

# **Förändringsskydd med sigill**

## **Teknisk manual**

Augusti 2008

## 1. Innehållsförteckning

---

2. Introduktion .....	2
3. Generell information om förändringsskydd och sigill .....	3
4. Sigillmetoder .....	5
5. Beräkning av checksiffra enligt 10-modul .....	7
6. Postbeskrivningar .....	8
6.1 Postbeskrivningar, leveranssigill (TK00 och TK99).....	8
6.2 Postbeskrivning, avsnittsigill för Leverantörsbetalningar (TK28) .....	10
6.3 Postbeskrivning, avsnittsigill för Utlandsbetalningar (TK8).....	12
6.4 Postbeskrivning, avsnittsigill för Löner (TK08).....	13
6.5 Postbeskrivning, avsnittsigill för Autogiro (TK08).....	14
7. Termer och definitioner.....	15

---

## 2. Introduktion

---

### 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.

Dokumentet är framtaget för att du ska läsa det på din dator, och alla termer är länkade till kapitel [7. Termer och definitioner](#). Det finns även länkar till vår webbplats.

**Användarhjälp:** Klicka på Föregående vy i Verktögsfältets sidnavigering, eller använd kortkommandot ”Alt + vänsterpil”, för att komma tillbaka till det ställe i dokumentet där du befann dig innan du klickade dig till termlistan.

---

### Vad är Bankgirot?

*Bankgirot* är

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

Alla banker som är verksamma i Sverige kan 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

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

**Kundanpassade betalningslösningar:** Bankgirot erbjuder allt från enkla betalningslösningar för små företag till automatiserade elektroniska betalningslösningar för företag med datoriserade ekonomifunktioner.

Bankgirot har ett etablerat 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.

---

### Vad är ett bankgiro-nummer?

Ett *bankgiro-nummer* är en adress som pekar på ett bankkonto. Bankgiro-numret kan kopplas till den bank och det bankkonto du själv väljer.

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

---

### 3. Generell information om förändringsskydd och sigill

#### 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 BGC. BGC kontrollerar kontrollvärdet och kan därmed säkerställa att filen inte har förändrats efter det att avsändaren har förändringsskyddat den. Förändringsskyddet verifierar även att underlaget kommer från rätt avsändare.

#### Förändringsskydd är obligatoriskt

Företaget måste av säkerhetsskäl förändringsskydda *alla* filer som sänds till BGC.

#### Två typer av förändringsskydd

Tabellen visar de två typer av förändringsskydd som BGC hanterar.

Typer av förändringsskydd	Beskrivning
Digital signatur	Används i BgCom samt Bankgiro Link.
Sigill	Används i annan kommunikation än BgCom och Bankgiro Link, till exempel: <ul style="list-style-type: none"> <li>• FTP-via-Internet</li> <li>• Connect:Direct</li> <li>• TCP/IP FTP</li> <li>• Netview FTP</li> </ul>

#### Sigillnyckel

Varje betalningsavsändare har en unik *sigillnyckel*. Sigillnyckeln, i kombination med en krypteringsalgorithm, 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 BGC. Sigillnyckeln är dold i BGC:s system, kan inte läsas av BGC:s personal och kan bara skrivas ut en gång. Skulle betalningsavsändarens sigillnyckel förkomma, måste en ny beställas via banken.

*Fortsättning på nästa sida*

### 3. Generell information om förändringsskydd och sigill, Fortsättning

Så här fungerar  
förändrings-  
skydd 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 BGC.
3	BGC tar emot den förändringsskyddade betalningsfilen och kontrollberäknar kontrollvärdet med samma sigillnyckel som användes av betalningsavsändaren. Om kontrollvärdet <i>inte</i> stämmer så har antingen <ul style="list-style-type: none"><li>• filen förändrats eller</li><li>• betalningsavsändaren använt fel sigillnyckel.</li></ul>

## 4. Sigillmetoder

### BGC stöder två metoder för att skapa sigill

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

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

**Observera:** BGC har ingen support för förändringsskydd.

### Viktigt: Program för att skapa sigillposten

Sigillposten ska alltid skapas av sigillprogramvaran och *inte* av programvaran som skapar [betalningsunderlaget](#).

### Två typer av sigill

Det finns två typer av sigill:

- Leveranssigill
- Avsnittsigill

### 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 \(TK00 och TK99\)](#).

*Fortsättning på nästa sida*

## 4. Sigillmetoder, Fortsättning

### Sigillering med avsnittsigill

Avsnittsigill innebär att *varje avsnitt* i filen sigilleras separat och sigillresultatet placeras i en separat sigillpost, sist eller näst sist i varje avsnitt.

