

E-Betalning

Teknisk handbok – Version 0712
(2018-10-01)

Innehåll

1	Inledning	3
1.1	E-betalning, Version 1.1	3
1.2	Att komma igång – Arbetsgången.....	3
1.3	Teknisk flödesbeskrivning - betalningstjänsterna	4
1.4	Teknisk flödesbeskrivning - betalningskontroll och återbetalning	5
2	Informationsflöde mellan webbutik och bank.....	8
2.1	”Betala direkt”	8
2.2	”Betalningskontroll”	11
2.3	”Återbetalning”	15
3	Förändringsskydd	19
3.1	HMAC-SHA256-128	19
3.2	Hemlig nyckel	20
3.3	KVV - Nyckelverifieringsvärde	20
4	Verifiering av informationsflöde.....	21
4.1	Skillnader i informationsflödet.....	21
4.2	Verifiering av transaktionsuppgifter	21
4.3	Simulerade returflöden	21
5	Betalningstjänstinformation	22
5.1	”Betala direkt”	22
5.2	”Betalningskontroll”	22
5.3	”Återbetalning”	22

Tabellförteckning

Tabell 1	
”Betala direkt”, Gränssnitt till betaltjänst från butik	8
Tabell 2	
”Betala direkt”, Gränssnitt från betaltjänst till butik	9
Tabell 3	
”Betalningskontroll”, Gränssnitt till betalningskontroll från butik	11
Tabell 4	
”Betalningskontroll”, Gränssnitt från betalningskontroll till butik	12
Tabell 5	
”Återbetalning”, Gränssnitt till återbetalningstjänst från butik	15
Tabell 6 ”	
Återbetalning”, Gränssnitt från återbetalningstjänst till butik	17

Denna butikshandbok är publicerad av Nordea Bank Abp, filial i Sverige. Revideringar och förändringar till följd av skrivfel eller felaktigheter kan komma att göras av Nordea, när som helst och utan förvarning. Sådana ändringar kommer att ingå i nya versioner av denna handbok. Handboken skall inte uppfattas som en garanti från Nordea om att i handboken beskrivna system skall ha en viss funktionalitet eller kvalitet.

Nordea ansvarar för att upprätthålla gränssnitt och definitioner enligt denna butikshandbok. Vid förändringar av gränssnitt och definitioner så kommer Nordea att gå ut med information om det i god tid. Ytterligare teknisk utveckling som butiken implementerar utöver det som beskrivs i denna handbok tar Nordea ej ta ansvar för eller förbinder sig att stödja vid framtida förändringar av e-betalningstjänsten.

Alla rättigheter förbehålls Nordea Bank Abp, filial i Sverige. 2018-10-01

1 Inledning

E-betalning är en elektronisk betaltjänst för säkra betalningar vid köp på nätet. Tjänsten är utvecklad för företag, organisationer, föreningar och enheter inom den offentliga sektorn som vill sälja varor eller tjänster i Sverige via Internet.

1.1 E-betalning, Version 1.1

I den uppdaterade versionen 1.1 av tjänsten kommer "Betala direkt" att erbjudas: "Betala senare" samt "Delbetalning" kommer inte att erbjudas från den uppdaterade versionen 1.1. Dessutom innefattar e-betalning även tjänsterna "Betalningskontroll" och "Återbetalning" för säljföretagen att kontrollera om betalningar är mottagna av banken samt för att återbetala hela eller delar av utförda direktbetalningar.

Denna installationsmanual omfattar den uppdaterade versionen 1.1 av e-betalning.

"Betala direkt"	innebär att transaktionen genomförs direkt. Köpesumman dras från köparens konto och krediteras säljföretagets konto. Överföringen sker i bankens betalsystem.
"Betalningskontroll"	innebär en möjlighet för säljföretaget att i efterhand kontrollera om enskilda betalningar har mottagits, behandlats och avslutats korrekt i betalningstjänsten.
"Återbetalning"	innebär en möjlighet för säljföretaget att i efterhand återbetala hela eller delar av beloppet för betalningar som skett via e-betalningens direktbetalning.

1.2 Att komma igång – Arbetsgången

1.2.1 Implementation

Säljföretaget bygger in länkar enligt beskrivning i denna manual från sin webbutik till betaltjänsten. Det krävs av säljföretaget att ett referensnummer för betalningen genereras för varje köporder. Dessutom krävs att säljföretaget implementerar rutin för generering av en kontrollsumma enligt en speciell algoritm, HMAC, genom egen utveckling eller med programvaruföretagets uppdateringar/program. För en mer utförlig beskrivning av HMAC, se kapitel 3 Förändringsskydd.

Säljföretaget erhåller en hemlig sigillnyckel från Nordea som måste installeras och hållas skyddad samt ett nyckelverifieringsvärde (KVV).

1.2.2 Teknisk support

Support ges av Internetsupport vardagar från kl. 08.00 till kl. 18.00 på telefonnummer 0771-776991.

1.3 Teknisk flödesbeskrivning - betalningstjänsterna

Nedan följer en teknisk beskrivning, i punktform, av vad som sker vid "Betala direkt"

- Köparen har plockat ihop sin beställning i webbutiken och vill betala genom e-betalning. Nödvändig information om köpet samlas i ett elektroniskt betalningsformulär, vars format är specificerat av Nordea. Detta betalningsformulär utgör webbutikens gränssnitt mot betaltjänsten. För att säkerställa att information inte ändras, räknar webbutiken ut en kontrollsumma på innehållet i formuläret. På så sätt kan eventuella ändringar i formuläret som gjorts på vägen mellan webbutik och betaltjänst upptäckas.

Exakt hur det går till när köparen handlar i webbutiken och hur betalnings sidorna ser ut är upp till sälj företaget att utforma. Det viktiga är att betalningsformuläret har rätt format.

Det enda krav som e-betalningstjänsten har på webbutiken är att hänvisningen till e-betalningen inte får vara i ramar (frames) eller att webbutiken agerar som en sorts hänvisare för köparen under köparens session med e-betalningstjänsten, utan att webbutiken endast hänvisar köparen vidare till e-betalningstjänsten genom att posta ett formulär.

