Verslag

Verkenning van methodieken voor veiligstellen chatberichten

Datum 7 december 2023

Versie: 0.9

Rijksprogramma
Duurzaam
Digitale
Informatiehuishouding

Versiebeheer

04-12-2023	Versie 0.9 t.b.v. MT RDDI
7-12-2023	Versie 0.9 t.b.v. Strategisch Beraad
x.x datum-maand-jaartal	Versie t.b.v. (gremium)
x.x datum-maand-jaartal	Versie t.b.v. (gremium)
x.x datum-maand-jaartal	Versie t.b.v. (gremium)
x.x datum-maand-jaartal	Versie t.b.v. (gremium)

Inhoudsopgave

Samenvatting

In 2023 is door RDDI en Doc-Direkt een marktverkenning uitgevoerd naar potentiële voorzieningen voor duurzaam toegankelijke chatberichten bij de (Rijks)overheid.

Tijdens de verkenning kregen diverse marktpartijen de kans om technische oplossingen te presenteren voor het veiligstellen, beheren en archiveren van chatberichten op uiteenlopende berichtenapps bij de Rijksoverheid.

Dit verslag biedt een overzicht van technische methodieken die in de marktconsultatie naar voren zijn gekomen voor het veiligstellen van chatberichten.

Technische methodieken voor veiligstellen van chatberichten:

	'Afvangen'	*'Routeren'*	*'Ophalen'*	*'Vastleggen'*
Werkwijze	Automatisch	Automatisch	Automatisch	Automatisch
Omschrijving	Capture/vastleggen via externe instantie van berichtenapp (Chat-Client)	Vastleggen/Doorsturen via back-up van mobiel (Chat-App / mobiel)	Ophalen bij de bron van berichtenapp (Chat-Interface)	Vastleggen in de bron van chatapplicatie (Chat-Applicatie)
Scope veiligstellen	- Alleen Signal of Whatsapp chatberichten - Deels terugwerkende kracht & Toekomstige berichten	- Alleen Signal of Whatsapp chatberichten - Toekomstige berichten	- Alleen Whatsapp chatberichten - Toekomstige berichten	- Chatberichten van uiteenlopende berichtenapps - Toekomstige berichten
Installatie	Chat-Client met software die chat- berichten uitleest en doorstuurt	Chat-App software die chatberichten uit back-up mobiel vastlegt en doorstuurt	Middleware die via interface chat-berichten ophaalt bij Chat-Platform en doorstuurt	Installatie van Multi-channel chat-app die alle chatberichten centraal opslaat
Look/Feel	Identieke look en feel voor gebruiker (wel accorderen archiveren – QR code)	Zo goed als identieke look en feel voor gebruiker	Bijna identieke look en feel voor gebruiker	Andere look en feel voor gebruiker
Disclaimer	Geen automatische privacy-/archivering disclaimer	Automatische privacy-/archivering disclaimer	Automatische privacy-/archivering disclaimer	Automatische privacy-/archivering disclaimer
Functies	- Chatten 1 op 1 - Groep-chat - Bijlagen - Video/Voice	- Chat 1 op 1 - Groep-chat - Bijlagen - Video/Voice	- Chatten 1 op 1 - Bijlagen	- Chatten 1 op 1 - Groep-chat vanuit chat-applicatie - Bijlagen - Voice

1 Inleiding

In opdracht van het Programma Open Overheid en onder begeleiding van de Rijksinkoop-samenwerking (RIS) is in 2023 door RDDI en Doc-Direkt een marktverkenning uitgevoerd naar potentiële voorzieningen voor het duurzaam toegankelijk maken van chatberichten bij de (Rijks)overheid.

De marktconsultatie bood diverse marktpartijen de gelegenheid om een toelichting te geven op de technische oplossingen (voorzieningen) die zij aanbieden voor het veiligstellen, in beheer krijgen en archiveren van chatberichten op uiteenlopende berichtenapps bij de Rijksoverheid.

In dit verslag volgt een overzicht van de (technische) methodieken die in de marktconsultatie naar voren zijn gekomen voor het veiligstellen van chatberichten. Het doel is om de hierbij opgedane informatie/ervaringen breed te delen en daarmee de keuzes voor technische voorzieningen en de implementatie van chat-archiveringbeleid te vergemakkelijken.

DISCLAIMER:

Dit verslag beschrijft de kennis en ervaringen, die zijn opgedaan tijdens de marktconsultatie. Er zijn zo min mogelijk product -en leverancier specifieke gegevens opgenomen vanwege potentiële concurrentie gevoeligheid. Ook is de mate van informatieverschaffing vanuit de leveranciers over oplossingen niet geheel evenredig en (nog) niet getoetst in de praktijk. Er is bewuster gekozen om de onderliggende (technische) methodieken van de leveranciers en bijbehorende oplossingen voor veiligstelling zo objectief mogelijk te beschrijven.

2 Aanleiding

De huidige werkwijze bij de (Rijks)overheid, waarbij chatberichten handmatig van telefoons worden gearchiveerd, is omslachtig, gebruikersonvriendelijk, heeft een lange doorlooptijd, levert niet de gewenste kwaliteit, voldoet niet aan alle (juridische) kaders en vraagt overmatige inzet van Rijksambtenaren en informatiebeheerders.

De (Rijks)overheid wenst de archivering efficiënter en effectiever in te richten door inzet van één of meerdere (technische) voorzieningen die het mogelijk maken om de chatberichten op uiteenlopende berichtenapps meer geautomatiseerd, gebruiksvriendelijk en kwalitatief hoogwaardig veilig te stellen, in beheer te krijgen en vervolgens duurzaam toegankelijk te maken.

