MOB
Maatschappelijk Overleg Betalingsverkeer

Datum
11 mei 2017

Kenmerk
MOB/ T018-1568171659-150

Biometrie in het betalingsverkeer

Onderwerp:
Biometrie in Betalingsverkeer

Datum
11 mei 2017

Kenmerk
MOB/ T018-1568171659-150

Samenvatting en aanbevelingen

Het gebruik van biometrie in het betalingsverkeer neemt snel in belang toe. De nieuwste high-end mobiele telefoons zijn bijvoorbeeld voorzien van vingerafdrukherkenning. De opkomst van biometrie heeft impact op de werking van het betalingsverkeer, vooral op gebied van veiligheid (inclusief privacy) en efficiëntie (inclusief toegankelijkheid).

In deze nota wordt biometrische toegangsbeveiliging voor mobiel betalen en bankieren beoordeeld aan de hand van het kader dat in mei 2015 door het MOB is vastgesteld. De nota is opgesteld door het MOB-secretariaat, en besproken in de Werkgroep Veiligheid met inbreng van de Werkgroepen Maatschappelijke Efficiency en Europese zaken en Toegankelijkheid en Bereikbaarheid. In deze bespreking gemaakte opmerkingen zijn in deze versie verwerkt.

De conclusies uit het onderzoek zijn:

- Biometrie kan **bijdragen** aan de veiligheid van betalingsverkeer doordat sterke klantauthenticatie eenvoudiger in het gebruik wordt.
- De mate van veiligheid is echter **sterk afhankelijk van de kwaliteit** van implementatie, zowel voor het proces (registratie) als de gebruikte techniek. Er is veel innovatie en internationale standaarden zijn nog in ontwikkeling. Onafhankelijke certificatie is nog niet beschikbaar.
- De **privacy regelgeving** is vanaf 2018 met de invoering van de General Data Protection Regulation verder aangescherpt voor opslag van persoonlijk identificeerbare informatie.
- **Juridisch** zijn er nog de nodige **onzekerheden** over regelgeving en mogelijke betwistingen.

Aanbevelingen aan marktpartijen

Het MOB roept financiële instellingen als aanbieders van betaalproducten op om de consument goed te informeren omtrent het veilig gebruik van biometrische identificatie en authenticatie en de keuzemogelijkheden zoals verschillende authenticatievormen daarbij.

Daarnaast vraagt het MOB de financiële instellingen het ontwerp van biometrische toepassingen vroegtijdig af te stemmen met de bij het MOB aangesloten belangengroepen voor toegankelijkheid zoals Ieder(in), Oogvereniging en ouderenorganisaties om de kansen voor betere toegankelijkheid van betalingsverkeer zo goed mogelijk uit te nutten.

Financiële instellingen, verwerkende bedrijven en winkeliers worden gewezen op het grote belang van veiligheid en privacy bij de opslag en verwerking van persoonskenmerken. Regelgeving zoals Payment Services Directive 2, de bijbehorende Regulatory Technical standards en de General Data Protection Regulation zijn daarbij maatgevend.

Het MOB zal de verdere ontwikkelingen van biometrische authenticatie, standaarden en privacy aspecten blijven monitoren binnen de Werkgroep Veiligheid. De Werkgroep Veiligheid zal hier over één jaar opnieuw over rapporteren.

Inhoud

1. Inleiding

Het gebruik van biometrie in het betalingsverkeer neemt snel in belang toe. De nieuwste high-end mobiele telefoons zijn bijvoorbeeld voorzien van vingerafdrukherkenning, die gebruikt kan worden om toegang tot de telefoon en specifieke apps te krijgen. Veel apps voor mobiel bankieren en betalen maken hier inmiddels gebruik van. Bij internet bankieren op de PC wordt nog geen gebruik gemaakt van biometrie, dus dat blijft in deze nota buiten beschouwing.

Het gaat hierbij om "biometrische authenticatie": het op basis van meetbare lichaamskenmerken vaststellen van de authenticiteit van de gebruiker. Naast vingerafdrukken zijn verschillende andere technieken in gebruik, zoals gezichtsherkenning, stemherkenning, irisscan, etc.

De opkomst van biometrie heeft impact op de werking van het betalingsverkeer, vooral op gebied van veiligheid (inclusief privacy) en efficiëntie (inclusief toegankelijkheid).

