Betaalvereniging Nederland

Guidance voor het gebruik van cryptografische hashfuncties bij bestanden van SEPA Credit Transfers (betaalopdrachten)

Hashing Batchbetalingen

18 november 2015 | Versie 1.1 | Final

Auteur
Jeroen Jacobs | 020 305 19 51 | j.jacobs@betaalvereniging.nl
Jos van Wijk | 020 205 1997| j.vanwijk@betaalvereniging.nl

Betaalvereniging Nederland

Inhoudsopgave

1. Voorwoord en leeswijzer

In dit document is beschreven wat “best practices” zijn in het proces van aanlevering van SEPA bestanden met betaalopdrachten als van cryptografische hashfuncties (hierna “hashing”) gebruik wordt gemaakt; hashing is een methode om te detecteren of een bestand - in dit geval een SEPA XML-bestand met betaalopdrachten - tussentijds is aangepast. Dit door een berekening van een initiële filehash te vergelijken met een later berekende controle filehash.

Hashing is specifiek van belang in situaties dat bestanden worden aangeleverd of doorgeleid via kanalen die niet beveiligd zijn; een voorbeeld van zo’n kanaal is internet.

De aanbevelingen in deze beschrijving hebben enerzijds als doel om het ontstaan van veel verschillende integriteitsoplossingen te vermijden en anderzijds om vast te leggen welke instellingen verantwoordelijk zijn voor een veilige uitwisseling van betaalbestanden in bepaalde trajecten van de procesketen en hierover afspraken dienen te maken.

In hoofdstuk 2 wordt de achtergrond van bestandsbeveiliging en keuze voor filehashing toegelicht. Hoofdstuk 3 gaat vervolgens dieper in op het doel van hashing en de aangeboden standaard hashing functionaliteit door de banken. Tevens is in dat hoofdstuk een aantal aandachtspunten opgenomen om hashing succesvol toe te kunnen passen. In hoofdstuk 4 zijn de verschillende betaalketens waarin hashing kan worden toegepast globaal beschreven. Tot slot is in hoofdstuk 5 een aantal verwijzingen opgenomen naar technische specificaties van SHA-256 en bevat hoofdstuk 6 aanvullend nog enige algemene maatregelen die organisaties in de (administratieve) organisatie rond betaalprocessen kunnen implementeren.

2. Inleiding

2.1 Achtergrond

Voorafgaand aan de migratie naar SEPA (afgerond in 2014) werden bestanden met betaalopdrachten door bedrijven veelal met het Nederlandse CLIEOP formaat aangeleverd. SEPA vraagt voor de verwerking van bestanden het Europese (XML) PAIN formaat.
Van de methoden voor bestandsbeveiliging, die voorheen voor CLIEOP werden gebruikt (som van de bedragen en som van de rekeningnummers) komt de som van rekeningnummers in de Europese XML standaard niet voor. Veel bedrijven gebruikten in het CLIEOP-tijdperk de controletelling “som van de rekeningnummers” onder meer om aan de eigen accountant aan te tonen dat de betalingen gecontroleerd waren uitgevoerd.

2.2 Verzoek marktpartijen

Bedrijven en software- c.q. service organisaties hebben gevraagd om functionaliteit ter vervanging van het wegvallen van de controle som rekeningnummers. Ook accountants hebben aangedrongen op een vorm van “beveiliging” van betaalbestanden, waarmee de integriteit gevalideerd kan worden.

2.3 Oplossingsrichting(en) en keuze voor hashing

Een geavanceerde oplossing voor end-to-end beveiliging is het gebruik van cryptografische handtekeningen en een end-to-end SSL verbinding tussen het ERP-systeem van een bedrijf, eventueel via één of meerdere tussenliggende partijen die specifieke services bieden, en de betaalinstelling. Banken, leveranciers van banken en grote klanten hebben de bestandsbeveiliging vaak op deze wijze ingericht. Voorzienbare problemen bij een brede implementatie van deze oplossing zijn de te verwachten kosten, de complexiteit in de implementatie bij alle ERP leveranciers en het beheer van de certificaten.

In situaties waarbij een geavanceerde oplossing – zoals hierboven genoemd – niet haalbaar wordt geacht, wordt geadviseerd om als functionaliteit de toepassing van een cryptografische hashfunctie (“hashing”) te gebruiken, die wordt berekend over de gehele batch met betalingen. Naar de huidige stand van beveiliging is gekozen voor hashing met SHA-256.

2.4 Interne controle rond betaalprocessen in hoofdlijnen

Een belangrijke doelstelling voor bedrijven rond betaalprocessen is om de interne organisatie zo in te richten dat uitsluitend geautoriseerde betalingen worden gedaan, dat wil zeggen dat intern door een bevoegd persoon is vastgesteld dat de overeengekomen prestatie is geleverd, de vergoeding voor de prestatie juist is en de bedragen worden overgemaakt naar de juiste bankrekening van de juiste begunstigde.

De twee meest voorkomende vormen van betalingen door bedrijven zijn crediteurenbetalingen en salarisbetalingen. In hoofdstuk 6 zijn een aantal controlemaatregelen genoemd die bedrijven kunnen treffen om de administratieve organisatie rond deze betaalprocessen op een verantwoorde wijze in te richten.

Het betaalbestand zelf is met de introductie van SEPA een XML-bestand. Dit bestand kan met enige technische kennis rechtstreeks worden gewijzigd. Een eerste vereiste vanuit de interne controle is dus dat dergelijke bestanden in een beveiligde omgeving worden aangemaakt waarbij uitsluitend bevoegde personen - binnen de genomen interne controle maatregelen - toegang hebben. Tevens verdient het aanbeveling om bij het genereren van dit bestand gebruik te maken van officiële (of daaraan gelijkwaardige) administratieve software en de gegenereerde betaalbestanden op te slaan op een locatie die niet door ongeautoriseerde gebruikers kan worden benaderd.

De in dit document verder uitgewerkte hashing oplossing kan als aanvullende maatregel worden toegepast om te kunnen detecteren of het betaalbestand verder in de betaalketen niet (ongeoorloofd) is gewijzigd.

3. Gebruik van hashing en aandachtspunten

Dit hoofdstuk gaat dieper in op het doel van hashing en de aangeboden standaard hashing functionaliteit door de banken. Tevens is in dit hoofdstuk een aantal aandachtspunten opgenomen om hashing succesvol toe te kunnen passen.