- Köparen uppmanas via en inloggningsdialog att upprätta en säker förbindelse (https/SSL) med betaltjänsten innan betalningsformuläret skickas. Den säkra förbindelsen innebär framförallt att:
 - Meddelanden som skickas mellan köpare och betaltjänst krypteras.
 - Köparen kan vara säker på att han verkligen kontaktat bankens betaltjänst och ingen annan server. Det beror på att betaltjänsten lämnar ifrån sig ett så kallat servercertifikat, som är ett sorts elektroniskt ID-kort köparen använder för att identifiera Nordea.
- Betalningsformuläret skickas nu till betaltjänsten, som räknar ut en kontrollsumma och jämför den med den som webbutiken räknat ut och skickat till betaltjänsten. Betaltjänsten kontrollerar också att formuläret har rätt format.
- Köparen vet att betaltjänsten är Nordea, men det omvända förhållandet gäller inte, d v s Nordea vet inte vem köparen är. Köparen måste därför identifiera sig.
- Köparen identifierar sig med av banken godkänd säkerhetslösning. Köparens identitet skickas till betaltjänsten.
- Nordea tar emot inloggningen och presenterar betalningsinformationen tillsammans med köparens kontoinformation. Information om betalningen alternativt betalningsuppdrag och köpare/sälj företag presenteras på en kontroll sida. Nordea ber köparen att signera betalningen.

- Köparen kontrollerar att uppgifterna för betalningen är korrekta, och bekräftar betalningen, genom att signera betalningsinformationen. Signeringen sker genom att köparen använder sig av en av banken godkänd säkerhetslösning.
- Betalningen utförs om signaturen är korrekt.
- Betaltjänsten presenterar en bekräftelse för köparen att betalningen är slutförd. Köparen länkas automatiskt tillbaka till webbutiken med en bekräftelse innehållande information om betalningen. Om förbindelsen med webbutiken skulle ha avbrutits så kan sälj företaget ändå kontrollera om betalningsuppdraget mottagits via en betalningskontroll.

Sälj företaget kan kontrollera att betalningen genomförts bl a via:

- Kontoutdrag (för PlusGirokonto och Nordeakonto)
- Företagstjänsten via PC - Nordea Axess (visar Nordeakonto)
- Företagstjänsten via Internet (visar Nordeakonto)
- Corporate Netbank (visar PlusGirokonto och Nordeakonto)
- ePlusGiro Företag (visar PlusGirokonto)
- GiroVision (visar PlusGirokonto)

Om sälj företaget använder ett PlusGirokonto som mottagarkonto för e-betalning visas endast 13 tecken av referensnumret på kontoutdraget, i ePlusGiro Företag och i GiroVision. Om sälj företaget använder ett Nordeakonto som mottagarkonto visas 25 tecken.

1.4 Teknisk flödesbeskrivning - betalningskontroll och återbetalning

Nedan följer en teknisk beskrivning, i punktform, av vad som sker vid "betalningskontroll" och "återbetalning". Bägge tjänsterna har samma flöde och därmed gäller beskrivningen för bägge.

- Sälj företaget tillhandahåller en webbsida där en av sälj företaget utsedd användare kan mata in nödvändig information för en återbetalning eller betalningskontroll i ett formulär. Denna webbsida räknar även ut en kontrollsumma för de inmatade värdena som används för att säkerställa att informationen inte ändras på vägen till banktjänsten. Värdena och kontrollsumman utgör butikens gränssnitt mot betalningskontrolls- och återbetalningstjänsten. Exakt hur formuläret ser ut är upp till butiken att utforma, det viktiga är att informationen som skickas har rätt format, enligt beskrivning i denna manual.
- När användaren sedan väljer att skicka iväg uppgifterna till banktjänsten uppmanas användaren att upprätta en säker förbindelse (https/SSL) med betalningskontrolls- och återbetalningstjänsten. Den säkra förbindelsen innebär framförallt att:
 - Meddelanden som skickas mellan användaren och betaltjänst krypteras.
 - Användaren kan vara säker på att han verkligen kontaktat e-betalningstjänsten och ingen annan server. Det beror på att betaltjänsten lämnar ifrån sig ett så kallat servercertifikat, som är ett sorts elektroniskt ID-kort som webbshopen använder för att identifiera Nordea.
- Informationen i formuläret skickas nu till e-betalningstjänsten, som också räknar ut en kontrollsumma på samma information och

jämför den med den som webbutiken räknat ut och skickat till e-betalningstjänsten. e-betalningstjänsten kontrollerar också att all information i formuläret har rätt format.

- Användaren vet vem e-betalningstjänsten är, men det omvända förhållandet gäller inte, d v s Nordea vet inte vem användaren är. För att göra en betalningskontroll eller återbetalning behövs heller inte detta, det räcker att e-betalningstjänsten vet att sälj företaget verkligen är det sälj företag det utger sig att vara. Detta säkerställs genom kontrollsumman som använts för den skickade informationen, en kontrollsumma uträknad med en speciell algoritm, HMAC, samt den hemliga sigillnyckel som bara sälj företaget skall känna till.
- Om kontrollsumman (MAC) stämmer hämtas information om den ursprungliga betalningen och om en återbetalning är efterfrågad kontrolleras att beloppet för återbetalningen inte överstiger den ursprungliga betalningen innan återbetalningen utförs. Återbetalningen innebär att den ursprungliga betalningen reverseras, dvs. återbetalningsbeloppet dras ifrån sälj företagets konto och överförs till köparens belastningskonto.
- e-betalningstjänsten presenterar en webbsida med bekräftelse för användaren med information om betalningen. Informationen presenteras i en tabell där det tydligt framgår den efterfrågade eller återbetalade betalningens status, belopp och valuta. Dessutom finns en knapp med en länk till sälj företagets webbutik där användaren kan välja att skicka en bekräftelse till webbutiken. Bekräftelse till webbutiken innehåller information om den efterfrågade eller återbetalade betalningen, som webbutiken kan spara undan eller behandla och registrera i sitt affärssystem.

Sälj företaget kan kontrollera att återbetalningen genomförts bland annat via:

- Kontoutdrag (för PlusGirokonto och Nordeakonto)
- Företagstjänsten via PC - Nordea Axess (visar Nordeakonto)
- Företagstjänsten via Internet (visar Nordeakonto)
- Corporate Netbank (visar PlusGirokonto och Nordeakonto)
- ePlusGiro Företag (visar PlusGirokonto)
- GiroVision (visar PlusGirokonto)

Om sälj företaget använder ett PlusGirokonto som mottagarkonto för e-betalning visas endast 13 tecken av referensnumret på kontoutdraget, i ePlusGiro Företag och i GiroVision. Om sälj företaget använder ett Nordeakonto som mottagarkonto visas 25 tecken.

