Warszawa, dnia 11 marca 2020 r.

Poz. 399

ROZPORZĄDZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 10 marca 2020 r.

w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników

Na podstawie art. 20a ust. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346) zarządza się, co następuje:

§ 1. Rozporządzenie określa szczegółowe warunki organizacyjne i techniczne, które powinien spełniać system teleinformatyczny służący do wydania certyfikatu oraz stosowania technologii, o których mowa w art. 20a ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zwanej dalej „ustawą", w tym zakres i okres przechowywania danych w systemie oraz obowiązki informacyjne, do których zobowiązany jest administrator systemu.

§ 2. 1. System teleinformatyczny służący do wydania certyfikatu wykorzystywanego przez podmioty publiczne do uwierzytelniania użytkowników spełnia następujące warunki techniczne i organizacyjne:

1) umożliwia wystawienie certyfikatu oraz jego wydanie użytkownikowi, dla którego został on wystawiony;

2) umożliwia niezwłoczne unieważnienie certyfikatu;

3) określa dokładny czas wystawienia i unieważnienia certyfikatu, zgodnie z czasem uniwersalnym koordynowanym UTC(PL);

4) potwierdza tożsamość użytkownika, któremu wydano certyfikat;

5) posiada zabezpieczenia na wypadek zagrożeń w zakresie bezpieczeństwa teleinformatycznego dobierane na podstawie szacowania ryzyka;

6) nie gromadzi ani nie kopiuje danych służących użytkownikom do potwierdzania tożsamości z wykorzystaniem certyfikatów.

2. System, o którym mowa w ust. 1, przechowuje dane dotyczące wystawionych certyfikatów przez okres 20 lat, licząc od dnia 1 stycznia roku następującego po roku, w którym certyfikat został wystawiony.

3. Zapewnienie bieżącej poprawności i użyteczności funkcjonalnej systemu, o którym mowa w ust. 1, wymaga spełnienia następujących warunków technicznych i organizacyjnych:

1) dokonywania systematycznego przeglądu skuteczności zastosowanych środków zabezpieczeń na wypadek zagrożeń bezpieczeństwa teleinformatycznego, w celu wprowadzania ich usprawnień;

2) utrzymywania w aktualnym stanie dokumentacji operacyjnej i technicznej systemu, w celu zapewnienia jego bezpiecznej eksploatacji;

3) zapewniania organizacyjnego, technicznego i kryptograficznego bezpieczeństwa działania systemu;

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 2270).

4) prowadzenia działań zapobiegających fałszowaniu certyfikatów, w tym zapewniania poufności podczas procesu tworzenia danych do potwierdzania tożsamości użytkownika;

5) informowania osób ubiegających się o certyfikat o warunkach stosowania certyfikatu zawartych w polityce certyfikacji.

4. Warunki, o których mowa w ust. 1–3, zostały spełnione, gdy:

1) została wdrożona polityka certyfikacji spełniająca wymagania wskazane w normie PN-ETSI EN 319 411 lub nowszej;

2) zapewnione zostały warunki organizacyjne i techniczne zgodne z wymaganiami specyfikacji technicznej CEN/TS 419261 lub nowszej w zakresie świadczenia usług innych niż wydawanie certyfikatów kwalifikowanych;

3) zastosowane zostały systemy i produkty zgodne z wymaganiami specyfikacji technicznej CEN/TS 419221 lub nowszej.

5. Administrator systemu, o którym mowa w ust. 1, udostępnia deklarację o spełnieniu wymagań określonych w ust. 3 oraz politykę certyfikacji:

1) w Biuletynie Informacji Publicznej albo

2) na stronie internetowej administratora – w przypadku podmiotów niezobowiązanych do udostępniania informacji publicznej w Biuletynie Informacji Publicznej.

§ 3. 1. System teleinformatyczny przetwarzający dane dotyczące tożsamości użytkowników wykorzystywany przez podmioty publiczne do uwierzytelniania użytkowników w oparciu o inne technologie niż certyfikat:

1) rejestruje użytkowników;

2) potwierdza tożsamość użytkowników;

3) przechowuje i udostępnia dane identyfikacyjne użytkowników systemom autoryzującym uprawnionym do ich otrzymania;

4) umożliwia zablokowanie konta użytkownika na jego żądanie;

5) zapewnia rozliczalność, rozumianą jako przypisanie określonego działania w systemie do osoby fizycznej lub procesu oraz umiejscowienie ich w czasie;

6) zapewnia integralność, autentyczność i poufność danych identyfikacyjnych i uwierzytelniających użytkownika;

7) zapewnia codzienną synchronizację czasu systemowego z czasem uniwersalnym koordynowanym UTC(PL).