3.1 Doel van hashing

Hashing biedt de zakelijke klant van de bank de mogelijkheid om te controleren of een betaalbestand dat in de eigen (beveiligde) omgeving en conform de juiste autorisaties en interne controles is aangemaakt en mogelijk via een (onbeveiligd) netwerk is verzonden, niet ongeautoriseerd is gewijzigd voordat het is aangekomen bij de bank.

3.2 Werking van hashing

Het uitvoeren van hashing op een bestand levert een filehash op; een korte, numerieke reeks van tekens die het digitaal equivalent van een vingerafdruk vormen van dat bestand. Een berekende hash is dus uniek voor ieder bestand; twee verschillende bestanden kunnen niet dezelfde hash opleveren.

Deze eigenschap kan worden gebruikt om in een proces te detecteren of een bestand in de tussentijd is gewijzigd, bijvoorbeeld na transport;

1. De verzender berekent van het bestand een filehash
2. De verzender stuurt vervolgens het bestand naar de ontvanger over een transport kanaal
3. De ontvanger berekent van het ontvangen bestand een filehash
4. De ontvanger presenteert zijn filehash aan de verzender over een alternatief communicatie kanaal
5. Beide filehashes worden met elkaar vergeleken en dienen identiek te zijn. Indien ze niet identiek zijn, dan is het bestand gemanipuleerd of gecorrumpeerd tijdens transport.

3.3 Aangeboden standaard hashing functionaliteit

De aanvullende dienst van de bank bestaat uit het herberekenen van de filehash over ontvangen betaalbestanden en het aanbieden van het resultaat aan de klant. Het is dan verder aan de klant om te besluiten of deze het betaalbestand voor verdere verwerking autoriseert. Ook de inhoudelijke verantwoordelijkheid voor aangemaakte betalingsopdrachten berust te allen tijde bij de klant.

Het aanbieden van de filehash door de bank kan op meerdere manieren worden ingericht. Banken kunnen bijvoorbeeld de filehash in beeld tonen na de upload of deze via een SMS-bericht naar een afgesproken telefoonnummer sturen.

Het gebruikte filehash algoritme is SHA-256. Optioneel kunnen banken ook andere hash algoritmes of aanvullende functionaliteit gebaseerd op hashing aanbieden. Dit valt buiten deze standaard hashing functionaliteit.

Standaard worden filehashes berekend over het hele betaalbestand. Banken archiveren de berekende filehashes over aangeleverde betaalbestanden t.b.v. latere navraag.

3.4 Aandachtspunten

Bij de inrichting van de administratieve processen rond het gebruik van hashing door zakelijke gebruikers wordt aanbevolen om rekening te houden met de navolgende aandachtspunten:

- **Bereken de filehash binnen een veilige omgeving en zo mogelijk direct na de aanmaak van het betaalbestand**
  Voor het berekenen van de filehash over het betaalbestand gelden in principe dezelfde eisen aan de beveiliging van de (netwerk)omgeving en de toepassing van de interne controle maatregelen als het voor aanmaken van het betaalbestand zelf. Dat wil zeggen dat de filehash berekening wordt geïnitieerd door een bevoegde persoon nadat conform de interne procedures is vastgesteld dat het betaalbestand correct is en de juiste gegevens bevat.

  Het verdient verder aanbeveling om de filehash direct na c.q. als onderdeel van het aanmaakproces van het betaalbestand te berekenen, vanuit of middels de officiële (of daaraan gelijkwaardige) administratieve software van het bedrijf.

- **Beveilig de opgeslagen filehashes**
  Bij de opslag van de berekende filehashes ten behoeve van latere vergelijking dient de opslag dusdanig plaats te vinden dat wijzigen van de filehash vrijwel onmogelijk is ofwel vrijwel onmogelijk door derden te benaderen of te manipuleren is. Mogelijkheden zijn separate opslag op papier, encryptie van het opslagmedium, opslag buiten het netwerk of het gebruik van eenmalig beschrijfbare media zoals een WORM drive (Write Once-Read Many).

  Het is van de integriteit van de initieel berekende filehash afhankelijk of deze voldoende bruikbaar is als controlemiddel voor de vergelijking van het betaalbestand aan de zendende en ontvangende zijde.

  N.b. Indien een persoon toch toegang weet te krijgen tot het betaalbestand en de opgeslagen filehash kan deze naast de betaalgegevens ook de filehash aanpassen. Zo bereikt een potentiële fraudeur dat de aanpassing van het betaalbestand later niet op basis van de vergelijking van filehashes kan worden gedetecteerd.

- **Gebruik een alternatief kanaal voor uitwisseling van filehashes**
  Maak voor het uitwisselen van filehashes altijd gebruik van ander kanaal dan het kanaal waarlangs het betaalbestand wordt verstuurd. Een voorbeeld van zo'n ander (ofwel een out-of-

band) kanaal is een SMS, een scanner code of het tonen van een bericht in een andere omgeving.

Stuur de hash in ieder geval nooit mee (ter controle door de ontvangende partij) met het betaalbestand zelf. Als de hash namelijk wordt meegestuurd en het bestand wordt onderschept dan kan tegelijk met het betaalbestand ook de filehash worden aangepast. Ook hier verliest de filehash dan de waarde als middel om tussentijdse wijzigingen in betaalbestanden te detecteren.

- **Wijzigingen in betaalbestanden maken de filehash onbruikbaar**
  Hashing kan in een betaalketen alleen succesvol worden toegepast als de het betaalbestand ongewijzigd tussen (meerdere) partijen wordt uitgewisseld. Elke wijziging of toevoeging, hoe klein ook, zal leiden tot een andere uitkomst en doet het gebruik van de filehash als controle teniet.

  Als een betaalbestand in de keten wordt doorgegeven en vinden wijzigingen plaats, kan hashing in meerdere keren (point-to-point) worden toegepast. Een voorbeeld van een dergelijk proces is opgenomen in paragraaf 4.2.2.

- **Houdbaarheid SHA-256 algoritme**
  File hashing algoritmes hebben een beperkte levensduur. Door de toenemende rekenkracht van computers zullen (nu als veilig beschouwde) algoritmes ooit ontsleuteld kunnen worden. Tevens doen wetenschappers (en hackers) onderzoek naar zwaktes in de algoritmes, waardoor ontsleuteling sneller mogelijk gemaakt kan worden. Oplossingen die gebruik maken van file hashing dienen daarom zo ontworpen te worden, dat het ene algoritme eenvoudig door een ander vervangen of aangevuld kan worden. De Betaalvereniging zal periodiek evalueren of SHA-256 nog steeds de juiste keuze is.

