E-identifiering

Beskrivning av tjänsten

Innehåll

E-identifiering

Med hjälp av e-identifiering och Nordeas identifieringsmetoder kan tjänsteleverantören identifiera sina privatkunder på ett säkert sätt. I tjänsten e-identifiering sköter Nordea identifieringen av kunden för tjänsteleverantörens räkning. Identifieringsuppgifterna i tjänsten kan också användas för att bilda en elektronisk signatur, när den kund som identifierar sig och tjänsteleverantören kommer överens om det.

Nordea ger ut de identifieringsverktyg som behövs i tjänsten e-identifiering. Nordea sänder MAC-nycklar till tjänsteleverantören och nätbankskoder till den privatkund som identifierar sig.

Nordeas e-identifiering baserar sig på den s.k. Tupas-standarden som tagits fram av Finansbranschens centralförbund. Tillsammans med de tjänster som övriga banker tillhandahåller kan tjänsteleverantören nå flera miljoner finländska privatpersoner som utnyttjar nättjänsten. Mera information om standarden finns på Finansbranschens centralförbunds webbplats www.fkl.fi.

Nordea ingår i Kommunikationsverkets register över stark autentisering. Nordeas e-identifieringstjänst är en i lagen avsedd tjänst för stark autentisering i de fall då identifieringen gäller en fysisk person med en finsk personbeteckning. En tjänst för identifiering av ett företag är inte stark autentisering som avses i lagen eftersom identifieringen sker på företagsnivå, och identifieringen fastställer då inte den fysiska personens identitet på det sätt som lagen förutsätter.

Nordea tillhandahåller två olika tjänster för e-identifiering.

Traditionell e-identifiering

- Ett identifieringssätt per identifieringstransaktion.
- Tillåter inte att egna användarkoder skapas.
- Banken ansvarar för identifieringstransaktionens riktighet.

E-identifiering för den som skapar egna användarkoder:

- Kunden identifierar sig endast en gång med hjälp av e-identifiering.
- Tjänsteleverantören kan bevilja kunden egna användarkoder. Då behövs identifiering med e-identifiering inte i fortsättningen.
- Banken ansvarar för identifieringstransaktionens riktighet då e-identifiering används.
- Tjänsteleverantören ansvarar för identifieringstransaktionens riktighet då identifieringen gjorts med egna användarkoder.

1.1 Fördelar med e-identifiering

Internettjänsterna uppskattas av användarna eftersom de är enkla att använda. Och hur enkel en tjänst är att använda beror bl.a. på om kunden kan använda sina välbekanta identifieringsmetoder. Nordeas e-identifiering gör det möjligt för tjänsteleverantören att utnyttja samma identifieringsmetoder som i Nordeas nätbankstjänster. Tjänsteleverantören når Nordeas alla nättjänstkunder med e-identifiering, vilket skapar potential att värva nya kunder.

Med hjälp av e-identifiering kan tjänsteleverantören identifiera sina kunder på ett säkert sätt utan separata kundnummer och lösenord. Detta innebär betydande inbesparingar i utvecklings- och underhållskostnader.

Tjänsteleverantören och kunden kan avtala om att tjänsteleverantören får använda tjänsten vid bildandet av den elektroniska signaturen när det gäller rättshandlingar mellan dem. Det möjliggör mottagande av olika ansökningar och ingående av avtal på nätet. I det fallet sörjer banken i sin e-identifieringstjänst dock endast för att kunden identifieras. Tjänsteleverantören ska ta hand om övriga ärenden som krävs för en elektronisk signatur, till exempel administrera de samlade uppgifterna, spara svarsmeddelandena och se till att den egna tjänsten inte ändras.

Med e-identifiering sker också betalningen i nätbutiker säkert. Tjänsteleverantören och kunden kan t.ex. komma överens om beställningar eller fakturering med hjälp av e-identifiering. Dessutom kan man

också öka e-betalningens säkerhet med e-identifiering, eftersom användningen av förfallodagsbetalningar är tryggare om beställarens identitet har fastställts och beställningen daterats.

1.2 Allmän beskrivning av e-identifiering

Den kund som identifierar sig har en central position vid användningen av tjänsten. Kunden styr förmedlingen av sina uppgifter mellan tjänsteleverantören och Nordea. Nordea och tjänsteleverantören har inte direkt kontakt sinsemellan under den tid kunden använder tjänsten.

Nordeas identifierare är av engångsnatur och den är knuten både till tjänsteleverantörens aktuella servicetransaktion och till kunden.

När tjänsteleverantören måste identifiera sin kund, sänder tjänsteleverantören en begäran om identifiering till kunden, som flyttar till Nordeas identifieringstjänst genom att trycka på Nordeas funktionsknapp.

Tjänsteleverantörens begäran om identifiering förmedlas av kunden till Nordeas identifieringstjänst, som sänder ett svarsmeddelande till kunden efter identifieringen. Kunden kontrollerar uppgifterna i svarsmeddelandet, godkänner uppgifterna och återvänder till tjänsteleverantörens tjänst, där han fortsätter att utföra funktioner som har att göra med tjänsten. Kunden kan annullera eller förkasta identifieringstransaktionen antingen före identifieringen eller efter kontrollen av svarsmeddelandet. Kundens uppgifter förmedlas då inte till tjänsteleverantören.

