

1. Wstęp

NemID jest rozwiązaniem zabezpieczającym, którego może Pan/Pani używać w banku internetowym (netbanku), na publicznych i prywatnych stronach internetowych. NemID można też używać przy składaniu podpisów cyfrowych.

NemID składa się z identyfikatora użytkownika (bruger ID), kodu dostępu i karty kluczy, która zawiera jednorazowe kody (zwane kluczami), których musi Pan/Pani używać w połączeniu z Pana/Pani identyfikatorem użytkownika i kodem dostępu.

W przypadku korzystania z systemu IVR (system Interaktywnych Odpowiedzi Głosowych) otrzymuje Pan/ Pani swoje klucze przy użyciu telefonu.

Ma też Pan/ Pani możliwość zakupienia elektronicznego czytnika kluczy, który może wskazywać Pana/ Pani klucze. W dalszym ciągu musi Pan/ Pani jednak przechowywać kartę kluczy i używać jej w określonych sytuacjach.

Możliwe jest również zainstalowanie NemID klucz App (następnie klucz App) na urządzeniu mobilnym (np. smartfonie lub tablecie) i użycie go jako kodu. Musisz jednak posiadać kartę kluczy w sytuacjach, w których Twoja aplikacja lub urządzenie mobilne jest niedostępne.

Jeśli ma Pan/ Pani zamiar używać NemID w celu składania podpisów cyfrowych, musi Pan/ Pani powiązać Pana/Pani NemID z certyfikatem OCES. Skrót OCES w tłumaczeniu oznacza Publiczny Certyfikat dla Serwisu Elektronicznego.

Poniżej znajdzie Pan/Pani zasady obowiązujące dla NemID. Jeśli ma Pan/ Pani zamiar używać NemID do korzystania z usług bankowych online, dotyczą Pana/ Panią zasady zawarte w rozdziałach 2 i 3. Korzystanie z NemID w banku online jest poza tym uregulowane przez Pana/ Pani umowę z bankiem, z której wynika też, w jakim stopniu stosowane są zasady o obowiązkach i odpowiedzialności regulowane przez Ustawę o Usługach Płatniczych.

Jeśli ma Pan/Pani zamiar używać NemID również do składania podpisów cyfrowych, dotyczą Pana/ Panią zasady zawarte w rozdziałach 2, 3 i 4. Zasady można znaleźć też na stronie internetowej: www.nemid.nu

Przez DanID rozumie się Nets DanID A/S numer cvr. 30808460.

Przez "urządzenie" rozumie się jednostkę, przy pomocy której używa się NemID, np. komputer, telefon komórkowy albo tablet.

2. Akty wiążące

Kiedy, posługując się NemID, wykonuje Pan/Pani rozmaite czynności, np. składa Pan/ Pani podpis elektroniczny, jest Pan/Pani tak samo zobowiązana w stosunku do odbiorcy, jak w przypadku złożenia podpisu na piśmie.

3. Zasady dotyczące użytkowania NemID

3.1. Utworzenie NemID

W momencie utworzenia NemID, zobowiązują się Pan/ Pani do udzielenia pełnych i prawdziwych informacji.

3.2 Przechowywanie identyfikatora użytkownika, kodu dostępu, karty kluczy/ czytnika kluczy/klucz app

Trzeba zwrócić uwagę na to, że:

- identyfikator użytkownika, kod dostępu i karta / czytnik kluczy / kod pin do Twojego klucza app muszą być przechowywane w bezpiecznym miejscu, tak aby uniemożliwić osobom trzecim dostęp do nich,
- nie można podawać swojego kodu i kluczy osobom trzecim albo pozostawiać ich pod opieką osób trzecich
- nie można skanować karty kluczy, wpisywać swoich kluczy na nośnikach zewnętrznych ani digitalizować czy też kopiować kluczy
- nie można zapisywać kodu dostępu / kodu pin do Twojego klucza app
- nie można przechowywać kodu dostępu razem z kartą/ czytnikiem kluczy, lub na urządzeniu mobilnym, na którym jest zainstalowany Twój klucz app, ani zapisywać kodu dostępu na karcie/ czytniku kluczy.
- klucz App może być zainstalowany tylko na swoim własnym urządzeniu mobilnym