- **Advies om canocalization toe te passen.**

SEPA bestanden zijn XML bestanden. Een van de voordelen het gebruik van XML is dat een XML bestand redelijk leesbaar is. Om deze leesbaarheid verder te vergroten maakt een ontwikkelaar ook nog wel eens gebruik van extra tabs, spaties en regeleindes. Bijvoorbeeld om een passage mooi uit te lijnen.

Bij het inlezen van het SEPA XML bestand in een andere applicatie worden deze (onnodige) leestekens zoals spaties echter vaak automatisch verwijderd. Functioneel verandert er niets. De aangeboden informatie blijft hetzelfde. Maar de filehash van zo'n bestand verandert wel. En is dus per definitie niet meer gelijk aan de filehash van het originele bestand.

Om te voorkomen dat ergens in de keten bij inlezen de overbodige leestekens worden verwijderd – en daarmee de filehash wijzigt – is het dus aan te bevelen om dergelijke (onnodige) leestekens niet te gebruiken. Of om het betaalbestand alvast te schonen voordat de initiële filehash wordt berekend. Het schonen of normaliseren van een XML-bestand wordt ook

wel ‘canocalization’ genoemd. Voor de meeste platformen is standaard een canocalization functie aanwezig.

Meer informatie en voorbeelden van canocalization verwijzen wij naar W3C Recommendation 15 March 2001 version of XML Canonicalization:
http://www.w3.org/TR/xml-c14n#XMLCanonicalization

4. Globale procesbeschrijvingen bij verschillende aanlevervormen

Dit hoofdstuk beschrijft de meest voorkomende routes voor de aanlevering van betaalbestanden. Het betreft:

- Proces bij rechtstreekse aanlevering van de zakelijke klant naar de bank.
- Proces waarbij de zakelijke klant gebruik maakt van een derde partij voor de aanmaak van het betaalbestand

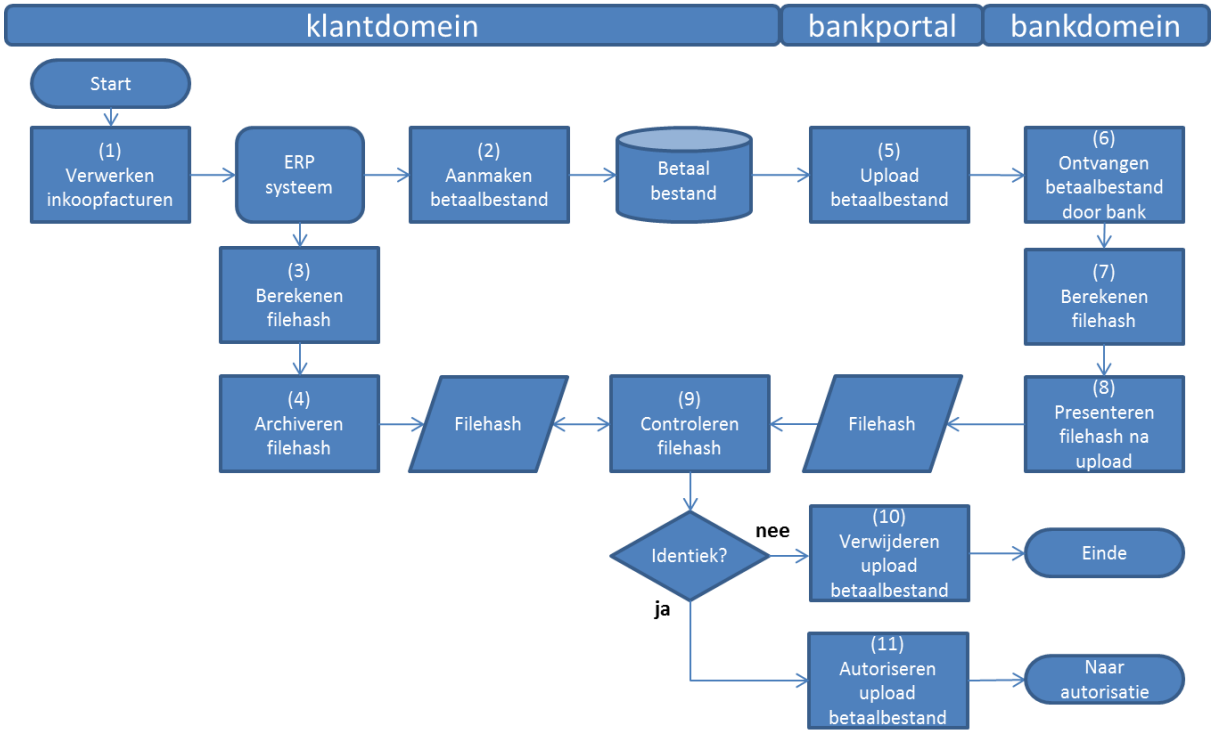
Tot slot van dit hoofdstuk wordt de situatie van directe aanlevering en multibank aanlevering toegelicht.

In de procesbeschrijvingen wordt specifiek ingezoomd op de toepassing van hashing. Nadrukkelijk wordt aangegeven dat het slechts voorbeelden betreft. In het kader van dit document wordt niet gestreefd naar een uitputtende/volledige beschrijving van de aanleverprocessen van betaalbestanden bij banken.

4.1 Proces bij aanlevering rechtstreeks van zakelijke klant naar bank

Deze paragraaf beschrijft de situatie waarbij een klant b.v. in een ERP-systeem een betaalbestand aanmaakt en deze via het interne netwerk en (later) via de internet bankieren omgeving als portal upload naar de bank.

De klant kan gebruik maken van hashing als hulpmiddel om ongeautoriseerde wijzigingen in dat betaalbestand tussen aanmaak en aankomst bij de bank te detecteren.

