TULLI
TULL·CUSTOMS

14.4.2020

Övervakningssystem för bank- och betalkonton

Beskrivning av Kontoregistrets uppdateringsgränssnitt

Dokumentversion 1.0.4

Versionshistorik

Version	Datum	Beskrivning
1.0	21.10.2019	Version 1.0
1.0.1	29.1.2020	firstName- och lastName-properties i JSON-schemats privatePerson-objekt har förenats till ett fullName-property
1.0.2	3.2.2020	En juridisk persons medborgarskap har ändrats till en medborgarskapslista.
1.0.3	3.2.2020	Av organisationens egenskaper har businessId ändrats till registrationNumber och businessIdCountryCode har tagits bort.
1.0.4	5.3.2020	Kraven gällande signaturen på meddelandenivå har uppdaterats. PKI och dess förklaring har lagts till. Gränssnittets högsta meddelandestorlek och beskrivningen av hur uppgifter lämnas till Kontoregistret har uppdaterats. Precisering av hur omtvistade/felaktiga uppgifter anmäls.

Innehåll

1. Inledning

1.1 Termer och förkortningar

Förkortning eller term	Förklaring
Gränssnitt	Standardenlig praxis eller kontaktyta som möjliggör överföring av information mellan enheter, programvara eller användare.
WS (Web Service)	Webbaserat datorprogram som med hjälp av standardiserade internetprotokoll ställer tjänster till förfogande för applikationerna. De tjänster som kontoregistret tillhandahåller är överföring av uppgifter samt begäran och förfrågan om uppgifter. Den tjänst som datasöksystemet tillhandahåller är förfrågan om uppgifter.
Endpoint	Gränssnittstjänst som finns tillgänglig på en viss webbadress.
REST	(Representational State Transfer) En arkitekturmodell som bygger på en HTTP-protokoll för genomförande av programmeringsgränssnitt.
JSON	(JavaScript Object Notation) filformat för dataöverföring enligt öppen standard.
PKI	Teknik med öppen nyckel. En elektronisk signatur som bygger på teknik med öppen nyckel skapas så att det av den uppgift som signeras skapas ett kondensat (med en hash-algoritm), som krypteras med nyckelparets privata nyckel. Det krypterade kondensatet sparas i anslutning till den signerade uppgiften eller det elektroniska dokumentet, eller så förmedlas uppgiften på annat sätt till mottagaren. Mottagaren dekrypterar kondensatets kryptering med nyckelparets öppna nyckel, återskapar kondensatet av meddelandets eller dokumentets uppgifter och jämför det med kondensatet som kopplats till signaturen. Meddelandets innehåll förblir oförändrat, såvida kondensaten är lika. (Anvisning om informationssäkerheten inom elektronisk ärendehantering)

1.2 Dokumentets syfte och omfattning

Detta dokument är en gränssnittsbeskrivning för uppdateringsgränssnittet för registret över bank- och betalkonton.

1.3 Allmän beskrivning

Detta dokument ingår i Tullens föreskrift om ett övervakningssystem för bank- och betalkonton. Dokumentets syfte är att instruera leverantörer av uppgifter om genomförandet av uppdateringsgränssnittet för bank- och betalkontoregistret (härefter Kontoregistret). Detta dokument kompletteras av Instruktioner för produktionssättning och underhåll av bank- och betalkontoregistret.

Systemet består av två delar: registret över bank- och betalkonton och datasöksystemet.

I detta dokument beskrivs Kontoregistrets uppdateringsgränssnitt.

2. Aktivitetsbeskrivning

I detta kapitel beskrivs överföring av bank- och betalkontouppgifter i form av flödesscheman.

2.1 Överföring av bank- och betalkontouppgifter till Kontoregistret

När uppgifter överförs till kontoregistret första gången ska alla berörda uppgifter överföras till registret. Därefter överförs bara uppdaterade eller nya uppgifter dagligen.

På bild 2.1 visas överföring av bank- och betalkontouppgifter till Kontoregistret i form av ett flödesschema.