3.3 Bezpieczeństwo użytkowania

Musi Pan/ Pani upewnić się, że:

- Pana /Pani identyfikator użytkownika, kod dostępu, karta/czytnik kluczy i klucz app są używane tylko i wyłącznie przez Pana/ Panią, zgodnie z obowiązującymi zasadami,
- osoby trzecie nie mogą podpatrzeć Pana/ Pani kodu dostępu, lub kodu pin, podczas gdy Pan/ Pani go wpisuje,
- używa Pan/ Pani NemID na takich urządzeniach, których system operacyjny, przeglądarka internetowa, i inne programy, są na bieżąco aktualizowane przy użyciu najnowszych zabezpieczeń.

Musi Pan/ Pani na bieżąco kontrolować, czy karta/czytnik kluczy lub urządzenie mobilne, gdzie jest zainstalowany klucz App nie zaginęły, i że NemID nie uległo nadużyciu. Ponadto istnieje możliwość, by na stronie internetowej www.nemid.nu, w zakładce „Hændelseslog” w rozwiązaniu samoobsługowym (selvbetjening) zgłosić, że chce Pan/ Pani, żeby system rejestrował, gdzie używa Pan/ Pani swojego NemID. Następnie może Pan/ Pani na bieżąco kontrolować, czy NemID było używane tylko i wyłącznie na tych stronach, z których Pan/ Pani korzystał/ korzystała .

3.4 Tymczasowy kod dostępu

Za pierwszym razem, kiedy używa Pan/ NemID, otrzyma Pan/Pani tymczasowy kod do zalogowania. Ta sama procedura obowiązuje w przypadku zablokowania kodu dostępu, por. rozdział 3.5 o zablokowaniu.

Musi Pan/ Pani natychmiast poprosić Nets DanID albo swój bank o przydzielenie nowego tymczasowego kodu dostępu, jeśli uważa Pan/ Pani, że osoby trzecie weszły w posiadanie albo mogły wejść w posiadanie tymczasowego kodu dostępu, np. jeśli list z kodem nie jest szczelnie zamknięty.

3.5. Zablokowanie

3.5.1. Pana/ Pani obowiązek do natychmiastowego zablokowania

Musi Pan/ Pani natychmiast zablokować:

- Kartę kluczy, jeśli uważa Pan/ Pani, że osoby trzecie weszły w posiadanie albo mogły wejść w posiadanie kluczy na Pana/ Pani karcie, np. jeśli list z kartą kluczy w momencie jego otrzymania nie jest szczelnie zamknięty.
- Czytnik kluczy, jeśli list z czytnikiem kluczy w momencie jego otrzymania nie jest szczelnie zamknięty
- Kartę kluczy/ czytnik kluczy, jeśli zostały zgubione. Jeśli znajdzie Pan/Pani swoją wcześniej zagubioną kartę kluczy/ czytnik kluczy, musi Pan/Pani je zniszczyć.
- Klucz App, jeśli zgubiłeś urządzenie mobilne, na którym był zainstalowany, lub masz podejrzenie, że inni mają doświadczenie do Twojego klucza App, lub ktoś zainstalował klucz App posługując się Twoim NemID.
- Kod dostępu, jeśli uważa Pan/ Pani, że osoby trzecie weszły albo mogły wejść w jego posiadanie, chyba że ma Pan/ Pani możliwość natychmiast zmienić kod na stronie internetowej www.nemid.nu

3.5.2 Zgłoszenie zablokowania

W przypadku konieczności zablokowania Pana/Pani kodu dostępu i/ albo karty kluczy/czytnika kluczy/kluczu App, musi Pan/Pani podać imię i nazwisko, ewentualnie adres i numer cpr, albo identyfikator użytkownika, albo numer widniejący na Pana/Pani karcie kluczy/czytniku kluczy/kluczu App.