Förloppet ovan är beskrivet för en manuell användning av betalningskontroll och återbetalning, där en av sälj företaget utsedd användare manuellt matar in informationen som är nödvändig för betalningskontrollen eller återbetalningen.

Sälj företaget kan även välja att låta hela förloppet ske mer automatiskt av sin webbutik eller annat affärssystem som har Internetkommunikation. Istället för att då en användare manuellt matar in informationen så sätter webbutiken själv ihop informationen som skickas till e-betalningstjänsten och läser sedan av informationen i bekräftelsen som returneras tillbaka ifrån e-betalningstjänsten.

Det ovan beskrivna flödet gäller även för den automatiska användningen med den skillnaden att användaren istället representeras av webbutiken.

2 Informationsflöde mellan webbutik och bank

I nedanstående text beskrivs det informationsflöde som äger rum mellan sälj företaget och Nordea för de tjänster som e-betalning innefattar:

- "Betala direkt", se avsnitt 2.1
- "Betalningskontroll", se avsnitt 2.2
- "Återbetalning", se avsnitt 2.3

2.1 "Betala direkt"

2.1.1 Transaktionsuppgifter till betaltjänsten från webbutiken

Webbutiken skickar följande transaktionsuppgifter till betaltjänsten via HTTP metoden POST:

#	Parameternamn	Beskrivning	Värde	Format	Användning
1.	NB_VERSION	Betalningsversion	0002	N4	Obligatorisk
2.	NB_RCV_ID	Butiks ID	Avtalsnummer	AN9	Obligatorisk
3.	NB_STAMP	Betalnings ID	Fritext	AN20	Obligatorisk
4a.	NB_DB_AMOUNT	Betalningssumma	Ex: 990,00	AN19	Obligatorisk
4b.	NB_DB_CUR	Valuta	Ex: SEK	AN3	Obligatorisk
4c.	NB_DB_REF	Referensnummer för betalningen	Fritt nummer utan inledande nollor	N25	Obligatorisk
5.	NB_RETURN	Returadress vid "OK" från banken	URL	AN240	Obligatorisk
6.	NB_CANCEL	Returadress vid "Cancel" från banken	URL	AN240	Obligatorisk
7.	NB_REJECT	Returadress vid "Reject" från banken	URL	AN240	Obligatorisk
8.	NB_HMAC	Kontrollsumma för köporder	MAC värde	AN32	Obligatorisk
9.	NB_KVV	Nyckelverifieringsvärde	KVV värde	AN32	Obligatorisk

Tabell 1 "Betala direkt", Gränssnitt till betaltjänst från webbutik

Beskrivning av fältens innehåll:

- 1 Betaltjänstens versionsnummer - 0002
- 2 Webbutikens identitet i Nordeas system.
- 3 Betalnings ID är webbutikens signatur på betalningen, vilket individualiserar betalningen hos webbutiken. Betalnings ID är unik för varje betalning, och används av webbutiken för att koppla ihop en order med ett betalningsuppdrag. Det används bl.a. för att förhindra dubbel fakturering. Signaturen kan vara av valfritt format, en referens eller kombination av datum, klockslag och löpnummer.
- 4a Betalningssumma avskilt med decimalkomma (,)
- 4b Valutaslag för angivet betalningsbelopp. Kan för närvarande endast vara SEK eller EUR.
- 4c Betalningens referens- eller faktura nummer, anges av webbutiken. Den syns som transaktionstext på köparens och webbutikens kontoutdrag. Observera att numret inte tillåts ha inledande nollor.

- 5 Webbutikens returlänk för lyckad transaktion.
Betalningsinformation bifogas i returen till URL-länken.
Returlänken måste vara en fullständig URL-address och hänvisa till en specifik sida.
- 6 Webbutikens returlänk för avbruten betalningstransaktion, om användaren avbryter transaktionen. Ingen betalningsinformation bifogas i returen till URL-länken. (För att särskilja vilken betalning som blivit avbruten, använd förslagsvis en så kallad Query String efter URL-länken, som till exempel "http://www.nb.se/cancel.html?NB_STAMP=12345".)
Returlänken måste vara en fullständig URL-address och hänvisa till en specifik sida.
- 7 Webbutikens returlänk för misslyckad betalningstransaktion.
Ingen betalningsinformation bifogas i returen till URL-länken.
(För att särskilja vilken betalning som blivit misslyckad, använd förslagsvis en så kallad Query String efter URL-länken, som till exempel "http://www.nb.se/cancel.html?NB_STAMP=12345".)
Returlänken måste vara en fullständig URL-address och hänvisa till en specifik sida.
- 8 HMAC hashat värde av transaktionsuppgifterna i fält 2, 3, 4a-c samt en särskild kodnyckel som sälj företaget erhållit i samband med avtalet om utnyttjande av e-betalning.
- 9 Nyckelverifierat värde som är beräknat som ett sigill för den aktuella nyckeln. Denna KVV behöver inte på något sätt vara hemligt på samma sätt som en nyckel och kan användas för att verifiera att nyckelns värde är korrekt utan att avslöja nyckelns värde.

2.1.2 Returnerade transaktionsuppgifter från betaltjänsten till webbutiken

Då banken returnerar information som kvittens till webbutiken levereras följande information via HTTP metoden POST:

#	Parameternamn	Beskrivning	Värde	Format	Användning
1.	NB_RETURN_STAMP	Samma betalnings ID som kom från butik	Fritext	AN20	Obligatorisk
2a.	NB_RETURN_DB_AMOUNT	Transaktionens belopp	Ex: 990,00	AN19	Obligatorisk
2b.	NB_RETURN_DB_CUR	Transaktionens valuta	Ex: SEK	AN3	Obligatorisk
2c.	NB_RETURN_DB_REF	Samma referensnummer som kom från butik	Fritt nummer	N25	Obligatorisk
3.	NB_PAID	Nordeas bekräftelse ID för direktbetalning	Transaktionens tidsstämpel	AN26	Obligatorisk
4.	NB_HMAC	Kontrollsumma för bekräftelsen	MAC värde	AN32	Obligatorisk
5.	NB_KVV	Nyckelverifierat värde	KVV värde	AN32	Obligatorisk

Tabell 2 "Betala direkt", Gränssnitt från betaltjänst till webbutik

Beskrivning av fältens innehåll:

- 1 Den signatur för betalningen som kom ifrån webbutiken tillsammans med betalningsinformationen.
- 2a Transaktionens belopp. Formatet på beloppet kan ha ändrats mot det format på beloppet som webbutiken skickade in till betalningstjänsten.