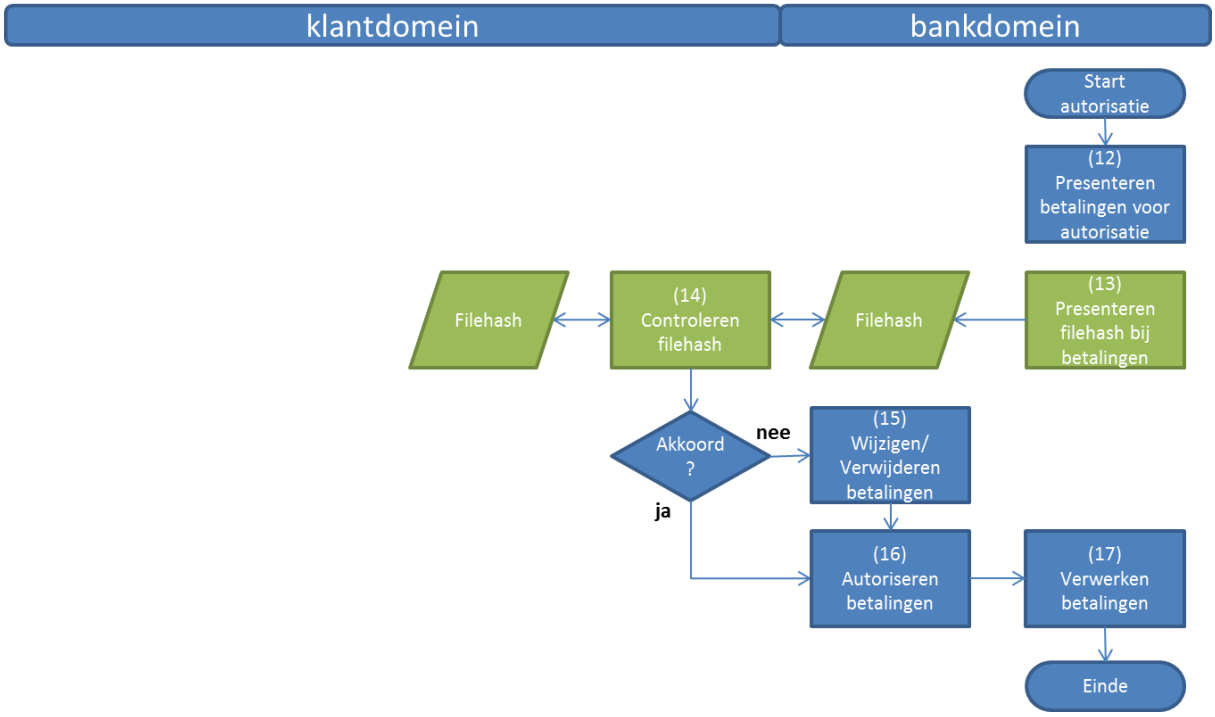


Figuur 1: Filehash controle bij upload betaalbestand naar bank

Een zakelijke klant (1) verwerkt inkoopfacturen in het ERP-systeem. Vanuit het ERP-systeem creëert de klant vervolgens een betaalbestand (2). Tijdens de creatie van dit bestand wordt door het ERP-systeem, over het hele bestand, een filehash berekend (3). Deze filehash wordt zodanig gearchiveerd (4) dat manipulatie van de filehash redelijkerwijze niet meer mogelijk is. Vervolgens upload de klant het betaalbestand via internet bankieren naar de bank (5).

Na ontvangst van het betaalbestand door de bank (6) berekent de bank de filehash (7) en presenteert deze aan de klant (8). Vervolgens vergelijkt de klant door de bank gegenereerde filehash met de eigen opgeslagen filehash (9). Zijn beide filehashes niet identiek, dan is het bestand mogelijk gewijzigd vanaf het moment van de bestandsgeneratie tot de ontvangst en de berekening van de filehash bij de bank. In dat geval kan de klant het bestand alsnog verwijderen (10) zonder deze verder te verwerken. Komen beide filehashes wel overeen dan autoriseert de klant het betaalbestand voor verdere verwerking (11).

Optioneel: sommige banken bieden als extra mogelijkheid dat de functionaris die bij de klant de betalingen autoriseert (nogmaals) de filehash te zien krijgt, of maakt de controle van de filehash onderdeel uit van het autorisatieproces. Het autorisatieproces kan er dan als volgt uit zien:



Figuur 2: Autorisatieproces na upload betaalbestand (inclusief filehash controle in groen)

Bij de start van de autorisatie presenteert de bank de betalingen die in de afgelopen periode zijn ingevoerd en/of aangeleverd (12). Daarbij kan de bank (nogmaals) de filehash presenteren (13) of de klant vragen ter controle een deel van de filehash in te voeren. Zo volgt een (laatste) controle of de door de bank berekende filehash niet afwijkt van de opgeslagen filehash (14) met de mogelijkheid om op het laatste moment nog betalingen te wijzigen of te verwijderen (15). Is alles oké dan autoriseert de klant vervolgens de correcte betalingen.

Tip: het upload- en autorisatieproces van betaalbestanden in het bankdomein biedt mogelijkheden om in de administratieve organisatie - b.v. via een autorisatieschema - de verantwoordelijkheden in het betaalproces (uitvoering en controle) te beleggen bij meerdere personen in de organisatie. Zie hoofdstuk 6 of informeer bij uw bank of accountant naar de mogelijkheden.

4.2 Proces bij inschakeling van derde partijen in klantdomein

In het betalingsverkeer kunnen verschillende schakels worden toegevoegd in het aanleverproces tussen de zakelijke klant en bank. Aangezien de zakelijke klant verantwoordelijk is voor de aanmaak en aanbieding van het betaalbestand bij de bank geldt dit ook voor de partijen die de zakelijke klant daarbij inschakelt. Deze partijen worden daarmee ook tot het klantdomein gerekend. Voorbeelden zijn:

