Veilig bellen

Implementatie opties

xxxxx, 9-12-2019
xxxxx, 12-12-2019
Versie 0.2

Het doel van 'veilig bellen' is het vaststellen van de identiteit van de beller, op een zekerder manier dan te vragen naar bijvoorbeeld naam en geboortedatum. In de hier besproken oplossingen realiseren we een betere authenticatie door gebruik te maken van IRMA.

Voorafgaand aan een telefoongesprek onthult een beller een of meer IRMA attributen. De gebelde ziet de waarde van die attributen bij het overgaan van de telefoon. Dat kan op verschillende manieren gerealiseerd worden, de verschillende opties zijn hieronder verder uitgewerkt.

A: Meesturen van een DTFM code

In deze oplossing genereert een backend server vooraf aan het vrijgeven van de attributen een DTMF-code bestaande uit 8 cijfers. De backend server maakt daarna de sessie op de IRMA server aan. Bij deze sessie wordt gespecificeerd naar welk telefoonnummer en met welke DTMF-code de IRMA app moet bellen. De backend server slaat de koppeling tussen de 8-cijferige DTMF-code en het IRMA sessie-id in een database op. De vrijgegeven attributen worden, zoals altijd, tijdelijk opgeslagen op de IRMA server.

Na het vrijgeven start de IRMA applicatie op de smartphone van de gebruiker de bel-applicatie op de smartphone van de gebruiker. Het te bellen telefoonnummer wordt meegegeven aan de bel-applicatie, samen met de 8 cijferige DTMF-code.

Bij het bellen, nadat de telefooncentrale heeft opgenomen, wordt de DTMF-code automatisch 'ingetoetst' door de bel-applicatie op de smartphone, in een tijdsbestek van ongeveer 5 seconden. De gebruiker kan deze tonen horen, en moet even wachten tot het proces voltooid is. Er wordt zo gebruik gemaakt van het DTFM[1] systeem. Elke telefoon ondersteunt dit. Dit is dezelfde methode die ook gebruikt wordt in telefonische keuze menu's.

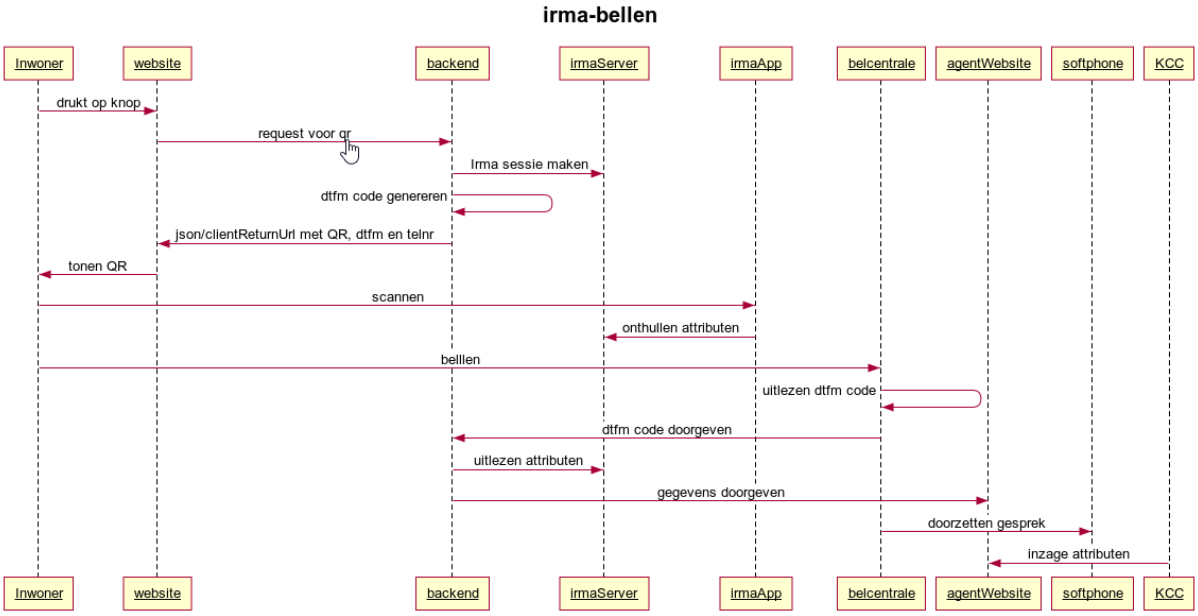
De ontvangende telefooncentrale moet in staat zijn de DTFM codes uit te lezen, en vervolgens een API call te doen naar de backend server. In de API-call wordt in ieder geval het tijdstip, het bellende telefoonnummer (zoals bekend bij de telefooncentrale) en de DTMF-code doorgegeven. Eventueel wordt er ook een 'doorschakelnummer' meegegeven; het nummer waar het gesprek naar wordt doorgeschakeld. Dat kan ook een VOIP cliënt zijn.