- 2b Aktuellt valutaslag. Formatet på valutaslaget kan ha ändrats mot det format på valutaslaget som webbutiken skickade in till betalningstjänsten.
- 2c Det referensnummer för betalningen som kom ifrån webbutiken tillsammans med betalningsinformationen.
- 3 Det ID-nummer som banken åsatt transaktionen.
- 4 HMAC hashat värde av transaktionsuppgifterna i fält 1, 2a-c, 3 samt en särskild kodnyckel som anges i avtal om e-betalning.
- 5 Nyckelverifierat värde som är beräknat som ett sigill för den aktuella nyckeln. Denna KVV behöver inte på något sätt vara hemligt på samma sätt som en nyckel och kan användas för att verifiera att nyckelns värde är korrekt utan att avslöja nyckelns värde.

2.1.3 Exempel på kommunikation mellan webbutik och direktbetalning

Ett exempel på hur kommunikationen mellan webbutik och betalningstjänst kan se ut för att begära en direktbetalning via kontoöverföring:

- Köparen klickar på en länk i webbutiken som hänvisar köparen till sidan <https://gfs.nb.se/e-betalning/direktbetalning> tillsammans med ett formulär innehållande dessa parametrar:

```
<INPUT TYPE=HIDDEN NAME="NB_VERSION" VALUE="0002 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RCV_ID" VALUE="55082">
```

```
<INPUT TYPE=HIDDEN NAME="NB_STAMP" VALUE="20090515001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_DB_AMOUNT" VALUE="550,00">
```

```
<INPUT TYPE=HIDDEN NAME="NB_DB_CUR" VALUE="SEK">
```

```
<INPUT TYPE=HIDDEN NAME="NB_DB_REF" VALUE="001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN"
VALUE="http://www.internetshopp.se/return.asp">
```

```
<INPUT TYPE=HIDDEN NAME="NB_REJECT"
VALUE="http://www.internetshopp.se/reject.asp?NB_STAMP=20090515001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_CANCEL"
VALUE="http://www.internetshopp.se/cancel.asp?NB_STAMP=20090515001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_HMAC" VALUE="
12345678901234567890123456789012">
```

```
<INPUT TYPE=HIDDEN NAME="NB_KVV" VALUE="
12345678901234567890123456789012">
```

- Köparen slutför överföringen i e-betalningstjänsten och länkas åter till webbutiken via returlänken NB_RETURN som angavs i orderformuläret tillsammans med ett formulär innehållande dessa parametrar:

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_STAMP"
VALUE="20090515001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_AMOUNT"
VALUE="550,00">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_CUR" VALUE=" SEK">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_REF" VALUE="001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_PAID" VALUE="2009-05-15  
13.22.41.155864">
```