In deze nota wordt biometrische toegangsbeveiliging voor mobiel betalen en bankieren beoordeeld aan de hand van het kader dat in mei 2015 door het MOB is vastgesteld. Daarbij wordt onderzocht of er veiligheids- of privacy risico's, robuustheid of toegankelijkheidsrisico's zijn, hoe de efficiency wordt bevorderd en of er sprake is van barrières.

2. Algemene informatie

De wereld van informatie beveiliging verandert snel. Waar de toegang tot vertrouwelijke systemen vaak beschermd wordt met een gebruikersnaam en wachtwoord, worden nu in hoog tempo veiliger alternatieven ontwikkeld. Dit is hard nodig, omdat het aantal toepassingen waar mensen gebruik van maken sterk is gegroeid en het aantal wachtwoorden onbeheersbaar groot is geworden. Ook de veiligheid van de wachtwoorden zelf laat vaak te wensen over.

Dit leidt tot een behoefte aan sterke cliëntauthenticatie (strong customer authentication). Dit is ook de achtergrond van nieuwe Europese eisen voor betalingsverkeer in de Payment Services Directive (PSD2) en de daarbij behorende Regulatory Technical Standard on Strong Customer Authentication (RTS SCA).

In PSD2 wordt de volgende definitie gehanteerd:

„sterke cliëntauthenticatie": authenticatie met gebruikmaking van twee of meer factoren die worden aangemerkt als kennis (iets wat alleen de gebruiker weet), bezit (iets wat alleen de gebruiker heeft) en inherente eigenschap (iets wat de gebruiker is) en die onderling onafhankelijk zijn, in die zin dat compromittering van één ervan geen afbreuk doet aan de betrouwbaarheid van de andere en dit zodanig is opgezet dat de vertrouwelijkheid van de authenticatiegegevens wordt beschermd;

Sterke cliëntauthenticatie is dus gebaseerd op een combinatie van twee elementen uit kennis (zoals een wachtwoord of pincode), bezit (zoals een bankpas of een aan een bankrekening gekoppelde mobiele telefoon) en een inherente eigenschap (zoals de biometrische kenmerken van vingerafdruk, stem, iris). Een aan een bankrekening gekoppelde mobiele telefoon met pincode of biometrische authenticatie is dus een vorm van sterke cliëntauthenticatie.

Het gebruik van biometrische kenmerken kan het gemak vergroten ten opzichte van het gebruik van een wachtwoord of pincode en heeft daarmee ook voordelen voor de toegankelijkheid.

De randvoorwaarde is uiteraard dat veiligheid en privacy op een adequate manier zijn geborgd. Belangrijk is ook dat de gebruiker zelf kan kiezen of deze

van een wachtwoord of pincode gebruik wil maken, of van biometrie. Dit omdat het vertrouwen van de gebruiker een persoonlijke afweging is.

Beoordeling van het veiligheidsniveau

In tegenstelling tot het gebruik van een pincode of password, is de uitkomst van een biometrische test niet "juist of onjuist" maar kent deze een "mate van waarschijnlijkheid".

Stel dat een ingelezen vingerafdruk voor 98% gelijk is aan een eerder ingelezen vingerafdruk van de geautoriseerde gebruiker, dan moet op basis van een "drempelwaarde" bepaald worden of de toegang wel of niet wordt verleend.

Als deze drempelwaarde erg hoog wordt ingesteld, zal in een groter aantal gevallen een authentieke gebruiker onterecht worden geweigerd ("false rejects"). Bij een te laag gekozen waarde wordt vaker een niet-authentieke gebruiker onterecht toegelaten ("false accepts").

Voor het bepalen van deze drempelwaarde moet een afweging worden gemaakt tussen gemak en veiligheid. Dit is van groot belang voor de efficiency, daar het bepaalt of de gebruiker op een verantwoorde wijze de betreffende functionaliteit kan en wil gebruiken.

