

Riksgäldskontorets författningssamling

Utgivare: chefsjuristen Charlotte Rydin, Riksgäldskontoret, 103 74 Stockholm
ISSN 1403-9346

Riksgäldskontorets föreskrifter om ändring av Riksgäldskontorets föreskrifter (RGKFS 2011:2) om instituts skyldighet att lämna uppgifter om insättare och deras insättningar;

RGKFS 2013:1

Utkom från trycket
den 28 augusti 2013

beslutade den 14 augusti 2013.

Riksgäldskontoret föreskriver, med stöd av 3 § förordningen (2011:834) om insättningsgaranti, att bilagan till Riksgäldskontorets föreskrifter om instituts skyldighet att lämna uppgifter om insättare och deras insättningar ska ha följande lydelse.

Dessa föreskrifter träder i kraft den 1 november 2013.

På Riksgäldskontorets vägnar

HANS LINDBLAD

Daniel Barr

RGKFS 2013:1 Bilaga

Informationsfilernas format och tekniska utformning

Informationsfilerna ska vara textfiler som skapas i ett flatfilmsformat med teckenuppsättningen Windows-1252. Filnamnen ska vara "kund.txt" för kundfilen, "konto.txt" för kontofilen, "kontofordelning.txt" för kontofördelningsfilen samt "transaktion.txt" för transaktionsfilerna.

I filerna ska varje rad separeras med radbrytning (CR-LF). Radbrytning får endast användas mellan varje rad. Radbrytning får inte användas efter den sista raden.

Varje kolumn ska separeras med ett s.k. pipe-tecken ("|", byte kod 0x7c). Pipe-tecken får endast användas mellan varje kolumn. Pipe-tecken får inte användas efter den sista kolumnen.

Det ska alltid finnas ett pipe-tecken som separerar varje kolumn, även när värdet i en viss kolumn är tomt.

Första raden i filerna ska alltid innehålla namnen på respektive kolumn.

Informationsfilernas innehåll och struktur

Informationsfilerna ska ha det innehåll och den struktur som framgår av tabellerna nedan.

Tabell 1 Kundfilen

Kolumnnamn	Beskrivning	Antal tecken	Dataformat
Kundnummer	Ett unikt nummer för insättaren.	Maximalt 50 tecken	Alfanumeriska tecken inom Windows-1252. Får ej vara tomt.
Namn	Samtliga namn (för fysiska personer) eller fullständig firma (för juridiska personer) på insättaren. Namnen ska skiljas med mellanslag.	Maximalt 150 tecken	Alfanumeriska tecken inom Windows-1252. Får ej vara tomt.
PersonOrgNummer	För insättare som är svenska privatpersoner ska fältet innehålla personnummer. För insättare som är svensk juridisk person ska organisationsnummer användas.	Maximalt 50 tecken	För personnummer ska 12 numeriska tecken användas, enligt ÅÅÅÅMMDDNNNN. För organisationsnummer ska 12 numeriska tecken användas enligt 16NNNNNNNNNN. För utländska insättare får anges ett globalt referensnummer. Detta ska börja med tecknen "REF" och kan sedan innehålla maximalt 47 alfanumeriska tecken.
	För utländska insättare kan ett s.k. globalt referensnummer användas om sådant finns.		Utländska insättare får ha ett tomt värde här om både person-/org.nummer och ett globalt referensnummer saknas.

Kolumnnamn	Beskrivning	Antal tecken	Dataformat
Utdelningsadress	Utdelningsadressen till insättaren.	Maximalt 250 tecken	Alfanumeriska tecken inom Windows-1252. Får vara tomt.
Postnummer	Postnummer till insättaren.	Maximalt 250 tecken	Alfanumeriska tecken inom Windows-1252. Får vara tomt.
Ort	Postort till insättaren.	Maximalt 250 tecken	Alfanumeriska tecken inom Windows-1252. Får vara tomt.
Postland	Land till insättaren. Anges bara om annat land än Sverige.	Maximalt 250 tecken	Alfanumeriska tecken inom Windows-1252. Får vara tomt.
Landskod	ISO-koden för landet som insättaren är registrerad i.	2 tecken	Landskod enligt ISO 3166-1. Får ej vara tomt.
CONamn	C/O-namn om sådant finns.	Maximalt 250 tecken	Alfanumeriska tecken inom Windows-1252. Får vara tomt.
TIN	Tax Identification Number. Skatteregistreringsnummer för insättare som är skattepliktiga i utlandet.	Maximalt 100 tecken	Alfanumeriska tecken inom Windows-1252. Får vara tomt för insättare som är skattepliktiga i Sverige.

Tabell 2 Kontofilen

Kolumnnamn	Beskrivning	Antal tecken	Dataformat
Kontonummer	Kontots nummer. Kontonumret ska vara unikt.	Maximalt 50 tecken.	Numeriska eller ickenumeriska tecken. Om clearingnummer finns så ska det anges tillsammans med kontonumret utan extra tecken. Får ej vara tomt.
Valuta	Valutakod enligt ISO 4217.	3 tecken	Treställig valutakod enligt ISO 4217. Får ej vara tomt.
Kapital	Det saldo som finns bokfört på kontot. Anges i den valuta som kontot är i. Ska inte innehålla upplupen ränta.	Maximalt 26 tecken	Decimaltal med komma (,) som decimalavskiljare. Kan innehålla värden från -2^{63} till 2^{63} med en precision på 1/10000. Får ej vara tomt.