De technische voorziening moet ervoor zorgen dat chatberichten (of een selectie daarvan) binnen de ICT infrastructuur en het applicatielandschap van de (Rijks)overheid wordt veiliggesteld, beheerd en bewaard conform (juridische) kaders en ontsloten voor informatieverzoeken.

3 Context

Het archiveren van chatberichten is nog niet ingericht conform wet- en regelgeving, zo heeft de Inspectie Overheidsinformatie en Erfgoed[1] (Inspectie) geconcludeerd in 2022. Aansluitend adviseerde het Adviescollege Openbaarheid en Informatiehuishouding[2] (ACOI) begin 2023 om alle chatberichten van de politieke en ambtelijke top in beheer te nemen en te bewaren. De Algemene Rijksarchivaris (ARA) staat achter deze adviezen en doet een oproep om hierop door te pakken.[3]

Het kabinet onderstreept de conclusies en aanbevelingen van de Inspectie, ACOI en ARA. Alle zakelijke appjes en sms'jes van sleutelfuncties (bewindslieden en hoge ambtenaren) moeten bewaard blijven. Het kabinet vindt het cruciaal dat de huidige situatie op het gebied van het beheren en openbaar maken van informatie aanzienlijk en zo snel mogelijk wordt verbeterd.

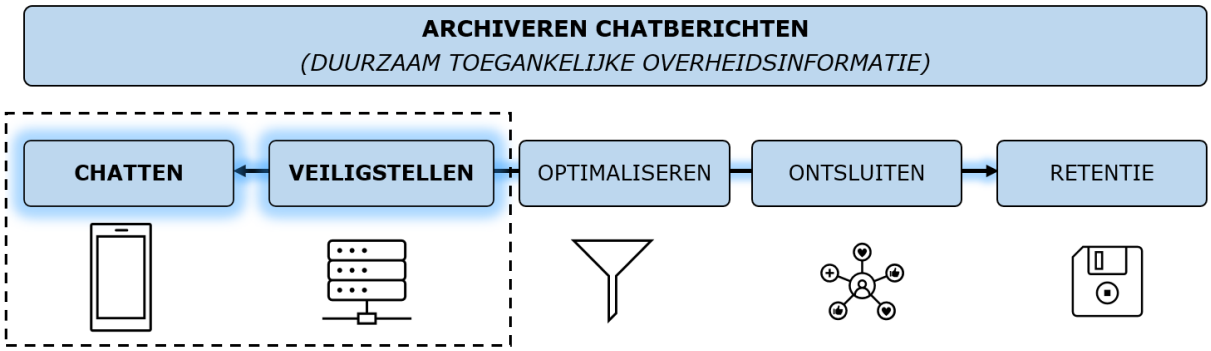
In haar reactie spreekt het kabinet de ambitie uit om aan de slag gaan met het beter op orde krijgen van de overheidsinformatie.[4] Daarbij is ook de maatregel benoemt om praktisch onderzoek te doen naar technische voorzieningen waarmee de archivering van chatberichten bij het Rijk in de toekomst wordt verbeterd.

[1] Inspectie van Overheidsinformatie en Erfgoed (IOE) – De archivering van chatberichten bij het ministerie van Algemene Zaken, link
[2] Adviescollege voor Openbaarheid en Informatiehuishouding (ACOI) – Advies over het beheren en bewaren van chatberichten bij de overheid, link
[3] De Algemene Rijksarchivaris (ARA) – Reactie algemene rijksarchivaris op ACOI-advies chatberichten, link
[4] Kamerbrief reactie op adviesrapporten chatberichtenarchivering en informatiebeheer, link.

4 Afbakening

Het veiligstellen, in beheer nemen en archiveren van chatberichten op uiteenlopende berichtenapps is redelijk onontgonnen terrein binnen de (Rijks)overheid. Wat het precies inhoudt en hoe dit het beste kan plaatsvinden is nog volop in ontwikkeling. Zowel bij professionals binnen de Rijksoverheid als bij de producten van leveranciers in de markt.

Waar wel consensus over bestaat is dat chatberichtarchivering een proces is dat bestaat uit meerdere opeenvolgende informatiebeheer stappen. In de marktverkenning zijn daarbij de volgende processtappen geïdentificeerd.



Toelichting op de stappen chatberichtarchivering:

I. **Chatten**: Het creëren van chatberichten(verkeer) waarbij de gebruiker ondersteund wordt door een voorziening die in staat is informatie te versturen en ontvangen via chatfunctionaliteit.
II. **Veiligstellen**: Het in beheer brengen van zakelijke chatberichten middels een functionaliteit die de informatie uit chatberichten (inclusief bijlagen en relevante metadata) veiligstelt met als uiteindelijke doel de archivering van de desbetreffende chatberichten.
III. **Optimaliseren**: Het bewerken/verrijken van de veiliggestelde chatberichten met als doel de overheidsinformatie daaruit duurzaam toegankelijk te maken.
IV. **Ontsluiten**: Het ontsluiten en gebruiken van gearchiveerde informatie uit chatberichten voor uiteenlopende doeleinden en processen, in het bijzonder informatieverzoeken.
V. **Retentie**: Het veilig en conform wet- en regelgeving vernietigen, bewaren en overbrengen van de chatberichten.

In dit verslag ligt de focus op technische methodieken die leveranciers (en hun producten) bieden voor de eerste twee stappen, te noemen: het creëren -en veiligstellen van chatberichten.