```
<INPUT TYPE=HIDDEN NAME="NB_HMAC" VALUE="  
12345678901234567890123456789012">
```

```
<INPUT TYPE=HIDDEN NAME="NB_KVV" VALUE="  
12345678901234567890123456789012">
```

- Om köparen väljer att avbryta och att inte slutföra direktbetalningen i banken hänvisas köparen tillbaka via returlänken NB_CANCEL som angavs i orderformuläret utan någon ytterligare information i formulär. Webbutiken kan dock ändå se vilken betalning som avbrutits genom den s.k. query string som webbutiken angivit i returlänken. Notera att det inte finns någon säkerhet att köparen verkligen går tillbaka till webbutiken via return länken.
- Om köparen inte kan slutföra direktbetalningen i banken hänvisas köparen tillbaka via returlänken NB_REJECT som angavs i orderformuläret utan någon ytterligare information i formulär. Webbutiken kan dock ändå se vilken betalning som inte genomfördes genom den s.k. query string som webbutiken angivit i returlänken. Notera att det inte finns någon säkerhet att köparen verkligen går tillbaka till webbutiken via return länken.
- Om köparen väljer att stänga ner fönstret när den kommer till banken och inte har påbörjat direktbetalningen returneras inget svar till webbutiken.

2.2 "Betalningskontroll"

Säljföretaget kan kontrollera att en betalning har genomförts genom att göra en betalningskontroll. Nedan beskrivs informationen som webbutiken och betalningstjänsten utbyter för en betalningskontroll.

Om kontrollsumman av värdet till betalningskontrollen är felaktig och inte kan verifieras så kommer betalningstjänsten svara med "Not Found". Om däremot något annat fel uppstår i betalningstjänsten så svarar betalningstjänsten på samma sätt som för en normal betalningskontroll, men med andra parametrar. En parameter visar att fel uppstod samt en parameter beskriver felet.

2.2.1 Betalningsuppgifter till betalningstjänsten för en betalningskontroll

Webbutiken skickar följande transaktionsuppgifter till betaltjänsten via HTTP metoden POST:

#	Parameternamn	Beskrivning	Värde	Format	Användning
1.	NB_VERSION	Betalningskontrollsversion	0002	AN4	Obligatorisk
2.	NB_RCV_ID	Butiks ID	Avtalsnummer	AN9	Obligatorisk
3.	NB_STAMP	Betalnings ID	Fritext	AN20	Obligatorisk
4.	NB_RETURN	Returadress vid "OK" från banken	URL	AN240	Valfri
5.	NB_HMAC	Kontrollsumma av betalningskontrollen	MAC värde	AN32	Obligatorisk
6.	NB_KVV	Nyckelverifierat värde	KVV värde	AN32	Obligatorisk

Beskrivning av fältens innehåll:

- 1 Betalningskontrollens versionsnummer - 0002
- 2 Webbutikens identitet i Nordeas system.
- 3 Betalnings ID är webbutikens signatur på betalningen, vilket individualiserar betalningen hos webbutiken. Betalnings ID är unik för varje betalning, och används av webbutiken för att koppla ihop en order med ett betalningsuppdrag. Det används bl.a. för att förhindra dubbel fakturering. Signaturen kan vara av valfritt format, en referens eller kombination av datum, klockslag och löpnummer.
OBS. Betalnings ID (NB_STAMP) i betalningskontrollen måste vara exakt överrensstämmande med det Betalnings ID (NB_STAMP) för det köp som betalningskontrollen avser!
- 4 Webbutikens returlänk för svaret från betalningskontrollen. Information om betalningen bifogas i returen till URL-länken. Returlänken måste vara en fullständig URL-adress och hänvisa till en specifik sida.
- 5 HMAC hashat värde av transaktionsuppgifterna i fält 2 och 3 samt en särskild kodnyckel.
- 6 Nyckelverifierat värde som är beräknat som ett sigill för den aktuella nyckeln. Denna KVV behöver inte på något sätt vara hemligt på samma sätt som en nyckel och kan användas för att verifiera att nyckelns värde är korrekt utan att avslöja nyckelns värde.

2.2.2 Returnerande uppgifter från betalningskontrollen

Då webbutiken efterfrågat kontroll sidan returnerar betalningstjänsten följande information i den efterfrågade sidan som parametrar till ett formulär:

#	Parameternamn	Beskrivning	Värde	Format	Användning
1.	NB_VERIFIED	Betalningens status	YES/NO/ERR	AN3	Obligatorisk
2.	NB_RETURN_STAMP	Samma betalnings ID som kom från butik	Fritext	AN20	Obligatorisk
3a.	NB_RETURN_DB_AMOUNT	Överföringens belopp	Ex: 990,00	AN19	Valfri
3b.	NB_RETURN_DB_CUR	Överföringens valuta	Ex: SEK	AN3	Valfri
3c.	NB_RETURN_DB_REF	Överföringens referensnummer	Fritt nummer	N25	Valfri
4.	NB_RETURN_BB_REF1 (- 8)	Samma referensnummer som kom från butik för betalning 1-8.	Fritext	AN25	Valfri
5.	NB_PAID	Nordeas bekräftelse ID för betalningen	Transaktionens tidsstämpel	AN26	Valfri
6.	NB_HMAC	Hashvärde av kvitto	MAC värde	AN32	Obligatorisk
7.	NB_KVV	Nyckelverifierat värde	KVV värde	AN32	Obligatorisk
8.	NB_ERROR_DESCR	Felbeskrivning	Fritext	AN50	Valfri

Tabell 4, Gränssnitt från betalningskontroll till webbutik

Beskrivning av fältens innehåll:

1. Returvärde för betalningens status
 "YES" om betalningen har slutförts
 "NO" om betalningen ej kan återfinnas i Nordeas Centrala System
 "ERR" då ett fel uppstod och korrekt svar ej kan ges.

- Vid "YES" och "NO" returneras parametrarna 3a-c, 4 och 5. Parameter 7 saknas i svaret. Vid "ERR" returneras parameter 7. Parametrarna 3a-c, 4 och 5 saknas i svaret, dessutom returnerar parameter 6 inget hashvärde tillbaka eftersom felet kan bero på problem med att sigillera bekräftelsen.
- 2 Samma signatur av betalningen som kom ifrån webbutiken.
 - 3a Överfört belopp vid direktbetalning. Parametern används endast i de fall då en betalning innehållandes kontoöverföring genomförts.
 - 3b Överförd valuta vid direktbetalning. Parametern används endast i de fall då en betalning innehållandes kontoöverföring genomförts.
 - 3c Referensnummer för direktbetalningen. Parametern används endast i de fall då en betalning innehållandes kontoöverföring genomförts.
 - 4 Referensvärde för betalning 1-8. Parametern används endast i de fall då en betalning innehållandes betalningsbevakningar genomförts.
 - 5 Bankens identifikation av transaktionen.
 - 6 HMAC hashat värde. Om parameter 1, returvärde för betalningens status, har följande värde så beräknas datasträngen för hashvärdet enligt följande:
 - "YES" : fält 1, 2, 3a-c, 4, 5
 - "NO" : fält 1, 2
 - "ERR" : inget hashvärde beräknas
 Transaktionsuppgifterna beräknas tillsammans med en särskild kodnyckel som sälj företaget erhållit i samband med avtalet om utnyttjande av e-betalning.
 - 7 Nyckelverifierat värde som är beräknat som ett sigill för den aktuella nyckeln. Denna KVV behöver inte på något sätt vara hemligt på samma sätt som en nyckel och kan användas för att verifiera att nyckelns värde är korrekt utan att avslöja nyckelns värde.
 - 8 Beskrivning av eventuellt uppkommet fel i betalningskontrollen. Parametern används endast i de fall något fel uppstår med betalningskontrollen.

Informationen ges i kontroll sidan som fås som svar och består av en tabell som redovisar de returnerade värdena med beskrivande text. De returnerade värdena anges även i HTML - format som gömda fält i ett HTML-formulär, för att enkelt kunna avläsas automatiskt av automatiserade applikationer.

Om webbutiken angivet en returlänk i fält 4 (NB_RETURN) så visas en knapp i samband med tabellen med hänvisning till den angivna returlänken. Denna länk kan användas för att skicka parametrarna till webbutiken på samma sätt som den returlänk som presenterades för köparen vid bekräftelsen för betalningen.

2.2.3 Exempel på kommunikation mellan webbutik och betalningskontroll

Ett exempel på hur kommunikationen mellan webbutik och betalningstjänst kan se ut för en kontroll av en betalning via kontoöverföring:

Webbutiken efterfrågar sidan https://gfs.nb.se/e-betalning/betalningskontroll?NB_VERSION=0002 &NB_RCV_ID=999999&NB_STAMP=20081009001&NB_HMAC=12345678901234567890123456789012

Betalningstjänsten svarar i sidan med en tabell som presenterar svaret samt dessa gömda parametrar vid en lyckad utförd förfrågan:

```
<INPUT TYPE=HIDDEN NAME="NB_VERIFIED" VALUE="YES">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_STAMP"
VALUE="20090515001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_AMOUNT"
VALUE="550,00">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_CUR" VALUE=" SEK">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_REF" VALUE="001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_PAID" VALUE="2009-05-15
13.22.41.155864">
```

