The S Unit Offensive Security

Managementsamenvatting

Technisch Assessment PDT-oplossing – Siip

04-09-2026 VERSIE 1.2

ZonMw
Laan van Nieuw Oost-Indië 334
2593 CE Den Haag
Nederland

The S-Unit
Savannahweg 71
3542 AW Utrecht
Nederland

1. Managementsamenvatting

The S-Unit heeft voor ZonMw, handelend namens Sportinnovator, een onafhankelijk technisch assessment uitgevoerd van de implementatie van Persoonlijke Digitale Toegang (PDT) door Siip. Dit onderzoek is gebaseerd op de implementatie van de PDT-functionaliteit van Siip binnen de PEC Zwolle app. De PDT-functionaliteit van Siip wordt hierbij toegevoegd aan de PEC Zwolle app in de vorm van een Software Development Kit (SDK) van Siip. The S-Unit heeft onafhankelijk onderzocht hoe de PDT-leverancier Siip directe persoonsgegevens en persoonsgegevens uit het identiteitsbewijs verwerkt voor het doeleind van PDT.

1.1. Onderzoeksvragen

De concrete onderzoeksvragen voor dit technisch assessment zijn:

1. Welke persoonlijke data verzendt de applicatie naar de server/backend?
2. Welke persoonlijke data wordt persistent opgeslagen of langdurig gecached in servers van Siip in het geval dat persoonlijke data wordt verwerkt door de server?
3. In hoeverre wordt het BSN van een gebruiker, kort- of langdurig, verwerkt of opgeslagen door de servers van Siip?
4. In hoeverre worden opgehaalde gegevens uit de Machine Readable Zone (MRZ) van het paspoort, kort- of langdurig, verwerkt of opgeslagen door de servers van Siip?
5. Wordt persoonlijke data ontsleuteld opgeslagen in servers van AWS waardoor AWS deze informatie zou kunnen uitlezen en kunnen delen met de Amerikaanse autoriteiten?
6. In hoeverre heeft Siip de dataverstrekking naar Google via een advertentie ID uitgezet?

1.2. Scopebeperkingen

Het technisch assessment betreft een feitelijke beschrijving van de technische implementatie van PDT door Siip op basis van en beperkt tot zes concrete onderzoeksvragen. De volgende onderwerpen zijn expliciet niet onderdeel van dit technische assessment:

1. The S-Unit geeft op basis van de resultaten geen mening over de PDT-apps van Siip of het PDT-proces in het algemeen. The S-Unit acteert als onafhankelijke neutrale partij voor een feitelijke analyse van de technische implementatie. De resultaten uit dit onderzoek kunnen wel worden gebruikt in de analyse van juridische adviseurs van ZonMw.
2. Dit technische assessment is gericht op de implementatie van PDT van Siip. Dit technisch assessment is expliciet geen analyse van het PDT-proces in het algemeen. Er bestaan andere leveranciers van PDT-apps die een andere implementatie kunnen gebruiken dan beschreven in dit document.
3. Dit technisch assessment is gericht op het gebruik van de Siip software en infrastructuur voor PDT. Infrastructuur of diensten van Siip die niet gebruikt worden voor PDT zijn expliciet buiten scope.
4. Dit technisch assessment betreft expliciet geen penetratietest of soortgelijk securityonderzoek.
5. Dit technische assessment betreft expliciet geen juridische analyse van de besproken onderwerpen.

6. Dit technisch assessment is beperkt tot de implementatie van PDT van Siip en de wijze waarop Siip gebruikmaakt van systemen en diensten van derden. Een technisch assessment van systemen van derden, zoals Amazon Web Services (AWS), is expliciet buiten scope.

1.3. Definitie persoonlijke data

Dit technisch assessment beperkt zich tot een feitelijke beschrijving van de verwerking van een subset van persoonsgegevens. De scope van dit assessment omvat een subset van de persoonsgegevens zoals bedoeld in artikel 4, lid 1, van de Algemene Verordening Gegevensbescherming (AVG). Voor dit assessment wordt onder 'persoonlijke data' verstaan: 1. directe persoonsgegevens die rechtstreeks naar een persoon verwijzen, zoals voornaam, achternaam en e-mailadres, en 2. persoonsgegevens die afkomstig zijn uit een identiteitsbewijs. Ook gegevens die het resultaat zijn van de verwerking van deze subset van persoonsgegevens vallen binnen de scope. Hieronder vallen onder meer hashes en versleutelde persoonlijke data. Een hash is een unieke reeks tekens die als digitale vingerafdruk van gegevens dient.