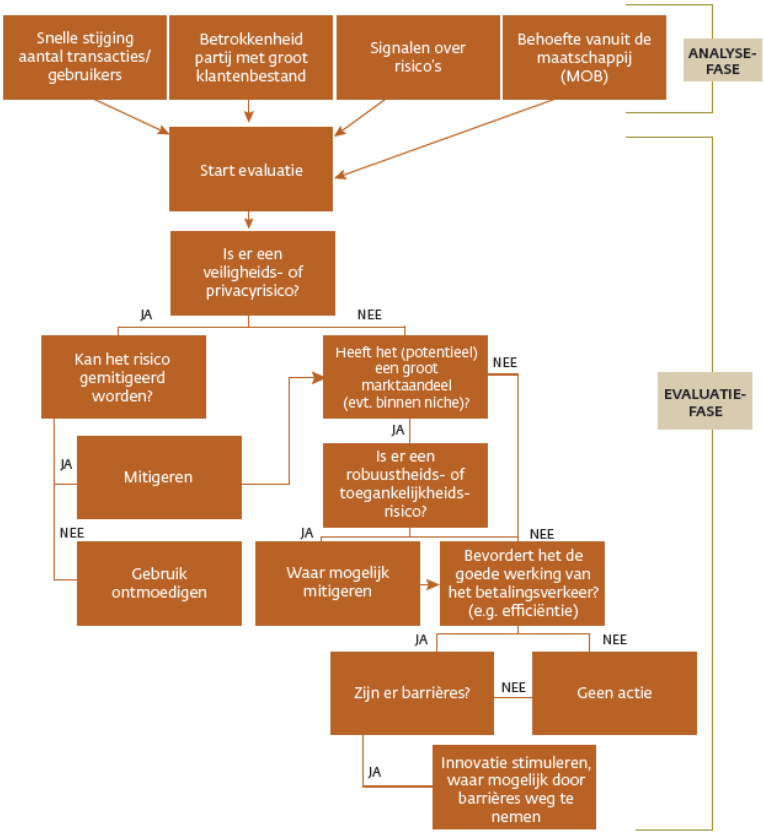
Certificering

In tegenstelling tot bijvoorbeeld pinpads voor betaalautomaten, worden de vingerafdruklezers in telefoons niet door banken gespecificeerd. Het zijn de technologieleveranciers zoals Apple en Samsung die bepalen welke lezers en sensoren voor consumenten beschikbaar zijn. Doordat het hier gaat om nieuwe technologie, is er nog geen onafhankelijk stelsel voor certificering beschikbaar zoals we dat kennen van betalingsverkeer met cards.

3. Beoordeling aan de hand van het beoordelingskader

Het toegepaste beoordelingskader zoals vastgesteld[1] in het MOB is als volgt:

Figuur 1: Beoordelingskader van innovaties en bijbehorende reacties



[1] Innovaties in het betalingsverkeer & de rol van DNB en het MOB, 2015

3.1 Veiligheid- en privacyrisico's

Bij de toepassing van biometrie zijn veiligheid- en privacyrisico's aanwezig. Bij veiligheid gaat het om mogelijk onvoldoende sterke bescherming van de authenticiteit van de gebruiker, bij privacy over het uitlekken en hergebruiken van de biometrische referentiegegevens.

3.1.1 Veiligheidsrisico's

Zoals aangegeven in de inleiding, wordt bij biometrische cliëntauthenticatie met een bepaalde mate van zekerheid vastgesteld of we met de authentieke gebruiker te maken hebben. Hoe groot die zekerheid is, hangt af van de gebruikte techniek en de gekozen drempelwaarde.

Van een pincode of wachtwoord kan honderd procent zeker worden bepaald of deze goed of fout is: de waarde is wel of niet gelijk. Maar bijvoorbeeld bij een vingerafdruk wordt beoordeeld of de aangeboden vinger voldoende lijkt op een eerder vastgelegde vingerafdruk.

Wat "voldoende" betekent, hangt af van de nauwkeurigheid van het gebruikte authenticatiesysteem. De controlemethode en de daarbij gehanteerde drempelwaarde bepaalt of een gebruiker wel of geen toegang krijgt (False Accept Rate, False Reject Rate).

Daarbij is het ook van groot belang dat een goede controle op "levend bewijs" plaatsvindt (de "liveness check"). De techniek kent hier een snelle ontwikkeling. Goede vingerafdruklezers zijn bijvoorbeeld moeilijker te misleiden met een rubber vingerafdruk doordat ze een 3D beeld gebruiken. Irisscanning biedt ook goede mogelijkheden maar is nog minder in gebruik. Gezichtsherkenning is lastiger te beveiligen tegen het afspelen van filmpjes of gebruik van foto's en stelt dus hogere eisen aan een goede controle.

De drempelwaarde voor acceptatie van de gebruiker ligt vast in het authenticatiesysteem. Hierbij zijn er twee mogelijkheden: het systeem is centraal of decentraal.

