Antwoord vragen Gemeente Nijmegen inzake IRMAbellen

1. Hoe wordt de IRMA api server afgeschermd en hoe gaat dit voor de afscherming van de uitgelezen irma attributen (hoe wordt voorkomen dat het BSN onderweg wijzigt bijvoorbeeld)

De gebruiker laat zijn of haar BSN-attribuut zien in een IRMA sessie. In die sessie worden berichten uitgewisseld tussen de telefoon van de gebruiker en de IRMA-server van Bloqzone. De gebruiker bewijst met IRMA-cryptografie dat hij of zij een BSN-attribuut bezit dat door de gemeente getekend en uitgegeven is (en kan niet zonder bewijs een ander BSN sturen). HTTPS-cryptografie zorgt ervoor dat niemand de berichten kan afluisteren.

2. Wat betreft de opzet aan de website kant; hoe verhoudt de knop op de webpagina zich tot de IRMA api server, zit daar nog een backend tussen, welk proces levert het BSN (en de naam) aan het portaal, en hoe is dat proces zo ingericht dat een inwoner geen invloed heeft op de gegevens die in dat portaal getoond worden (oftewel: het resultaat van de irma-disclosure moet volledig server-side afgehandeld worden en mag niet over de browser lopen).

De knop aan de kant van Nijmegen.nl werkt door middel van een stuk Javascript dat een endpoint aanroept op de server van Bloqzone. De server van Bloqzone start hiermee een vooraf vastgestelde IRMA sessie, bijvoorbeeld een sessie die het BSN-attribuut vraagt, of de volledige naam van de gebruiker.

Enkel de inhoud van de QR-code gaat terug naar de browser op nijmegen.nl, en wordt weergeven door hetzelfde stuk Javascript. In de QR is ook een telefoonnummer aanwezig met een willekeurige 8-cijferige code (ook gegenereerd op de server). De (aangepaste) IRMA app biedt de gebruik aan dit nummer te bellen na afloop van de sessie.

De vrijgegeven gegevens worden enkel (tijdelijk) opgeslagen op de server van Bloqzone, en komen niet in de browser terecht. Op een later moment, als de gebruiker belt, wordt de koppeling gemaakt tussen het inbellende telefoonnummer, en de vrijgegeven attributen van de gebruiker.

De portal waarop de gegevens van beller in te zien zijn, zal alleen vanaf de IP-adressen van de Gemeente Nijmegen toegankelijk zijn. Specifieke KCC-medewerkers krijgen toegang krijgen tot de portal met gebruikersnaam en wachtwoord, maar ook hier zou IRMA gebruikt kunnen worden.

3. Een plaatje met de verschillende componenten en de verbindingen zou heel erg helpen.

In verband met de patentaanvraag zijn er op dit moment geen diagrammen beschikbaar.

4. Hoe gaat bloqzone zich beschermen tegen misbruikpogingen (iemand die het nummer gaat bellen en daar zelf een zelfbedacht cijfer achterplakt om een fake sessie op de irma server aan te maken). Of bellers die het nummer direct bellen zonder cijfer erachter (die calls willen we denk ik meteen blokken of omleiden naar ons 14-024 nummer).

Als de token afwezig is of niet klopt, zullen de schermen geen persoonsgegevens tonen. De agent zal dus niet beschikken over de bsn van de beller en daarmee geen persoonlijke vragen kunnen beantwoorden. Pogingen tot misbruik zijn daarmee duidelijk herkenbaar en tot mislukken gedoemd.

In de huidige situatie wordt zo'n gesprek wel doorverbonden naar de twee agenten. Dat is o.i. voor de proef een goede oplossing, omdat we dan te weten kunnen komen wat er expres of per ongeluk misging.