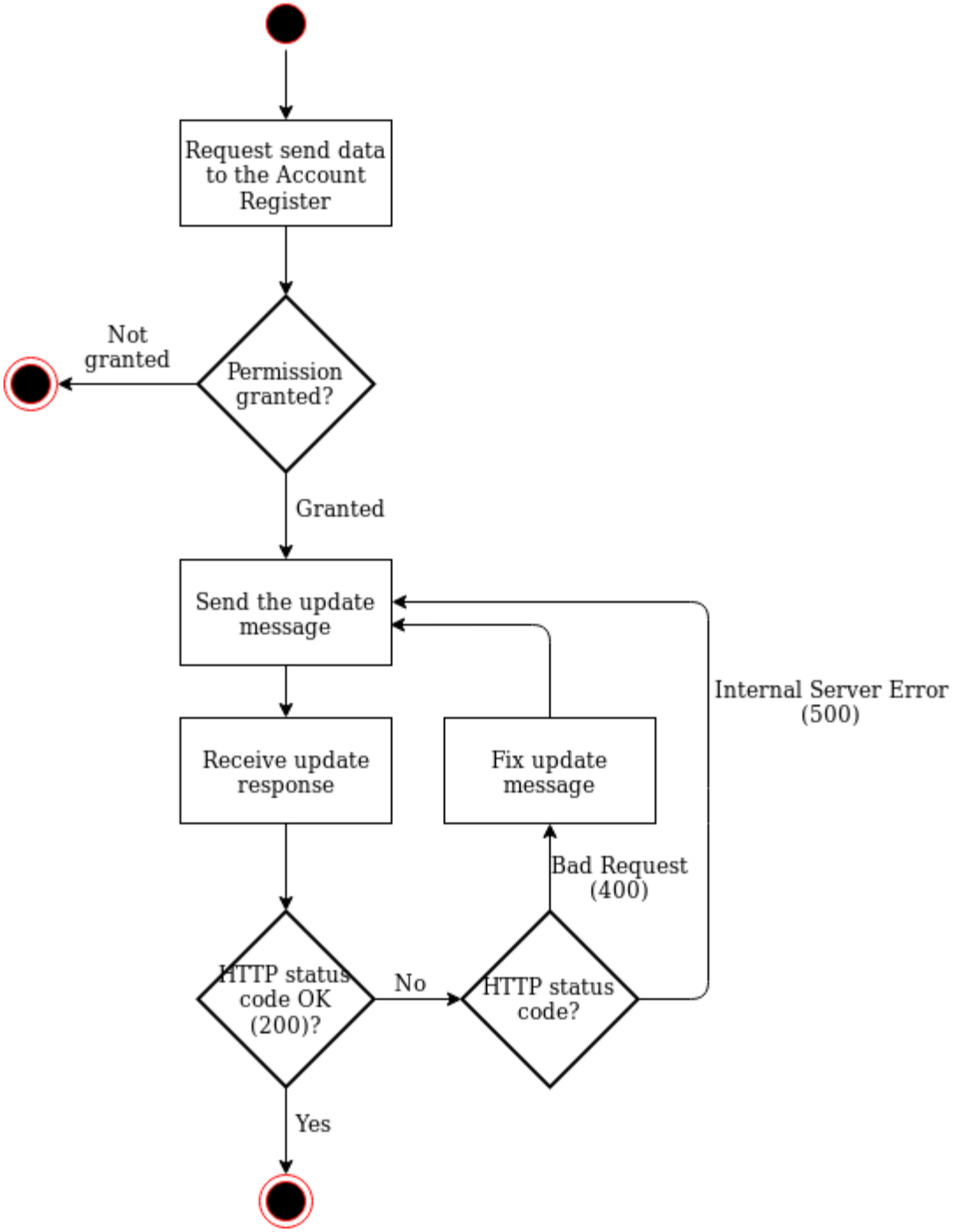

Bild 2.1 *Överföring av bank- och betalkontouppgifter.*

Av bilden framgår att uppdateringsgränssnittet är synkront. I brödtexten till ett HTTP-svar returneras antingen en uppgift om att uppdateringen lyckats eller en uppgift om fel vid exempelvis validering av meddelandet.

3. Dataskydd

3.1 Identifiering

Signeringscertifikat för utgående meddelanden

Utgående meddelanden ska automatiskt signeras med servercertifikatet x.509 (version 3), av vilket FO-nummer eller momsnummer för uppgiftslämnaren ska framgå. Godkännande av signaturen förutsätter

antingen

a) att certifikatet har utfärdats av BRC, är i kraft och inte finns på BRC:s spärrlista och att attributet serialNumber för objektet för certifikatet är FO-numret eller momsnumret för uppgiftslämnaren

eller

b) att certifikatet är ett identifieringscertifikat för eIDAS-godkända webbplatser, är i kraft och inte finns på certifikatutfärdarens uppdaterade spärrlista och att attributet organizationIdentifier för objektet för certifikatet är FO-numret eller momsnumret för uppgiftslämnaren.

Signeringscertifikat för inkommande meddelanden

Signaturen i meddelanden från Kontoregistret ska godkännas, förutsatt att

a) certifikatet som används för signering har utfärdats av BRC, är i kraft och inte finns på BRC:s spärrlista

b) attributet serialNumber för objektet för certifikatet är Tullens FO-nummer ”0245442-8” eller bokstäverna FI och sifferdelen i Tullens momsnummer: ”FI02454428”.