- Salarisbureaus
- (On-line) Boekhoudpakketleveranciers
- ERP-leveranciers

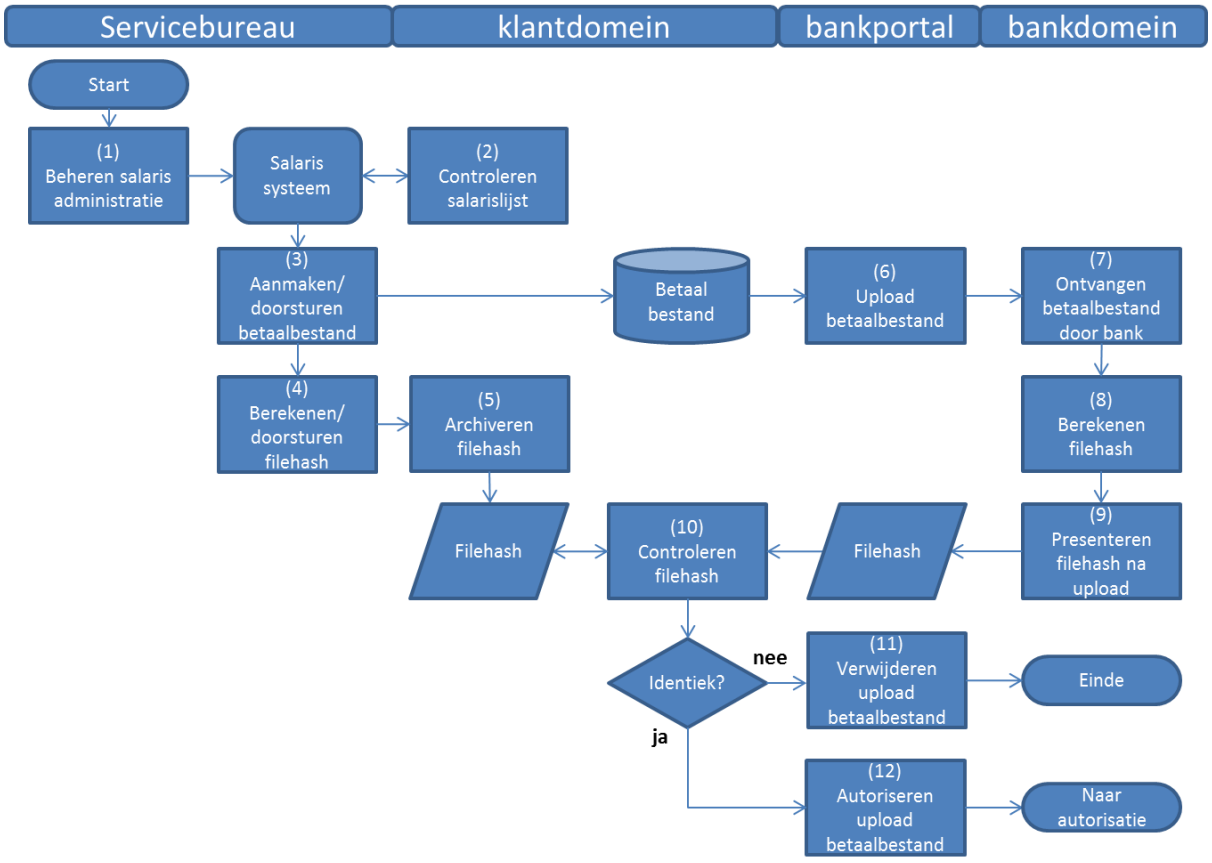
- Servicebureaus

Bij het inschakelen van derde partijen zijn er grofweg twee smaken:

- De derde partij kan het betaalbestand aanmaken waarna de klant het bestand zelf aanbiedt bij de bank of
- De derde partij kan het betaalbestand aanmaken, samenvoegen of aanvullen en namens de klant aanbieden bij de bank.

4.2.1 Derde partij levert betaalbestand aan; zakelijke klant stuurt door naar bank

In het onderstaande voorbeeld is sprake van een salarisbureau dat voor de zakelijke klant de salarisadministratie beheert. Het salarisbureau levert als extra service maandelijks een betaalbestand aan met alle salarisbetalingen. Hashing wordt in dit geval toegepast als hulpmiddel om te controleren of het betaalbestand dat door het salarisbureau wordt aangemaakt, ongewijzigd is gebleven vanaf de aanmaak door het salarisbureau t/m de upload naar de bank.



Figuur 3: Toepassing hashing in de aanleverketen

Een salarisbureau (1) verwerkt de salarisgegevens van de zakelijke klant in het salarissysteem. De zakelijke klant controleert daarbij via een salarislijst (2) of de salarissen correct in het systeem staan. Op een vast moment in de maand maakt het salarisbureau een betaalbestand met de salarisbetalingen aan (3) en stuurt deze b.v. via internet naar de zakelijke klant. Bij de aanmaak

berekent het salarisbureau tevens de filehash (4) en stuurt deze via een separaat kanaal zoals SMS naar de zakelijke klant. De zakelijke klant bewaart/archiveert de filehash voor de latere controle.

Als de datum voor de uitbetaling van de salarissen nadert, uploadt de klant het betaalbestand via internet bankieren naar de bank (6).

Verder is het proces van verwerking en autorisatie gelijk aan het proces bij aanlevering rechtstreeks van zakelijke klant naar bank (zie paragraaf 3.3.1)

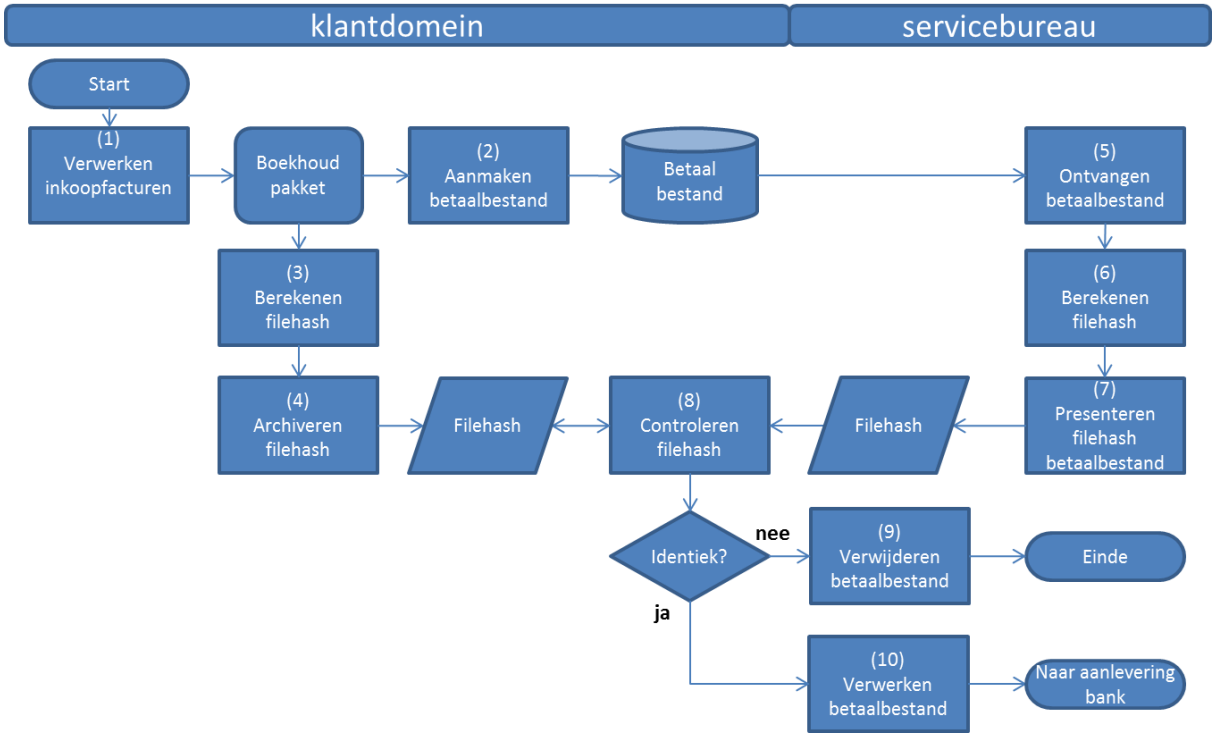
4.2.2 Derde partij levert namens de zakelijk klant het betaalbestand aan bij de bank

In het onderstaande voorbeeld is sprake van een zakelijke klant die betaalgegevens aanlevert bij een servicebureau, waarna het servicebureau het betaalbestand bewerkt en aanlevert bij de bank. Dit met als doel om verschillende betaalstromen zoals Incasso, Acceptgiro en crediteurenbetalingen bij elkaar te brengen en te reconciliëren.