Poza tym musi Pan/Pani podać, czy ma zostać zablokowany kod dostępu, karta/czytnik kluczy, czy klucz App. Kiedy kod dostępu zostanie zablokowany, Nets DanID prześle Panu/ Pani potwierdzenie wraz z informacją na temat czasu i przyczyny zablokowania kodu dostępu.

Może Pan/ Pani zablokować kod dostępu, kartę/ czytnik kluczy i/ lub klucz App:

- Poprzez stronę internetową www.nemid.nu (całodobowo), telefonicznie pod numerem: 72 24 70 10 (całodobowo)
- Poprzez zgłoszenie się do banku lub też do Wydziału Spraw Obywatelskich (Borgerservice), jeśli ma Pan/ Pani NemID z opcją podpisu cyfrowego).

W zakładce „Hændelseslog” w rozwiązaniu samoobsługowym na stronie www.nemid.nu może Pan/Pani na bieżąco kontrolować czas i przyczynę zablokowania kodu dostępu, karty kluczy/czytnika kluczy lub kluczu App.

3.5.3 Zablokowanie przez DanID

DanID blokuje

- Pana/ Pani kod dostępu, jeśli DanID podejrzewa lub posiada wiedzę na temat tego, że osoby trzecie znają Pana/ Pani kod dostępu
- Pana/ Pani kod dostępu, jeśli zostanie on błędnie wprowadzony określoną liczbę razy
- Pana/ Pani kartę kluczy/ czytnik kluczy, klucz App, jeśli DanID podejrzewa lub posiada wiedzę na temat tego, że osoby trzecie znają klucze z Pana/Pani karty kluczy/czytnika kluczy lub klucza App
- Pana/ Pani klucz App, jeśli DanID podejrzewa lub posiada wiedzę na temat tego, że urządzenie mobilne, które używasz zostało przejęte lub ma poważne luki w zabezpieczeniach.
- NemID, jeśli Nets DanID dowie się, że nie stosował/ stosowała się Pan/Pani do zasad korzystania z NemID
- NemID, jeśli poda/ł poda/ła Pan/Pani nieprawdziwe informacje w momencie zakładania NemID
- NemID, jeśli Nets DanID otrzyma informację na temat Pana/ Pani śmierci.

3.5.4 Używanie NemID po zablokowaniu

Nie może Pan/ Pani używać NemID, kiedy NemID albo kod dostępu jest zablokowany. W przypadku jeśli zablokowania została tylko karta kluczy/ czytnik kluczy, niektóre banki umożliwiają zalogowanie się określoną liczbę razy do netbanku, np. w celu skontrolowania informacji na temat konta.

3.6 Zakończenie użytkowania NemID

W każdym momencie ma Pan/ Pani możliwość zablokowania swojego dostępu do NemID, jeśli nie wyraża Pan/ pani dłużej chęci korzystania z NemID, por. rozdział 3.5.2 o zablokowaniu. Proszę zwrócić uwagę na fakt, że od momentu zablokowania, korzystanie z usług wymagających NemID, nie będzie możliwe.

3.7 Ochrona danych osobowych

Jeśli utworzył/ utworzyła Pan/ Pani NemID poprzez swój bank, Nets DanID przechowuje Pana/Pani dane w imieniu banku. Nets DanID przechowuje Pana/ Pani dane, tzn. imię i nazwisko, adres i numer cpr po to, by móc Pana/ Panią zidentyfikować, i ewentualnie używa podanego adresu e-mail w kontaktach z Panem/ Panią, np. w celu potwierdzenia zablokowania.