Vid avsnittsigillering 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 avsnittsigill används olika sigillposter för olika produkter.

**Hänvisning:** För postbeskrivningar se

- [6.2 Postbeskrivning, avsnittsigill för Leverantörsbetalningar \(TK28\)](#)
- [6.3 Postbeskrivning, avsnittsigill för Utlandsbetalningar \(TK8\)](#)
- [6.4 Postbeskrivning, avsnittsigill för Löner \(TK08\)](#)
- [6.5 Postbeskrivning, avsnittsigill för Autogiro \(TK08\)](#).

### Testsigillnycklar

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

Metod	Testsigillnyckel
Nexus Elektroniskt Sigill	123456789012345678901234567890123456
HMAC	1234567890ABCDEF1234567890ABCDEF

### 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](mailto:info.sigillet@nexussafe.com)  
[www.nexussafe.com](http://www.nexussafe.com)

Ytterligare information om HMAC finns antingen

- på BGCs hemsida, [www.bgc.se/HMAC](http://www.bgc.se/HMAC) eller
- i standarden FIPS PUB 198 - The Keyed-Hash Message Authentication Code (HMAC)

## 5. Beräkning av checksiffra enligt 10-modul

**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.

**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.

**Gör så här**

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

Steg	Åtgärd	Exempel																											
1	Ta fram det nummer du ska beräkna.	Nummer: 12345682 <b>Notera:</b> Checksiffran är den sista siffran, 2.																											
2	<ul style="list-style-type: none"> <li>• Ignorera checksiffran.</li> <li>• Multiplicera sedan delsiffrorna med vikterna 2 och 1, med början från höger.</li> </ul>	<table border="1"> <thead> <tr> <th>Delsiffra</th> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> <th>6</th> <th>8</th> <th>2</th> </tr> </thead> <tbody> <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> </tbody> </table>	Delsiffra	1	2	3	4	5	6	8	2	x	2	1	2	1	2	1	2	-	=	2	2	6	4	10	6	16	-
Delsiffra	1	2	3	4	5	6	8	2																					
x	2	1	2	1	2	1	2	-																					
=	2	2	6	4	10	6	16	-																					
3	Bryt upp tvåsiffriga tal i resultatet genom att subtrahera dem med 9.	$10 - 9 = 1$ $16 - 9 = 7$																											
4	Addera de siffror du har fått fram.	$2 + 2 + 6 + 4 + 1 + 6 + 7 = 28$																											
5	Räkna ut mellanskillnaden mellan summan och närmaste högre tiotal. Resultatet ska vara detsamma som den korrekta checksiffran.	Närmaste högre tiotal: 30 <u>Summan från steg 1-4: -28</u> Resultat = checksiffra: 2 <b>Slutsats:</b> Checksiffran är korrekt här.																											

**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)

---

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

---

**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.
- 

**Sigillstartpost (TK00)** Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagringsform
1–2	Transaktionskod	00	2	N
3–8	Nyckeldatum	ÅÅMMDD Det datum då filen skyddades.	6	N
9–12	Typ av kondensat	Antingen <ul style="list-style-type: none"> <li>• SAK1 = Nexus Elektroniskt Sigill eller</li> <li>• HMAC = HMAC SHA-256</li> </ul>	4	A
13–80	Reservfält	Blankt.	68	A

*Fortsättning på nästa sida*

## 6.1 Postbeskrivningar, leveranssigill (TK00 och TK99),

### Fortsättning

---

**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	Lagringsform
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

---

**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	Lagringsform
1–2	Transaktionskod	99	2	N
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)

**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	<ul style="list-style-type: none"> <li>• 1–2 (Transaktionskod)</li> <li>• 3–12 (Avsändarens bankgiro-nummer)</li> <li>• 13–18 (Skrivdatum)</li> </ul>	18
14	<ul style="list-style-type: none"> <li>• 1–2 (Transaktionskod)</li> <li>• 3–12 (Mottagarens bankgiro-, eller utbetalningsnummer)</li> <li>• 38–49 (Belopp)</li> </ul>	24
15		
16		
17		
40	<ul style="list-style-type: none"> <li>• 1–2 (Transaktionskod)</li> <li>• 3–6 (Nollor)</li> <li>• 7–12 (Utbetalningsnummer)</li> <li>• 13–28 (Mottagarens bankkontonummer)</li> </ul>	28
26	<ul style="list-style-type: none"> <li>• 1–2 (Transaktionskod)</li> <li>• 3–6 (Nollor)</li> <li>• 7–12 (Utbetalningsnummer)</li> <li>• 13–28 (Mottagarens namn)</li> </ul>	28
27	<ul style="list-style-type: none"> <li>• 1–2 (Transaktionskod)</li> <li>• 3–6 (Nollor)</li> <li>• 7–12 (Utbetalningsnummer)</li> <li>• 13–28 (Mottagarens adress)</li> </ul>	28