1.4. Verstuurde persoonlijke data

The S-Unit heeft onderzocht welke directe persoonsgegevens of persoonsgegevens uit het identiteitsbewijs worden verstuurd naar servers van Siip op basis van de volgende onderzoeksvraag: *"Welke persoonlijke data verzendt de applicatie naar de server/backend?"*

Tijdens het onderzoek van de broncode van de PDT-app zijn drie functionaliteiten vastgesteld waarbij directe persoonsgegevens of persoonsgegevens uit het identiteitsbewijs uit de mobiele app van een Siip-gebruiker naar de servers van Siip worden gestuurd. Deze functionaliteiten zijn:

1. **Het identificeren en onboarden**: Het scannen van het identiteitsbewijs.
2. **De e-mailverificatie**: Het invoeren van een e-mailadres en het e-mailverificatieproces.
3. **De PDT-service**: Het accepteren van een ticket en het versturen van gevalideerde persoonsgegevens uit de decentrale opslag op de mobiele telefoon van de gebruiker naar de bezoekerslijst.

1.4.1. Onboarding

Tijdens onboarding worden ruwe datagroepen uit de NFC-chip van het gescande identiteitsbewijs verstuurd naar een onboarding server voor een authenticiteitscontrole op basis van "passieve authenticatie". De passieve authenticatie is gebaseerd op de ICAO doc 9303 specificatie voor paspoorten en identiteitskaarten, en de ISO/IEC 18013-3:2017 standaard voor rijbewijzen. De volgende ruwe datagroepen worden verstuurd op basis van het gekozen identiteitsbewijs:

- **Paspoorten en identiteitskaarten**
  - **DG1**: Primaire bron van identiteitsgegevens
  - **DG2**: Pasfoto en geassocieerde metadata
  - **DG11**: Optionele aanvullende identiteitsgegevens
  - **DG12**: Optionele aanvullende gegevens over identiteitsbewijs
  - **EF.SOD**: Digitale handtekeningen

- **Rijbewijzen**
    - **DG1**: Primaire bron van identiteitsgegevens
    - **DG6**: Pasfoto en geassocieerde metadata
    - **EF.SOD**: Digitale handtekeningen

De ruwe datagroepen worden verstuurd voor de authenticiteitscontrole. De persoonsgegevens uit het identiteitsbewijs worden niet in leesbare of versleutelde vorm centraal opgeslagen. Na de authenticiteitscontrole wordt de pasfoto uit DG2 (paspoort en identiteitskaart) of DG6 (rijbewijs) gehaald en de additionele metadata weggehaald. Na de authenticiteitscontrole worden de gevalideerde voornaam/-namen, achternaam, geboortedatum en pasfoto decentraal in de mobiele telefoon van de gebruiker opgeslagen.

Een gebruiker met een mobiele telefoon zonder werkende camera of NFC-scanner kan via een andere mobiele telefoon met de PDT-app van Siip hun identiteitsdocument laten scannen. Siip faciliteert voor deze externe onboarding een communicatiekanaal via de onboarding server tussen de twee mobiele telefoons. Siip ontvangt in dit communicatiekanaal versleutelde datagroepen uit het identiteitsbewijs, maar Siip ontvangt niet de sleutel voor het ontsleutelen van dit verkeer. Siip slaat de gegevens uit het communicatiekanaal voor externe onboarding niet op. Na de ontvangst van de gescande datagroepen bij de geholpen partij verloopt de onboarding zoals beschreven in dit deelhoofdstuk.

1.4.2. E-mailverificatie

Bij e-mailverificatie wordt het e-mailadres verstuurd. Dit e-mailadres is ingevoerd door de gebruiker. Het e-mailadres wordt tijdens en na e-mailverificatie centraal opgeslagen.

1.4.3. Ticketacceptatie

Bij ticketacceptatie worden de gevalideerde voornaam/-namen, achternaam, geboortedatum, pasfoto en e-mailadres uit de decentrale opslag van de mobiele telefoon naar de PDT bezoekerslijst server gestuurd. Daarnaast kan een gebruiker-gespecificeerde roepnaam uit de decentrale opslag van de mobiele telefoon worden gestuurd. De pasfoto wordt na ontvangst op de PDT bezoekerslijst server geconverteerd van JP2-formaat naar een PNG-formaat.

