standardowego dokumentu tożsamości.

K5.11 Zdalna identyfikacja wnioskodawcy w istniejącymzwiązku:

Poziom 3: Wydawcy szwedzkich eID, którzy zidentyfikowali już wnioskodawcę w związku obejmującym transakcje istotne z ekonomicznego lub prawnego punktu widzenia oraz w przypadku, gdy wnioskodawcę można zidentyfikować zdalnie za pomocą innych wiarygodnych środków równoważnych wymogom poziomu 3 szwedzkiego znaku jakości eID, mogą skorzystać z tej metody w celu ustalenia tożsamości wnioskodawcy.

Poziom 4: Nie dotyczy.

K5.12 Identyfikacja za pomocą szwedzkiego eID:

Wydawca szwedzkich eID może zidentyfikować wnioskodawcę zdalnie za pomocą istniejącego ważnego szwedzkiego eID o co najmniej takim samym poziomie bezpieczeństwa jak ten, który ma zostać wydany, jeżeli może bez przeszkód umownych wykorzystać taką identyfikację jako podstawę do wydania nowego eID.

Poziom 4: Okres ważności nowo wydanego eID nie może wykraczać poza okres ważności istniejącego eID.

K5.13 Zdalna identyfikacja wnioskodawcy:

Poziom 2: Wydawcy szwedzkich eID mogą korzystać z wiarygodnych zapisów wizerunku ważnego standardowego dokumentu tożsamości i wizerunku twarzy wnioskodawcy jako podstawy do zdalnego ustalenia tożsamości wnioskodawcy, jeżeli porównanie nie budzi wątpliwości co do jego prawdziwej tożsamości.

Poziom 3: Wydawcy szwedzkich eID mogą, za pomocą bezpiecznego odczytu ważnego standardowego dokumentu tożsamości zawierającego dane

biometryczne przechowywane w formie elektronicznej, ustalić tożsamość wnioskodawcy zdalnie na podstawie tych danych, jeżeli odpowiednie dane biometryczne osoby, która ma zostać zidentyfikowana, można zebrać w wystarczająco bezpieczny sposób, tak aby można było dokonać porównania z taką samą wiarygodnością, jak w przypadku wizyty bezpośredniej, oraz jeżeli porównanie nie budzi wątpliwości co do prawdziwej tożsamości wnioskodawcy.

Poziom 4: Nie dotyczy.

Rejestracja

K5.14 Biorąc pod uwagę mające zastosowanie przepisy dotyczące ochrony danych osobowych, wydawcy szwedzkich eID prowadzą rejestr połączonych użytkowników i przydzielonych dokumentów identyfikacji elektronicznej oraz aktualizują ten rejestr.

6. Wydawanie i blokowanie eID

Projektowanie środków technicznych

K6.1 Środki techniczne:

Poziomy 2 i 3: Środki techniczne identyfikacji elektronicznej za pomocą eID ze szwedzkim znakiem jakości eID projektuje się zgodnie z zasadą dwuskładnikową, zgodnie z którą jedna część składa się z informacji przechowywanych elektronicznie, które posiada użytkownik, a druga z tego, co użytkownik musi wykorzystać do aktywacji eID.

Poziom 4: Środki techniczne identyfikacji elektronicznej za pomocą eID ze szwedzkim znakiem jakości eID projektuje się zgodnie z zasadą dwuskładnikową, zgodnie z którą jedna część składa się z osobistego modułu bezpieczeństwa, który musi posiadać użytkownik, a druga z tego, co użytkownik musi wykorzystać do aktywacji modułu bezpieczeństwa.

K6.2 Mechanizm aktywacji i spersonalizowany kod muszą być zaprojektowane w taki sposób, aby było mało prawdopodobne, że osoby trzecie naruszą ochronę, nawet za pomocą środków mechanicznych.

Poziomy 3 i 4: Ochrona obejmuje mechanizmy zapobiegające kopiowaniu i manipulowaniu dokumentem identyfikacji elektronicznej.

K6.3 Użytkownicy eIDj ze szwedzkim znakiem jakości eID mają możliwość, z własnej inicjatywy, w okresie ważności eID, bezpłatnie i bez znacznych niedogodności, wymiany lub zażądania nowego kodu osobowego oraz, poprzez wytyczne lub automatyczne generowanie, uzyskania pomocy w utrzymaniu wymogów K6.2.

Jeżeli eID jest zaprojektowany w taki sposób, że spersonalizowanego kodu nie można wymienić, użytkownik powinien zamiast tego, na tych samych warunkach, niezwłocznie mieć możliwość uzyskania nowego eID z nowym spersonalizowanym kodem, który zastępuje poprzedni w drodze procedury blokowania.

K6.4 Wydawcy szwedzkich eID zapewniają, aby dane zarejestrowane do celów identyfikacji elektronicznej posiadaczy jednoznacznie reprezentowały wnioskodawcę i były przypisywane danej osobie przy wydawaniu dokumentu eID.