Servercertifikat för uppgiftslämnaren eller en aktör som befullmäktigats av uppgiftslämnaren

Datakommunikationen ska skyddas (kryptering och identifiering av motpart) med x.509-certifikat (version 3).

Ett servercertifikat ska användas för att bilda en förbindelse, och FO-nummer eller momsnummer för uppgiftslämnaren eller en aktör som befullmäktigats av denne ska framgå av certifikatet. Med en aktör som befullmäktigats av uppgiftslämnaren avses exempelvis en servicecentral som uppgiftslämnaren har befullmäktigat att upprätta och/eller skicka anmälningar. En fullmakt gällande detta ska lämnas in skriftligen till Tullen.

Godkännande av signaturen förutsätter

antingen

a) att servercertifikatet har utfärdats av BRC, är i kraft och inte finns på BRC:s spärrlista

och att attributet serialNumber för objektet för certifikatet är FO-numret eller momsnumret för uppgiftslämnaren eller en aktör som befullmäktigats av denne

eller

b) att servercertifikatet är ett identifieringscertifikat för eIDAS-godkända webbplatser, är i kraft och inte finns på certifikatutfärdarens uppdaterade spärrlista och att attributet organizationIdentifier för objektet för certifikatet är FO-numret eller momsnumret för uppgiftslämnaren eller en aktör som befullmäktigats av denne.

Om datakommunikationscertifikatet för uppgiftslämnaren och signeringscertifikatet för det utgående meddelanden har samma FO-nummer eller momsnummer, kan samma certifikat användas för båda ändamålen.

Kontoregistrets servercertifikat

Uppgiftslämnaren identifierar förbindelsens motpart som Kontoregistret på basis av ett servercertifikat, förutsatt att
a) servercertifikatet för den som ansvarar för Kontoregistret (Tullen) har utfärdats av BRC och inte finns på BRC:s spärrlista
b) attributet serialNumber för objektet för certifikatet är ”FI02454428” eller ”0245442-8”.

3.2 Skydd för förbindelser

Förbindelserna i Kontoregistrets uppdateringsgränssnitt är skyddade med TLS-kryptering med TLS-protokollets version 1.2 eller högre. Båda ändarna av förbindelsen identifieras med servercertifikatet som beskrivs ovan genom ömsesidig TLS-autentisering. Förbindelsen ska bildas med hjälp av ett ephemeral Diffie-Hellman (DHE) nyckelbyte där det för varje session skapas en ny unik privat krypteringsnyckel. Syftet med detta förfarande är att säkerställa krypteringens forward secrecy-egenskap så att ett röjande av krypteringsnyckeln inte leder till att den krypterade informationen röjs.

De kryptografiska algoritmer som används vid TLS-kryptering ska ha minst samma kryptografiska styrka som de kryptografiska styrkekrav som Kommunikationsverket fastställt för den nationella krypteringsnivån ST IV. Nuvarande styrkekrav beskrivs i dokumentet https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf (Dnr: 190/651/2015).

3.3 Tillåten HTTP-version

De förbindelser som används av uppdateringsgränssnittet använder version 1.1 av HTTP-protokollet.

3.4 Signering på meddelandenivå

Meddelanden i uppdateringsgränssnittet förses med JWS-signatur (PKI). För JWS-signaturen används algoritmen RS256 och meddelandena signeras med avsändarens privata nyckel. Anvisningar om inlämning av den öppna nyckeln till Tullen finns i Instruktioner för produktionssättning och underhåll av bank- och betalkontoregistret.

De kryptografiska algoritmer som används i signaturen ska till sin kryptografiska styrka motsvara minst Kommunikationsverkets krav på kryptografisk styrka för den nationella skyddsnivån ST IV. De nuvarande kraven gällande styrkan beskrivs på finska i dokumentet https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf (Dnro: 190/651/2015).

Uppdateringsmeddelandet ska ha två separata JWS-signaturer (exemplen nedan):
a) Authorization header ska ha Bearer token JWS innehållande avsändarens FO-nummer.
b) Request body ska ha JWS där “reportUpdate” property innehåller ett uppdateringsmeddelande enligt JSON schemat.