Möjligheten att använda uppgifterna i tjänsten som ett element i den elektroniska signaturen baserar sig på ett inbördes avtal mellan tjänsteleverantören och kunden om att identifieringsuppgifterna också kan användas för den elektroniska signaturen vid rättshandlingar dem emellan. Användningen av e-identifiering som elektronisk signatur stöds dessutom av villkoren för Nordeas nätbanksavtal, svarsmeddelandenas tidstämplar och Nordeas logguppgifter. Om man vill dra nytta av tjänsten då avtal ingås eller ansökningar görs, ska tjänsteleverantören dock sköta övriga ärenden som krävs för den elektroniska signaturen. Han ska till exempel administrera de samlade uppgifterna, spara svarsmeddelandena och se till att det inte sker ändringar i hans egen tjänst. Nordea ansvarar inte för giltigheten av eller innehållet i avtalet, eller någon annan rättshandling, mellan tjänsteleverantören och kunden, inte heller för att den person som använder företagets identifieringsuppgifter har behörighet eller befogenhet att representera företaget eller organisationen.

1.3 E-identifieringens funktioner

I e-identifieringstjänsten finns det olika funktioner och användningsmöjligheter beroende på hurdant svarsmeddelande man i serviceavtalet har kommit överens om att förmedla. I Nordeas svarsmeddelande innehåller identifieringsuppgiften alltid kundens namn. Identifieringsuppgiften kan dessutom stå i klartext eller vara krypterad.

När svarsmeddelandet är i klartext, förmedlar Nordea kundens personbeteckning, personbeteckningens kontrolldel eller FO-nummer, beroende på vad man kommit överens om i serviceavtalet. Nordea förmedlar personbeteckningen i klartext bara till de tjänsteleverantörer som har rätt att handlägga den.

När identifieringsuppgiften i ett svarsmeddelande är krypterad förmedlar Nordea ett kontrolltal som grundar sig på kundens personbeteckning eller FO-nummer till tjänsteleverantören. Själva beteckningen förmedlas inte i svarsmeddelandet. Tjänsteleverantören ska i autentiseringsskedet ha tillgång till kundens personbeteckning eller FO-nummer för att han med hjälp av uppgifterna i Nordeas svarsmeddelande ska kunna försäkra sig om kundens identitet. Om tjänsteleverantören inte har kundens beteckning, ska han be om den innan han sänder en identifieringsbegäran. Funktionen lämpar sig sålunda för att kontrollera med banken att de uppgifter kunden har meddelat är korrekta.

De funktioner där kundens personbeteckning används lämpar sig bl.a. för identifiering av kunden, inloggning i tjänsten och ingående av bindande avtal. Personbeteckningens kontrolldel kan till exempel användas för inloggning efter registreringen i tjänsten.

1.4 Tillämpningsområden och tillgänglighet

E-identifiering lämpar sig för elektroniska tjänster som kräver stark autentisering och som är riktade till finländska privatpersoner. Stark autentisering baserar sig på personliga bankkoder. Därför är det inte möjligt att i tjänsten e-identifiering identifiera personer som saknar en finländsk personbeteckning, personer med konstgjord beteckning eller dödsbon.

E-identifieringstjänsten kan också användas för identifiering av företags- och organisationskunder. När banken ger företagets FO-nummer eller annan specificerande uppgift om företaget som identifieringsuppgift är det inte fråga om stark autentisering.

E-identifieringstjänsten är tillgänglig dygnet runt, alla veckodagar, utom vid avbrott som beror på underhåll, uppdateringar och liknande orsaker.

1.5 E-identifieringens säkerhet

Krypteringsprotokollet SSL/ TLS används för datakommunikationen mellan parterna vid identifieringen. Utomstående kan således inte läsa eller ändra uppgifterna. Tjänsteleverantörens serverprogram måste stödja 128 bitars SSL/TLS-kryptering. Längden på nyckeln som används vid förbindelsen fastställs emellertid på basis av egenskaperna i kundens webbläsare.

