Mars 2014

Förändringsskydd med sigill

Teknisk manual

bankgirot

Innehåll

1 Introduktion

1.1 Det här dokumentet

Det här dokumentet innehåller detaljerad information om förändringsskydd med sigill, och är till för dig som ska skapa program som ska använda någon metod för att förändringsskydda filer med sigill.

1.2 Vad är Bankgirot?

Bankgirot är ett europeiskt clearinghus med uppdrag att leverera marknadsledande lösningar inom betalområdet som ökar kundernas konkurrenskraft.

Som det enda clearinghuset för massbetalningar i Sverige har Bankgirot en central roll i den svenska betalningsinfrastrukturen och hanterar den stora merparten av denna typ av betalningar.

Bankgirosystemet är

- ett öppet system för både betalare och betalningsmottagare *och*
- länken mellan avsändare och mottagare

Alla betalningsinstitut som är verksamma i Sverige kan teckna avtal om att vara med i bankgirosystemet. Bankgirot förmedlar betalningar och information kring ut- och inbetalningar till alla parter. Betalningar och information kommer alltid fram.

Oavsett bankförbindelse, kan du som

- betalningsmottagare få betalt från alla *och*
- dina betalare nå alla betalningsmottagare

Inom ramen för bankgirosystemet har Bankgirot etablerat ett samarbete med flera av de största tillverkarna av affärs-, ekonomi- och kommunikationsprogram. Tillsammans skapar vi effektiva affärslösningar på betalningsområdet, som spar tid och pengar åt företagen.

1.3 Vad är ett bankgironummer?

Ett *bankgironummer* är en adress som pekar på ett bankkonto. Bankgironumret kan kopplas till den bank och det bankkonto du själv väljer.

När du ska få betalt behöver du bara uppge ditt bankgironummer – du behöver aldrig lämna ut ditt bankkontonummer. Det är i alla lägen dolt för betalaren. Om du byter bank behåller du ditt bankgironummer och dina bankgirobetalningar fortsätter fungera på det sätt du är van vid.

2 Termer och definitioner

Den här tabellen visar Bankgirots definitioner av termer som hör ihop med Förändringsskydd.

Term	Definitioner
Betalningsunderlag	Den fil som skickas från företaget till Bankgirot och innehåller de betalningar som ska utföras.
Betalningsuppdrag	De betalningar som Bankgirot tar emot och behandlar.
Checksiffra	En kontrollsiffra som alltid står sist i till exempel ett kontonummer, OCR-referensnummer eller ett bankgironummer.
Digital/Elektronisk signatur	En typ av förändringsskydd som skapas med hjälp av filen och ett personligt certifikat, en så kallad *e-legitimation*. Den digitala signaturen knyter en person till filen via en personligt elektronisk ID-handling och skyddar samtidigt innehållet mot förändring.
Förändringsskydd	Att förändringsskydda en fil innebär att filen skyddas mot otillåten förändring under transport. Förändringsskyddet verifierar även att underlaget kommer från rätt avsändare.
Kommunikationssätt	Det sätt företaget använder för att skicka och hämta filer, till och från Bankgirot.
Kondensat	Det uträknade sigillet. Kondensatet är ett resultat av fyra komponenter: en algoritm, ett regelverk, en fil och en sigillnyckel och ska placeras i den skapade sigillslutposten.
OCR	Optical Character Recognition. Optisk teckenigenkänning, vilket innebär att skrivtecken avsöks med fotocell och registreras automatiskt, oftast i samband med inmatning till dator.
OCR-referensnummer	Numeriskt begrepp som alltid innehåller en checksiffra och kontroll av längden på referensnumret i vissa fall. Syftet är att betalningsmottagaren ska kunna identifiera betalaren och betalningen.
Post	En del av en fil eller ett avsnitt med specifik information om uppdrag som skickas till Bankgirot. Varje post har en egen transaktionskod (TK.)
Referensnummer	Ett begrepp som identifierar betalningen för betalningsmottagaren. Det kan exempelvis vara ett fakturanummer, räkningsnummer, OCR-referensnummer eller en annan referens.
Sigill	En typ av förändringsskydd som skapas med hjälp av filen och en unik sigillnyckel.
Sigillnyckel	En sifferkombination/kod som, i kombination med en krypteringsalgoritm, låser kontrollvärdet för den som inte har tillgång till koden.

