Data Protection Impact Assessment rapport template v0.1

* Naam van het systeem: ID Contact
* Details: XXXX
* Auteurs: XXXX, XXXX
* Datum: 7/4/2021

# Introductie

De AVG verplicht in sommige gevallen om een DPIA uit te voeren. Zie hiervoor de volgende criteria: <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668>. In het geval van ID contact is het niet verplicht, maar wel aangeraden.

De structuur van dit rapport is sterk gebaseerd op de DPIA op IRMA: <https://privacybydesign.foundation/pdf/DPIA-IRMA-dec-2018.pdf>

# Beschrijving van het systeem

ID Contact is een systeem om geauthenticeerde communicatie op te zetten tussen gebruikers en een organisatie. ID Contact maakt het voor de organisatie mogelijk om de identiteit en andere gegevens van personen waarmee gecommuniceerd wordt, met grote zekerheid vast te stellen. ID Contact combineert hiertoe integraties met authenticatiemethoden met integraties met communicatiemethoden. Zo kan met ID Contact een met IRMA vastgestelde identiteit gekoppeld worden aan een chatgesprek, of aan een telefoongesprek. Op die manier kunnen organisaties op afstand meer processen doorlopen met gebruikers. ID Contact bestaat uit een systeem van een kern ('core'), en een configuratie van authenticatie- en communicatieplugins. Authenticatieplugins vormen de laag tussen een authenticatieplatform zoals IRMA en ID Contact, en communicatieplugins vormen de laag tussen een communicatieplatform zoals Amazon connect en ID Contact. De kern voorziet het syteem van informatie over welke processen er zijn, welke gegevens er benodigd zijn om de processen te doorlopen, welke authenticatiemethoden beschikbaar zijn, en per proces welke communicatiemethoden gebruikt kunnen worden. Alle gegevens die de core beschikbaar maakt, zijn configureerbaar door de organisatie. Elk van de onderdelen biedt een eigen gebruikersinterface aan om het doorlopen van authenticatie dan wel communicatie te faciliteren. De onderdelen zijn opgezet als microservices: losse servers die slechts een kleine verzameling verantwoordelijkheden hebben en die via een op HTTP gebaseerd protocol met elkaar communiceren.

## Aard van verwerking

ID Contact is erop gericht om de persoonsgegevens slechts gedurende de gebruikerssessie op te slaan en slechts die gegevens van de gebruiker te vragen die noodzakelijk zijn om het doorlopen proces te voltooien. Welke gegevens dit zijn verschilt per proces en is door de organisatie te configureren. Daarbij wordt gebruikers toestemming gevraagd om persoonsgegevens te delen met de organisatie, alvorens deze worden doorgegeven.

## Doel van verwerking

Het doel van het systeem is om ervoor te zorgen dat de te versturen gegevens tot het minimum worden beperkt om de diensten te kunnen verlenen, terwijl de organisatie erop kan vertrouwen dat de verstrekte gegevens gevalideerd zijn.

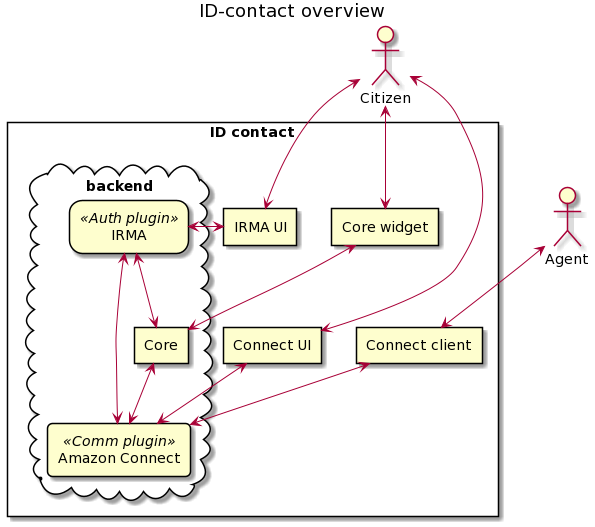
## Omvang van verwerking

De omvang is beperkt tot het doorgeven van de gegevens van de gebruiker aan de organisatie. Hierbij worden de gegevens slechts gedurende de sessie in ID Contact zelf opgeslagen. Er worden slechts die gegevens aan de organisatie doorgegeven, die noodzakelijk geacht worden om een proces te doorlopen. Welke gegevens precies verwerkt worden, is afhankelijk van de configuratie van het systeem door de organisatie.