Bij een centraal systeem worden de ingelezen gegevens beveiligd verzonden naar een speciaal systeem waarin de controles worden uitgevoerd. Voorbeelden hiervan zijn stemherkenning (zoals stem-bankieren) en gezichtsherkenning (zoals MasterCard "Selfie Pay" identity check). In deze centrale systemen kunnen de gebruikte algoritmen en drempelwaarden door de financiële instelling worden bepaald en waar nodig bijgesteld.

Bij een decentraal systeem vindt de controle plaats in het apparaat van de gebruiker, zoals de mobiele telefoon. Daarbij is het algoritme en de drempelwaarde door de fabrikant (zoals Apple of Samsung) gekozen.
De app van de financiële instelling krijgt bij gebruik een melding of de gebruiker is herkend, maar heeft geen verdere informatie over de mate van waarschijnlijkheid daarvan.

Voor het ontwerp van biometrische controles zijn verschillende internationale standaards in ontwikkeling waarbij ook de mogelijke aanvallen zijn gecategoriseerd. In bijlage 2 wordt dieper ingegaan op de mogelijke aanvallen op biometrische controles. Bijlage 3 geeft een overzicht van de aanwezige standaards.

Waar standaards worden toegepast is het ook mogelijk om de juistheid en veiligheid van de implementatie in een certificatieproces te beoordelen. Dat is bij betaalpassen en automaten ingericht met onafhankelijke beoordelaars. Voor biometrische toepassingen is dit echter nog niet aanwezig. Daardoor zullen financiële instellingen bij decentrale systemen moeten vertrouwen op een voldoende veilige implementatie door de fabrikant.

Vaststellen van de juiste gebruiker

Bij het gebruik van vingerafdruklezers bestaat het risico dat in de telefoon ook vingerafdrukken van anderen zijn opgeslagen in het registratieproces ("enrollment"). Bij sommige implementaties is het mogelijk om vast te stellen welke vinger is gebruikt, bij andere niet.

Bij het nieuwe irisscanning kan dit worden voorkomen als er slechts één paar ogen kan worden vastgelegd., maar moet wel rekening worden gehouden met het feit dat iemand die over de toegangscode van de telefoon beschikt, ook zijn biometrisch kenmerk daarin kan vastleggen.

Mitigerende maatregelen

Bij gebruik van vingerafdruklezers wordt de klant door de app expliciet gewezen op de eigen verantwoordelijkheid om alleen de eigen vingerafdrukken in de telefoon te registreren.

De financiële instellingen onderkennen de beperktere invloed op het beveiligingsniveau en passen aanvullende maatregelen toe zoals vastlegging van de gebruikte telefoon ("device binding") en beperkingen aan de transacties (zoals alleen overboekingen naar bekende rekeningnummers en tot een bepaald maximum bedrag). Ook kan de transactie aan verdere risico analyse worden onderworpen ("transaction risk analysis").

3.1.2 Privacyrisico's

De privacyrisico's van biometrische authenticatie liggen in het uitlekken en oneigenlijk gebruik van de opgeslagen kenmerken. Een uitgelekte pincode of wachtwoord kan door de gebruiker worden vervangen, maar dit geldt niet voor bijvoorbeeld een vingerafdruk. Aan de opslag van deze kenmerken worden daarom zeer hoge eisen gesteld.

De EBA Regulatory Technical Standards on Strong Customer Authentication stellen eisen aan de gescheiden opslag van verschillende gegevens in beveiligde omgevingen zoals de mobiele telefoon.

Bij centrale verwerking is de privacywetgeving van grote invloed op de wijze van opslag en verwerking. In 2018 wordt de Europese General Data Protection Regulation ingevoerd waarin sterke beperkingen worden opgelegd aan opslag en gebruik van biometrische gegevens.

Mitigerende maatregelen

Biometrische kenmerken kunnen als “templates” worden opgeslagen. Deze templates worden volgens een bepaald algoritme afgeleid van de oorspronkelijke kenmerken zoals het beeld van de vingerafdruk. Het template dient niet terug herleidbaar te zijn naar het oorspronkelijke beeld. Voor deze systematiek zijn standaarden ontwikkeld (zie bijlage 3). Dat is zowel voor centrale als decentrale authenticatiesystemen van toepassing.

De gebruiker dient expliciet toestemming te geven voor de opslag en gebruik van de biometrische gegevens en de financiële instelling dient dit vast te leggen. De vastlegging en gebruik van biometrische kenmerken dient op zeer veilige wijze te gebeuren. Hiervoor zijn in de EBA Regulatory Standards on Strong Customer Authentication[2] eisen geformuleerd.