Term	Definitioner
Transaktionskod	Alla poster i en fil har en transaktionskod (TK). Varje transkationskod påbörjar en ny post. I Leverantörsbetalningar är till exempel en betalning = TK14 kreditfaktura = TK16/TK17 kontonummerpost = TK40.
Betalningsunderlag	Den fil som skickas från företaget till Bankgirot och innehåller de betalningar som ska utföras.
Betalningsuppdrag	De betalningar som Bankgirot tar emot och behandlar.
Checksiffra	En kontrollsiffra som alltid står sist i till exempel ett kontonummer, OCR-referensnummer eller ett bankgironummer.

3 Generell information om förändringsskydd och sigill

3.1 Förändringsskydd

Att förändringsskydda en fil innebär att filen skyddas mot otillåten förändring under transport. Filen förses med ett krypterat kontrollvärde(kondensat) som beräknas från filens innehåll och en unik kod, innan filen sänds till Bankgirot. Bankgirot kontrollerar kontrollvärdet och kan därmed säkerställa att filen inte har förändrats efter det att avsändaren har förändringsskyddat den.

3.2 Förändrings-skydd är obligatoriskt

Företaget måste av säkerhetsskäl förändringsskydda alla filer som sänds till Bankgirot.

3.3 Två typer av förändringsskydd

Tabellen visar de två typer av förändringsskydd som Bankgirot hanterar.

Typer av förändringsskydd	Beskrivning
Digital signatur	Används i Bankgirotom samt Bankgiro Link.
Sigill	Används i annan kommunikation än Bankgirotom och Bankgiro Link, till exempel: FTP-via-Internet Connect:Direct TCP/IP FTP Netview FTP

3.4 Sigillnyckel

Varje betalningsavsändare har en unik sigillnyckel. Sigillnyckeln, i kombination med en krypteringsalgoritm, låser kontrollvärdet för den som inte har tillgång till den.

Observera: Nyckeln för förändringsskydd är en värdehandling! Eftersom algoritmen är känd bygger graden av säkerhet på att sigillnyckeln hålls hemlig för obehöriga. Sigillnycklar beställs via banken och sänds till utställaren direkt från Bankgirot. Sigillnyckeln är dold i Bankgirots system, kan inte läsas av Bankgirots personal och kan bara skrivas ut en gång. Skulle betalningsavsändarens sigillnyckel förkomma, måste en ny beställas via banken.

3.5 Så här fungerar förändringsskydd med sigill

Tabellen beskriver hur förändringsskydd med sigill fungerar.

Fas	Beskrivning
1	Betalningsavsändaren sigillerar filen med hjälp av sigillnyckeln, och ett krypterat kontrollvärde skapas.
2	Betalningsavsändaren skickar filen med kontrollvärde till Bankgirot.
3	Bankgirot tar emot den förändringsskyddade betalningsfilen och kontrollberäknar kontrollvärdet med samma sigillnyckel som användes av betalningsavsändaren. Om kontrollvärdet inte stämmer så har antingen

4 Sigillmetoder

4.1 Bankgirot stöder två metoder för att skapa sigill

Det finns ett antal olika metoder för att skapa sigill. Tabellen visar de två godkända sigillmetoder som Bankgirot stöder.

Observera: Bankgirot har ingen support för förändringsskydd.

Metod	Beskrivning
Nexus Elektroniskt Sigill (före detta SÄKDATA)	Licensierad produkt från Nexus. Nyckeln består av 36 siffror, där den sista siffran alltid är en checksiffra. Kan förekomma både som leveranssigill och som avsnittssigill.

Metod	Beskrivning
HMAC SHA-256	Keyed-Hash Message Authentication Code. En öppen, internationell standard för sigillering av filer. Varianten som Bankgirot använder är HMAC-SHA256 med 128bitars nyckel, där nyckeln består av 32 alfanumeriska tecken och saknar checksiffra. Förekommer endast som leveranssigill.

4.2 Viktigt: Program för att skapa sigillposten

Sigillposten ska alltid skapas av sigillprogramvaran och inte av programvaran som skapar betalningsunderlaget.