## Context van verwerking

De context van gegevensverwerking is per organisatie die van ID Contact specifiek

# Visuele beschrijving



*Overzicht van een ID Contact-configuratie met daarin een IRMA-authenticatieplugin, een Amazon Connect-communicatieplugin, de kern en alle bijbehorende gebruikersinterfaces.*

# Vragenlijst

* Q: Worden er persoonsgegevens verwerkt door ID contact? Zo ja, welke?  
  A: Ja. Persoonsgegevens die de gemeente nodig heeft om een inwoner te identificeren voor het proces dat doorlopen moet worden.
* Q: Worden er persoonsgegevens opgeslagen door ID contact? Zo ja, welke?  
  A: Deze worden enkel voor de duur van het contact opgeslagen om getoond te kunnen worden aan medewerkers van de organisatie.
* Q: Wie is de verwerker? Oftewel, wie stelt het doel van en de middelen voor de verwerking van persoonsgegevens vast?  
  A: De organisatie die gebruikmaakt van ID Contact.
* Q: Wat zijn andere actoren betrokken in het ID contact systeem?   
  A: Burger, medewerkers van de organisatie en softwareleveranciers van authenticatie- en communicatieplugins en de kern. Hiernaast de leverancier die de hosting van ID Contact op zich neemt.
* Q: Wat zijn de betrokkenen? Oftewel, over wie gaan de gegevens?   
  A: De gebruiker die bij de organisatie een met ID Contact gefaciliteerd proces wil doorlopen.
* Q: Wat is de juridische grond voor het verwerken?   
  A: De intentie van een gebruiker om contact op te nemen met zijn/haar vraag impliceert toestemming voor kortdurende verwerking ten behoeve van het identificeren en authenticeren van de burger.
* Q: Wat is het doel van de verwerking?   
  A: Het identificeren en authenticeren van de burger zodat door de organisatie gedefinieerde processen doorlopen kunnen worden.
* Q: Hoe is er rekening gehouden met "data protection by design"?   
  A: Persoonsgegevens worden tijdens transport te allen tijde versleuteld verstuurd. Daarnaast worden persoonsgegevens slechts tijdens de communicatiesessie versleuteld opgeslagen, om zo snel mogelijk weer verwijderd te worden.
* Q: Verwerkt de verwerker slechts de noodzakelijke gegevens voor het einddoel?   
  A: De organisatie definieert per proces van een burger wat de minimale set van persoonsgegevens betreft. Bijvoorbeeld, alleen het adres voor het aanvragen van een nieuwe kliko, of alleen het BSN voor het aanvragen van een paspoort. Dit is dus per organisatie verschillend.
* Q: Hoe wordt nauwkeurigheid/integriteit van de persoonsgegevens bewaakt?   
  A: Persoonsgegevens worden tijdens transport te allen tijde ondertekend verstuurd over beveiligde verbindingen. *TODO: in fase 2 verder uitwerken*
* Q: Hoe lang worden persoonsgegevens verwerkt?   
  A: Voor de duur van de sessie (duur van het contact).
* Q: Hoe worden betrokkenen geïnformeerd over de verwerking?   
  A: Voor verwerking worden de te delen persoonsgegevens aan de gebruiker getoond, waarbij om toestemming gevraagd wordt om de gegevens te delen.
* Q: Hoe worden de rechten van de betrokkene gerespecteerd?   
  A: Rectificatie is niet van toepassing, aangezien data slechts voor de duur van het contact wordt verwerkt. Inzage en toegang van gegevens zijn verwerkt in het protocol. Indien de gemeente kiest voor het bijhouden van contact geschiedenis, dan is de gemeente hier verantwoordelijk voor.