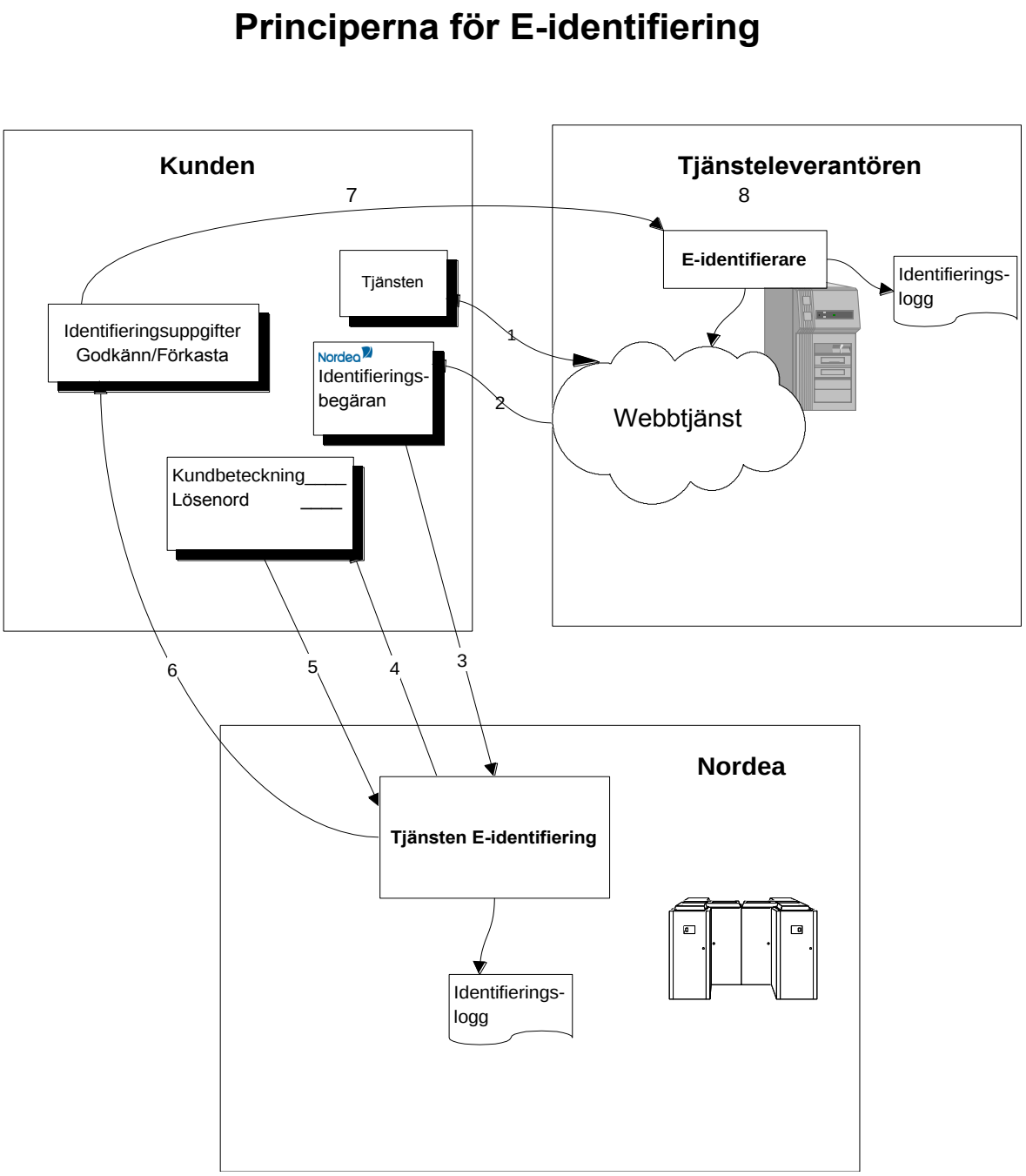
Uppgifterna i identifieringsbegäran och svarsmeddelandet är skyddade med ett kontrolltal som tryggar dataintegriteten. Kunden som styr förmedlingen av identifieringsuppgifterna kan därför inte ändra uppgifterna utan att tjänsteleverantören och Nordea märker det.

Parterna ansvarar själva för säkerheten och sekretessen i sina egna tjänster samt för att registrerade data är korrekta. Kunden ansvarar för att en obehörig inte får tillgång till de koder och andra identifieringsverktyg som Nordea tillhandahåller.

Användaren av tjänsten ansvarar för att en obehörig inte får tillgång till hans bankkoder och att koderna bara ges till den dator i vilken Nordeas identifieringstjänst tillhandahålls. Användaren av tjänsten kontrollerar tjänsteleverantören på basis av de identifieringsuppgifter som Nordea returnerar och godkänner förmedlingen av e-identifieringen.

2 Beskrivning av e-identifieringens funktioner

2.1 Flödet i tjänsten



2.2 Förklaring av flödet i tjänsten

1. Kunden kopplar upp sig till tjänsteleverantörens tjänst. Datakommunikationen mellan kunden och tjänsteleverantören måste vara SSL/TLS-krypterad, när kunden övergår till att registrera uppgifter som gäller identifieringstjänsten. Under skedena 2 - 7 är dataöverföringen alltid SSL/TLS-krypterad.

2. Tjänsteleverantören sänder till kunden en identifieringsbegäran med uppgifter som specificerar transaktionen. I och med att tjänsteleverantören sänder identifieringsbegäran får kunden Nordea-knappen och knappen med vilken transaktionen kan avbrytas på sin skärm.

3. Kunden trycker på funktionsknappen som flyttar honom till Nordeas identifieringstjänst. Identifieringsbegäran som förmedlas till Nordea innehåller de uppgifter tjänsten behöver om tjänsteleverantören och transaktionen. Nordea kontrollerar att identifieringsbegäran är oförvanskad och uppgifterna korrekta.

4. Nordea sänder en identifieringsbegäran till kunden, om den begäran som kommit från tjänsteleverantören är felfri. Nordea sänder till kunden ett felmeddelande ifall Nordea upptäcker felaktigheter i identifieringsbegäran.

5. Kunden identifierar sig hos Nordea. Nordea returnerar ett felmeddelande till kunden om identifieringen misslyckas.

6. Efter en lyckad identifiering bildar Nordea ett svarsmeddelande. Nordeas identifieringstjänst öppnar knapparna för godkännande och avbrytande av identifieringen på kundens skärm och sänder ett svarsmeddelande till kundens webbläsare.