K6.5 Okres ważności wydanych eID jest ograniczony, biorąc pod uwagę zabezpieczenia dokumentu eID i ryzyko niewłaściwego wykorzystania. Maksymalny okres ważności eID wynosi pięć lat.

Przekazanie dokumentu eID

K6.6 Przekazanie zdalne:

Poziom 2: Wydawca szwedzkich eID przekazuje dokument e-ID w sposób potwierdzający dane kontaktowe przechowywane w rejestrze urzędowym lub takie informacje zarejestrowane w związku z procedurą elektroniczną zgodnie z K5.13 poziom 2.

Poziom 3: Wydawca szwedzkich eID, który przekazuje eID za pomocą procedury elektronicznej zgodnej z K5.11 poziom 3, K5.12 poziom 3 lub K5.13 poziom 3, w przypadku wydania nowego eID, oddzielnie i niezależnie od przekazania pod względem bezpieczeństwa, zapewnia, aby użytkownik został poinformowany, że taki dokument e-ID został przekazany, lub za pomocą innych środków zapewnia równoważny stopień kontroli, aby dana osoba została powiadomiona o ryzyku kradzieży tożsamości w związku z przekazaniem.

Poziom 4: Wydawca szwedzkich eID, który zapewnia eID w drodze procedury elektronicznej zgodnej z K5.12 poziom 4, w przypadku nowego wydania, oddzielnie i niezależnie od przekazania pod względem bezpieczeństwa, zapewnia, aby użytkownik został poinformowany, że taki dokument eID został przekazany.

K6.7 Przekazanie podczas wizyty bezpośredniej:

Wydawca szwedzkich eID podczas wizyty bezpośredniej i po kontroli tożsamości zgodnie z K5.10 przekazuje elektroniczny dokument identyfikacyjny za podpisanym potwierdzeniem odbioru, a ponadto przekazuje część, którą użytkownik wykorzystuje do aktywacji eID, oddzielnie i niezależnie od przekazania dokumentu eID pod względem bezpieczeństwa, na podstawie danych kontaktowych przechowywanych w rejestrze urzędowym lub innych informacji o równoważnej wiarygodności.

Usługa blokowania

K6.8 Wydawcy szwedzkich eID zapewniają usługę blokowania o dobrej dostępności dla użytkownika, aby mógł zablokować swój eID.

K6.9 Wydawcy szwedzkich eID niezwłocznie i bezpiecznie przetwarzają i realizują wnioski o zablokowanie oraz podejmują środki zapobiegające systematycznemu nadużywaniu usługi blokowania lub innym celowym działaniom, które prowadzą do powszechnego blokowania dokumentów identyfikacji elektronicznej, oraz zapewniają w razie potrzeby dostępność eID użytkowników.

7. Weryfikacja elektronicznych tożsamości posiadaczy

K7.1 Wydawcy szwedzkich eID zapewniają, aby podczas weryfikacji tożsamości posiadacza przeprowadzano wiarygodne kontrole autentyczności i ważności dokumentu eID.

K7.2 Wydawcy szwedzkich eID zapewniają wdrożenie technicznych środków kontroli bezpieczeństwa podczas weryfikacji tożsamości elektronicznej posiadaczy, tak aby było mało prawdopodobne, by osoby trzecie mogły naruszyć mechanizmy ochrony poprzez zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie procesem.

8. Wydawanie certyfikatów tożsamości

Wydawcy szwedzkich eID, którzy świadczą usługi wydawania certyfikatów tożsamości na potrzeby e-usług opartych na tych środkach, również przestrzegają przepisów niniejszej sekcji.

K8.1 Wydawcy szwedzkich eID zapewniają, aby usługa wydawania certyfikatów tożsamości była dobrze dostępna oraz aby wydawanie certyfikatów tożsamości było poprzedzone wiarygodną identyfikacją zgodnie z przepisami sekcji 7.

Poziom 4: Certyfikaty zawierają odniesienie do kryptograficznego materiału klucza zweryfikowanego przez wydawcę jako będącego w wyłącznym posiadaniu posiadacza.

K8.2 Przedłożone certyfikaty tożsamości są ważne tylko tak długo, jak jest to konieczne, aby umożliwić użytkownikowi dostęp do żądanej e-usługi, i są chronione w taki sposób, aby informacje mógł odczytywać wyłącznie zamierzony odbiorca oraz aby odbiorcy certyfikatów mogli zweryfikować autentyczność certyfikatów.

K8.3 Biorąc pod uwagę ryzyko niewłaściwego wykorzystania usługi certyfikacyjnej, emitenci szwedzkich eID ograniczają okres, w którym można wydać danemu posiadaczowi kilka kolejnych certyfikatów tożsamości, zanim posiadacz zostanie ponownie zidentyfikowany zgodnie z przepisami sekcji 7.