Jeśli zarejestrował Pan/Pani numer swojego telefonu komórkowego w systemie Nets DanID, to wtedy Nets DanID będzie go używać do przesłania wiadomości, np. na temat tymczasowych kodów dostępu.

Korzystając z NemID, można skonfigurować pliki do logowania na Pana/ Pani urządzeniu. Te pliki mogą zostać w razie życzenia skasowane przez użytkownika. W ramach polityki bezpieczeństwa, Nets DanID rejestruje czas, w którym Pan/ Pani korzysta z NemID, adres IP i inne informacje na temat urządzenia, za pomocą którego korzysta Pan/ Pani z NemID.

Więcej informacji na temat plików do logowania i bezpieczeństwa można znaleźć na stronie internetowej: https://www.nemid.nu/dk-da/om_nemid/sikkerhedden_bad_nemid/

Jeśli korzystając z opcji samoobsługi na stronie www.nemid.nu wybierzesz Pan/ Pani możliwość rejestracji miejsca użycia NemID, to wtedy Nets DanID także rejestruje, przy użyciu których dostawców korzysta/ korzystała Pan/ Pani z NemID. W każdym momencie można zrezygnować z tej opcji. Następnie Nets DanID nie będzie rejestrować, gdzie Pan/ Pani używał/ używała NemID.

Nets DanID przechowuje dane w bieżącym roku i przez następne 5 lat, po czym dane są usuwane.

3.8 Roszczenia związane z NemID

Roszczenia związane z korzystaniem z NemID w netbanku, należy zgłaszać w banku, odwołując się do umowy dotyczącej korzystania z banku online.

Roszczenia, które powstają w związku z korzystaniem z NemID na innych stronach internetowych, kieruje się do dostawcy usług lub do Nets DanID.

3.9 Dotyczy rozwiązania IVR

Rozwiązanie IVR przeznaczone jest dla osób niewidomych i słabowidzących. Jeśli otrzymuje Pan/ Pani klucze przy pomocy systemu IVR, musi Pan/ Pani wyposażyć telefon, którego używa Pan/Pani do odbierania kluczy, w zabezpieczenia, o których mowa w opisywanych zasadach.

To znaczy, że:

- Musi Pan/ Pani się upewnić, że telefon, którego używa Pan/ Pani do odbierania kluczy, jest niezależny od

komputera/telefonu, którego później używa Pan/Pani do wpisywania klucza

- Musi Pan/Pani natychmiast zablokować kod dostępu, jeśli zgubi Pan/Pani telefon, przy pomocy którego odbiera Pan/Pani klucze lub jeśli zauważy Pan/Pani, że linia telefoniczna została nadużyta.

3.10 Zmiana zasad dotyczących użytkowania NemID

Nets DanID ma prawo zmienić zasady bez uprzedzenia, jeśli dzieje się to w następstwie zmian w wymogach bezpieczeństwa, obowiązujących dla NemID. Zmiany zaczynają obowiązywać w momencie ich opublikowania na stronie www.nemid.nu. O wprowadzeniu innych zmian ostrzega się na stronie www.nemid.nu minimum trzy miesiące, zanim wejdą one w życie.

4. Szczególne zasady dotyczące podpisu cyfrowego

- Jeśli zdecyduje się Pan/ Pani na używanie NemID do składania podpisów cyfrowych, wtedy zasady zawarte w rozdziale 4 mają charakter uzupełniający w stosunku do zasad opisanych w rozdziałach 2 i 3.
- Jeśli ma Pan/ Pani takie życzenie, można ubiegać się o przydzielenie kilku różnych NemID, a co za tym idzie - różnych kart kluczy/ czytników kluczy i identyfikatorów użytkownika, do używania odpowiednio w netbanku i do składania podpisów cyfrowych.