5 Doelgroep

Dit verslag is primair bedoeld voor i-professionals bij (Rijks)overheidsorganisaties:

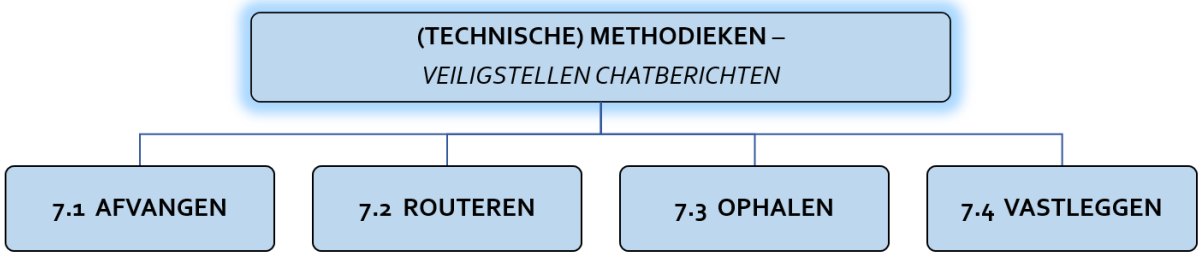
- Die verantwoordelijk zijn voor (strategisch) advies en beleidsvorming rondom chatberichtenarchivering.
- Die de opdracht uitvoeren voor ontwerp en implementatie van (voorzieningen voor) chatarchivering.
- Die verantwoordelijk zijn voor het management of de coördinatie van de informatie in werkprocessen en de bijbehorende informatiesystemen.

Het doel is om deze groepen te voorzien van waardevolle inzichten met betrekking tot de beschikbare (technische) methodieken op het gebied van het in beheer krijgen en veiligstellen van chatberichten voor archivering.

6 Methodieken

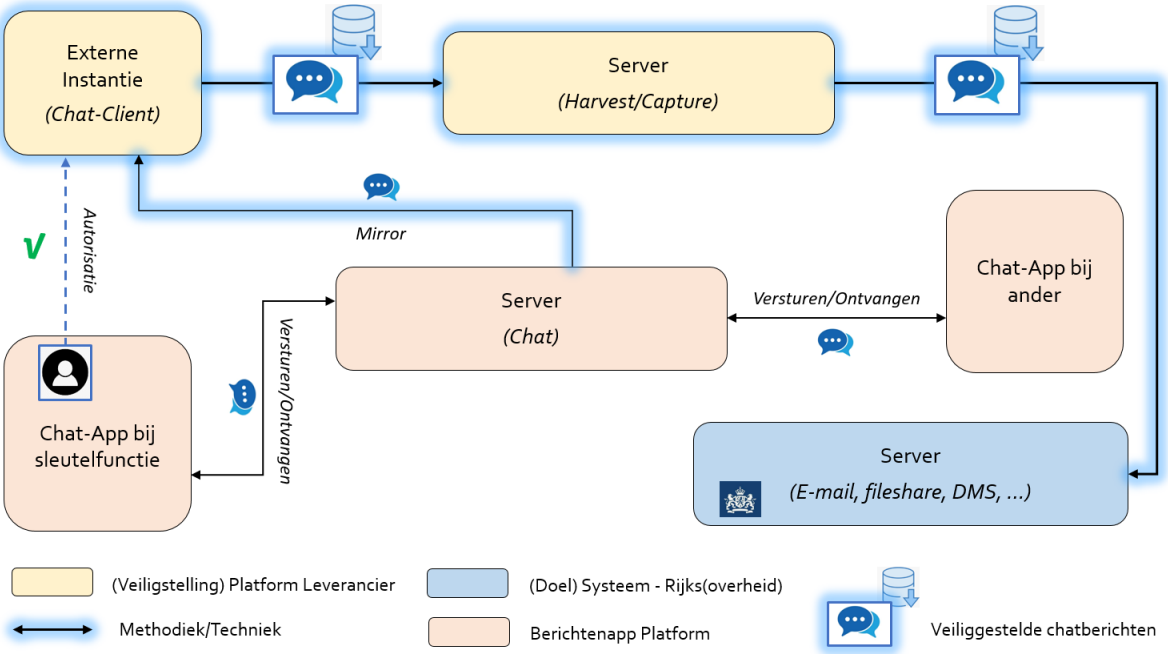
Dit hoofdstuk beschrijft de (technische) methodieken voor het veiligstellen van chatberichten op uiteenlopende berichtenapp platformen teneinde deze te kunnen archiveren. Hiermee kunnen (Rijks)overheidsorganisaties een zorgvuldige afweging maken wat geschikte strategieën zijn voor het veiligstellen en duurzaam toegankelijk maken van deze informatiestroom.

Binnen de marktconsultatie zijn de volgende vier verschillende methodieken te onderscheiden die de leveranciers in hun producten toepassen bij het (technisch) veiligstellen van chatberichten.



6.1 Afvangen

De eerste methode, 'afvangen', bestaat uit het activeren van een externe (client) instantie voor een specifiek berichtenapp platform die parallel loopt aan de mobiele chat-app. Met behulp van (harvesting/capture) software worden alle chatberichten van een gebruiker via deze instantie uitgelezen, vastgelegd en vervolgens doorgestuurd naar het gewenste doelsysteem.



Voor inzicht in hoe deze methodiek werkt volgt hieronder een beschrijving van de functionele kenmerken die in de marktconsultatie naar voren zijn gekomen.