2. System, o którym mowa w ust. 1, przechowuje dane dotyczące tożsamości użytkownika przez okres 20 lat, licząc od dnia 1 stycznia roku następującego po roku, w którym wykonano w systemie ostatnią operację z użyciem tożsamości tego użytkownika.

3. System, o którym mowa w ust. 1, spełnia następujące warunki techniczne i organizacyjne w zakresie administrowania:

1) zapewnianie wiarygodności procesu rejestracji użytkowników i potwierdzania ich tożsamości;

2) utrzymywanie w aktualnym stanie dokumentacji operacyjnej i technicznej systemu, w celu zapewnienia jego bezpiecznej eksploatacji;

3) opracowywanie i ustanawianie, wdrażanie i eksploatowanie, monitorowanie i przeglądanie oraz utrzymywanie i doskonalenie systemu zarządzania bezpieczeństwem informacji spełniającego wymagania Polskiej Normy PN-EN ISO/IEC 27001, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy.

4. Warunki określone w ust. 3 uważa się za spełnione, jeżeli:

1) system zarządzania bezpieczeństwem informacji, o którym mowa w ust. 3 pkt 3, został oceniony pozytywnie przez jednostkę oceniającą zgodność, zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2019 r. poz. 544), albo

2) administrator systemu, o którym mowa w ust. 1, udostępnił deklarację o spełnieniu wymagań określonych w ust. 3:

   a) w Biuletynie Informacji Publicznej albo

   b) na stronie internetowej administratora – w przypadku podmiotów niezobowiązanych do udostępniania informacji publicznej w Biuletynie Informacji Publicznej.

§ 4. 1. System teleinformatyczny, o którym mowa w art. 20a ust. 2 ustawy, uwierzytelniając użytkowników, dokonuje weryfikacji tożsamości użytkowników, wykorzystując certyfikaty wydane w systemie, o którym mowa w § 2 ust. 1, lub usługi systemu, o którym mowa w § 3 ust. 1, oraz przechowuje dane potwierdzające tę weryfikację.

2. Dane potwierdzające weryfikację, o których mowa w ust. 1, umożliwiają w sposób jednoznaczny:

1) ustalenie tożsamości użytkownika, który dokonał czynności w postaci elektronicznej;

2) ustalenie czasu dokonania czynności;

3) stwierdzenie ważności uprawnień w momencie dokonania czynności.

§ 5. 1. Zakres danych przetwarzanych w certyfikatach wydawanych w systemie, o którym mowa w § 2 ust. 1, w przypadku wydawania certyfikatów:

1) osobom fizycznym – jest zgodny z profilem certyfikatu określonym w normie PN-ETSI EN 319 412-2 lub nowszej;

2) osobom prawnym – jest zgodny z profilem certyfikatu określonym w normie PN-ETSI EN 319 412-3 lub nowszej.

2. Zakres danych przetwarzanych w systemie, o którym mowa w § 3 ust. 1, odnoszących się do tożsamości użytkowników jest odpowiedni do zakresu danych profilu zaufanego, określonego w przepisach wydanych na podstawie art. 20d ustawy.

§ 6. Systemy teleinformatyczne podmiotów realizujących zadania publiczne, służące do wydania certyfikatu oraz stosowania technologii, o których mowa w art. 20a ust. 2 ustawy, funkcjonujące w dniu wejścia w życie niniejszego rozporządzenia, należy dostosować do wymagań określonych w przepisach niniejszego rozporządzenia nie później niż do dnia 12 marca 2022 r.

§ 7. Rozporządzenie wchodzi w życie z dniem 12 marca 2020 r.[2)]

Minister Cyfryzacji: *M. Zagórski*

[2)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz. U. poz. 1627), które traci moc z dniem 11 marca 2020 r. na podstawie art. 61 ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (Dz. U. poz. 1544 oraz z 2019 r. poz. 60 i 934).