4.1 Przechowywanie danych osobowych

W momencie otrzymania certyfikatu OCES, który powiązany jest z NemID

- wyraża Pan/ Pani zgodę na to, że Nets DanID skorzysta z systemu CPR w celu zweryfikowania Pana/ Pani imienia i nazwiska oraz adresu
- wyraża Pan/Pani zgodę na to, że Nets DanID przekazuje powiązanie między Pana/Pani podpisem cyfrowym a numerem cpr do publicznej usługi PID w Urzędzie Digitalizacji. Usługa PID jest używana przez dostawców usług publicznych w celu Pana/ Pani identyfikacji. Prywatny wykonawca usług może zostać poinformowany o Pana/Pani numerze cpr, jeśli wyrazi/ wyraziła Pan/Pani na to zgodę, logując się na stronie wykonawcy usług.
- wyraża Pan/ Pani zgodę na to, że Nets DanID zweryfikuje Pana/ Pani wcześniejszy podpis cyfrowy przy użyciu publicznej usługi PDI.

Jeśli założy/ł założyła Pan/Pani NemID w powiązaniu z netbankiem i będzie Pan/Pani używać Nem ID do składania podpisów cyfrowych, to jednocześnie wyraża Pan/Pani zgodę na to, że bank przekazuje Pana/Pani dane osobowe (imię i nazwisko, adres, numer cpr, ewentualnie adres e-mail i numer telefonu komórkowego) do Nets DanID po to, by Nets DanID mógł używać Pana/Pani danych osobowych do wysyłania i administrowania Pana/ Pani podpisu cyfrowego.

Jeśli otrzyma/ł otrzymała Pan/Pani NemID w celu składania podpisów cyfrowych i wyraża Pan/Pani chęć używania NemID dla potrzeb netbanku, to na żądanie banku wyraża Pan /Pani jednocześnie zgodę na to, żeby system DanID przekazał dane na temat NemID bankowi, tak żeby korzystanie z NemID było możliwe w netbanku.

Jeśli nie życzy sobie Pan/Pani, aby Pana/Pani dane osobowe i/albo dane na temat NemID były traktowane jak w sposób opisany powyżej, może Pan/Pani zablokować swój podpis cyfrowy poprzez zgłoszenie tego do Nets DanID albo do Urzędu d/s Obywatelskich (Borgerservice) i/albo zakończyć korzystanie z usług netbanku poprzez zgłoszenie tego bankowi.

Jeśli zablokuje Pan/Pani podpis cyfrowy, może Pan/Pani korzystać z NemID tylko w netbanku; jeśli zamknie Pan/Pani dostęp do banku online, może Pan/Pani używać NemID tylko do podpisu cyfrowego.

4.2 Obowiązki i odpowiedzialność posiadacza podpisu cyfrowego z powiązaniem certyfikatem OCES.

Musi Pan/Pani upewnić się, że dane na temat imienia, nazwiska, adresu e-mail w certyfikacie OCES są poprawne.

W przypadku zmiany danych, zawartych w certyfikacie OCES, np. w przypadku zmiany nazwiska, musi Pan/ Pani w ciągu 30 dni odnowić certyfikat OCES. Jeśli certyfikat nie zostanie odnowiony w ciągu 30 dni, a Nets DanID posiada informacje na temat tego, że dane nie są prawdziwe, to wtedy Nets DanID zablokuje certyfikat OCES.

Nie może Pan/ Pani używać swojego certyfikatu OCES do wydawania certyfikatów osobom trzecim.

4.3 Zablokowanie certyfikatu OCES

Nets DanID zablokuje Pana/Pani certyfikat OCES

- jeśli Pan/Pani poinformuje Nets DanID o chęci zablokowania certyfikatu OCES
- Jeśli NetsDanID ustali, że zasady korzystania z NemID zostały przez Pana/Panią złamane.

