Root Cause analyse "dubbele betaling"

08-09-2025

Incident ID	M2508 13474
Oorzaak:	Applicatie
Sub-oorzaak:	Implementatie fout i.c.m. menselijke fout
Root Cause:	In de applicatie is automatisch een vinkje "Payment run" aangezet.
Incident:	Tijdens het aanmaken van een paymentvoorstel is door de applicatie automatisch een vinkje aangezet. De instelling uit een vorige sessie wordt namelijk onthouden. De medewerker heeft dit niet opgemerkt. Vervolgens is er een Payment run aangemaakt waarbij het vinkje Create Payment Medium correct door de gebruiker is aangezet. Als gevolg hiervan worden twee niet identieke batches - ze hebben verschillende referenties maar wel met dezelfde inhoud - aangeboden aan Rabobank. Doordat de twee batches verschillen en daardoor niet door de controle voor dubbele batches worden afgevangen worden ze beiden door Rabobank verwerkt. Daarentegen is de boeking maar 1x in SAP verwerkt. Gemeente Amsterdam was niet op de hoogte van het risico van het aanzetten van het vinkje.

In de bijlage is een Excel opgenomen met 50 vragen/antwoorden over het incident en de achtergrond ervan. Daarnaast is aan het einde van dit document de analyse vanuit de Rabobank toegevoegd. In deze notitie schetsen we chronologisch hoe het incident heeft kunnen plaatsvinden.

Overigens: in SAP S4HANA blijkt het dubbel betaalbaarstellen een bekend en goed gedocumenteerd probleem te zijn. Dit was niet bij de gemeente bekend. Als een gebruiker per ongeluk nogmaals een payment medium genereert of de betaalrun dubbel uitvoert zonder de juiste blokkeringscontroles, kan dit leiden tot een dubbele betaling. Er zijn hiervoor SAP Notes beschikbaar op userapps.support.sap.com (o.a. ref 2526388, 2341907, 2768575, 3604413, 2863917, 3168196). Dit is een bekend risico van de basisinrichting van SAP S4HANA. Er zijn door Capgemini geen mitigerende maatregelen voorgesteld of genomen door bijv. het inzetten van een Payment Medium Workbench (PMW) controle om dubbele betalingen te kunnen voorkomen.

Functie vinkje

- Het vinkje bij de stap betaalvoorstel is een standaard SAP voorziening, die geen doel heeft voor gebruik in Amsterdam. Deze functie is tot op heden dan ook niet gebruikt.
- Indien het vinkje wordt geactiveerd wordt een extra betaalbestand aangemaakt onder een andere batchnaam en per direct naar Rabobank gezonden.

Ontwerp/implementatie AFIS en procesbeschrijving

- Gemeente Amsterdam heeft bewust het proces in twee stappen onderverdeeld: het maken van een betaalvoorstel (om eventueel nog in te grijpen in het proces, bijv. betalingen verwijderen) en vervolgens het genereren de betaalrun.
- In AFS was dit een systeeminstelling. In AFIS gebeurt het opstarten van het betaalvoorstel en de betaalrun nu nog handmatig, dit om in de eerste fase na livegang het proces goed te kunnen monitoren en steekproeven te kunnen doen. Dit conform het advies van AO/IC procescontrol Financiën en Inkoop. De bedoeling is dat dit proces wordt geautomatiseerd
- De werkwijze rondom het genereren van een betaalvoorstel en betaalrun is sinds de ontwerpsessies en totstandkoming van het FOD niet gewijzigd.
- Capgemini heeft de gemeente niet geïnformeerd over het risico dat met het zetten van een vinkje een dubbele betaalbatch wordt gegenereerd. Medewerkers geven aan dat als het geval was geweest, zij dit hadden geïdentificeerd als groot risico.
- Dubbele betaling van batches is niet als risico geïdentificeerd door gemeente Amsterdam en Capgemini. Er is wel gesproken over dubbele identieke betaalbatches en de controle die de Rabobank hierop doet. Capgemini heeft deelgenomen aan de risicosessies en heeft input geleverd. Dit risico staat ook niet in het RCA beschreven.
- In de AFS-werkwijze, was ook één programma voor het genereren van het voorstel en de definitieve run, maar was deze als twee verschillende versies opgenomen in het menu (in de AFIS termen twee tegels): een met de term voorstel (waar de parameter genereer betaalbestand uit stond), en een met de term definitieve run (waar de parameter genereer betaalbestand aan stond).
- De schermen voor het betaalvoorstel en de betaalrun zijn identiek, maar het bewuste vinkje dient alleen aangevinkt te worden bij de betaalrun. Dit wordt verwarrend genoemd.
- Ook onthoudt het scherm de gemaakte keuzes van de vorige sessie, dit wordt als niet wenselijk gezien.