Aangezien het bestand in de keten wijzigt wordt in dit geval een point-to-point filehash toegepast. Dat wil zeggen dat bij elke uitwisseling van gegevens tussen de schakels in de keten (points) een filehash wordt berekend en gecontroleerd. Zo kan steeds per schakel worden bekeken of hash-waardes niet afwijken om misbruik mogelijk te detecteren.

Aanlevering van de betaalgegevens bij het servicebureau

De zakelijke klant dient de betaalgegevens aan te leveren bij het servicebureau. Daarvoor is geen formaat voorgeschreven. Het kan dus een SEPA-XML bestand betreffen maar ook andere formaten zijn mogelijk. Uit hoofde van de integriteit van de betaalgegevens geldt ook hier de aanbeveling om gebruik te maken van filehashing om de integriteit te borgen. Zeker als de aanlevering aan het servicebureau via het internet loopt. In onderstaande figuur is deze initiële point-to-point aanlevering met gebruikmaking van een filehash in processtappen uitgewerkt.

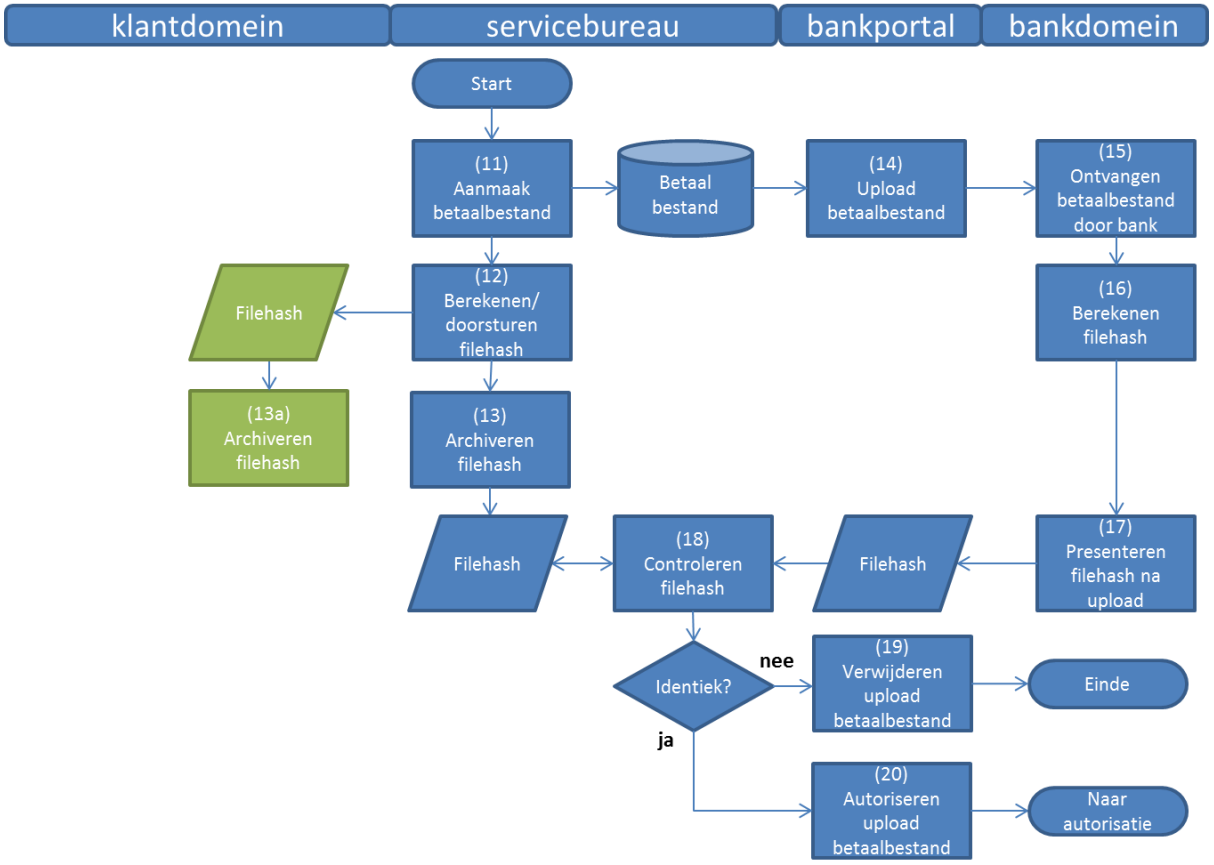


Figuur 4: Point-to-Point Filehash van klant naar servicebureau

De zakelijke klant verwerkt de inkoopfacturen in het eigen boekhoudpakket (1). Periodiek maakt de klant een betaalbestand aan met de betalingen aan leveranciers (2). Voordat het bestand naar het servicebureau wordt gestuurd, berekent de klant een filehash (3) over het betaalbestand en archiveert deze (4).

Bij ontvangst van het betaalbestand door het servicebureau (5) berekent het servicebureau de filehash over het ontvangen bestand (6) en presenteert deze op een afgesproken wijze aan de klant (7). Vervolgens vergelijkt de klant door het servicebureau gegenereerde filehash met de eigen opgeslagen filehash (8). Is de filehash niet identiek, dan is het bestand mogelijk gewijzigd vanaf het moment van de bestandsgeneratie tot de ontvangst bij het servicebureau en berekening van de filehash. Het is dan aan de klant om opdracht te geven het bestand te verwijderen (9) zonder deze verder te verwerken. Is de filehash wel identiek dan kan het servicebureau de betalingen verder verwerken (10).

Aanvullende verwerking door servicebureau en aanlevering van het betaalbestand bij de bank
De betaalgegevens bevinden zich nu bij het servicebureau. Hier worden de betaalgegevens conform de afgesproken services met de klant bewerkt/aangevuld en verzonden naar de bank (zie figuur 5). Het servicebureau moet dan door de zakelijke klant gemachtigd zijn om als derde partij betaalbestanden bij de bank aan te kunnen leveren. Dit is mogelijk maar dient uiteraard wel met de bank overeengekomen en ingeregeld te worden.