4.3 Två typer av sigill

Det finns två typer av sigill:

- Leveranssigill
- Avsnittssigill

4.4 Sigillering med leveranssigill

Leveranssigill (helfilssigill) innebär att hela leveransen sigilleras oavsett hur många avsnitt som ingår. Vid leveranssigillering skapas följande:

- Två sigillposter: en start- och en slutpost (TK00 och TK99) som omsluter hela leveransen, inklusive själva filens öppnings- och slutsummapost, oavsett hur många avsnitt filen innehåller.
- Ett kondensat, som är ett resultat av fyra komponenter (algoritmen, regelverket, filen och sigillnyckeln) och som läggs i slutposten för sigill.

Hänvisning: För postbeskrivningar, se 6.1 Postbeskrivningar, leveranssigill (TK00 och TK99).

4.5 Sigillering med avsnittssigill

Avsnittssigill innebär att varje avsnitt i filen sigilleras separat och sigillresultatet placeras i en separat sigillpost, sist eller näst sist i varje avsnitt.
Vid avsnittssigillering skapas följande:

- En sigillpost per avsnitt i filen.
- Ett kondensat per avsnitt, där kondensatet är ett resultat av fyra komponenter (algoritmen, regelverket, filen och sigillnyckeln) och läggs i avsnittets slutpost för sigill.

Vid avsnittssigill används olika sigillposter för olika produkter.
Hänvisning: För postbeskrivningar se

- 6.2 Postbeskrivning, avsnittssigill för Leverantörsbetalningar (TK28)
- 6.3 Postbeskrivning, avsnittssigill för Utlandsbetalningar (TK8)
- 6.4 Postbeskrivning, avsnittssigill för Löner (TK08)
- 6.5 Postbeskrivning, avsnittssigill för Autogiro (TK08).

4.6 Testsigillnycklar

Tabellen innehåller testsigillnycklar för de två godkända sigillmetoder som Bankgirot stöder.

Metod	Beskrivning
Nexus Elektroniskt Sigill	12345678901234567890123456789012345 6
HMAC	1234567890ABCDEF1234567890ABCDEF

4.7 Om du behöver mer information

För ytterligare information om Nexus Elektroniskt Sigill, kontakta Technology Nexus AB.

Technology Nexus AB
Nämndemansgatan 3
431 33 Mölndal
e-post: info.sigillet@nexussafe.com
www.nexussafe.com

Ytterligare information om HMAC finns antingen

- på Bankgirots hemsida, www.bankgirot.se/HMAC eller
- i standarden FIPS PUB 198 - The Keyed-Hash Message Authentication Code (HMAC)

5 Beräkning av checksiffra enligt 10-modul

5.1 Vad är Beräkning av checksiffra enligt 10-modul?

Beräkning av checksiffra enligt 10-modul är en metod för att försäkra sig mot till exempel felregistrering eller förvanskning av numeriska begrepp. Benämningen av metoden kommer av att beräkningsresultatet är lika med mellanskillnaden mellan en slutsumma och närmsta högre tiotal.

5.2 Vad är en checksiffra?

En checksiffra är en obligatorisk del som anges som sista siffra i vissa numeriska begrepp.

Exempel: Checksiffran förekommer till exempel i

- personnummer och organisationsnummer
- bankkontonummer
- bankgiro- och postgironummer
- sigillnyckel.

5.3 Gör så här

Så här beräknar du checksiffra för numeriska begrepp enligt 10-modul.