Gebruikerstraining en werkinstructie

- In de werkinstructie gemaakt door team Betalen staat de omgang met de vinkjes beschreven.
- In het configuratiehandboek staat het vinkje benoemd, maar niet wat het doel is van deze functionaliteit.
- De werkwijze, die bij alle medewerkers goed bekend is, wordt als frustrerend ervaren maar is niet gemeld of geëscaleerd omdat het risico niet bekend was en dit dan een van de vele nuicances is. Men dacht “Zo werkt het systeem” en ”Dit is de standaard".

Incident

- Er is een wekelijks standaardcontrole met het hele betaalteam gedaan op dinsdag en de voorstellijst is toen verwijderd, hierbij is het vinkje aangeklikt of tevoorschijn gekomen. Het komt voor dat het vinkje opeens aan staat, dus de medewerkers zijn geattendeerd dat ze altijd moeten controleren of de vinkjes aan of uit staan.
- Tijdens het aanmaken van een paymentvoorstel op de woensdag erna is door de applicatie automatisch een vinkje aangezet (Applicatie fout). De instelling uit een vorige sessie wordt namelijk onthouden.
- De betreffende medewerker heeft niet gelet op het vinkje op het eerste scherm (want deze hoeft normaalgesproken niet geplaatst te worden) en heeft zo gemist dat het vinkje al aan stond (Menselijke fout).

Controle

- De procesbeschrijving moet nog worden geactualiseerd voor de stroom betalingen vanuit AFIS. Later in het ontwerpproces zijn er stappen geautomatiseerd en is de aanlevering van de bestanden technisch gewijzigd en dit is nog niet verwerkt in de procesbeschrijving. Met het automatiseren van de stappen, veranderen of verdwijnen er controles. De procesbeschrijving is wel actueel voor losse betalingen en de betalingen die langs AFIS gaan (Inkomen/Belastingen).
- Bij het uitdokteren van de API/PGP route in q2 2023 is de dubbele batch problematiek besproken. Er is door JWM (PO in AFIS en Adviseur betalingsverkeer) bij Rabobank indertijd geïnformeerd of zij dubbele batches konden afvangen. Dat is het geval en ook ingericht bij Rabobank. Op inhoud kan men niet checken omdat niet kan worden vastgesteld of het uitvoeren van dubbele betalingen per ongeluk is of met opzet. Let wel dit is een controle op IDENTIEKE batches. Ook bij inrichten met automatische autorisatie is dit nogmaals besproken met Rabobank in het kader van onze mogelijkheden om alsnog bestanden te kunnen intrekken.
- AFIS/SAP vanaf 1 jan 2025: In SAP is het niet mogelijk om een SHA256 te genereren. CBT heeft daardoor in beginsel niets om op te kunnen controleren. Door het betaalbestand encrypted (PGP) via een API te versturen is er geen transportrisico; (NB deze oplossing is in 2023 zeer intensief besproken in het AFIS-projectteam en de business en informatie-architecten van dienst, als oplossing voor het ontbreken van de hash) Omdat de betaalbestanden niet gecontroleerd kunnen (geen hash) én hoeven te worden op transportintegriteit voert CBT geen handmatige controles en autorisatie uit.