7. Kunden kontrollerar identifierarens uppgifter och godkänner att identifieraren sänds till tjänsteleverantören. Kunden kan förkasta identifieraren med knappen Avbryt och återgå till tjänsteleverantörens tjänst.

8. Tjänsteleverantören kontrollerar att det mottagna svarsmeddelandet är oförvanskat och unikt. Tjänsteleverantören fogar identifieraren till kundens servicetransaktion och förvarar den lika länge som övriga uppgifter i anslutning till tjänsten. Identifierare får inte registreras eller användas för annat ändamål.

3 Beskrivning av meddelanden

3.1 Identifieringsbegäran

Identifieringsbegärans uppgifter finns som dolda variabler i en FORM-datagrupp bakom Nordeas ikon.

FORM-datagruppens struktur är på HTLM-språk:

```
<FORM
METHOD=”POST”
ACTION=”https://tupas.nordea.fi/cgi-bin/SOLO3011”>
<INPUT NAME=”...” TYPE=”...” VALUE=”...”>
<INPUT NAME=”...” TYPE=”...” VALUE=”...”>
</FORM>
```

FORM-DATAGRUPP				
Fält	**Uppgiftens namn**	**Längd**	**Användning**	**Anmärkning**
1. Meddelandetyp	A01Y_ACTION_ID	3 - 4	O	Standard, "701"
2. Version	A01Y_VERS	4	O	0002
3. Tjänsteleverantör	A01Y_RCVID	10 -15	O	Kundbeteckning
4. Tjänstens språk	A01Y_LANGCODE	2	O	FI = finska SV = svenska EN = engelska
5. Specificering av förfrågan	A01Y_STAMP	20	O	Åååämmddhhmmssxxxxxx
6. Typ av identifierare	A01Y_IDTYPE	2	O	01 = Krypterad grundbeteckning 01 = Grundbeteckning i klartext 03 = Kort beteckning i klartext
7. Returadress	A01Y_RETLINK	199	O	OK returadress för identifieraren
8. Avbryta-adress	A01Y_CANLINK	199	O	Returadress vid avbrott
9. Förkastad-adress	A01Y_REJLINK	199	O	Returadress vid felsituationer
10. Nyckelversion	A01Y_KEYVERS	4	O	Uppgift om nyckelgeneration
11. Algoritm	A01Y_ALG	2	O	03= SHA- 256
12. Kontrolltal	A01Y_MAC	32-64	O	Förfrågans säkerhetsfält

Namnen på uppgifterna skrivs med stora bokstäver i datafälten. FORM-datagruppens struktur på HTLM-språk är

<FORM METHOD=”POST” ACTION=”*Nordeas E-identifieringstjänst URL*”>
<INPUT NAME=”A01Y_ACTION_ID” TYPE=”hidden” VALUE=”701”>
<INPUT NAME=”A01Y_VERS” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_RCVID” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_LANGCODE” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_STAMP” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_IDTYPE” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_RETLINK” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_CANLINK” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_REJLINK” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_KEYVERS” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_ALG” TYPE="hidden” VALUE=”...”>
<INPUT NAME=”A01Y_MAC” TYPE="hidden” VALUE=”...”>
</FORM>

3.2 Förklaringar av fälten:

1. Meddelandetyp, som har standard 701.

2. Versionsnumret för identifieringsbegäran, som är 0002.

3. Tjänsteleverantörens kundbeteckning. Nordea identifierar tjänsteleverantören med hjälp av kundbeteckningen och fogar tjänsteleverantörens namn, som finns i Nordeas register, till identifieringsmeddelandet.

4. Språkkoden anger på vilket språk tjänsteleverantörens sida visas och Nordeas tjänst öppnas på det språket, om det finns med bland de språk som används i Nordeas e-identifiering.

5. Specificerande kod som tjänsteleverantören gett för identifieringsbegäran. Koden kan vara en referens, ett kundnummer eller en kombination av datum, klockslag och löpande beteckning samt referens.

6. Typen av identifierare anger vilken specificerande uppgift tjänsteleverantören vill ha om den kund som ska identifieras. Den ska överensstämma med det som har avtalats i serviceavtalet.

> 01 = Krypterad grundbeteckning. MAC-kontrolltal i hexadecimalform som uträknats på basis av kundens identifieringsinformation. Innehåller kundens fullständiga personbeteckning eller FO-nummer.
>
> 02 = Grundbeteckning i klartext. Innehåller kundens fullständiga personbeteckning eller FO-nummer.
>
> 03 = Kort beteckning i klartext. Innehåller personbeteckningens kontrolldel utan skiljetecken för århundrade eller ett hellångt FO-nummer.

7. Adressen till tjänsteleverantörens webbsida, dit kunden fortsätter om han väljer OK. Returadressen ska börja med https, dvs. vara en SSL/TLS-skyddad sida.

Exempel: VALUE="https://tuote.kauppa.fi/tilaus/vahvistus.htm"

8. Härifrån går kunden vidare i tjänsteleverantörens tjänst, om han avbryter förmedlingen av identifieraren.

Exempel: VALUE="https://tuote.kauppa.fi/tilaus/vahvistus.htm"

9. Härifrån fortsätter kunden i tjänsteleverantörens tjänst, om det finns ett tekniskt fel i identifieringen. Returadressen kan vara densamma som i fält 10.