Zodra de backend server deze API-call ontvangt, kan deze met de DTMF code en via de IRMA server, de sessie inclusief vrijgegeven attributen ophalen. Deze kan de gegevens dan beschikbaar stellen aan een andere applicatie, bijvoorbeeld een web portaal. Dat web portaal wordt door bijvoorbeeld een KCC medewerker geraadpleegd om te zien wie er belt. Dat web portaal kan allerlei logica bevatten en uitvoeren op basis van de binnenkomende gegevens.

Het gesprek is tot stand gebracht, en de ontvanger heeft via IRMA gegevens van de beller ontvangen.

[1] https://nl.wikipedia.org/wiki/DTMF

- Dit proces is in onderstaand sequence diagram weergegeven.



Benodigde techniek

1. De IRMA applicatie op de smartphone moet in staat zijn een ‘bellen’ knop te tonen en daarmee de telefonie applicatie op de smartphone te starten. Een demo versie hiervan is al gemaakt door PBDF.
2. Een backend server die 8-cijferige codes genereert, opslaat en een IRMA sessie aanmaakt.
3. Een knop op de website van de betreffende gemeente. Die knop geeft als resultaat een pop-up met een IRMA QR-code die gescand moet worden om attributen te onthullen.
   Om die knop te laten werken moet de webpagina een extern javascript bestand opnemen. Daarin bevindt zich de benodigde code.
4. Een backend voor de publieke webpagina (zelfde als 2,3). Daar wordt de javascript gehost voor de website. Daar zit ook de functionaliteit om een sessie aan te maken op de IRMA server
5. Een telefonie centrale die in staat is de DTMF-code uit de binnenkomende oproep te lezen en door te geven aan een ander softwarecomponent.
6. Een backend (zie 2,3,4) voor de telefonie centrale die de 8 cijferige code ontvangt, het bijbehorende IRMA sessie-id ophaalt en daarmee de IRMA server aanroept, de informatie ophaalt en beschikbaar stelt aan, in dit geval, de backend van een ‘agent website’.
7. Een ‘agent website’, front-end en back-end. De backend bevat de onthulde attributen, gekoppeld aan het bellende nummer. De front-end wordt bekeken door een KCC-medewerker. In de front-end worden de onthulde gegevens getoond, daar kunnen ook hyperlinks naar eigen systemen getoond worden. In de front-end zit ook een ‘opnemen’ knop. Daarop drukken zorgt ervoor dat het binnenkomende gesprek wordt doorgeleid naar de telefoon/voipclient van de KCC-medewerker die op de knop drukt.

Telefonie centrale

Er zijn verschillende opties voor het implementeren van de benodigde telefonie centrale:

1. Gebruik maken van een bestaande telefonie centrale binnen een gemeente

2. Een echte opensource telefonie centrale implementeren; Asterisk[2]
3. Een telefoniecentrale specifiek voor de pilot afnemen bij een leverancier
4. Een telefoniecentrale as-a-service afnemen

   Optie 1: Ligt niet voor de hand. Bij een pilot met 3 gemeenten moeten er bij 3 gemeenten aanpassingen gedaan worden in de centrale (i.v.m. het verwerken van de DTMF code). Deze optie is ook niet heel geschikt om in een later stadium landelijk op te schalen.