Anmälan om ett felaktigt meddelande eller om ett meddelande som misstänks vara felaktigt skiljer sig från uppdateringsmeddelandet så att “reportUpdate” claim lämnas bort helt och hållet och ersätts av antingen “reportDisputable” eller “reportIncorrect” beroende på situationen (se den allmänna beskrivningen av Kontoregistrets uppdateringsgränssnitt).

a) Authorization header JWS:

JWT Header

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

JWT Payload

```
{
  "sub": "[SUBJECT]",
  "senderBusinessId": "[BUSINESS_ID]"
}
```

b) Request body JWS:

JWT Header

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

JWT Payload

```
{
  "sub": "[SUBJECT]",
  "reportUpdate": "[JSON STRING]"
}
```

3.5 Skyldighet att anmäla informationssäkerhetsincidenter

Den som använder gränssnittet är skyldig att utan dröjsmål anmäla till såväl den som utfärdat certifikatet som Tullen att certifikaten eller deras krypterade nycklar som används har äventyrats.

Den som använder gränssnittet är även skyldig att utan dröjsmål anmäla till Tullen om det observeras informationssäkerhetsincidenter i datasystemet som använder gränssnittet.

3.6 Gränssnittets kapacitet

Den högsta tillåtna meddelandestorleken för gränssnittet är 5MB. Gränssnittets högsta tillåtna uppdateringsfrekvens läggs till detta dokument senare.

4. Allmän beskrivning av kontoregistrets uppdateringsgränssnitt

Uppdateringsgränssnittet implementeras med REST/JSON.

Användaren av gränssnittet (den som överför uppgifter) ska skicka minst ett (1) minimimeddelande (se till att de *-märkta fälten nedan har ifyllts) inom utsatt tid, t.ex. en gång per månad (watchdog timer reset). Om inget meddelande har skickats under denna tid, skickas en begäran om utredning av fel. Om man inte reagerar på detta inom utsatt tid, inleds ett sanktionsförfarande.

Varje meddelande ska innehålla datum då det skapats.

Varje meddelande ska innehålla uppgiftsleverantörens FO-nummer i senderBusinessId-fältet.

I uppdateringsmeddelandets meddelandestruktur anmäls juridiska personer, kundrelationer, konton och bankfack som nyckel-värde-par, där nyckeln utgör ett individuellt id UUIDv4 (Universally unique identifier) för posten. Tullen utfärdar inte dessa id, utan de skapas av den som överför uppgifter och de kan användas för att specificera kunduppgifter. Utifrån detta id kan posterna identifieras, till exempel om personens namn eller personbeteckning ändras. Exempel på uppdateringsmeddelandets meddelandestruktur finns under Beskrivning av meddelandestrukturen.

För specificering av meddelanden används id:t X-Correlation-ID (UUIDv4) som finns i meddelandets header. Om ett sådant inte finns i meddelandet genereras det automatiskt och returneras i svarsmeddelandet.

Man kan anmäla inlämnade uppgifter som felaktiga eller så kan man anmäla att man misstänker att de är felaktiga med separata meddelanden och endpoints. För detta används det ovannämnda, for posten individuella id:t UUIDv4. Exempel på meddelanden finns Beskrivning av meddelandestrukturen.

I tabellen nedan finns en lista över gränssnittets endpoints.

HTTP-metod	Sökväg	Syfte och funktion
POST	/report-update	Sådana som är skyldiga att leverera uppgifter (betalningsinstitut, institut för elektroniska pengar, tillhandahållare av virtuell valuta eller kreditinstitut som erhållit undantagstillstånd av Finansinspektionen) använder denna endpoint för att överföra uppgifter om kundrelationer, kontouppgifter och bankfack till Kontoregistret.
POST	/report-disputable	Används för att anmäla att en tidigare överförd uppgift eventuellt är felaktig/omtvistad. Med denna endpoint kan man även häva uppgiftens omtvistade status om uppgiften visar sig vara riktig. En uppgift som anmälts som omtvistad anmäls som faktiskt felaktig med POST /report-incorrect.
POST	/report-incorrect	Används för att anmäla att en tidigare överförd uppgift eventuellt är felaktig. När ett fel anmäls i en uppgift som anmärkts som omtvistad tolkas tvisten som löst och uppgiften som felaktig.

Endpointen används för att överföra uppgifter till Kontoregistret. I meddelandet skickas uppgifter om kundrelationer, konton och bankfack.

Notation

För strukturerad beskrivning av gränssnittsposter används följande notation:

```
Objekt {
  post                uppgiftstyp
}
```

Beskrivning av meddelandestrukturen

Exempelmeddelanden finns via länkarna nedan:

Uppdateringsmeddelande

Anmälan om omtvistad uppgift

Anmälan om felaktig uppgift

För validering av uppdateringsmeddelandets JSON-struktur har man gjort ett schema enligt JSON Schema draft 7.

HTTP-svar

200 OK

400 Bad Request

Body

{
errorMessage string
}

405 Method Not Allowed

Body

```
{
  errorMessage              string
}
```

500 Internal Server Error

Body

```
{
  errorMessage              string
}
```