# Risicoanalyse

Dit rapport focust op security risico's: verlies van vertrouwelijkheid, verlies van integriteit, verlies van beschikbaarheid en identificeerbaarheid/relateerbaarheid.

## Verlies van vertrouwelijkheid

Onder vertrouwelijkheid wordt verstaan dat gegevens niet gedeeld worden met ongeauthenticeerde entiteiten en dus slechts voor geauthenticeerde entiteiten beschikbaar zijn.

## Dreigingen

1. Een kwaadwillende luistert het internet verkeer van een gebruiker af.
2. Een kwaadwillende luistert het internet verkeer van een helpdeskmedewerker af.
3. Een kwaadwillende luistert het internet verkeer van de authenticatie plugin-server af.
4. Een aanvaller krijgt toegang tot de servers van ID Contact.
5. Een organisatie vraagt om meer gegevens dan noodzakelijk.

#### Maatregelen

1. Er wordt te allen tijde gebruik gemaakt van een TLS-verbinding met de sterkste encryptiestandaarden.
2. Alleen de hoogst noodzakelijke data wordt verstuurd.
3. Een gebruiker krijgt de te versturen gegevens eerst te zien voordat deze verzonden worden en moet expliciet toestemming verlenen om de gegevens te delen.
4. Verstuurde persoonsgegevens worden slechts voor de duur van de communicatiesessie in ID Contact opgeslagen.

#### Kwetsbaarheden

*TODO te beschrijven in fase 2*

#### Plan

*TODO te beschrijven in fase 2*

## Verlies van integriteit

Onder integriteit wordt verstaan dat gegevens tijdens het versturen niet onopgemerkt veranderd kunnen worden en dus betrouwbaar is.

#### Dreigingen

1. Een kwaadwillende weet het internetverkeer van een gebruiker aan te passen.
2. Een kwaadwillende weet het internetverkeer, en zo de te versturen gegevens, van een authenticatie plugin-server aan te passen.
3. Een kwaadwillende weet het internetverkeer van een helpdeskmedewerker van de organisatie aan te passen.

#### Maatregelen

1. Gegevens worden te allen tijde cryptografisch ondertekend verstuurd.
2. Er wordt te allen tijde gebruik gemaakt van een TLS-verbinding.

#### Kwetsbaarheden

*TODO te beschrijven in fase 2*

#### Plan

*TODO te beschrijven in fase 2*

## Verlies van beschikbaarheid

Onder beschikbaarheid wordt verstaan dat de gegevens te allen tijde toegankelijk zijn voor geauthenticeerde partijen, oftewel dat het systeem naar behoren functioneert.

#### Dreigingen

1. Een server van ID contact is onbereikbaar door een (D)DOS aanval.
2. Een server van ID contact is onbereikbaar door een storing (zonder kwaadwillende in het spel).
3. Een authenticatie-service is onbereikbaar.
4. Een communicatie-service is onbereikbaar.

### Maatregelen

1. Er worden meerdere authenticatie-plugins beschikbaar gesteld, zodat in het geval van een storing een andere optie gebruikt zou kunnen worden. Bijvoorbeeld IRMA wanneer DigiD onbereikbaar is.
2. *TODO te beschrijven in fase 2*

### Kwetsbaarheden

1. Indien de benodigde gegevens voor een bepaald type communicatie slechts bij een enkele authenticatie-service beschikbaar zijn, vormt dit een SPOF.
2. Indien een organisatie slechts via een enkele communicatiemethode beschikbaar is, vormt dit een SPOF.

#### Plan

*TODO te beschrijven in fase 2*

## Identificatie van de gebruiker/relateerbaarheid

*TODO te beschrijven in fase 2*

#### Dreigingen

*TODO te beschrijven in fase 2*

#### Maatregelen

*TODO te beschrijven in fase 2*

#### Kwetsbaarheden

*TODO te beschrijven in fase 2*

#### Plan

*TODO te beschrijven in fase 2*