<table>
<tr><th>Steg</th><th>Åtgärd</th><th colspan="9">Exempel</th></tr>
<tr><td>1</td><td>Ta fram det nummer du ska beräkna.</td><td colspan="9">Nummer: 12345682
Notera: Checksiffran är den sista siffran, 2.</td></tr>
<tr><td rowspan="3">2</td><td rowspan="3">Ignorera checksiffran.
Multiplicera sedan delsiffrorna med vikterna 2 och 1, med början från höger.</td><td>Delsiffra</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>8</td><td>2</td></tr>
<tr><td>x</td><td>2</td><td>1</td><td>2</td><td>1</td><td>2</td><td>1</td><td>2</td><td>-</td></tr>
<tr><td>=</td><td>2</td><td>2</td><td>6</td><td>4</td><td>10</td><td>6</td><td>16</td><td>-</td></tr>
<tr><td>3</td><td>Bryt upp tvåsiffriga tal i resultatet genom att subtrahera dem med 9.</td><td colspan="9">10 – 9 = 1
16 – 9 = 7</td></tr>
<tr><td>4</td><td>Addera de siffror du har fått fram.</td><td colspan="9">2 + 2 + 6 + 4 + 1 + 6 + 7 = 28</td></tr>
<tr><td>5</td><td>Räkna ut mellanskillnaden mellan summan och närmaste högre tiotal.
Resultatet ska vara detsamma som den korrekta checksiffran.</td><td colspan="9">Närmaste högre tiotal: 30
Summan från steg 1-4: -28
Resultat = checksiffra: 2
Slutsats: Checksiffran är korrekt här.</td></tr>
</table>

5.4 Beräkning av checksiffra för belopp

Beräkning av checksiffra på belopp görs på samma sätt som ovan.

6 Postbeskrivningar

6.1 Postbeskrivningar, leveranssigill (TK00 och TK99)

6.1.1 Sigillberäkning

Sigillet beräknas på alla tecken i alla poster inklusive leveranssigillets startpost (TK 00) och eventuella makulerings- och datumändringsposter (TKLB).
Undantag: Sigillet beräknas inte på slutposten (TK 99).

6.1.2 Placering

Vid leveranssigillering omsluter sigillstartposten (TK 00) och sigillslutposten (TK 99) hela leveransen (filen) oavsett hur många avsnitt som ingår i den.
Posterna ser likadana ut för alla bankgiroprodukter.

Sigillstartposten (TK00): Sigillstartposten ska

- ligga först i filen
- vara 80 tecken lång, oavsett efterföljande postlängder i filen.

Sigillslutposten (TK99): Sigillslutposten

- innehåller kondensatet

- ligger allra sist i filen.

6.1.3 Sigillstartpost (TK00)

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form
1–2	Transaktionskod	00	2	N
3–8	Nyckeldatum	ÅÅMMDD Det datum då filen skyddades.	6	N
9–12	Typ av kondensat	Antingen SAK1 = Nexus Elektroniskt Sigill eller HMAC = HMAC SHA-256	4	A
13–80	Reservfält	Blankt.	68	A

6.1.4 Sigillslutpost (TK99) för Nexus

Postens innehåll varierar något beroende på vilken metod som används. Tabellen beskriver posten i detalj vid sigillberäkning med Nexus Elektroniskt Sigill.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form
1–2	Transaktionskod	99	2	N
3–8	Nyckeldatum	ÅÅMMDD Det datum då filen skyddades.	6	N
9–26	Kondensat	Det framräknade sigillet.	18	N
27–33	Sigillinformation	Tilläggsinformation om sigillet.	7	A
34–80	Reservfält	Blankt.	47	A

6.1.5 Sigillslutpost (TK99) för HMAC

Postens innehåll varierar något beroende på vilken metod som används. Tabellen beskriver posten i detalj vid sigillberäkning med HMAC SHA-256.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form
1–2	Transaktionskod	99	2	N

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form
3–8	Nyckeldatum	ÅÅMMDD Det datum då filen skyddades.	6	N
9–40	KVV	Kontrollvärde för använd nyckel.	32	A
41–72	Kondensat	Det framräknade sigillet	32	A
73–80	Reservfält	Blankt.	8	A

6.2 Postbeskrivning, avsnittssigill för Leverantörsbetalningar (TK28)

6.2.1 Sigillberäkning

Tabellen visar vilka fält i respektive post som ska ingå i sigillberäkningen.
Observera: TK12, TK13, TK25, TK28 och TK29 ska inte ingå i beräkningen.