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

*Fortsättning på nästa sida*

## 6.2 Postbeskrivning, avsnittssigill för Leverantörsbetalningar (TK28), Fortsättning

**Sigillpost för Leverantörsbetalningar (TK28)** Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagringsform
1–2	Transaktionskod	28	2	N
3–12	Avsändarens bankgironummer	<ul style="list-style-type: none"> <li>• Högerställt</li> <li>• Nollutfyllt</li> </ul>	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, avsnittsigill för Utlandsbetalningar (TK8)

---

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

---

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

---

**Sigillpost för utlandsbetalningar (TK8)** Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagringsform
1	Transaktionskod	8	1	N
2–9	Avsändarens bankgironummer	<ul style="list-style-type: none"> <li>• Högerställt</li> <li>• Nollutfyllt</li> </ul>	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, avsnittsigill för Löner (TK08)

**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	<ul style="list-style-type: none"> <li>• 1–2 (Transaktionskod)</li> <li>• 3-8 (Skrivdag)</li> <li>• 63-69 (Löngivarens kundnummer)</li> </ul>	15
35	<ul style="list-style-type: none"> <li>• 1–2 (Transaktionskod)</li> <li>• 3–8 (Löneutbetalningsdag)</li> <li>• 13-28 (Löntagarens /mottagarens kontonummer)</li> <li>• 29-40 (Belopp)</li> <li>• 53-58 (Blanka)</li> <li>• 59-68 (Personnummer, anställningsnummer eller blankt)</li> </ul>	52
09	<ul style="list-style-type: none"> <li>• 1-2 (Transaktionskod)</li> <li>• 3-8 (Skrivdatum)</li> <li>• 29-40 (Totalsumma)</li> <li>• 41-46 (Totalantal)</li> </ul>	26

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

**Sigillpost för Löner (TK08)** Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagringsform
1–2	Transaktionskod	08	2	N
3–12	Avsändarens kundnummer	<ul style="list-style-type: none"> <li>• Högerställt</li> <li>• Nollutfyllt</li> </ul>	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)

---

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

---

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

---

**Sigillpost för Autogiro (TK08)** Tabellen beskriver posten i detalj.

Position	Innehåll	Giltiga värden/Kommentar	Antal positioner	Lagringsform
1-2	Transaktionskod	08	2	N
3-6	Reservfält	Nollor	4	N
7-12	Avsändarens kundnummer	<ul style="list-style-type: none"> <li>• Högerställt</li> <li>• Nollutfyllt</li> </ul>	6	N
13-30	Kondensat	Det framräknade sigillet.	18	N
31-37	Sigillinformation	Tilläggsinformation om sigillet	7	A
38-80	Reservfält	Blankt.	43	A

---

## 7. Termer och definitioner

**Termer i dokumentet** Den här tabellen visar BGC:s definitioner av termer som hör ihop med tjänsten Leverantörsbetalningar och är relevanta för dig som programmerar.

Term	Definition
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.
Checksiffr	En kontrollsiffr som alltid står sist i till exempel ett kontonummer, <a href="#">OCR-referensnummer</a> eller ett bankgironummer.
Digital/Elektronisk signatur	En typ av förändringsskydd som skapas med hjälp av filen och ett personligt certifikat, en så kallad <i>e-legitimation</i> .  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.
Kommunikations-sätt	Det sätt företaget använder för att skicka och hämta filer, till och från BGC.
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 avsökas med fotocell och registreras automatiskt, oftast i samband med inmatning till dator.
OCR-referensnummer	Numeriskt begrepp som alltid innehåller en <a href="#">checksiffr</a> 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 BGC. Varje post har en egen <a href="#">transaktionskod</a> (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.
Transaktionskod	Alla poster i en fil har en transaktionskod (TK). Varje transaktionskod påbörjar en ny post. I Leverantörsbetalningar är till exempel en <ul style="list-style-type: none"> <li>• betalning = TK14</li> <li>• kreditfaktura = TK16/TK17</li> <li>• kontonummerpost = TK40.</li> </ul>