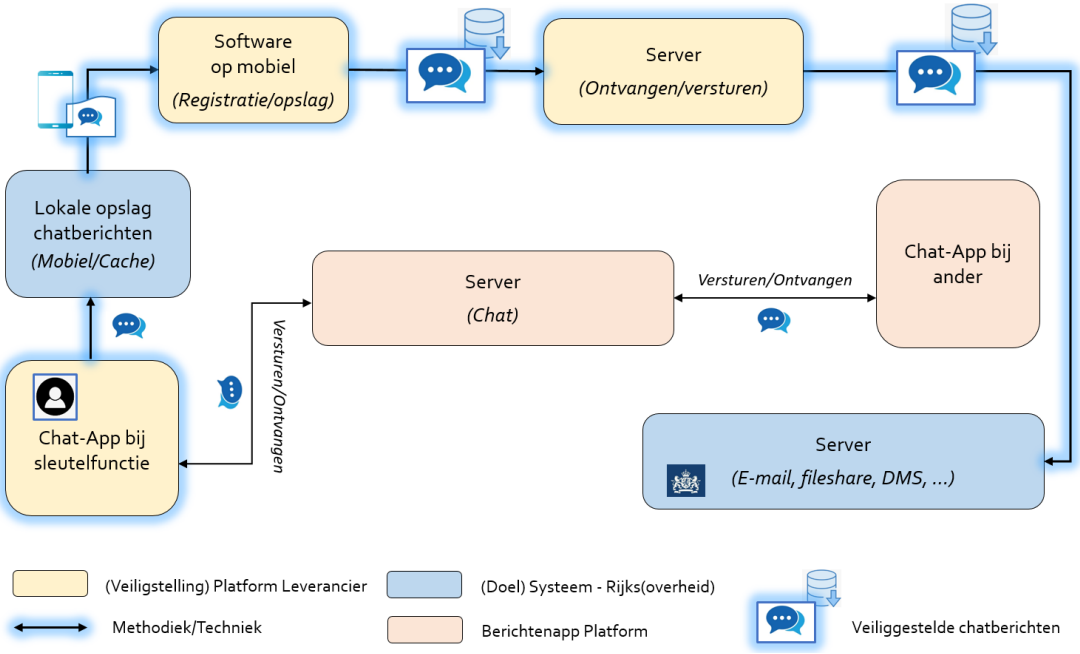
- **Veiligstellen**: De chatberichten van gebruikers worden softwarematig veiliggesteld via (web/desktop-client) instanties die gespiegeld zijn aan de mobiele chatapplicaties om vervolgens te worden doorgestuurd naar een doelsysteem voor nadere archiveringstappen.
- **Content:** De technische methode is in staat om tekst, emoji/GIFs, foto's, video's, tekstberichten als bijlage, audioberichten en links veilig te stellen.
- **Gebruik:** De gebruikers gebruiken de vertrouwde (native/oorspronkelijke) chatapplicatie zonder verschil in de gebruikerservaring. Voorafgaand aan het veiligstellen dient de gebruiker een volmacht af te geven (bijvoorbeeld via email) en de technische oplossing te activeren (bijvoorbeeld via een web-portaal middels een QR-code).
- **Periode:** De chatberichten worden real-time of binnen specifieke intervallen veiliggesteld afhankelijk van de behoeften. Het veiligstellen wordt beïnvloed door factoren als netwerksnelheid en dataomvang. Verder is het mogelijk om chatberichten een beperkte periode terug in de tijd veilig te stellen.
- **Disclaimer:** Het is niet mogelijk om geautomatiseerd een (privacy)disclaimer mee te sturen waarin wordt gewezen op de veiligstelling van de chatconversatie.
- **Gebruiker beheer:** Het toevoegen van gebruikers gaat via een centraal beheerportaal. Verder zullen volmacht-aanvragen moeten worden onderzocht waarvoor geen volmacht is afgeven door gebruikers (en archivering dus niet plaatsvindt). Ook kan de connectie wegvallen tussen de instantie en het chatplatform waarin veiligstelling plaatsvindt. De gebruiker moet dan geïnstrueerd worden om de oplossing opnieuw te activeren.
- **Applicatie beheer:** Monitoring van de connectie tussen de externe instantie en het platform of wegvallen van de verbinding via een centraal beheerportaal. Eventueel is er aanvullende controle op volledigheid en herstelacties benodigd.

Voor inzicht in de technische achtergrond van de methodiek volgt hieronder een beschrijving van de technische kenmerken die in de marktconsultatie naar voren zijn gekomen.

- **Software:** De techniek maakt gebruik van harvesting en capture software die de gespiegelde chatconversatie op de web- of desktop client binnenhaalt en vastlegt. Veiliggestelde berichten worden vervolgens doorgestuurd naar een doelsysteem (bijvoorbeeld via een SMTP format).
- **Chatapplicaties**: De techniek is toepasbaar op het veiligstellen van chatberichten op verschillende berichtenapp platformen. In de markconsultatie zijn WhatsApp en Signal als use-cases naar voren gekomen.
- **Systeemeisen:** De methode is geschikt voor zowel iOS als Android.
- **Technisch beheer**: De harvesting/capture software dient te worden geüpdatet wanneer (veelal onaangekondigd) wijzigingen worden doorgevoerd door het desbetreffende berichtenapp platformen aan de chat-client.
- **Integratie:** De techniek kan worden aangesloten op bestaande componenten binnen de architectuur van de organisatie. Deze omvatten o.a. het Power Platform, email en het centrale DMS/archiefsysteem van de organisatie.
- **Infrastructuur:** De registratie van chatberichten omvat het hosten van een (Web/Desktop) instantie op een server. Deze instantie draait parallel aan de conversatie op het apparaat van de gebruiker. De oplossingen uit de markt worden standaard als SaaS (cloud-gebaseerd) aangeboden maar kunnen ook on-premise worden gerealiseerd.