```
<INPUT TYPE=HIDDEN NAME="NB_HMAC" VALUE="
12345678901234567890123456789012">
```

```
<INPUT TYPE=HIDDEN NAME="NB_KVV" VALUE="
12345678901234567890123456789012">
```

Vid en lyckad utförd förfrågan men där betalningen ej kan återfinnas svarar betalningstjänsten i sidan med en tabell samt dessa gömda parametrar:

```
<INPUT TYPE=HIDDEN NAME="NB_VERIFIED" VALUE="NO">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_STAMP"
VALUE="20090515001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_AMOUNT" VALUE= "">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_CUR" VALUE= "">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_REF" VALUE=" ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_PAID" VALUE=" ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_HMAC" VALUE="
12345678901234567890123456789012">
```

```
<INPUT TYPE=HIDDEN NAME="NB_KVV" VALUE="
12345678901234567890123456789012">
```

Och vid en misslyckad utförd förfrågan svarar betalningstjänsten i sidan med en tabell samt dessa gömda parametrar:

```
<INPUT TYPE=HIDDEN NAME="NB_VERIFIED" VALUE="ERR">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_STAMP"
VALUE="20090515001 ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_AMOUNT" VALUE= "">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_CUR" VALUE= "">
```

```
<INPUT TYPE=HIDDEN NAME="NB_RETURN_DB_REF" VALUE=" ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_PAID" VALUE=" ">
```

