Deel A: Vragen gericht aan Siip

1. Herkent Siip de bevindingen van uw experts?

Wat door uw experts is gemeten is de echtheidscontrole van het document (Passive Authentication). Het klopt dat er bij het scannen van een identiteitsdocument meer chipgegevens kortstondig naar onze backend gaan dan de vier attributen die uiteindelijk in de wallet komen (voornaam, achternaam, geboortedatum en pasfoto). Dat is een noodzakelijke en bewuste stap in de echtheidscontrole en is de norm voor veilige identiteitsverificatie. U kent dit van banken, identity wallets en partijen (KYC leveranciers) die gevalideerde identiteitsverificatie uitvoeren. De NFC echtheidsvalidatie is een vereiste binnen de PDT-voorwaarden.

De echtheidscontrole kan niet veilig op de telefoon zelf plaatsvinden, omdat de authenticiteit van de echtheidscontrole dan niet kan worden vastgesteld. De echtheidscontrole vindt versleuteld plaats. De voornaam, achternaam, geboortedatum en pasfoto worden na voltooiing van de echtheidscontrole als gevalideerde gegevens in de kluis op de mobiele telefoon geplaatst. De echtheidscontrole is een vluchtig proces waarbij er geen gegevens achterblijven op de servers van Siip of andere partijen. Dit proces is onafhankelijk geverifieerd door The S-unit. We sturen u het rapport mee als bijlage.

2. Welke gegevens leest de Siip-app uit een paspoort, identiteitskaart of rijbewijs?

Wij lezen de datagroepen uit die nodig zijn om de echtheid van het document vast te stellen volgens de internationale standaarden (ICAO 9303 voor paspoort en ID, ISO/IEC 18013-3 voor rijbewijs):

- Paspoort en identiteitskaart: DG1 (de MRZ-identiteitsgegevens), DG2 (pasfoto), DG11 en DG12 (optionele aanvullende gegevens) en het EF.SOD (de digitale handtekening van de uitgevende staat).
- Rijbewijs: DG1, DG6 (pasfoto) en het EF.SOD.

Deze datagroepen zijn nodig om te controleren of het document echt en/of onvervalst is. Dit proces is onafhankelijk geverifieerd door The S-unit. We sturen u het rapport mee als bijlage.

3. Welke gegevens verlaten het toestel en gaan naar servers van Siip of andere partijen?

De hierboven genoemde datagroepen gaan kortstondig van het toestel naar de Siip-onboarding-backend, uitsluitend om de echtheidscontrole (Passive Authentication) uit te voeren. Dit hoort bij de gekozen, meest veilige methode. Bij server-side Passive

Authentication controleren wij de digitale handtekening van de uitgevende overheid. Naar andere partijen, zoals de Betaald Voetbal Organisatie (BVO), gaan deze ruwe chipgegevens niet.

De BVO ontvangt alleen de gevalideerde eindattributen: voornaam, achternaam, geboortedatum en pasfoto na het accepteren van een ticket door de bezoeker t.b.v. de bezoekerslijst. Deze gegevens worden door Siip volledig automatisch verwijderd 28 dagen na het evenement.

Passive Authentication is geen ontwerp van Siip maar een internationale standaard onder ICAO 9303 voor het doen van echtheidscontroles van identiteitsdocumenten. We begrijpen de zorgen die kunnen ontstaan bij verzending van andere attributen dan die strikt noodzakelijk zijn (vanuit het uitgangspunt van dataminimalisatie) voor de echtheidscontrole. Ook voor ons wat dit een vraagstuk, waar wij een goede oplossing voor hebben gevonden. De keuze om de echtheidscontrole server-side te doen heeft geen negatieve invloed stuit met de gebruikte methode niet op wezenlijke juridische bezwaren Het uitlezen van de NFC-chip en de echtheidscontrole vindt slechts (in enkele seconden) versleuteld plaats, waarbij de gegevens vervolgens automatisch worden vernietigd. Het gestelde alternatief van een echtheidscontrole op het toestel biedt geen valide en betrouwbaar alternatief. Nog daargelaten dat de echtheidscontrole op het toestel ook leidt tot verwerking in de zin van de AVG, maar heeft een dergelijke echtheidscontrole op het toestel negatieve invloed op betrouwbaarheid.