6.2 Routeren

De tweede methode, 'routeren', bestaat uit het installeren van chat-app ('wrapper') software op de mobiele telefoon van de gebruiker. De chat-app software registreert de inkomende en uitgaande chatberichten lokaal en maakt daarbij gebruik van een opslaglocatie (cache) op de mobiele telefoon. Vervolgens worden de geregistreerde chatberichten uit de opslaglocatie (periodiek) via een externe router doorgestuurd naar het doelsysteem.



Voor inzicht in de werkwijze van deze methodiek volgt hieronder een beschrijving van de functionele kenmerken die in de marktconsultatie naar voren zijn gekomen.

- **Veiligstellen:** De chatberichten worden door de chat-app ('wrapper') lokaal geregistreerd op de mobiele telefoon van de gebruiker en vervolgens periodiek doorgestuurd naar een extern doelsysteem van de organisatie voor nadere archiveringstappen.
- **Content:** De technische methode is in staat om tekst, emoji/GIFs, foto's, video's, tekstberichten als bijlage, audioberichten en links veilig te stellen.
- **Gebruik:** De gebruikers krijgen, veelal als vervanging, een nieuwe chatapplicatie op de mobiele telefoon die qua look en feel hetzelfde is als de gangbare chat-/berichtenapps. De gebruiker ontvangt een activeringscode. Zodra deze is ingevoerd begint de technische methodiek met het vastleggen van alle chatberichtenverkeer.
- **Periode:** Het veiligstellen van actuele chatberichten gebeurt 'near realtime' en kan geconfigureerd worden in segmenten van bijvoorbeeld 24 uur of semi-continu. Het is niet mogelijk om berichtenverkeer dat eerder is uitgewisseld met het specifieke chat-/berichtenapp platform veilig te stellen.
- **Disclaimer:** De methodiek is in staat om geautomatiseerd een (privacy-) disclaimer mee te sturen waarin wordt gewezen op de veiligstelling van de chatconversatie.
- **Gebruiker beheer:** Het toevoegen van gebruikers gaat via een centraal beheerportaal. Verder zullen activering-aanvragen moeten worden onderzocht die niet door gebruikers worden opgevolgd (en archivering dus niet plaatsvindt).

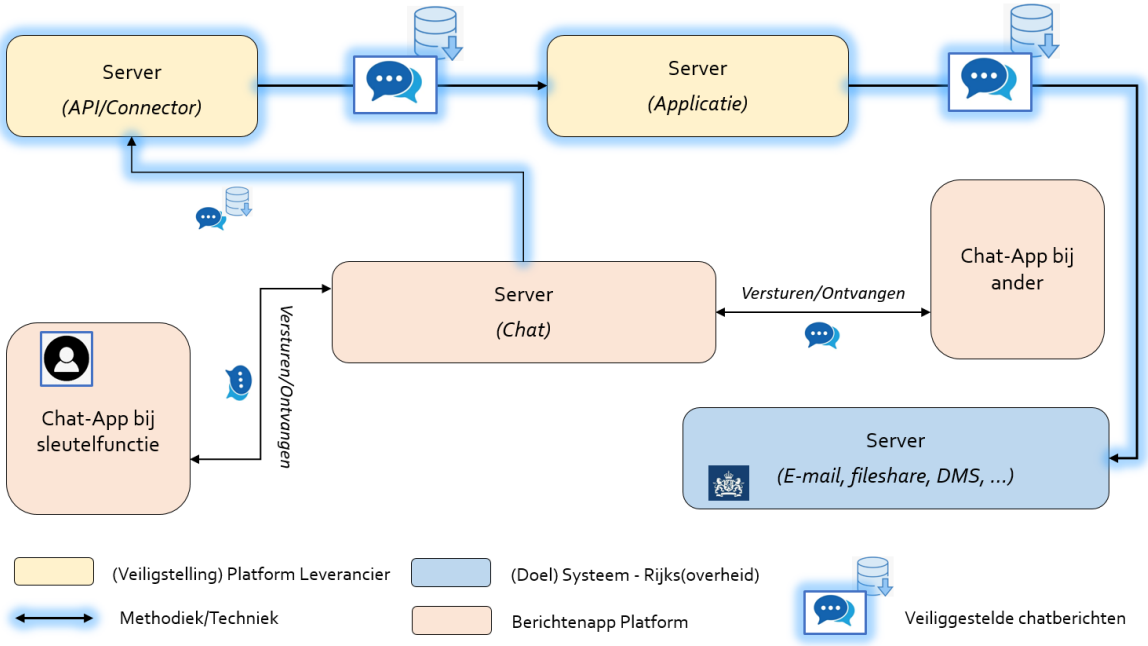
- **Applicatie beheer:** Het monitoren van updates voor het (mobiele) besturingssysteem of wijzigingen op het chat-/ berichtenapp platform om vervolgens te beoordelen of deze impact hebben op de werking van de technische methodiek. Eventueel dient de chat-app software ('wrapper') daarop te worden aangepast en zijn controles op volledigheid van de veiliggestelde chatberichten noodzakelijk.

Voor inzicht in de technische achtergronden van de methodiek volgt hieronder een beschrijving van de belangrijkste technische kenmerken.