```
<INPUT TYPE=HIDDEN NAME="NB_HMAC" VALUE= "">
```

```
<INPUT TYPE=HIDDEN NAME="NB_KVV" VALUE="">
```

```
<INPUT TYPE=HIDDEN NAME="NB_ERR_DESCR" VALUE="Tekniskt fel, var  
god försök igen senare">
```

2.3 "Återbetalning"

Sälj företaget kan återbetala hela eller delar av en betalning som har genomförts via direktbetalning genom att göra en återbetalning. Nedan beskrivs informationen som webbutiken och betalningstjänsten utbyter för en återbetalning.

Om hash värdet till återbetalningen är felaktigt och inte kan verifieras så kommer betalningstjänsten svara med "Not Found". Om däremot något annat fel uppstår i betalnings tjänsten så svarar betalningstjänsten på samma sätt som för en normal återbetalning, men med andra parametrar. En parameter visar att fel uppstod samt en parameter beskriver felet.

Flödet för återbetalningen är detsamma som för betalningskontroll och skiljer sig endast genom uppgifterna som utbyts mellan webbutik och tjänst. För ett exempel på hur kommunikationen mellan webbutik och återbetalningstjänst kan se ut, se vidare avsnitt 2.3.3 ovan för betalningskontroll som har samma flöde som en återbetalning.

2.3.1 Betalningsuppgifter till betalningstjänsten för en återbetalning

Webbutiken skickar följande transaktionsuppgifter till betaltjänsten via HTTP metoden POST:

#	Parameternamn	Beskrivning	Värde	Format	Användning
1.	NB_VERSION	Återbetalningsversion	0002	AN4	Obligatorisk
2.	NB_RCV_ID	Butiks ID	Avtalsnummer	AN9	Obligatorisk
3.	NB_STAMP	Betalnings ID	Fritext	AN20	Obligatorisk
4.	NB_DB_REF	Överföringens referensnummer	Fritt nummer	N25	Obligatorisk
5.	NB_PAID	Nordeas bekräftelse ID för betalningen	Transaktionens tidsstämpel	AN26	Obligatorisk
6.	NB_REPAY_AMOUNT	Återbetalningens belopp	Ex: 120,00	AN19	Obligatorisk
7.	NB_REPAY_CUR	Återbetalningens valuta	Ex: SEK	AN3	Obligatorisk
8.	NB_RETURN	Returadress vid "OK" från banken	URL	AN240	Valfri
9.	NB_HMAC	Hashvärde av återbetalningen	MAC värde	AN32	Obligatorisk
10.	NB_KVV	Nyckelverifierat värde	KVV värde	AN32	Obligatorisk

Tabell 5 Gränssnitt till återbetalning för butik

Beskrivning av fältens innehåll:

1. Återbetalningens versionsnummer – 0002.
2. Webbutikens identitet i Nordeas system.
3. Betalnings ID är webbutikens signatur på betalningen, vilket individualiserar betalningen hos webbutiken. Betalnings ID är unik för varje betalning, och används av webbutiken för att koppla ihop en order med ett betalningsuppdrag. Det används bl.a. för att förhindra dubbel fakturering. Signaturen kan vara av valfritt format, en referens eller kombination av datum, klockslag och löpnummer.

OBS. Betalnings ID (NB_STAMP) i återbetalningen måste vara exakt överrensstämmande med det Betalnings ID (NB_STAMP) för det köp som återbetalningen avser!

- 4 Referensnumret för direktbetalningen.
- 5 Bankens identifikation av transaktionen som webbutiken erhållit i betalningsbekräftelsen ifrån banken.
- 6 Beloppet, avskilt med decimalkomma (,), som skall återbetalas till kunden. Det totala beloppet återbetalat till kund kan ej överstiga beloppet för den ursprungliga betalningen.
- 7 Valutan för beloppet som skall återbetalas till kunden. OBS! Måste vara samma valuta som för den ursprungliga betalningen.
- 8 Webbutikens returlänk för svaret från betalningskontrollen. Information om betalningen bifogas i returlänken om webbutiken valt att ta emot returnerad information.
- 9 HMAC hashat värde av transaktionsuppgifterna i fält 2, 3, 4, 5, 6 och 7 samt en särskild kodnyckel som butiken erhållit i samband med avtalet om utnyttjande av Nordeas betaltjänst.
- 10 Nyckelverifierat värde som är beräknat som ett sigill för den aktuella nyckeln. Denna KVV behöver inte på något sätt vara hemligt på samma sätt som en nyckel och kan användas för att verifiera att nyckelns värde är korrekt utan att avslöja nyckelns värde.

2.3.2 Returnerande uppgifter från återbetalningen

Då webbutiken efterfrågat återbetalningssidan returnerar betalningstjänsten följande information via den efterfrågade HTTP länken:

#	Parameternamn	Beskrivning	Värde	Format	Användning
1.	NB_VERIFIED	Betalningens status	YES/ERR	AN3	Obligatorisk
2.	NB_RETURN_STAMP	Butikens betalnings ID	Fritext	AN20	Obligatorisk
3.	NB_RETURN_DB_REF	Överföringens referensnummer	Fritt nummer	N25	Obligatorisk
4a.	NB_RETURN_REPAY_AMOUNT	Återbetalningens belopp	Ex: 990,00	AN19	Obligatorisk
4b.	NB_RETURN_REPAY_CUR	Återbetalningens valuta	Ex: SEK	AN3	Obligatorisk
5a.	NB_WITHDRAWAL_AMOUNT	Uttagsbeloppet från butikens konto	Ex: 990,00	AN19	Valfri
5b.	NB_WITHDRAWAL_CUR	Uttagsbeloppets valuta	Ex: SEK	AN3	Valfri
5c.	NB_WITHDRAWAL_DATE	Datum för uttag från butikens konto	Ex: 2009-05-15	AN10	Valfri
5d.	NB_DEPOSIT_DATE	Datum för insättning på kundens konto	Ex: 2009-05-16	AN10	Valfri
5e.	NB_RATE	Avropskurs	Ex: 8,91	AN12	Valfri
6.	NB_PAID	Nordeas bekräftelse ID för betalningen	Transaktionens tidsstämpel	AN26	Obligatorisk
7.	NB_HMAC	Hashvärde av bekräftelsen	MAC värde	AN32	Obligatorisk
8.	NB_KVV	Nyckelverifierings värde	KVV värde	AN32	Obligatorisk
9.	NB_ERROR_DESCR	Felbeskrivning	Fritext	AN120	Valfri

Tabell 6 Gränssnitt till webbutik från betalningstjänst

Beskrivning av fältens innehåll:

- 1 Returvärde för återbetalningens status; är "YES" om återbetalningen har slutförts och "ERR" då ett fel uppstod. Om fel uppstår och återbetalningen ej kan genomföras returneras parameter 8 med en textsträng beskrivandes orsaken till felet, i annat fall returneras ej parameter 8. Dessutom returnerar parameter 7 inget hashvärde tillbaka eftersom felet kan bero på problem med att sigillera bekräftelsen.
- 2 Betalningsidentifikationen till direktbetalningen som återbetalats, samma betalningsidentifikation som kom ifrån webbutiken.
- 3 Referensnumret till direktbetalningen som återbetalats, samma referensnummer som kom från webbutiken.
- 4a Beloppet som återbetalats till kunden.
- 4b Valutan för beloppet som återbetalats till kunden.
- 5a Uttagsbeloppet ifrån säljföretagets belastningskonto för återbetalningen. Detta fält används endast i de fall växling utförs.
- 5b Valutan för uttagsbeloppet ifrån säljföretagets belastningskonto. Detta fält används endast i de fall växling utförs.
- 5c Datum när beloppet för återbetalningen dras ifrån säljföretagets konto. Detta fält används endast i de fall växling utförs.
- 5d Datum när beloppet för återbetalningen är tillgängligt på kundens konto. Detta fält används endast i de fall växling utförs.
- 5e Avropskurs (kalkylkurs) för växlingen som skett. Detta fält används endast i de fall växling utförs.
- 6 Bankens identifikation av transaktionen, inte samma bekräftelseidentifikation som kom ifrån webbutiken och som returnerades för den ursprungliga betalningen utan en ny bekräftelseidentifikation. Denna nya bekräftelseidentifikation används i fortsättningen för att koppla ihop en betalning från butik med en transaktion, till exempel för en eventuell ytterligare återbetalning. Den används även för att undvika att samma återbetalning genomförs flera gånger.
- 7 HMAC hashat värde av transaktionsuppgifterna i fält 1, 2, 3, 4a-b, 5a-e (används endast när växling utförts), 6 samt en särskild kodnyckel som säljföretaget erhållit i samband med avtalet om utnyttjande av e-betalningstjänsten.
OBS! Om parameter 1, returvärde för betalningens status, är "ERR" kommer inte ett uträknat hashvärde returneras tillbaka eftersom felet kan bero på problem med att sigillera bekräftelsen.
- 8 Nyckelverifierat värde som är beräknat som ett sigill för den aktuella nyckeln. Denna KVV behöver inte på något sätt vara hemligt på samma sätt som en nyckel och kan användas för att verifiera att nyckelns värde är korrekt utan att avslöja nyckelns värde.