Exempel: VALUE="https://tuote.kauppa.fi/tilaus/vahvistus.htm"

10. Den nyckelversion som används vid uträkningen av MAC-kontrolltalet.

11. Typkoden för den algoritm som används vid uträkningen av MAC-kontrolltalet. Nordeas e-identifiering har algoritmen 03 =SHA256

12. MAC-kontrolltal som har räknats ut på basis av uppgifterna i identifieringsbegäran och tjänsteleverantörens nyckel med den i fältet 11 angivna algoritmen. Mottagaren kontrollerar identifieringsbegärans integritet och avsändaren med hjälp av kontrolltalet.

3.3 Bildande av identifieringsbegärans MAC-kontrolltal

Tjänsteleverantören bildar en identifieringsbegäran som behövs för Nordea-knappen och skyddar sin begäran med ett MAC-kontrolltal. Kontrolltalet uträknas med den nyckel som Nordeas tjänsteleverantör fått i FORM-datagruppen.

När uträkningen inleds bildas en teckensträng av VALUE-värdet i FORM-datagruppens alla datafält som finns före kontrolltalet (fälten 1–11) och av tjänsteleverantören nyckel. Uppgifterna läggs ihop till en teckensträng så att de blanksteg som är utfyllnadstecken i fälten lämnas bort. Teckensträngens datagrupper åtskiljs med ett &-tecken. Tecknet ”&” läggs också in mellan den sista informationen (fält 12) och nyckeln samt i slutet av nyckeln. Tecknen ”&” tas med i beräkningen av meddelandets MAC-

kontrolltal. Uppgiften finns på en rad. Tecknet "↵" visar radbyte i dokumentet.

A01Y_ACTION_ID&A01Y_VERS&A01Y_RCVID&A01Y_LANGCODE&A01Y_STAMP&↵
A01Y_IDTYPE&A01Y_RETLINK&A01Y_CANLINK&A01Y_REJLINK&A01Y_KEYVERS&↵
A01Y_ALG&nyckel&

Det uträknade MAC omvandlas till hexadecimalform, där A - F anges med stora bokstäver. Det hexadecimala värdet förs in i fältet för MAC-kontrolltalet.

3.4 Svarsmeddelande och identifierare

Nordea fogar uppgifterna i svarsmeddelandet till OK-returlänken i ett query-string format

Kontrolltalet uträknas utgående från det ursprungliga meddelandet, varefter de skandinaviska tecknen och vissa specialtecken (t.ex. blanksteg, lika med och citationstecken) ersätts med motsvarande hexadecimaltecken (t.ex. %20) i datakommunikationsmeddelandet.

Nordea räknar ut svarsmeddelandets MAC-kontrolltal med hjälp av den tjänsteleverantörspecifika nyckeln. Med hjälp av kontrolltalet kan tjänsteleverantören vara säker på att identifieraren har bildats i kundens bank och att informationen i identifieringsmeddelandet inte har ändrats. Tjänsteleverantören måste försäkra sig om MAC-kontrolltalets riktighet efter att ha mottagit identifieringstransaktionen.

SVARSMEDDELANDE				
Fält	**Uppgiftens namn**	**Längd**	**Använd-ning**	**Anmärkning**
1. Version	B02K_VERS	4	O	0002
2. Specificering av identifierare	B02K_TIMESTMP	23	O	NNNåååå-åmmddhhmmssxxxxxx
3. Identifierarens nummer	B02K_IDNBR	10	O	Nummer som Nordea gett identifieraren
4. Specificering av förfrågan	B02K_STAMP	20	O	Förfrågans datafält 7 (A01Y_STAMP)
5. Kund	B02K_CUSTNAME	40	O	Kundens namn
6. Nyckelversion	B02K_KEYVERS	4	O	Nyckelgeneration
7. Algoritm	B02K_ALG	2	O	03 = SHA-256
8. Identifierare	B02K_CUSTID	-64	O	Krypterad identifierare eller kundkod i klartext
9. Typ av identifierare	B02K_CUSTTYPE	2	O	01 = personbeteckning i klartext 02 = person-beteckningens kontrolldel i klartext 03 = FO-nummer i klartext 05 = krypterad personbeteckning 06 = krypterat FO-nummer
10. Kontrolltal	B02K_MAC	AN 32-64	O	Svarets säkerhetskontrolltal

3.5 Förklaringar:

1. Svarsmeddelandets versionsnummer, som är 0002.

2. Tidstämpel som skapas av Nordeas system, där NNN alltid är 200 och visar att det är fråga om Nordea. Nordea returnerar den 19 tecken långa formen NNNååååmmddttmmssxx där tecknen xx efter tidsstämpeln betyder hundradedelssekunder.

3. Information som Nordeas datasystem ger identifieraren och som specificerar den i Nordeas system.

4. Individualiserar identifieringsbegäran och tas från ifrågavarande identifieringsbegärans fält 7 (A01Y_STAMP)

5. Kundens namn i Nordeas kundregister

6. Anger vilken generation MAC-nyckeln tillhör

7. MAC-kontrollalgoritmens kod

8. Kundens identifieringsuppgift. Beteckning i klartext eller krypterat kontrolltal, beroende på innehållet i identifieringsbegärans fält A01Y_IDTYPE. FO-numret i klartext förmedlas med bindestreck i formatet xxxxxxx-x.