Jeśli Pan/Pani sam/sama zablokuje certyfikat OCES, to wtedy Nets DanID prześle Panu/Pani potwierdzenie zablokowania poprzez e-mail albo w liście wysłanym na Pana/ Pani adres zameldowania, jeśli Nets DanID ma do niego dostęp. Jeśli Nets DanID nie jest w posiadaniu Pana/Pani adresu zameldowania, potwierdzenie zostanie przesłane na adres podany przez Pana/Panią do Nets DanID. Jeśli Nets DanID zablokuje certyfikat nie na Pana/ Pani prośbę, to wtedy Nets DanID prześle Panu/ Pani informacje na temat przyczyn zablokowania poprzez e-mail i -jeśli to możliwe- również listownie.

4.4 Odnowienie certyfikatu OCES

Data ważności certyfikatu OCES jest zaznaczona w Pana/ Pani certyfikacie OCES. Okres ważności certyfikatu OCES może sięgać 4 lat. Najpóźniej 4 tygodnie przed wygaśnięciem terminu ważności certyfikatu, Nets DanID prześle informację na ten temat poprzez e-mail albo w liście wysłanym na adres zameldowania, jeśli Nets DanID jest w jego posiadaniu. Przed wygaśnięciem terminu ważności certyfikatu OCES, może Pan/ Pani odnowić swój certyfikat poprzez użycie starego certyfikatu. Jeśli okres ważności Pana/Pani certyfikatu OCES upłynie albo certyfikat został zablokowany, musi Pan/ Pani zamówić nowy.

4.5 Obowiązki i odpowiedzialność w przypadku otrzymywania danych, potwierdzonych podpisem cyfrowym

Jeśli otrzymuje Pan/ Pani dane potwierdzone podpisem cyfrowym, np. ponieważ wymienia Pan/ Pani podpisane cyfrowo e-maile lub dokumenty, musi Pan/ Pani sprawdzić, żeby móc polegać na certyfikacie, czy certyfikat OCES nadawcy

- Jest ważny- tzn. że czas jego ważności nie jest przekroczony
- Nie jest zablokowany- tzn. że nie figuruje na liście zablokowanych certyfikatów opublikowanej na stronie internetowej Nets DanID
- Jest używany zgodnie z wszystkimi ograniczeniami, wynikającymi z certyfikatu OCES

4.6 Odpowiedzialność Net DanID w stosunku do posiadaczy certyfikatów OCES

W przypadku nadużyć Net DanID jest obarczony odpowiedzialnością uiszczenia roszczenia na podstawie duńskiego prawa. Nets DanID nie ponosi jednak odpowiedzialności za poniesioną stratę, jeśli Pan/Pani nie stosował się do zasad NemID. Ewentualny roszczenie musi zostać przedstawione Nets DanID.

Zasady dotyczące NemID są podporządkowane prawu duńskiemu. Ewentualne spory między Panem/Panią a Nets DanID, których nie można rozwiązać poprzez negocjacje, mogą być wnoszone do Kopenhaskiego Sądu.

4.7 Odpowiedzialność ze strony Nets DanID w stosunku do osób odbierających korespondencję potwierdzoną podpisem cyfrowym

Nets DanID jest odpowiedzialny za Pana/ Pani szkodę, kiedy Pan/ Pani w sposób rozsądny polega na certyfikacie OCES nadawcy, jeśli przyczyną straty jest błąd popełniony przez Nets DanID w procesie rejestracji, wysłania lub też zablokowania certyfikatu. Nets DanID nie ponosi odpowiedzialności za szkodę, jeśli Nets DanID udowodni, że nie działał niedbale ani celowo.

5. Pozostałe informacje

Jeśli ma Pan/ Pani pytania dotyczące NemID i podpisu cyfrowego, może Pan/ Pani zgłosić się z nimi do swojego banku, wydziału do spraw obywatelskich lub też do Nets DanID. Dodatkowe informacje zamieszczone są na stronie www.nemid.nu, na której wytłumaczono kluczowe pojęcia i opisano technologię certyfikatów.