1.5. Opslag persoonlijke data

The S-Unit heeft onderzocht welke directe persoonsgegevens en persoonsgegevens uit het identiteitsbewijs blijvend worden opgeslagen door Siip op basis van de volgende onderzoeksvraag: *"Welke persoonlijke data wordt persistent opgeslagen of langdurig gecached in servers van Siip in het geval dat persoonlijke data wordt verwerkt door de server?"*

1.5.1. Mobiele telefoon

De gevalideerde persoonsgegevens worden decentraal opgeslagen op de mobiele telefoon van de gebruiker. De mobiele opslag bevat de volgende gegevens:

- **E-mailadres:** Door de gebruiker ingegeven
- **Roepnaam:** Door de gebruiker ingegeven
- **Voornaam/-namen:** Afkomstig uit DG1 (en waar nodig DG11)
- **Achternaam:** Afkomstig uit DG1 (en waar nodig DG11)

- **Geboortedatum:** Afkomstig uit DG1
- **Pasfoto:** Afkomstig uit DG2 (paspoort of identiteitskaart) of DG6 (rijbewijs)

1.5.2. Centrale gebruikersprofiel

In de centrale opslag binnen de servers van Siip wordt een profiel opgeslagen. Het profiel bevat het e-mailadres en niet-leesbare identifiers. De identifiers worden gebruikt voor anti-identiteitsfraude en voor het identificeren van een gebruiker. Deze identifiers zijn niet herleidbaar naar de gegevens uit het identiteitsdocument. Er worden geen persoonsgegevens uit het identiteitsbewijs in leesbare of versleutelde vorm centraal opgeslagen.

1.5.3. Opslag voor BVO

De PDT bezoekerslijst server van Siip bevat gastenlijstgegevens voor evenementen bij de BVO. De gastenlijsten zijn gevuld met gegevens die worden verstuurd tijdens ticketacceptatie en zijn afkomstig uit de decentrale opslag van de mobiele telefoon van de gebruiker:

- **E-mailadres:** Door de gebruiker ingegeven
- **Roepnaam:** Door de gebruiker ingegeven
- **Voornaam/-namen:** Afkomstig uit DG1 (en waar nodig DG11)
- **Achternaam:** Afkomstig uit DG1 (en waar nodig DG11)
- **Geboortedatum:** Afkomstig uit DG1
- **Pasfoto:** Afkomstig uit DG2 (paspoort of identiteitskaart) of DG6 (rijbewijs) geconverteerd naar PNG-formaat.

Na het retentietermijn van 28 dagen na het betreffende evenement worden deze persoonsgegevens automatisch uit de gastenlijsten verwijderd.

1.6. Gebruik en opslag van BSN

The S-Unit heeft onderzocht in hoeverre het BSN van de Siip-gebruiker wordt verwerkt of opgeslagen op basis van de volgende onderzoeksvraag: *"In hoeverre wordt het BSN van een gebruiker, kort- of langdurig, verwerkt of opgeslagen door de servers van Siip?"*

Het BSN wordt niet opgeslagen in een database of verwerkt in hashwaardes. Een hash is een unieke reeks tekens die als digitale vingerafdruk van gegevens dient. Het BSN wordt niet gebruikt als identificatienummer. Het BSN wordt niet verwerkt bij het onboardingsproces met een rijbewijs of met een paspoort of identiteitskaart van na augustus 2021. Het BSN is niet aanwezig op deze documenten binnen de verwerkte onderdelen.

In paspoorten en identiteitskaarten van vóór augustus 2021 is het BSN aanwezig in de MRZ-data en de NFC-chip datagroep DG1. Dit betekent dat bij het onboardingsproces met een paspoort of identiteitskaart van vóór augustus 2021 het BSN wordt verwerkt wanneer de authenticiteitscontrole wordt uitgevoerd. Hierbij wordt het BSN voor twee doeleinden verwerkt:

- De MRZ wordt optisch uitgelezen door de PDT-app op de mobiele telefoon voor toegang tot de datagroepen op de NFC-chip van het identiteitsbewijs. Hierbij controleert de PDT-app op de mobiele telefoon ook dat het optisch uitlezen correct is verlopen met een integriteitscheck. Het BSN is onderdeel van de MRZ in een paspoort of identiteitskaart van vóór augustus 2021, waardoor het BSN als onderdeel van het geheel wordt geraadpleegd.

- Datagroep DG1 wordt op zowel de mobiele telefoon als de onboarding server gecontroleerd met een authenticiteitscontrole op basis van "passieve authenticatie". Het BSN is onderdeel van DG1 in een paspoort of identiteitskaart van vóór augustus 2021, waardoor het BSN als onderdeel van het geheel wordt geraadpleegd.