- 9 Beskrivning av eventuellt uppkommet fel i återbetalningen. Parametern används endast i de fall något fel uppstår med återbetalningen.

Informationen ges i återbetalningssidan som fås som svar och består av en tabell som redovisar de returnerade värdena med beskrivande text. De returnerade värdena anges även i HTML-format som gömda fält i ett HTML-formulär, för att enkelt kunna avläsas automatiskt av automatiserade applikationer.

Om webbutiken angivet en returlänk i fält 8 (NB_RETURN) så visas en knapp i samband med tabellen med hänvisning till den angivna

returlänken. Denna länk kan användas för att skicka parametrarna till webbutiken på samma sätt som den returlänk som presenterades för köparen vid bekräftelsen för betalningen.

3 Förändringsskydd

Flera olika metoder finns för beräkning av sigill. När det gäller e-betalning använder sig Nordea av sigill som är beräknade med en metod kallad HMAC-SHA256-128. Det innebär att all data som skickas till Nordea går igenom en algoritm (256 bitar säker hash algoritm) som beräknar en kryptografisk kontrollsumma av datat, en hash baserad verifierings metod (MAC).

Metoden är publik och säkerheten bygger på att en del av beräkningsunderlaget är hemligt, nämligen sigillnyckeln.

3.1 HMAC-SHA256-128

För att skydda informationen som skickas krävs att sälj företaget implementerar en rutin för generering av en kontrollsumma (hashvärde) enligt en särskild algoritm. I samtliga e-betalningstjänster använder sälj företaget HMAC för att:

- 1) Räkna ut kontrollsumman i ordern eller förfrågan som går från webbutiken till Nordea.
- 2) Kontrollera kontrollsumman i bekräftelsen som Nordea skickar till webbutiken.

Mer information om HMAC-SHA256-128 finns i följande dokument:

FIPS-180-3 (Beskriver HMAC)

FIPS-198-1 (Beskriver SHA256)

RFC4868 (Beskriver HMAC-SHA256-128 och hur hashvärdet är trunkerat)

Själva MAC värdet räknas ut genom att bilda en lång datasträng av de parametrar som skall ingå i MAC beräkningen, åtskiljda med en ampersand (&). Det ger att MAC värdet för ex. "Betala direkt" bildas på en datasträng som sätts samman på följande sätt:
webbutiksidentifikation&betalningsidentifikation&belopp&valuta&referens.

Det ger en sträng som till exempel kan se ut på följande sätt:
"999999&00002&899,00&SEK&123450".

Eventuella icke obligatoriska värden som inte används i ordern, förfrågan eller bekräftelsen tas ej heller med i datasträngen och därför inte heller några avskiljningstecken.

Genom att använda denna datasträng tillsammans med den hemliga nyckeln i algoritmen fås ett värde tillbaka där de första 32 tecknen är det värde som utgör MAC värdet.

Notera att värdena i bekräftelsen ifrån e-betalningstjänsten kan ha ändrat format gentemot det format som säljföretaget använt i förfrågan eller ordern. Det är därför viktigt att alltid sätta ihop datasträngen med exakt de värden som e-betalningstjänsten skickat med i bekräftelsen, annars riskeras att de uträknade hashvärdena blir olika.

3.2 Hemlig nyckel

För att räkna ut kontrollsumman med HMAC måste säljföretaget ha erhållit en egen hemlig kodnyckel. Denna hemliga nyckel distribueras av Nordea och måste hållas skyddad från obehöriga.

Den hemliga nyckel är 128 bitar lång (32 tecken) och används för att generera en MAC som också är 128 bitar. Notera att MAC bör trunkeras till 128 bitar eftersom SHA256 normalt genererar ett 256 bitar värde. Det är de första 128 bitar som ska användas till MAC.

Nordea genererar sigillnycklarna och sänder dessa till sina kunder i god tid innan byte.

3.2.1 Giltighetstid

Den hemliga nyckeln har en exakt tilldelad giltighetstid och byts med regelbundna intervall vid övergången mellan två datum. För att tjänsten skall ha fullgod funktionalitet krävs att rätt sigillnyckel används under rätt giltighetstid. Någon tolerans tid då två olika nycklar fungerar finns inte i e-betalning via Nordea.

Tid: - - 23.59.59 (Sigillnyckel för period X är giltig)

Tid: 00.00.00 - - (Sigillnyckel för period X+1 är giltig)

3.3 KVV - Nyckelverifieringsvärde

Det finns ett nyckelverifieringsvärde (KVV) för varje nyckel.

Denna KVV behöver inte på något sätt vara hemligt på samma sätt som en nyckel och kan användas för att verifiera att nyckelns värde är korrekt utan att avslöja nyckelns värde.

För att kontrollera inmatningen ska det KVV som tillhör varje nyckel användas. KVV kan i sin tur sparas i systemet för att jämföras med den KVV som erhållits med det införda nyckelvärdet.

4 Verifiering av informationsflöde

För att underlätta utvecklingen av transaktionsuppgifterna i betalningsformuläret ges en möjlighet att verifiera dessa mot en särskild testsida, utan att någon betalning genomförs. Nordea rekommenderar sälj företaget att testa informationsflödet ordentligt mot denna testsida innan testköp från Nordea skall initieras samt betalningstjänsten i webbutiken öppnas för riktiga köpare.

4.1 Skillnader i informationsflödet

Till skillnad från vanliga betalningar behövs ingen köpare i vanlig mening för att testa informationsflödet. Sälj företaget agerar anonym köpare när man kör mot testsidorna. Förutom att betalningsformuläret ska skickas till en annan adress (se avsnitt 5 Betalnings-tjänstinformation) är transaktionsuppgifterna samma som för skarpa betalningar med ett undantag – kontrollsumman. Sälj företaget ska inte räkna ut checksumman med hjälp av den hemliga nyckeln. Istället ska följande användas vid verifiering:

Nyckel:

- 1234 5678 90AB CDEF 1234 5678 90AB CDEF

KVV:

- FF36 5893 D899 291C 3BF5 05FB 3175 E880

4.2 Verifiering av transaktionsuppgifter

Testsidan liknar inte de sidor köparen kommer till vid en skarp betalning. På testsidan krävs till exempel ingen inloggning. Här presenteras istället en tabell över inskickade transaktionsuppgifter där varje rad motsvarar en rad i betalningsformuläret. För varje rad/fält presenteras följande information:

- Fältnamn.
- Fältvärde.
- Längd på fältvärdet.
- Status. Om fältvärdet kunde verifieras utan fel visas "OK" här. Om verifieringen inte lyckades visas istället ett felmeddelande.

4.3 Simulerade returflöden

På testsidan ges sedan ett antal möjligheter att simulera olika betalningsflöden:

- Lyckad betalning. Detta flöde motsvarar att en köpare genomför en lyckad betalning och sedan återvänder till webbutiken med kvittot, d v s "OK" från banken. Detta flöde kan endast väljas om hela betalningsformuläret kunde verifieras utan att några fel hittades.
- Avbruten betalning, "cancel". Detta flöde motsvarar att en köpare avbryter betalningen.
- Avvisade betalning, "reject". Detta flöde motsvarar att köparens betalningsförsök avvisas av någon anledning.

5 Betalningstjänstinformation

Nedan följer de länkar och den information som gäller för de olika e-betalningstjänsterna.

5.1 "Betala direkt"

För denna version av betalningstjänsten "Betala direkt" måste versionsnummer anges till "0002".

- Adressen som köparen skall hänvisas till för "Betala direkt" är:
<https://gfs.nb.se/e-betalning/direktbetalning>
- För verifiering/test ska följande adress användas:
https://gfs.nb.se/e-betalning/test_direktbetalning

5.2 "Betalningskontroll"

För denna version av betalningskontrollen måste versionsnummer anges till "0002".

- Adressen för betalningskontroll är:
<https://gfs.nb.se/e-betalning/betalningskontroll>

5.3 "Återbetalning"

För denna version av återbetalning måste versionsnummer anges till "0002".

- Adressen för återbetalning är:
<https://gfs.nb.se/e-betalning/aterbetalning>
- För verifiering/test ska följande adress användas:
https://gfs.nb.se/e-betalning/test_aterbetalning