3.2 Robuustheids- en toegankelijkheidsrisico’s

3.2.1 Robuustheid

De robuustheid van biometrische authenticatie is afhankelijk van de kwaliteit van de implementatie en de gebruikte processen.
Daarbij speelt een rol dat de technologie zich snel ontwikkelt (zie hoofdstuk 4), dat standaarden in ontwikkeling zijn en dat er geen onafhankelijke certificatie beschikbaar is.

Financiële instellingen worden meer afhankelijk van dienstverlening van derden. Bij pinbetalingen met een betaalautomaat en bankpas zijn de specificaties volgens internationale standaards opgesteld en wordt de implementatie onafhankelijk beoordeeld. De financiële instelling kan daar een afgewogen oordeel vormen over het veiligheidsniveau hiervan.
Bij nieuwe betaalvormen en authenticatiemiddelen zoals biometrie is dit in mindere mate het geval en zal de financiële instelling aanvullende maatregelen moeten nemen om de risico’s te beheersen.

[2] https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

Mitigerende maatregelen

DNB beschouwt het identificeren en authentiseren van klanten en betalingen als wezenlijke bedrijfsprocessen voor een financiële instelling. Dat betekent dan ook dat de biometrische oplossingen gezien worden als een mogelijke vorm van uitbesteding. Als gevolg daarvan dient een financiële instelling passende maatregelen te treffen voor de beheersing van de risico's en het monitoren daarvan.

Financiële instellingen dienen zorgvuldig om te gaan met de selectie van technologie en toepassingen voor biometrische authenticatie, zowel bij centrale als decentrale modellen. Toepassing van gestandaardiseerde technieken maakt de implementatie beter meet- en toetsbaar. Een formele certificering van toepassingen kan dit aanmerkelijk versterken, maar deze is nog niet beschikbaar. De ontwikkelingen op dit gebied, zowel voor technische innovatie als de ontwikkeling van normen en certificering dienen actief te worden gevolgd.

3.2.2 Toegankelijkheid

Bij de toegankelijkheid speelt de bruikbaarheid voor alle gebruikers een rol. Belangrijk is dat biometrische authenticatie een alternatief is naast de reeds bestaande authenticatiemogelijkheden zoals password of pincode. In dat geval heeft de gebruiker de keuze om al dan niet gebruik te maken van biometrische verificatie.

Voordelen van biometrie

Het gebruik van biometrie kan de toegankelijkheid verder verhogen doordat het eenvoudiger te gebruiken kan zijn voor mensen met een beperking. Te denken valt aan vingerafdrukherkenning voor authenticatie en stemherkenning voor bediening van applicaties.

Nadelen van biometrie

Een nadeel voor de toegankelijkheid is de grote diversiteit in het aantal biometrische authenticatiemethoden zoals vingerafdruk, gezichtsherkenning, irisscanning en stemherkenning. De gebruiker moet er van uit kunnen gaan, dat

ALLE methodes veilig zijn. Maar het kan wel verwarrend zijn, dat bijvoorbeeld met een vingerafdruk alleen transacties kan doen naar bankrekeningen in de adressenlijst, met gezichtsherkenning naar alle bankrekeningen tot een bepaald bedrag en met een irisscan ongelimiteerd naar alle bankrekeningen. Dat vereist zorgvuldige voorlichting door de betaalinstellingen.

Afstemming van ontwerp

Belangenverenigingen hebben het belang onderstreept dat bij het ontwerp van een toepassing in een vroeg stadium rekening wordt gehouden met de wensen van deze doelgroepen.

3.3 Potentiële positieve effecten op de werking van het betalingsverkeer

De grootste bijdrage aan de werking van het betalingsverkeer ligt in het grotere gebruiksgemak. Het testen van bijvoorbeeld een vingerafdruk kan eenvoudiger en sneller zijn dan het ingeven van een pincode of wachtwoord.
Doordat de authenticatie van de gebruiker op een eenvoudiger manier kan plaatsvinden, kan deze ook vaker of voor meer handelingen worden ingezet.
Daarmee kan de veiligheid van betalingsverkeer verder worden verhoogd.
De afhankelijkheid van passwords met al hun risico's voor onveilige opslag en zwakke waarden wordt aanzienlijk verkleind.