9. Typ av identifierare. Detta fält anger vilken identifieringsinformation som används i fält 8. Eventuella värden är 00 = ej känd (används inte i Nordea) 01 = personbeteckning i klartext 02 = kontrolltalet för en personbeteckning i klartext 03 = FO-nummer i klartext. 04 = beteckning i klartext för elektroniska ärenden. Används inte i Nordea. 05 = skyddad personbeteckning 06 = skyddat FO-nummer. 07 = krypterad kod för elektroniska ärenden. Används inte i Nordea.

10. Svarsmeddelandets kontrolltal.

3.6 Uträkning av svarsmeddelandets kontrolltal

Vid kontroll av det mottagna svarsmeddelandets integritet, uträknas först ett kontrolltal av svarsmeddelandet som jämförs med meddelandets kontrolltal. Kontrolltalet uträknas på basis av datafälten 1–9. Innehållet i fälten B02K_CUSTID bestäms utgående från vad som begärts i identifieringsbegäran, dvs. det är antingen ett krypterat kontrolltal eller en kundbeteckning i klartext. Vid uträkningen av kontrolltalet åtskiljs uppgifterna och nyckeln med ett &-tecken som också läggs till i slutet av nyckeln. Vid uträkningen av kontrolltalet används en tjänsteleverantörsspecifik nyckel.

B02K_VERS&B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&↵
B02K_CUSTNAME&B02K_KEYVERS&B02K_ALG&↵ B02K_CUSTID&B02K_CUSTTYPE&nyckel&

3.7 Typ av identifierare

Uträkningen av svarsmeddelandets kontrolltal beror på typen av kundbeteckning. Den anges i identifieringsbegärans fält A01Y_IDTYPE. Kundens identifierare är antingen 1) en kundbeteckning i klartext eller 2) ett krypterat kontrolltal.

1. Identifiering av kunden med en kundbeteckning i klartext

Identifieringsbegärans fält A01Y_IDTYPE har värdena ”02” och ”03”: grundbeteckning i klartext eller kort grundbeteckning.

Kundens beteckning är en teckensträng i klartext, t.ex. personbeteckningen eller dess kontrolldel i enlighet med fält A01Y_IDTYPE i identifieringsbegäran. Beteckningen läggs som sådan in i svarsmeddelandets B02K_CUSTID.

2. Identifiering av kunden med ett krypterat kontrolltal

Identifieringsbegärans fält A01Y_IDTYPE har värdet ”01” dvs. en krypterad grundbeteckning.

Vid krypteringen av kundbeteckningen använder banken samma korta algoritm som vid

kontrollräkningen av meddelandena. Identifieringsuppgiften krypteras genom användning av uppgifterna i svarsmeddelandets fält 2–4 och i banken registrerad kundbeteckning (personbeteckning eller FO-nummer). Vid uträkningen av den krypterade beteckningen åtskiljs uppgifterna och nyckeln med ett &-tecken som också läggs till i slutet av nyckeln. Vid kryptering används en tjänsteleverantörsspecifik nyckel.

B02K_TIMESTMP&B02K_IDNBR&B02K_STAMP&↵
kundbeteckning&nyckel&

Den krypterade beteckningen omvandlas till hexadecimalform, där A–F anges med stora bokstäver. Då fås slutligen en teckensträng som identifierar kunden och som läggs in som uppgift B02K_CUSTID i svarsmeddelandet.

3.8 Kontroll av meddelandets kontrolltal och identifiering av kunden

Tjänsteleverantören räknar ut MAC-kontrolltalet för det mottagna meddelandet enligt beskrivningen i punkt 3.6. Om det överensstämmer med det kontrolltal som finns i bankens svarsmeddelande, har inga ändringar skett i svarsmeddelandet.

Om en krypterad beteckning har använts i svarsmeddelandet, kontrollerar tjänsteleverantören att kundbeteckningen är korrekt genom att räkna ut kontrolltalet utgående från informationen i svarsmeddelandets datafält och den beteckning han har tillgång till, i enlighet med beskrivningen i punkt 3.7. Om det erhållna kontrolltalet motsvarar innehållet i svarsmeddelandets identifierarfält (B02K_CUSTID), är den identifierare som tjänsteleverantören har korrekt.

4 Exceptionella situationer

Tjänsteleverantören ska vara förberedd på följande situationer:

1. Kunden avbryter identifieringstransaktionen. Kunden kan avbryta transaktionen antingen innan identifieraren förmedlas till Nordea eller med knappen Avbryt efter att identifieraren bildats. I knappen finns Avbryt-adressen som anges i identifieringsbegärans FORM-datafält 10.

2. Verifieringen av kunden misslyckas antingen på grund av att de identifieringsuppgifter kunden gett är felaktiga eller kunden bett om verifiering i fel bank.

3. Nordea upptäcker ett fel i meddelandet med identifieringsbegäran.

4. Tjänsteleverantören upptäcker ett fel i svarsmeddelandet, som kan bero på att det finns ett fel i meddelandets innehåll eller på att identifieraren inte överensstämmer med de personuppgifter kunden uppgett. Tjänsteleverantören ska sända ett korresponderande meddelande om situationen till kunden.

5. Inget svar fås från kunden. Avbrottet kan bero på ett avbrott i förbindelsen eller en annan teknisk störning, eller på att kunden avbryter sessionen.