Post (TK)	Fält som ska beräknas	Fältens totala längd
11	• 1–2 (Transaktionskod) • 3–12 (Avsändarens bankgironummer) • 13–18 (Skrivdatum)	18
14	• 1–2 (Transaktionskod) • 3–12 (Mottagarens bankgiro-, eller utbetalningsnummer) • 38–49 (Belopp)	24
15		
16		
17		
40	• 1–2 (Transaktionskod) • 3–6 (Nollor) • 7–12 (Utbetalningsnummer) • 13–28 (Mottagarens bankkontonummer)	28
26	• 1–2 (Transaktionskod) • 3–6 (Nollor) • 7–12 (Utbetalningsnummer) • 13–28 (Mottagarens namn)	28

Post (TK)	Fält som ska beräknas	Fältens totala längd
27	• 1–2 (Transaktionskod) • 3–6 (Nollor) • 7–12 (Utbetalningsnummer) • 13–28 (Mottagarens adress)	28

6.2.2 Placering

Sigillresultatet ska placeras i en separat sigillpost före slutsummaposten i varje betalningsavsnitt.

6.2.3 Sigillpost för Leverantörsbetalninar (TK28)

Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form
1–2	Transaktionskod	28	2	N
3–12	Avsändarens bankgironummer	• Högerställt • Nollutfyllt	10	N
13–30	Kondensat	Det framräknade sigillet.	18	N
31–37	Sigillinformation	Tilläggsinformation om sigillet	7	A
38–80	Reservfält	Blankt.	43	A

6.3 Postbeskrivning, avsnittssigill för Utlandsbetalningar (TK8)

6.3.1 Sigillberäkning

Sigillet beräknas på alla tecken i alla poster utom slutsummaposten (TK9) och sigillposten (TK8).

6.3.2 Placering

Sigillresultatet ska placeras i en separat sigillpost före slutsummaposten i varje betalningsavsnitt.

6.3.3 Sigillpost för utlands-betalningar (TK8)

Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form
1	Transaktionskod	8	1	N
2–9	Avsändarens bankgironummer	Högerställt Nollutfyllt	8	N
10–27	Kondensat	Det framräknade sigillet.	18	N
28–34	Sigillinformation	Tilläggsinformation om sigillet	7	A
35–80	Reservfält	Blankt.	46	A

6.4 Postbeskrivning, avsnittssigill för Löner (TK08)

6.4.1 Sigillberäkning

Tabellen visar vilka fält i vilka poster som ska ingå i beräkningen.
Observera: TK25, TK28 och TK29 ska inte ingå i sigillberäkningen.

Post (TK)	Fält som ska beräknas	Fältens totala längd
01	• 1–2 (Transaktionskod) • 3-8 (Skrivdag) • 63-69 (Löngivarens kundnummer)	15
35	• 1–2 (Transaktionskod) • 3–8 (Löneutbetalningsdag) • 13-28 (Löntagarens /mottagarens kontonummer) • 29-40 (Belopp) • 53-58 (Blanka) • 59-68 (Personummer, anställningsnummer eller blankt	52
09	• 1-2 (Transaktionskod) • 3-8 (Skrivdatum) • 29-40 (Totalsumma) • 41-46 (Totalantal)	26

6.4.2 Placering

Sigillresultatet ska placeras i en separat sigillpost sist i varje betalningsavsnitt.

6.4.3 Sigillpost för Löner (TK08)

Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form
1–2	Transaktionskod	08	2	N
3–12	Avsändarens kundnummer	• Högerställt • Nollutfyllt	10	N
13–30	Kondensat	Det framräknade sigillet.	18	N
31–37	Sigillinformation	Tilläggsinformation om sigillet	7	A
38–80	Reservfält	Blankt.	43	A

6.5 Postbeskrivning, avsnittssigill för Autogiro (TK08)

6.5.1 Sigillberäkning

Sigillet beräknas på alla tecken i alla poster i avsnittet dock inte på sigillposten (TK08).

6.5.2 Placering

Sigillresultatet ska placeras i en separat sigillpost sist i varje betalningsavsnitt.

6.5.3 Sigillpost för Autogiro (TK08)

Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagrings-form
1–2	Transaktionskod	08	2	N
3-6	Reservfält	Nollor	4	N
7-12	Avsändarens kundnummer	Högerställt Nollutfyllt	6	N
13–30	Kondensat	Det framräknade sigillet.	18	N
31-37	Sigillinformation	Tilläggsinformation om sigillet	7	A