Figuur 5: Point-to-Point Filehash van servicebureau naar bank

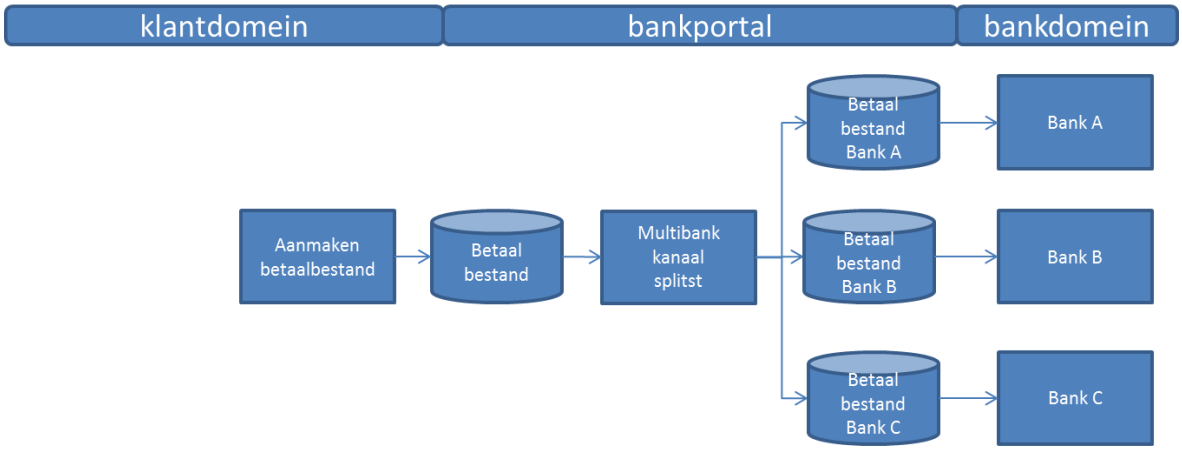
Het servicebureau ontvangt de betaalgegevens van de zakelijke klant. Het servicebureau bewerkt/verwerkt deze gegevens en maakt een betaalbestand aan (11). Over het betaalbestand berekent het servicebureau de filehash (12). En indien dat voor de latere autorisatie nodig is stuurt het servicebureau de filehash ook door naar de klant[1]. Vervolgens wordt de filehash gearchiveerd (13 en 13a).

Het servicebureau verzorgt nu namens de klant de upload naar de bank (14). De bank ontvangt het betaalbestand (15), berekent de filehash (16) en presenteert deze aan het servicebureau (17). Vervolgens vergelijkt het servicebureau de filehash van de bank met de eigen opgeslagen filehash (18). Is de filehash niet identiek, dan is het bestand mogelijk gewijzigd vanaf het moment van de bestandsgeneratie tot de upload bij de bank. Het is dan aan het servicebureau om in overleg met de klant het bestand te verwijderen (19). Is de filehash wel identiek dan kan het servicebureau de upload autoriseren (20).

[1] Ook hier geldt een risico dat een protentiële fraudeur zowel het betaalbestand als de filehash onderschept en aanpast. Deze optie kan dus alleen worden benut als de uitwisseling van de filehash op een afdoende beveiligde wijze plaatsvindt.

4.3 Multibank aanlevering

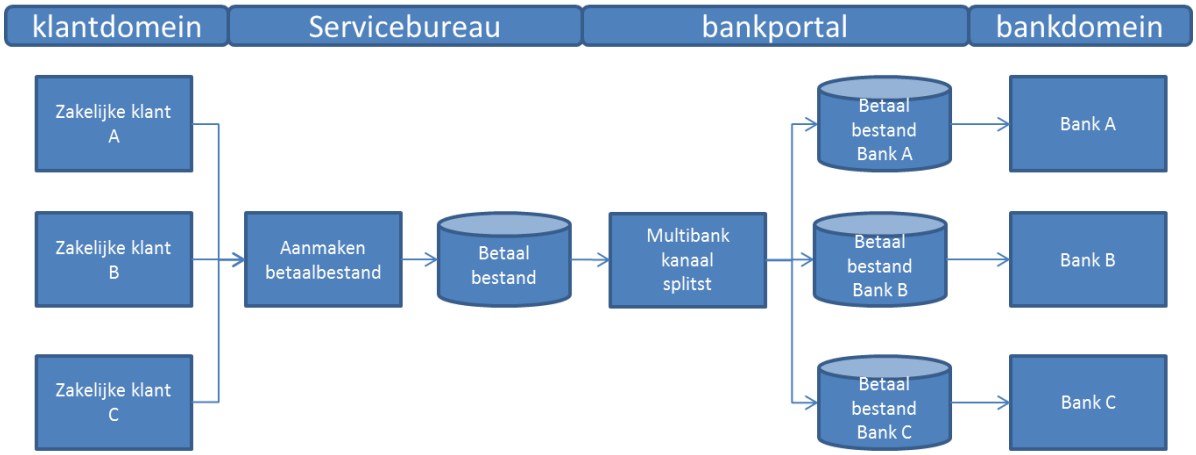
Zakelijke klanten kunnen bij meerdere banken bankieren. Dit heeft als consequentie dat deze ‘multibank’ klanten betaalbestanden bij meerdere individuele banken moeten kunnen aanleveren. Als alternatief kunnen banken de mogelijkheid bieden om de betaalbestanden bij één centraal loket aan te leveren. We noemen dit multibank aanlevering. De zakelijke klant dient hiervoor een overeenkomst met de betreffende banken te sluiten. Een voorbeeld van een dergelijke service is het multibank aanleverportal ‘Corporate Payment Services’ (van Equens).



Figuur 6: Multibank aanlevering, directe aanlevering zakelijke klant

In het bovenstaande figuur bankiert de zakelijke klant bij banken A, B en C. De klant levert één betaalbestand aan bij het Multibank aanleverportal. Daar wordt het bestand gesplitst in bestanden per bank en door/via de bank verder verwerkt.

Dit loket is ook te gebruiken door servicebureaus of salarisverwerkers die namens meerdere klanten én bij meerdere banken betaalbestanden willen aanleveren.



Figuur 7: Multibank aanlevering door/via servicebureau

In dat geval maak het servicebureau voor meerdere klanten (die bankieren bij meerdere banken) een betaalbestand aan. Het servicebureau levert dit bestand vervolgens aan bij de Multibank aanleverportal. Daar wordt het bestand gesplitst in bestanden per bank en door/via de bank verder verwerkt.