4. Welke gegevens worden daadwerkelijk door Siip ontvangen en verwerkt?

De versleutelde ruwe chipgegevens passeren uitsluitend voor identificatiedoeleinden de server, maar alleen om te worden gecontroleerd en gevalideerd. Er is geen opslag, logging of caching. The S-unit heeft dit vastgesteld:

- Persoonsgegevens uit het identiteitsdocument worden niet centraal leesbaar of versleuteld opgeslagen.
- Het centrale gebruikersprofiel bevat alleen het e-mailadres en niet-herleidbare identifiers.
- De gevalideerde voornaam, achternaam, geboortedatum en pasfoto worden decentraal op het toestel van de gebruiker bewaard, onder diens eigen controle.
- MRZ-gegevens worden niet naar de server gestuurd om te bewaren en niet opgeslagen.

5. Als er gegevens op de server binnenkomen die niet nodig zijn voor PDT, wat gebeurt daarmee?

De via de NFC-chip opgehaalde gegevens worden na voltooiing van de echtheidscontrole binnen enkele seconden vernietigd. Siip verwerkt uitsluitend gegevens die noodzakelijk zijn voor de dienstverlening. Het vaststellen van de identiteit is daar onderdeel van. Deze noodzakelijke gegevens worden uitsluitend verwerkt voor de echtheidscontrole op dat moment en ook die gegeven worden daarna niet bewaard. De verwerking is vluchtig en in transit. Er is geen server-side opslag, logging of caching van de ruwe datagroepen en de data die daarin worden gecontroleerd. Ook dit is door The S-unit onafhankelijk bevestigd.

6. Kan Siip uitsluiten dat het BSN het toestel verlaat?

Voor gebruikers die zich identificeren met een rijbewijs, een identiteitskaart uitgegeven vanaf 1 augustus 2021 of een paspoort uitgegeven na 30 augustus 2021 komt het BSN in de echtheidscontrole niet voor: bij deze identiteitskaarten en paspoorten staat het BSN niet in de NFC-chip. Bij rijbewijzen heeft Siip ingeregeld dat de gegevensgroep waarin het BSN staat, niet wordt uitgelezen.

Voor gebruikers die zich identificeren met een identiteitskaart uitgegeven vóór 1 augustus 2021 of een paspoort uitgegeven vóór 31 augustus 2021 geldt dat de NFC-chip het BSN bevat. Bij de echtheidscontrole loopt het BSN kortstondig (enkele seconden) en versleuteld mee als onlosmakelijk onderdeel van de gegevensgroep die voor de controle noodzakelijk is. Direct na voltooiing van de echtheidscontrole worden de via de NFC-chip opgehaalde gegevens (waaronder het BSN) vernietigd.

Het uitlezen van de volledige NFC-chip is nodig voor een betrouwbare echtheidscontrole. Dit volgt rechtstreeks uit de internationale ICAO 9303 standaard. Deze standaard beschrijft dat de MRZ in datagroep DG1 staat, dat DG1 als geheel wordt gehasht en dat die hashwaarde is opgenomen in de ondertekende EF.SOD. Een deel van DG1 aanpassen of weglaten, zoals het BSN, maakt de berekende hash ongelijk aan de door de staat ondertekende waarde en laat de echtheidscontrole mislukken. Een bewerkte variant van een echte chip bestaat dus niet.

Onder ons privacy-by-design-principe wordt het BSN niet als waarde gebruikt, gekoppeld of bewaard. Het wordt nooit als identificatienummer gebruikt.

7. Hoe kijkt Siip naar de bevindingen in het kader van dataminimalisatie?

Voor dataminimalisatie is van belang dat wordt bekeken of het middel evenredig is voor het gestelde doel (evenredigheidsbeginsel), geen geschikte alternatieve middelen bestaan die minder inbreuk maken op de privacy van betrokkenen (‘subsidiariteit’) en of de verwerkte persoonsgegevens strikt noodzakelijk zijn voor het beoogde doel.