- **Software:** De techniek maakt gebruik van een chat-app software die op de mobiele telefoon wordt geïnstalleerd voor lokale vastlegging van de chatberichten. De berichten worden vervolgens middels een datarouter doorgestuurd naar het doelsysteem.
- **Chatapplicaties**: De techniek is toepasbaar op het veiligstellen van chatberichten op verschillende berichtenapp platformen. In de markconsultatie zijn WhatsApp, Telegram en Signal als use-cases naar voren gekomen.
- **Exportmethode**: De vastgelegde chatberichten worden via het SMTP-protocol geëxporteerd. Deze bevatten zowel tekst als eventuele bijlagen.
- **Systeemeisen:** De methodiek vereist ondersteunde mobiele apparaten met iOS of Android.
- **Technisch beheer**: De software op de mobiel dient (eventueel) te worden geüpdatet bij updates van het besturingssysteem of updates van berichtenapp platformen.
- **Integratie:** De oplossing kan worden aangesloten op bestaande componenten binnen de architectuur van de organisatie. Deze omvatten o.a. e-mail en het centrale DMS/archiefsysteem van de organisatie.
- **Infrastructuur:** De veiligstelling van chatberichten omvat het installeren van (chat-app) software op mobiele telefoon en het gebruik van een datarouter. De oplossingen uit de marktverkenning waren SaaS (cloud-gebaseerd), wat betekent dat het beheer en de hosting volledig worden afgehandeld door de leverancier.

6.3 Ophalen

De derde methode, 'ophalen', bestaat uit het activeren/installeren van een interface-koppeling die (continu) het berichtenverkeer uit de bron van het berichtenapp platform ophaalt en deze doorgeeft aan een (proces)applicatie, waar de chatberichten worden opgeslagen, geëxporteerd of doorgestuurd naar het gewenste doelsysteem.



Voor inzicht in hoe deze methodiek werkt volgt hieronder een beschrijving van de functionele kenmerken die in de marktconsultatie naar voren zijn gekomen.

- **Veiligstellen:** De chatberichten van een gebruiker worden rechtstreeks opgehaald uit het chat-berichtenapp platform, doorgestuurd naar een gekoppeld processysteem en vervolgens periodiek geëxporteerd of doorgestuurd naar het doelsysteem.
- **Content:** De technische methode is in staat om tekst, emoji/ GIFs en links veilig te stellen. Of dit ook mogelijk is voor foto's, video's, tekstberichten als bijlage en audioberichten moet nader worden onderzocht.
- **Gebruik:** In de marktverkenning is deze methodiek alleen voor het berichtenapp platform WhatsApp for Business naar voren gekomen. De gebruikers krijgen een specifieke "Business" versie van de WhatsApp chatapplicatie op de mobiele telefoon die qua look en feel hetzelfde is als de gangbare consumentenversie van WhatsApp, alleen dan zonder functionaliteiten zoals groepsconversaties en videochat. De mogelijkheden om een dergelijke methodiek toe te passen op Signal heeft potentie vanwege het 'Open Source' karakter maar is niet door leverancier oplossingen aangedragen.
- **Periode:** Het veiligstellen van actuele chatberichten gebeurt 'realtime'. Het is niet mogelijk om berichtenverkeer veilig te stellen dat eerder is uitgewisseld via een specifiek chat-/berichtenapp platform.
- **Disclaimer:** De methodiek is in staat om geautomatiseerd een (privacy-) disclaimer mee te sturen waarin wordt gewezen op de veiligstelling van de chatconversatie.

- **Gebruiker beheer:** Deze methodiek kan alleen worden gebruikt na goedkeuring door Meta (het moederbedrijf van WhatsApp). In de marktverkenning is door leveranciers aangegeven dat dit proces voor de centrale overheid problematisch kan zijn en zij achten daarom de haalbaarheid van deze methodiek klein.
- **Applicatie beheer:** De gebruikersabonnementen en het goedkeuringsproces verloopt voor Whatsapp via speciaal door META geselecteerde vendors.

Voor inzicht in de technische achtergronden van de methodiek volgt hieronder een beschrijving van de belangrijkste technische kenmerken.

- **Software:** Deze methodiek betreft een API techniek die organisaties kan integreren in hun eigen (nog te ontwikkelen) softwaretoepassingen en infrastructuur via specifieke – door META aangewezen - vendors.
- **Chatapplicaties**: De techniek is toepasbaar op het veiligstellen van chatberichten op het chat-berichtenplatform WhatsApp. Voor Signal dient dit nader te worden onderzocht.
- **Exportmethode**: De vastgelegde chatberichten worden via het SMTP-protocol geëxporteerd. Deze bevatten zowel tekst als eventuele bijlagen.
- **Infrastructuur:** Voor deze methodiek moeten organisaties een server implementeren om te communiceren met de WhatsApp-servers via API-calls. Aanvullend vereist het integratie met processystemen, databases en doelsysteem om gesprekshistorie te beheren
- **Verificatieproces:** Voordat een organisatie WhatsApp Business API kan gebruiken moet er een verificatieproces worden doorlopen waarbij goedkeuring moet worden gegeven door META om het te mogen gebruiken.