6. Samma svar fås flera gånger. Tjänsteleverantören ska vara förberedd på att kunden sänder samma svar flera gånger eller att kunden sänder ett gammalt svarsmeddelande när han med hjälp av knapparna bakåt/framåt flyttar från en skärm till en annan i webbläsaren.

5 Byte och förvaring av nycklar

Den MAC-nyckel som används vid uträkningen av kontrolltal kan bytas ut på Nordeas eller tjänsteleverantörens önskan.

Nyckeln sänds till den kontaktperson som anges i avtalet. Samtidigt meddelas också vilket

versionsnummer den nya nyckeln har och när den träder i kraft, dvs. från vilken dag kontrolltalet räknas med ifrågavarande nyckel.

För att nyckeln ska kunna bytas ut så smidigt som möjligt ska tjänsteleverantörens system kunna registrera den nya nyckeln i systemet på förhand, dvs. minst två nycklar ska kunna användas samtidigt. Vid tidpunkten för bytet, under ca 15 minuter, är det möjligt att kontrolltalet i en del av de identifierare som tjänsteleverantören mottar har uträknats med en gammal nyckel och att en del har uträknats med en ny.

När en ny nyckel har använts på ett lyckat sätt, kan den gamla nyckeln tas bort eller dess användning spärras i tjänsteleverantörens system.

5.1 Spärrning av MAC-nyckel

Tjänsteleverantören ska förvara MAC-nyckeln omsorgsfullt så att obehöriga inte kan använda den. Om det finns misstankar om att MAC-nyckeln har råkat i fel händer ska nyckeln omedelbart spärras via Betalningsrådgivning för företag.

Kontakta spärrtjänsten +358 20 333 utanför bankens öppettider.

6 Funktioner och Nordea-knappen

I tjänsteleverantörens nättjänst får endast följande namn användas om Nordea:

Nordea
Nordea Bank
Nordea Bank Finland Abp

I tjänsteleverantörens Internettjänst ska användningen av e-identifieringen anges med Nordea-knappen eller med texten Nordea e-identifiering som ska vara väl synlig.

Hur Nordea-knappen ska presenteras och anvisningar samt förutsättningar för användningen finns i villkoren för avtalet om tjänsten. Nordea-knappen fås från Nordeas server på adressen www.nordea.fi/nordeaknappen efter att avtalet har ingåtts. Knappen får inte överlåtas eller användas för något annat ändamål än vad som har avtalats i avtalet om tjänsten. Tjänsteleverantören får inte själv utarbeta eller ändra Nordea-knappen.

7 Användning av e-identifiering

7.1 Förutsättningar

Tjänsteleverantörens system ska med www-teknik kunna bilda en identifieringsbegäran åt användaren av tjänsten. När användaren har godkänt att identifieraren ska förmedlas till tjänsteleverantören, ska den fogas till användarens uppdrag och förvaras lika länge som uppdraget. Identifierare får inte registreras eller användas för annat ändamål. Tjänsteleverantören måste föra en logg i vilken identifieringsbegäran kan specificeras i eventuella problemfall eller om utredningar behövs.

E-identifieringen kräver inte någon viss typ av www-serverprogram, men den ska stöda 128 bitars SSL/TLS-kryptering.

7.2 Avtal

Tjänsteleverantören ingår ett skriftligt avtal med Nordea om användningen av e-identifiering. Tjänsteleverantörens uppgifter registreras i banken och en MAC-nyckel sänds till den kontaktperson som anges i avtalet.

Ett serviceavtal ska ingås för varje enskilt avtal och för varje funktion. En tjänst kan dock omfatta flera funktioner. Nordea ingår ett avtal om förmedling av personbeteckning bara i det fall att tjänsteleverantören har rätt att registrera en personbeteckning.

I avtalet antecknas hur lång nyckeln är och tjänsteleverantörens rätt att registrera personbeteckningen.

Tjänsteleverantören ska meddela bankens kontor om det sker ändringar i hans tjänst eller uppgifter. Vid behov kompletterar kontoret avtalet med de ändrade uppgifterna.

7.3 Testning

När avtalet ingås avtalar man om när tjänsten ska tas i bruk.

Med hjälp av Nordeas testkoder kan tjänsteleverantören testa tjänsten i produktionsmiljö redan innan avtalet har ingåtts. Om tjänsteleverantören vill testa tjänsten med riktiga bankkoder och/eller hur avtalet fungerar, ska ett avtal ingås med Nordea som görs direkt i produktionsmiljö. Det är dock möjligt att bestämma en testadress för tjänsteleverantören för testtiden.