Het doel van de echtheidscontrole is het borgen van de betrouwbare validatie van de identiteit van de gebruiker. Het valideren van de identiteit van de gebruiker strekt in

geval van de PDT oplossing van PSV tot het kunnen verrichten van toegangscontrole, onder meer om stadionverboden te handhaven en de veiligheid in haar stadion te borgen. De keuze om gebruik te maken van de NFC-chip is voor de hiervoor beschreven doeleinden evenredig.

Siip heeft bezien of andere betrouwbare alternatieven zijn voor het uitlezen van de NFC-chip. Dergelijke betrouwbare alternatieven zijn niet voorhanden. Voor het digitaal uitlezen van de NFC-chip heeft Siip onderbouwd en aangetoond dat optische alternatieven voor het digitaal uitlezen van de NFC-chip op afstand geen valide optie is. Een kopie uploaden met gelakt BSN plus tekstherkenning (OCR) levert geen echtheidscontrole. Het bewijst niet dat een document echt is en is gevoelig voor manipulatie en AI-vervalsing. Dat alternatief verwerkt bovendien meer persoonsgegevens (een volledige documentafbeelding) met minder waarborgen. Dergelijke alternatieven leveren geen echtheidscontrole op van het identiteitsdocumenten en daarmee geen gevalideerde identiteit. Dit maakt dat geen alternatieven voorhanden zijn.

Doordat het uitlezen van de NFC-chip de meest betrouwbare manier is om de identiteit van gebruikers te valideren, en geen betrouwbare alternatieve voorhanden zijn, is de keuze voor het uitlezen van de NFC-chip gerechtvaardigd. Bij het uitlezen van de NFC-chip valt geen keuze te maken in de soort gegevens die worden opgehaald. De echtheidscontrole is technisch onsplitsbaar. Het document wordt als geheel geverifieerd tegen de handtekening van de uitgevende staat. Een voorselectie van alleen de nodige velden bestaat op chipniveau niet. Passive Authentication onder ICAO 9303 is een verplicht mechanisme dat de integriteit van de chipinhoud als geheel controleert.

Dataminimalisatie moet bij het uitlezen van de NFC-chip dus zo worden begrepen, dat technische maatregelen worden getroffen die maken dat de gegevens uit de NFC-chip na de echtheidscontrole direct (na voltooiing van de echtheidscontrole) worden vernietigd. Siip heeft in dat kader verstrekkende maatregelen getroffen. De gegevens uit de NFC-chip worden versleuteld opgehaald en, na voltooiing van de echtheidscontrole, automatisch vernietigd. Daarmee wordt voldaan aan het beginsel van dataminimalisatie. De resterende dataset, die decentraal wordt opgeslagen op het toestel van de betrokkene en bij ticketacceptatie naar de BVO wordt verzonden, is beperkt tot de persoonsgegevens die strikt noodzakelijk zijn voor de PDT, namelijk: voornaam, achternaam, geboortedatum en pasfoto. Door de persoonsgegevens decentraal op te slaan op het toestel van de gebruiker wordt voldaan aan het beginsel van dataminimalisatie en privacy by design.

8. Pels Rijcken stelt dat BVO's geen grondslag hebben voor het verwerken van het BSN, en dat ook kortstondige verwerking een risico kan zijn. Hoe voorkomt Siip dat apps het BSN toch verwerken?

Pels Rijcken heeft de PDT-oplossing van Siip getoetst en ziet, na opvolging van haar aanbevelingen, geen wezenlijke juridische belemmeringen. Ook niet voor wat betreft het verwerken van het BSN. Deze aanbevelingen zijn opgevolgd. We verwijzen naar de bijlage van Pels Rijcken.

9. Hoe kijkt Siip naar de privacy- en veiligheidszorgen van supporters en deskundigen?

Wij nemen die zorgen serieus. Het doel van onze organisatie is gebruikers regie te geven op hun eigen data. Daarbij zijn dataminimalisatie, privacy-by-design en security-by design altijd leidend geweest. Dit hebben wij en zullen wij altijd onafhankelijk blijven en laten toetsen.