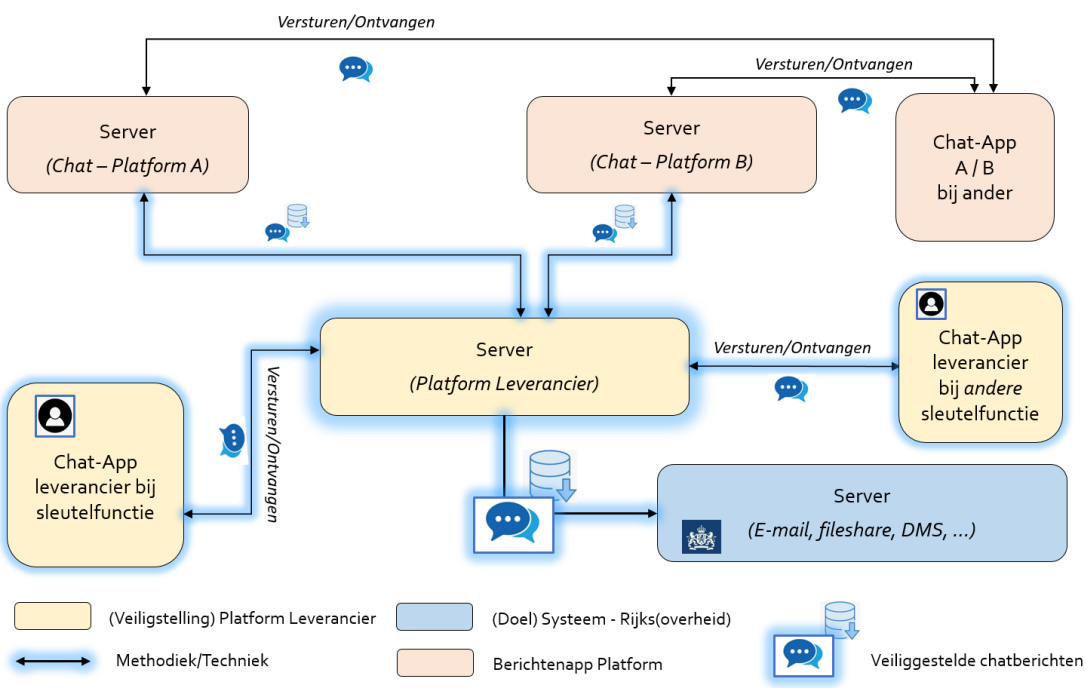
6.4 Vastleggen

De vierde methode, 'vastleggen', consolideert de chat-app op de mobiele telefoon, het chatberichtenverkeer en de veiligstelling van chatberichten van gebruikers binnen één integrale applicatie.

Deze methodiek bestaat uit het installeren, gebruiken en in beheer nemen van één chatplatform, inclusief bijbehorende chat-app op de mobiele telefoon van de gebruikers. In de marktconsultatie zijn twee configuraties naar voren gekomen:

A. Multi-Channel

Een multi-channel chatplatform waarbij één chat-app op de mobiele telefoon van gebruikers wordt geïnstalleerd. Via deze chat-app kunnen gebruikers onderling communiceren én met gebruikers van andere veelgebruikte berichtenapp platformen. Alle chatberichten worden (automatisch) binnen het chat-platform veiliggesteld, opgeslagen, geëxporteerd en/of doorgestuurd naar het gewenste doelsysteem.



Voor inzicht in hoe deze methodiek werkt volgt hieronder een beschrijving van de functionele kenmerken die in de marktconsultatie naar voren zijn gekomen.

- **Veiligstellen:** De veiligstelling van al het inkomende en uitgaande berichtenverkeer van gebruikers vindt centraal en automatisch plaats binnen de chatapplicatie.
- **Gebruik:** Via één chat-app op de mobiele telefoon kunnen de gebruikers zowel onderling chatten en documenten/media uitwisselen als met gebruikers van de meest gangbare berichtenapps in de markt. De chat-app is qua look en feel vergelijkbaar met de meest gangbare chat-/berichtenapps.
- **Content:** Alle inhoud van chatberichten, multimedia en metadata worden vastgelegd en veiliggesteld.
- **Disclaimer:** Bij chatconversaties is eenvoudig een automatische disclaimer mee te sturen die contacten informeert over het privacy- en archiveringsbeleid van de organisatie.

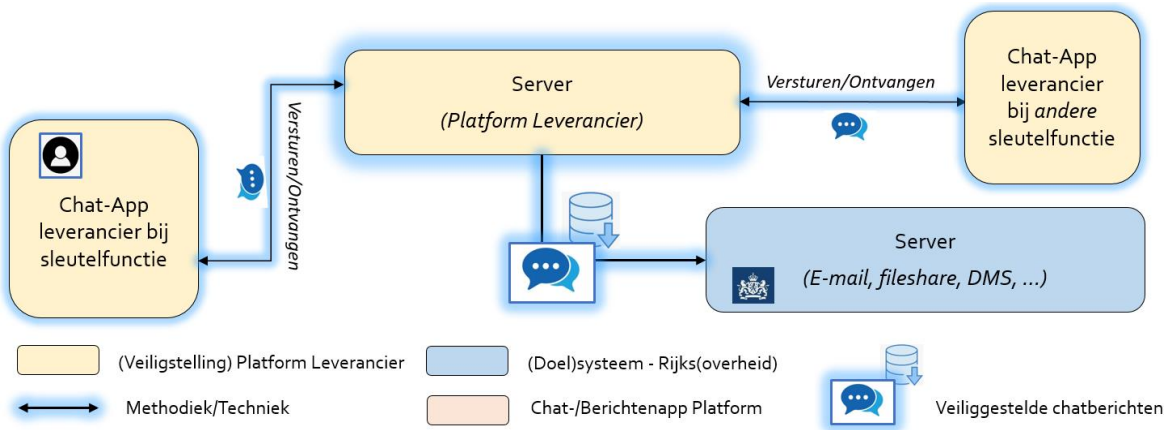
- **Periode:** Het veiligstellen van actuele chatberichten gebeurt 'realtime' en start op moment van ingebruikname.
- **Gebruiker beheer:** De chat-app is gekoppeld aan een telefoonnummer en 'en vervangt andere chatapplicaties op de mobiele telefoons. Beheerders kunnen gebruikersrechten en toegang beheren.
- **Applicatiebeheer:** Binnen de voorziening kunnen regelgeving en compliance-normen worden ingeregeld en geautomatiseerd.
- **Berichtenbeheer:** De gebruikers en beheerders kunnen berichten en conversaties beheren middels de applicatie of de portal, waaronder labelen, doorzoeken en archiveren.
- **Rapportage:** De multi-channel methodiek biedt rapportagetools waarmee inzicht kan worden verkregen in het chatverkeer binnen het platform.