4.3.1 Multibank aanlevering en hashing

Zoals al aangegeven bij de aandachtspunten kan hashing in een betaalketen alleen succesvol worden toegepast als het betaalbestand ongewijzigd tussen meerdere partijen wordt uitgewisseld. Elke wijziging of toevoeging, hoe klein ook, zal leiden tot een andere uitkomst en doet het gebruik van de filehash als controle teniet.

Bij multibank aanlevering worden bestanden samengevoegd en later weer gesplitst. De controle van de filehash end-to-end door de keten is daarmee niet mogelijk. De filehash wordt daarom bij multibank aanlevering desgewenst uitsluitend berekend bij aanlevering bij het Multibank aanleverportal en later niet meer per individuele bank getoond en/of herrekend. Een berekende filehash door de bank zal immers per definitie afwijken van eerder berekende filehashes.

Het Multibank kanaal wordt door de bank aangewezen[2] als manier om betaalbestanden aan te leveren. Zoals gebruikelijk in de bancaire omgeving wordt in de verdere aanlevering en verwerking gebruik gemaakt van beveiligde kanalen en is hashing dus niet meer nodig.

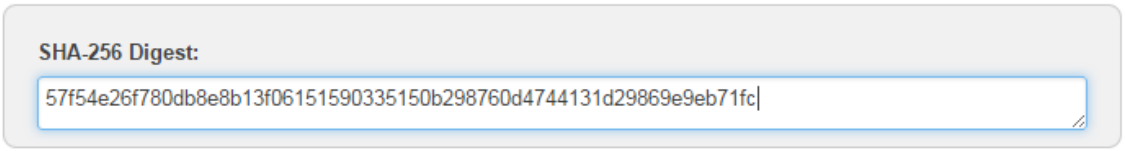
Gebruikers van een door de bank aangewezen multibank kanaal zijn in de regel professionele financiële dienstverleners die eveneens langs beveiligde verbindingen zullen aanleveren. In dergelijke gevallen is hashing dus ook niet nodig.

[2] Een zakelijke klant dient het gebruik van het multibank kanaal dus ook formeel met de eigen bank overeen te komen. Is dit niet het geval dan betreft het geen door de bank aangewezen kanaal.

5. Technische specificaties

Het te gebruiken filehash algoritme is SHA-256 (met streepje). Het toepassen van SHA-256 hashing gebeurt op file niveau, dat betekent dat elke karakter in de file (inclusief header, footer en non-printable markup) meetelt bij de berekening.

Het algoritme voor de SHA-256 berekening is generiek en platform onafhankelijk. Een hash berekening over hetzelfde bestand zal dus altijd - en op iedere plaats - dezelfde uitkomst geven. Tevens geldt dat een goed hash algoritme, zoals SHA-265, berekend over twee verschillende bestanden met een aan zekerheid grenzende waarschijnlijkheid een verschillende uitkomst geeft.



Figuur 8: Voorbeeld van een filehash in (in hex- format)

Zie voor een nadere toelichting op hashing en hash berekeningen de navolgende bronnen:

- Een formele beschrijving van de standaard is te vinden op de website van de National Institute of Standards and Technology (NIST).
  http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

6. Maatregelen interne controle

Hashing past in een set van maatregelen/hulpmiddelen die organisaties kunnen benutten bij de inrichting van de administratieve organisatie en de interne controle (AO/IC) rond het betalingsverkeer.

De twee meest voorkomende vormen van betalingen door bedrijven zijn crediteurenbetalingen en salarisbetalingen. In hoofdlijnen zijn hiervoor de volgende interne controlemaatregelen van belang:

Inkopen/crediteuren:

- Functiescheiding tussen inkoop/bestelling, goederenontvangst/ gereed melding dienst, factuurverwerking en feitelijke betaling
- Controle dat bestelling, goederenontvangst (indien van toepassing) en factuur overeenstemmen qua aantallen en bedragen (zogenaamde ‘three way match’) en procedures om eventuele verschillen uit te zoeken
- Adequaat beheer stamgegevens van crediteuren met controle op mutaties, met name inzake bankrekeningnummers
- Goedgekeurde facturen (voldaan aan three way match dan wel verschil geaccepteerd en geautoriseerd door bevoegd persoon) worden op basis van vervaldatum geselecteerd voor verzending aan bank. Bankrekeningnummer wordt opgehaald uit stambestand en kan niet rechtstreeks worden aangepast
- Het aldus gecreëerde betaalbestand wordt op een beveiligde locatie opgeslagen zodat deze niet door onbevoegden kan worden benaderd
- Het betaalbestand wordt geautoriseerd door daartoe aangewezen personen in de organisatie (bv financieel directeur), die ook bij de bank als zodanig bekend zijn. Deze actie kan zowel binnen het bedrijf plaatsvinden als door het autoriseren van het betaalbestand zoals dat na ontvangst door de bank voor verwerking is klaargezet.

Salarissen

- Functiescheiding tussen HR afdeling (in- en uitdiensttreding, arbeidsvoorwaarden), lijnverantwoordelijke/afdelingshoofd en salarisadministratie (uitbetaling)
- Adequaat beheer van het personeelsstambestand inclusief salarisbedragen en bankrekeningnummer
- Maandelijks genereert de salarisadministratie een betaalbestand op basis van de op dat moment geregistreerde in dienst zijnde personen, waarbij salarisgegevens en bankrekeningnummers uit het stambestand worden opgehaald
- Het aldus gecreëerde betaalbestand wordt op een beveiligde locatie opgeslagen zodat deze niet door onbevoegden kan worden benaderd
- Het betaalbestand wordt geautoriseerd door daartoe aangewezen personen in de organisatie (bv financieel directeur), die ook bij de bank als zodanig bekend zijn. Deze actie kan zowel binnen het bedrijf plaatsvinden als door het autoriseren van het betaalbestand zoals dat na ontvangst door de bank voor verwerking is klaargezet.

In sommige organisaties wordt het toegestaan om met eenmalige betalingen te werken zonder dat de gegevens van de begunstigde in het crediteurenstambestand worden verwerkt. Dergelijke posten dienen apart te worden gesignaleerd en gegevens te worden gecontroleerd.

U kunt uw accountant benaderen voor verdere adviezen over de inrichting van de Administratieve Organisatie/Interne Controle binnen uw organisatie. Voor informatie over beveiligde aanlevering, hashing en (functiescheiding bij) autorisatie van betalingen kunt u terecht bij uw bank.