RGKFS 2013:1

Kolumnnamn	Beskrivning	Antal tecken	Dataformat
UpplupenRänta	Den upplupna räntan fram till den dag då ersättningsrätt inträder.	Maximalt 26 tecken	Decimaltal med komma (,) som decimalavskiljare. Kan innehålla värden från -2^{63} till 2^{63} med en precision på 1/10000. Får ej vara tomt.
Pantsatt	"Ja" om kontot är pantsatt, "Nej" om konton inte är pantsatt.	Maximalt 3 tecken	"Ja" eller "Nej". Får ej vara tomt.
Spärrat	"Ja" om kontot är spärrat för utbetalning till kontohavaren och "Nej" om konton inte är spärrat.	Maximalt 3 tecken	"Ja" eller "Nej". Får ej vara tomt.

Tabell 3 Kontofördelningsfilen

Kolumnnamn	Beskrivning	Antal tecken	Dataformat
Kontonummer	Används för koppling mellan konton och insättare.	Maximalt 50 tecken	Ska matcha kontonummer i kontofilen. Får ej vara tomt.
Kundnummer	Används för koppling mellan konton och insättare.	Maximalt 50 tecken	Ska matcha kundnummer i kundfilen. Får ej vara tomt.
KundensAndel	Andel i decimalform där 1 är högst och 0 är lägst.	Maximalt 6 tecken	Anges med fyra decimalers noggrannhet. Får ej vara tomt.

Samma kundnummer och kontonummer får förekomma flera gånger i kontofördelningsfilen, men kombinationer av kundnummer och kontonummer ska vara unika.

Tabell 4 Transaktionsfilen

Kolumnnamn	Beskrivning	Antal tecken	Dataformat
Kontonummer	Används för koppling mellan transaktioner och konto.	Maximalt 50 tecken	Ska matcha kontonummer i kontofilen. Får ej vara tomt.
Transaktionsdatum	Datum och tidpunkt för transaktionen.	Maximalt 20 tecken	Anges i formatet: "ÅÅÅÅ-MM-DD TT:MM:SS". Får ej vara tomt.
Bokföringsdatum	Datum och tidpunkt för bokföringen.	Maximalt 20 tecken	Anges i formatet: "ÅÅÅÅ-MM-DD TT:MM:SS". Ska vara tomt i första filen. Får ej vara tomt i andra filen.
Referens	Vem som är transaktionens betalningsavsändare eller betalningsmottagare.	Maximalt 50 tecken	Alfanumeriska tecken inom Windows-1252. Får vara tomt
Belopp	Belopp på transaktionen.	Maximalt 26 tecken	Ska vara i samma valuta som kontot avser. Decimaltal med komma (,) som decimalavskiljare. Kan innehålla värden från -2^{63} till 2^{63} med en precision på 1/10000. Får ej vara tomt.

Transaktionsfil 1 ska visa transaktioner som vid slutet av dag 1 är registrerade men inte bokförda på de konton som finns i kontofilen.

Transaktionsfil 2 ska visa de transaktioner som faktiskt bokförts på de konton som finns i kontofilen från och med dag 2 till och med dag 4, och som avser tiden fram till och med dag 1.

Arkivering och komprimering av informationsfilerna

Informationsfilerna ska arkiveras och komprimeras till ett s.k. 7z-arkiv med programvaran 7-zip. Filformatet för 7z-arkivet ska följa specifikationen i källkoden till 7-zip.

Kryptering och signering av informationsfilerna

Det komprimerade arkivet ska krypteras och signeras med programvaran GnuPG/gpgsm, OpenSSL eller annan programvara som är kompatibel med följande krav:

1. Kryptering ska ske med krypteringsalgoritmen AES256.
2. Signering ska ske med hashalgoritmen SHA512.
3. Meddelandeformatet ska följa CMS (RFC5652).

RGKFS 2013:1

4. Anonyma metoder för nyckelutbyte får inte användas.
5. Minsta tillåtna längd på kryptografiska nycklar för asymmetriska algoritmer är 2048 bitar.
6. Väl kända och granskade implementeringar av kryptografiska programvaror ska användas.
7. Det kryptografiska systemet ska ha skydd mot angrepp såsom (i) att någon ställer sig som mellanhand mellan server och klient och på så sätt obehörigen tar del av information (s.k. man-in-the-middle), (ii) repetition och (iii) fördröjningsattacker.

Tekniska krav på institutets unika IP-adress

Den eller de IP-adresser som institutet uppger till Riksgäldskontoret ska vara adresser enligt formatet IPv4.

Förklaringar av tekniska begrepp som används i denna bilaga

7-zip	Ett komprimeringsprogram som finns tillgängligt som fri programvara med öppen källkod och som kan laddas ner på internetadressen 7-zip.org .
AES256	En krypteringsalgoritm enligt standarden FIPS PUB 197 publicerad av National Institute of Standards and Technology (NIST).
CMS	Förkortning för Cryptographic Message Syntax som är ett format (angivet i dokumentet RFC 5652) för kryptografiskt skyddade meddelanden, fastställt av Internet Engineering Task Force (IETF).
hashalgoritm	Matematisk funktion eller algoritm som bland annat kan användas vid signering av data.
GnuPG/Gpgsm	Programvara för digital kryptering och signering, som ingår i programpaketet GnuPG.
IPv4	Internet Protocol version 4 (IPv4) är idag den version som Internet i huvudsak baseras på.
krypteringsalgoritm	Matematisk funktion eller algoritm som användas vid kryptering av data.
OpenSSL	Programvara för digital kryptering och signering, som är tillgänglig som öppen källkod och som kan laddas ner på internetadressen www.openssl.org .
SHA512	En hashalgoritm enligt standarden FIPS PUB 180-3 publicerad av National Institute of Standards and Technology (NIST).
Windows-1252	En teckenkodning för det latinska alfabetet som används i operativsystemet Microsoft Windows.