Voor inzicht in de technische achtergronden van de methodiek volgt hieronder een beschrijving van de belangrijkste technische kenmerken.

- **Software:** De methodiek bestaat naast het activeren of installeren van het chatplatform (SaaS of private cloud) uit de lokale installatie van een chat-app op de mobiele telefoons.
- **Interoperabiliteit:** Gebruikers kunnen via de chat-app op de mobiele telefoon vanuit één interface zowel onderling als van-/naar de meest gangbare commerciële chatplatformen communiceren via encrypted chatberichten. De berichten worden automatisch gesynchroniseerd met het (interne) chatplatform en niet lokaal opgeslagen op het mobiel.
- **Chatapplicaties:** De techniek stelt het berichtenverkeer veilig binnen de chat-applicatie als ook het berichtenverkeer dat wordt uitgewisseld met andere berichtenapp platformen. In de markconsultatie zijn WhatsApp, Telegram en Signal als use-cases naar voren gekomen als berichtenplatformen waarmee gebruikers kunnen communiceren.
- **Integratie:** De chatapplicatie ondersteunt single-sign-on, mobile device management en active directory integratie.
- **Systeemeisen:** De chat-app is geschikt voor zowel iOS als Android.
- **API en SDK:** De techniek maakt gebruikt van de officiële API's of SDK's van uiteenlopende berichtenapp platformen om deze (externe) chatberichten vast te leggen.
- **Infrastructuur:** De chatapplicatie draait volledig op Microsoft Azure infrastructuur en kan zowel SaaS als lokaal in een Private Cloud worden geïmplementeerd.

B. Single-Channel

Een single-channel chatapplicatie waarbij één chat-app beschikbaar komt op de mobiele telefoon van gebruikers. Deze chattoepassing is specifiek voor gebruik tussen gebruikers die op het platform zijn aangesloten, waarbij alle chatberichten automatisch binnen het chat-platform worden veiliggesteld, opgeslagen en eventueel geëxporteerd en/of doorgestuurd naar het gewenste doelsysteem.



Voor inzicht in hoe deze methodiek werkt volgt hieronder een beschrijving van de functionele kenmerken die in de marktconsultatie naar voren zijn gekomen.

- **Veiligstellen:** De veiligstelling van al het inkomende en uitgaande berichtenverkeer van gebruikers vindt centraal en automatisch plaats binnen de chatapplicatie. Via een koppeling kunnen de berichten worden uitgewisseld met een specifiek doelsysteem van de organisatie
- **Gebruik:** De gebruikers krijgen een chat-app op de mobiele telefoon beschikbaar voor interne uitwisseling van chatberichten. De look, feel en het gebruik is anders dan de gangbare (‘externe’) berichtenapps.
- **Content:** De technische methode stelt geautomatiseerd tekst, emoticons/GIFs, foto’s, video’s, tekstberichten als bijlage, audioberichten en links veilig.
- **Disclaimer:** Bij chatconversaties is eenvoudig een automatische disclaimer mee te sturen die contacten informeert over het privacy- en archiveringsbeleid van de organisatie.
- **Periode:** Het veiligstellen van actuele chatberichten gebeurt ‘realtime’ en start op moment van ingebruikname.
- **Gebruikers beheer:** De chatapplicatie is niet gekoppeld aan een telefoonnummer. Bij de technische oplossing uit de marktverkenning ontvangt een gebruiker een activeringscode. Zodra deze is ingevoerd start een chatconversatie en begint de technische methodiek met het vastleggen van alle chatberichtenverkeer.
- **Uitnodigingslink:** De gebruikers gaan chatconversaties aan op basis van een link die de na initiatie door de verzender wordt gestuurd naar de ontvanger.

Voor inzicht in de technische achtergrond van de methodiek volgt hieronder een beschrijving van de belangrijkste technische kenmerken.

- **Software:** De techniek die in de marktconsultatie naar voren is gekomen betreft een chatapplicatie die voor gebruikers lijkt op een app maar werkt via een web-based toepassing. Het installatie van een chat-app op de mobiele telefoon is dan ook niet nodig.

- **Infrastructuur:** De techniek van chat-applicatie uit de marktconsultatie kan volledig worden ingericht op de infrastructuur van de organisatie en vereist een standaard Windows server en Oracle database.
- **Applicatiebeheer:** Het applicatie -en technisch beheer worden uitgevoerd door de leverancier. Bij start worden zaken zoals de huisstijl eenmalig ingericht.
- **Schaalbaar:** de oplossing is schaalbaar en kent in principe geen beperkingen qua gebruikers.
- **Compatibiliteit:** De techniek is web-based en is daardoor makkelijk te integreren met standaard gangbare smartphones, tablets, (pc) browsers.

Colofon

Programma	RDDI
Projectnaam	Voorziening Chat archivering
Versienummer	0.9
Projectleider	Arjan Rompelman
Projectadviseur	Bram Claessens en Wouter IJzerman
Projectsecretaris	Yoëlle Bal T +31 6 46849084 w.a.j.rompelman@minocw.nl Rijnstraat 50 | Den Haag Postbus 16375 | 2500 BJ Den Haag
Auteurs	B. Claessens W.A.J Rompelman W.T IJzerman