Deel B Vragen gericht aan PSV

1. Hoe kijkt PSV naar de bevindingen, in het bijzonder rond dataminimalisatie?

PSV kent uiteraard de werking van de PSV-App en is in die zin dus ook niet verrast door wat jullie 'de bevindingen' noemen. In technische zin heeft Siip deze vraag bovenstaand reeds beantwoord. Privacy en dataveiligheid neemt PSV zeer serieus. Het is daarom goed dat onafhankelijk is vastgesteld door Pels Rijcken en The S-Unit dat de applicatie juridisch noch technisch conflicteert met de geldende wet- en regelgeving.

2. Het Pels Rijcken-rapport stelt dat BVO's geen grondslag hebben voor verwerking van het BSN. Hoe zorgt PSV dat het BSN niet wordt verwerkt?

In het PDT-proces ontvangt PSV geen BSN. Zie hiervoor ook de rapporten van The S-Unit en Pels-Rijcken.

3. PSV schrijft in de 'Voorwaarden PSV Seizoen Club Card 2026-2027' dat er maatregelen zijn om het BSN niet uit te lezen. Toch lijkt het BSN wel verwerkt te worden. Hoe kijkt PSV hiernaar?

PSV ontvangt nergens in het PDT-proces BSN-nummers. Voor nadere toelichting verwijst PSV naar de bijlage van Pels Rijcken en The S-Unit.

4. Welke gegevens worden door Siip verwerkt, welke ontvangt PSV, welke slaat Siip op?

Siip verwerkt kortstondig de chipdatagroepen voor de echtheidscontrole (zie A2 en A3). PSV ontvangt alleen de vier gevalideerde eindattributen (voornaam, achternaam, geboortedatum en pasfoto). Die attributen worden met ons gedeeld op het moment dat iemand een ticket accepteert. Het delen gebeurt met toestemming van de gebruiker. 28 dagen na het evenement worden deze gegevens automatisch verwijderd.

Siip slaat de identiteitsgegevens niet centraal op. Die staan decentraal op het toestel. Centraal staat alleen het e-mailadres met niet-herleidbare identifiers. Onafhankelijk bevestigd door The S-unit.

5. Hoe heeft PSV Siip als leverancier gekozen en welke privacy- en beveiligingseisen zijn gesteld?

PSV heeft Siip gekozen op basis van de door Sportinnovator en KNVB gestelde juridische en technische randvoorwaarden. Siip kan desgevraagd de doorlopen audits, de DPIA's en het onafhankelijke The S-unit-assessment aanleveren als onderbouwing.

6. Hoe kijkt PSV aan tegen de privacy- en veiligheidszorgen die door supporters en deskundigen worden geuit?

Die begrijpen we volledig. Laten we overigens niet vergeten dat dit instrument (PDT) juist in het leven is geroepen in het belang van de veiligheid van onze bezoekers. Neemt niet weg dat de bescherming van data en privacy van onze supporters grote prioriteit heeft en voor ons absolute voorwaarde was bij de implementatie van PDT. Voor PSV is dat reden geweest om (aanvullende) juridische analyses, DPIA's en een onafhankelijk technisch onderzoek te laten uitvoeren. Daarbij vinden wij het belangrijk onderscheid te maken tussen feitelijke bevindingen en de conclusies die daaruit worden getrokken: sommige aandachtspunten verdienen terecht uitleg en nadere toelichting. Pels Rijcken en de The S-Unit bevestigen nu nogmaals dat zij, na opvolging van de aanbevelingen (hetgeen inmiddels heeft plaatsgevonden) geen belemmeringen zien voor het gebruik van onze app binnen de geldende wet- en regelgeving en noodzakelijk technische- en beveiligingsmaatregelen. Wij zullen de oplossing blijven toetsen, verbeteren waar mogelijk en transparant het gesprek blijven voeren met supporters, deskundigen en toezichthouders.

7. Welke veiligheidsmaatregelen neemt PSV om supportersgegevens te beschermen?

PSV neemt verschillende technische en organisatorische maatregelen om persoonsgegevens van supporters te beschermen, waaronder versleutelde gegevensoverdracht, toegangsbeveiliging, rolgebaseerde autorisaties, logging van toegang en beperkte bewaartermijnen. Daarnaast werkt PSV uitsluitend samen met zorgvuldig geselecteerde leveranciers die contractueel zijn gebonden aan privacy- en beveiligingseisen en worden verwerkingen periodiek beoordeeld via DPIA's, audits en leverancierscontroles.