Bijlage: Root cause analyse dubbele betaling MH JWM 20250827.xlsx

Analyse Rabobank

Op 20 augustus jl. zijn twee betaalbatches van Gemeente Amsterdam verwerkt, met dezelfde posten en hetzelfde batchbedrag. Naar aanleiding van het verzoek van de gemeente Amsterdam, hierbij een reactie op de werkwijze.

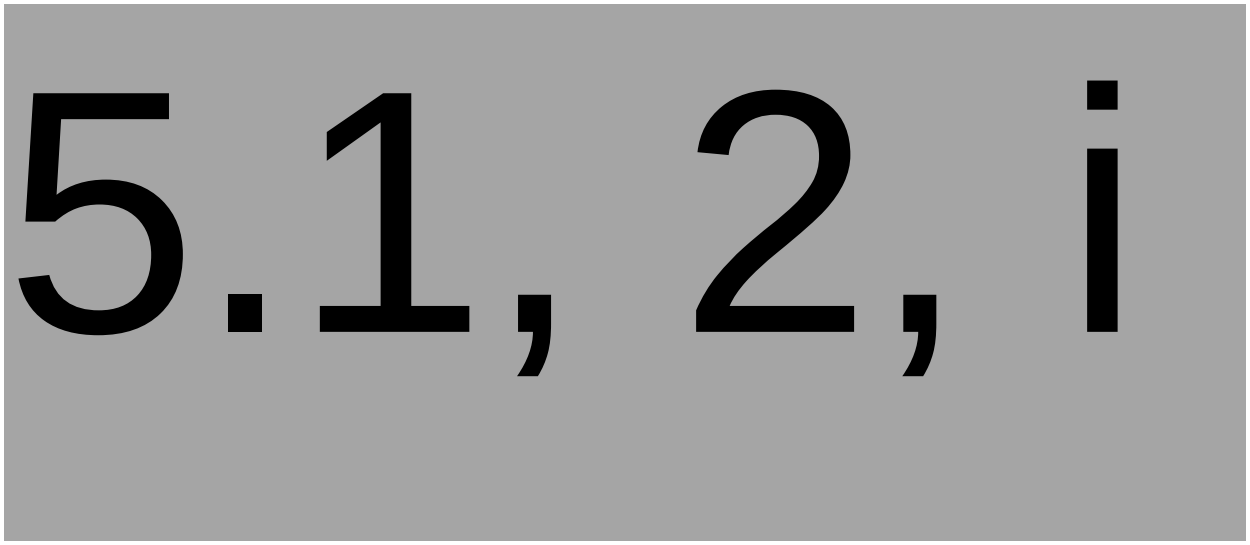
Gemeente Amsterdam maakt voor de betalingen vanuit AFIS (SAP) gebruik van de host-to-host verbinding van Rabobank, Rabo Direct Connect (RDC). Hierbij is de keuze door Gemeente Amsterdam gemaakt dat er geen (additionele) handtekening in Rabo Business Banking hoeft te worden gezet.