Internettjänstens adress: https://tupas.nordea.fi

Tjänsteleverantör 87654321
Nyckel: LEHTI

Bankkoder som kunden använder på identifieringsskärmen
Kundnummer 123456
Kod: 1111

IDENTIFIERINGSBEGÄRAN - TESTMEDDELANDE FORM-datafält	
A01Y_ACTION_ID	701
A01Y_VERS	0002
A0IY_RCVID	87654321
A01Y_LANGCODE	se beskrivning
A01Y_STAMP	se beskrivning
A01Y_IDTYPE	se beskrivning
A01Y_RETLINK	se beskrivning
A01Y_CANLINK	se beskrivning
A01Y_REJLINK	se beskrivning
A01Y_KEYVERS	0001
A01Y_ALG	03
A01Y_MAC	se beskrivning

SVARSMEDDELANDE	
B02K_VERS	0002
B02K_TIMESTMP	se beskrivning
B02K_IDNBR	se beskrivning
B02K_STAMP	Förfrågans datafält A01Y_STAMP
B02K_CUSTNAM	SOLO DEMO
B02K_KEYVERS	0001
B02K_ALG	03

B02K_CUSTID	**Grundkod**: 210281-9988 **Kort kod**: 9988
	Krypterad kod: Räknad av koden 210281-9988
B02K_CUSTTYPE	se beskrivning
B02K_MAC	se beskrivning

8 Rådgivning och tekniskt stöd

Betalningsrådgivning för företag

I problemsituationer får du under bankdagar hjälp av Betalningsrådgivning för företag (kontrollera öppettiderna alltid på bankens webbplats eller på kontoret):

På finska: 0200 67210 (klo 8–18), lna/ msa eller pris för utrikessamtal

På svenska: 0200 67220 (kl. 9–16.30), lna/ msa eller pris för utrikessamtal

På engelska: (+358) 200 67230 (9–18), lna/ msa eller pris för utrikessamtal

Om du meddelar tjänsteleverantörens kod går betjäningen snabbare.

9 Tecken som används i tjänsten

I tjänsten används 8 bitars ISO 8859-1 latinsk teckenuppsättning, vars koder upptas i bifogade tabell.

æ	%00	0	%30	`	%60		%90	À	%c0	ð	%f0
	%01	1	%31	a	%61	‘	%91	Á	%c1	ñ	%f1
	%02	2	%32	b	%62	’	%92	Â	%c2	ò	%f2
	%03	3	%33	c	%63	“	%93	Ã	%c3	ó	%f3
	%04	4	%34	d	%64	”	%94	Ä	%c4	ô	%f4
	%05	5	%35	e	%65	•	%95	Å	%c5	õ	%f5
	%06	6	%36	f	%66	–	%96	Æ	%c6	ö	%f6
	%07	7	%37	g	%67	—	%97	Ç	%c7	÷	%f7
backspace	%08	8	%38	h	%68	˜	%98	È	%c8	ř	%f8
tab	%09	9	%39	i	%69	™	%99	É	%c9	ů	%f9
linefeed	%0a	:	%3a	j	%6a	š	%9a	Ê	%ca	ú	%fa
	%0b	;	%3b	k	%6b	›	%9b	Ë	%cb	ű	%fb
	%0c	<	%3c	l	%6c	œ	%9c	Ì	%cc	ü	%fc
c return	%0d	=	%3d	m	%6d		%9d	Í	%cd	ý	%fd
	%0e	>	%3e	n	%6e		%9e	Î	%ce	ţ	%fe
	%0f	?	%3f	o	%6f	Ÿ	%9f	Ï	%cf	˙	%ff
	%10	@	%40	p	%70		%a0	Đ	%d0		
	%11	A	%41	q	%71	¡	%a1	Ñ	%d1		
	%12	B	%42	r	%72	¢	%a2	Ò	%d2		
	%13	C	%43	s	%73	£	%a3	Ó	%d3		
	%14	D	%44	t	%74		%a4	Ô	%d4		
	%15	E	%45	u	%75	¥	%a5	Õ	%d5		
	%16	F	%46	v	%76	¦	%a6	Ö	%d6		
	%17	G	%47	w	%77	§	%a7		%d7		
	%18	H	%48	x	%78	¨	%a8	Ø	%d8		
	%19	I	%49	y	%79	©	%a9	Ù	%d9		
	%1a	J	%4a	z	%7a	ª	%aa	Ú	%da		
	%1b	K	%4b	{	%7b	«	%ab	Û	%db		
	%1c	L	%4c	|	%7c	¬	%ac	Ü	%dc		
	%1d	M	%4d	}	%7d	¯	%ad	Ý	%dd		
	%1e	N	%4e	~	%7e	®	%ae	Þ	%de		
	%1f	O	%4f		%7f	¯	%af	ß	%df		
Space	%20	P	%50	€	%80	°	%b0	ŕ	%e0		
!	%21	Q	%51		%81	±	%b1	á	%e1		
"	%22	R	%52	‚	%82	˛	%b2	â	%e2		
#	%23	S	%53	ƒ	%83	ł	%b3	ă	%e3		
$	%24	T	%54	„	%84	´	%b4	ä	%e4		
%	%25	U	%55	…	%85	µ	%b5	Í	%e5		
&	%26	V	%56	†	%86	¶	%b6	ć	%e6		
'	%27	W	%57	‡	%87	·	%b7	ç	%e7		
(	%28	X	%58	ˆ	%88	¸	%b8	è	%e8		
)	%29	Y	%59	‰	%89	¹	%b9	é	%e9		
*	%2a	Z	%5a	Š	%8a	º	%ba	ê	%ea		
+	%2b	[	%5b	‹	%8b	»	%bb	ë	%eb		
,	%2c	\	%5c	Ś	%8c	¼	%bc	ì	%ec		
-	%2d	]	%5d		%8d	½	%bd	í	%ed		
.	%2e	^	%5e	Ž	%8e	¾	%be	î	%ee		
/	%2f	_	%5f		%8f	¿	%bf	ï	%ef		