   Optie 2: Volledig opensource. Maar vereist ook specialistische kennis, het neerzetten en onderhouden van een server, waarschijnlijk een instantie voor of bij elke deelnemende gemeente. Bij overgang naar GT-connect kan/wordt van deze oplossing geen gebruik gemaakt.

   Optie 3: Dit is de route die we nu met verkennen. Naast de telefonie centrale kan ook de backend, webpagina voor KCC en telefonie functionaliteit (bv een software voip client) geleverd worden door een dergelijke leverancier.

   Optie 4: Deze is interessant als het niet luk om er met de bestaande leverancier uit te komen. Er zijn verschillende grote platforms, waaronder twillio.com en cm.com, waarmee het mogelijk is deze functionaliteit te realiseren. Er is al een proof-of-concept implementatie gemaakt met CM.com, die eventueel makkelijk uit te breiden is naar andere providers.

Techniek uitvoerders

Punt 1:
Voor de aanpassingen in de IRMA applicatie ligt het voor de hand om de Stichting Privacy By Design te vragen die uit te voeren. De Stichting heeft een zeer beperkte capaciteit die ook ingezet moet worden voor onder meer doorontwikkeling van IRMA.

Een optie is het inhuren, door de deelnemende gemeenten, van een partij als xxxxx om de benodigde aanpassing in IRMA te realiseren. Nagevraagd moet worden in hoeverre er nog code aanpassingen nodig zijn in de IRMA cliënt hiervoor.

Punt 2-7:
De backend, javascript voor opnemen in de gemeentelijke website en een web front-end voor KCC medewerkers kan gerealiseerd worden door een partij die ook een telefonie systeem levert.

Het grote voordeel is dat we als gemeenten redelijk ‘ontzorgd’ worden.
Elke gemeenten moet nog een paar simpele dingen doen om een knop op de eigen website te krijgen, en bij het klantcontactcentrum moet op 1 of meer pc’s een VOIP cliënt geïnstalleerd worden.

Wanneer we kiezen voor optie 4, een telefonie centrale as-a-service afnemen, en niet met een telefonie leverancier in zee gaan, moet naast de inrichting van die centrale (niet heel ingewikkeld) ook punt 2-7 door de gemeenten, gezamenlijk, gerealiseerd worden.
Dit kan met eigen technische mensen, als die er zijn, of door inhuur. Bijvoorbeeld met een partij als xxxxx.

[2] https://www.asterisk.org/

Het zal van de specifieke omstandigheden bij Arnhem, Drechtsteden en Nijmegen afhangen hoe de oplossing er uit moet zien (kunnen we iets centraal neerzetten, of moet het perse decentraal, kunnen de deelnemers met Docker overweg, of moet het op een andere manier opgeleverd worden).

B: Web-RTC als alternatief voor DTFM

Al enige jaren bestaat het opensource project https://webrtc.org/
Via een aantal simpele api's kan er daarmee vanuit een webbrowser, en niet vanuit een telefoon applicatie, gebeld worden.

Deze variant heeft als voordelen boven de DTFM oplossing dat er, via de api's, al de nodige gegevens meegestuurd kunnen worden. Het gebruik van een DTFM code is niet nodig.
Het dataverkeer kan zelfs tweeweg plaatsvinden, tijdens een gesprek kan een KCC medewerker bijvoorbeeld om een ondertekening vragen, of andere attributen, waarbij een beller, tijdens het bellen, aan dat verzoek kan voldoen.

In grote lijnen zijn dezelfde backend-processen nodig als bij de DTFM code variant, alleen wordt de 8-cijferige DTFM code vervangen door een UUID.
Qua uitvoerders van de techniek is er geen verschil met variant A.

Een groot verschil tov de DTFM variant is dat er geen gebruik gemaakt wordt van 'normale' telefonie, maar ook het spraakverkeer via de data lijn loopt, direct vanuit een browser.
Een beller moet dus beschikken over voldoende datategoed of een wifi-verbinding.

Er moet meer uitzoek werk gedaan worden voor duidelijk is of deze route inderdaad bruikbaar is voor ons.