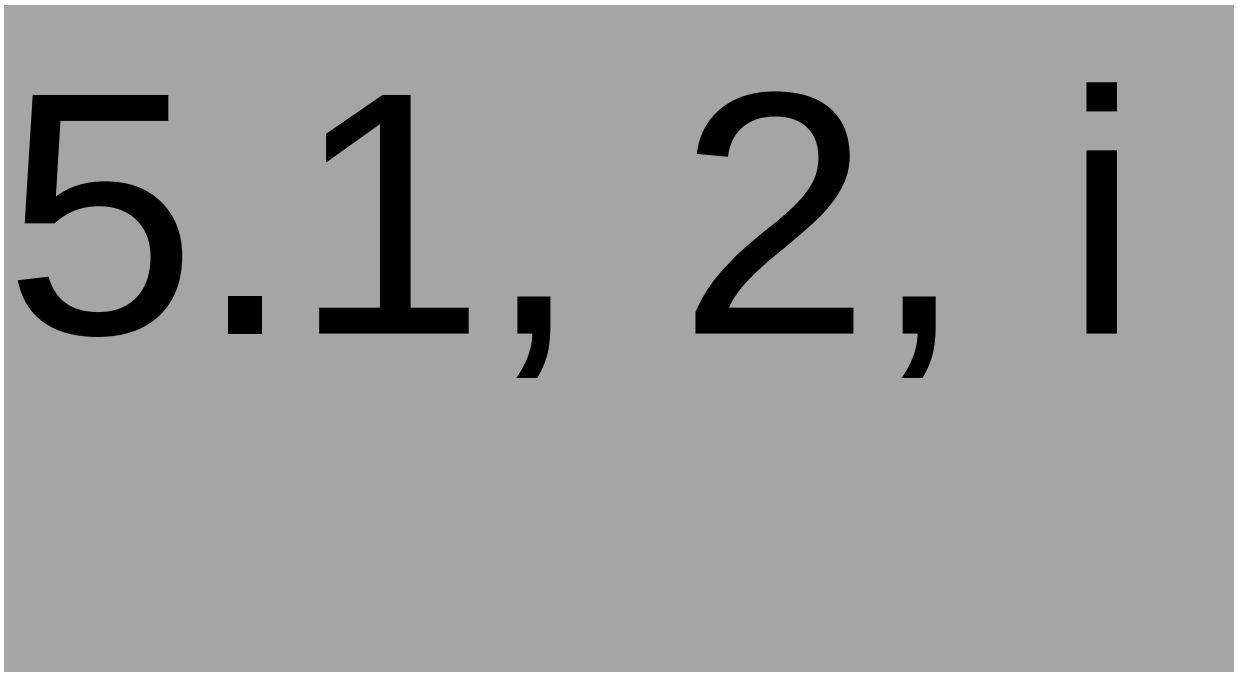
Goedkeuring van betalingen, dan wel bestanden gebeurt in AFIS. De in AFIS goedgekeurde batches worden vanuit een door de Gemeente Amsterdam beveiligde cloudomgeving naar RDC verzonden om te verwerken.

Na ontvangst door Rabobank vinden er verschillende controles plaats. Deze zijn terug te vinden in de Handleiding Rabo Direct Connect (Handleiding Rabop Direct Connect). Zoals in Hoofdstuk 6 'Wat kunt u verwachten indien er iets niet goed gaat?' staat aangegeven, wordt er gecontroleerd of hetzelfde bestand niet al eerder is aangeleverd, om te voorkomen dat een bestand per ongeluk tweemaal verwerkt wordt.

Indien er sprake is van een duplicaat dan wordt de batch afgekeurd. Deze informatie wordt daarnaast zo opgeslagen dat eenzelfde batch ook niet via een ander aanleverkanaal opnieuw aangeboden en verwerkt kan worden.

Om te beoordelen of er sprake is van een duplicaat worden batches door Rabobank gecontroleerd op de payload, in de vorm van MsgID en PmtInfID. Beide zijn verschillend in de aangeleverde bestanden die op 20 augustus jl. verwerkt zijn:





Bij aanlevering van bovengenoemde twee batches is er dus geen sprake geweest van een duplicaat bestand en zijn de batches conform instructie van Gemeente Amsterdam door Rabobank verwerkt.

Er zijn situaties waarin wel eenzelfde batch nogmaals aangeboden kan worden:

- Een batch welke bijvoorbeeld afgekeurd is vanwege onvoldoende saldo. In dat geval kan de batch nogmaals worden aangeboden met dezelfde kenmerken (PmtInfId/MsgID)
- Na 90 dagen worden bestanden normaliter opgeschoond door het systeem, dan zou je wel nogmaals hetzelfde PmtInfId/MsgID kunnen gebruiken. Een batch met uitvoerdatum te ver in het verleden wordt afgekeurd (meer dan 14 dagen).

Als een batch gedeeltelijk afgekeurd is, dan zullen de afgekeurde "losse" betalingen in een nieuwe batch (met nieuw PmtInfID/MsgID) opgenomen en aangeboden moeten worden, om deze alsnog te kunnen verwerken.