1.7. Gebruik en opslag van MRZ-data

The S-Unit heeft onderzocht in hoeverre directe persoonsgegevens en persoonsgegevens uit het identiteitsbewijs van de Siip-gebruiker wordt verwerkt of opgeslagen op basis van de volgende onderzoeksvraag: *"In hoeverre worden opgehaalde gegevens uit de Machine Readable Zone (MRZ) van het paspoort, kort- of langdurig, verwerkt of opgeslagen door de servers van Siip?"*

De optisch uitgelezen MRZ-data wordt verwerkt binnen de mobiele telefoon voor het verkrijgen van toegang tot de data in de NFC-chip. Hiervoor wordt de MRZ-data op de volgende manier verwerkt:

- De MRZ wordt door de PDT-app op de mobiele telefoon met de camera uitgelezen.
- Een integriteitscontrole wordt uitgevoerd over de MRZ-data om te controleren dat de MRZ correct is uitgelezen tijdens de optische tekenherkenning bij paspoorten en identiteitskaarten of QR-code scan bij het rijbewijs.
- De MRZ-data wordt gebruikt als toegangssleutel voor de datagroepen op de NFC-chip. Voor paspoorten en identiteitskaarten wordt alleen het documentnummer, vervaldatum en geboortedatum uit de MRZ als toegangssleutel gebruikt. Voor rijbewijzen wordt de gehele MRZ gebruikt die via QR-code wordt uitgelezen.

Tijdens de broncode-analyse is vastgesteld dat de optisch uitgelezen MRZ-data uit het tekstblok of QR-code niet verstuurd wordt naar een server van Siip. De MRZ-data wordt niet opgeslagen.

In het geval van het gebruik van een paspoort of identiteitskaart bevat de datagroep DG1 een digitale representatie van dezelfde data uit de MRZ. DG1 wordt verstuurd naar de onboarding server voor een authenticiteitscontrole, maar deze data is afkomstig uit een datagroep op de NFC-chip en niet uit de optische scan van de MRZ.

1.8. Versleuteling tijdens opslag

The S-Unit heeft onderzocht in hoeverre directe persoonsgegevens en persoonsgegevens uit het identiteitsbewijs onversleuteld opgeslagen wordt op AWS-services op basis van de volgende onderzoeksvraag: *"Wordt persoonlijke data onversleuteld opgeslagen op AWS-servers, waardoor AWS deze zou kunnen uitlezen en delen met de Amerikaanse autoriteiten?"*

Twee aspecten zijn buiten scope in dit technische assessment om te bepalen of AWS persoonsgegevens kan delen met Amerikaanse autoriteiten:

1. De juridische grondslag die de Amerikaanse autoriteiten hebben om de persoonsgegevens gericht of als geheel op te vragen. Dit is een juridische analyse en is daarmee expliciet buiten scope van dit technische assessment.
2. De mogelijkheden die AWS zelf heeft om toegang te krijgen tot systemen van klanten gehost binnen haar infrastructuur. Dit betreft een technisch assessment van AWS als

derde partij. The S-Unit heeft geen interne inzage in de technische omgeving van AWS. Dit onderwerp is daardoor expliciet buiten scope van dit technische assessment.

De versleuteling van de dataopslag op de servers van Siip in AWS verloopt op twee niveaus:

- **Infrastructuur-niveau (AWS)**: Automatische versleuteling met ingebouwde functionaliteit van AWS in de databases en bestandsopslag binnen AWS.
- **Applicatie-niveau**: Versleuteling binnen de server van Siip zelf, voordat de data in een database wordt opgeslagen. Binnen de PDT-oplossing is dit van toepassing binnen de PDT bezoekerslijst server van Siip.

Tijdens het onderzoek is vastgesteld dat de verwerking en opslag verloopt op AWS-infrastructuur binnen de Europese Economische Ruimte (EER) op zowel de primaire als de back-up locatie.

1.8.1. Versleuteling op infrastructuur-niveau

De volledige gegevensopslag wordt automatisch versleuteld door het opslagsysteem zelf met ingebouwde functionaliteit binnen Amazon Web Services (AWS). De in de database opgeslagen persoonsgegevens, het centrale gebruikersprofiel en de bezoekerslijsten, worden versleuteld met sleutels die door Siip zelf worden beheerd in een eigen AWS-account. De pasfoto's worden op infrastructuur-niveau versleuteld met sleutels die door AWS worden beheerd.

1.8.2. Versleuteling op applicatie-niveau

Voor de bezoekerslijsten worden het e-mailadres, de roepnaam, voornaam/-namen, achternaam en geboortedatum daarnaast, voorafgaand aan de opslag, aanvullend versleuteld binnen de PDT bezoekerslijst server van Siip zelf. De sleutels voor deze versleuteling zijn in beheer van Siip.

1.9. Dataverstrekking naar Google

The S-Unit heeft onderzocht in hoeverre Siip de dataverstrekking naar Google via een advertising ID heeft uitgeschakeld op basis van de volgende onderzoeksvraag: *"In hoeverre heeft Siip de dataverstrekking naar Google via een advertising ID uitgezet?"*

Tijdens het onderzoek is vastgesteld dat Siip de toegang tot de Google advertising ID expliciet heeft uitgezet.

Disclaimer

The S-Unit | Your Security Companion