3.4 Barrières

Mogelijke barrières die het succes van biometrische authenticatie belemmeren zijn:

- Beperkingen in de toestellen waarvoor de verschillende biometrische authenticatie vormen beschikbaar zijn
- Onzekerheid over toekomstige technologische ontwikkelingen
- Juridische onduidelijkheden
- Acceptatie door de gebruiker

3.4.1 Beperkingen in de toestellen waarvoor de verschillende biometrische authenticatie vormen beschikbaar zijn

De beschikbaarheid van biometrische sensoren is afhankelijk van de fabrikanten. Mobiele telefoons worden inmiddels vaak met vingerafdruklezers uitgerust, en geleidelijk ook met andere technieken zoals irisscanners.
Er is echter een grote variatie in ondersteuning van verschillende soorten sensoren in mobiele telefoons, dus niet elke techniek is voor elk toestel inzetbaar.

Doordat certificering nog ontbreekt, dienen financiële instellingen de kwaliteit van implementatie per toestel zelf in te schatten en te bepalen welke toestellen en technieken voldoende veilig zijn en welke aanvullende beveiligingsmaatregelen zijn vereist.

3.4.2 Onzekerheid over toekomstige technologische ontwikkelingen

Het aantal beschikbare technieken voor biometrische authenticatie groeit snel. De verschillende technieken hebben ook een verschillende kwaliteit. Dat betekent dat sommige implementaties niet geschikt zijn voor gebruik in betalingsverkeer. Informatie van de consument daarover is van groot belang.

3.4.3 Juridische onduidelijkheden

De regelgeving rond het gebruik van biometrische kenmerken in betalingsverkeer is deels nog in ontwikkeling.

De EBA Regulatory Standard on Strong Customer Authentication geeft een algemeen (high level) kader voor de inrichting van strong customer authentication, maar deze standaard is nu nog een concept.

Ook de impact van de nieuwe privacy regelgeving (General Data Protection Regulation) op het gebruik van biometrische kenmerken zal door de gebruikende partijen (zoals financiële instellingen, betaalinstellingen) moeten worden beoordeeld.

Daar het gebruik van biometrische authenticatie in betalingsverkeer nog relatief nieuw is, ontbreekt een uitgebreide jurisprudentie over geschillen daarover.

3.4.4 Acceptatie door de consument

Niet elke consument is bereid biometrische authenticatie te gebruiken. Zo kunnen er zorgen zijn over privacy en veilige opslag en gebruik.
Ook het gebruik van vingerafdrukken om criminelen te identificeren kan bijvoorbeeld een reden zijn om deze techniek af te wijzen.
Het is daarom van groot belang dat consumenten zelf de keuze kunnen maken tussen “reguliere” authenticatievormen (zoals een pincode of wachtwoord) en het gebruik van biometrie.

4. Gebruikte technieken en innovatie

4.1 Vingerafdrukherkenning

Vingerafdrukherkenning wordt al sinds 2015 toegepast bij mobiel bankieren. Het is de meest gebruikte biometrische techniek die zowel in iOS van Apple als in Android wordt ondersteund. Alle high-end mobiele toestellen hebben inmiddels een vingerafdruksensor. De werking van deze sensor kan wel verschillen, waarbij de kwaliteit van de implementatie de betrouwbaarheid bepaalt. Moderne sensors maken bijvoorbeeld een 3D-beeld van de vingerafdruk en kunnen die onder verschillende hoeken controleren.
Belangrijk is dat de vingerafdruk niet als beeld wordt opgeslagen, maar in de vorm van een “template” wordt gecodeerd en dat ook wordt gecontroleerd of er een levende vinger wordt gebruikt.
Bij vingerafdrukherkenning wordt de controle in het mobiele toestel uitgevoerd, waardoor de risico’s voor privacy gering zijn. Doordat in een toestel meerdere vingers kunnen worden geregistreerd, is het niet met zekerheid te zeggen of de vinger van de rechtmatige eigenaar is gebruikt. Daarom wordt bij het inschakelen van vingerafdrukherkenning in een bancaire app de gebruiker expliciet gevraagd te bevestigen dat alleen zijn eigen vinger(s) zijn geregistreerd.

4.2 Irisscanning

Irisscanning technologie komt geleidelijk in de nieuwe high-end toestellen beschikbaar (zoals de Samsung S8). Deze technologie vereist aparte sensoren in het toestel en is dus nog beperkt beschikbaar. Ook de gebruiksvriendelijkheid moet zich nog bewijzen.

Het registreren van de irissen gebeurt voor slechts één persoon, waarmee een beter bewijs van de rechtmatige eigenaar te maken is. Uiteraard blijft het de verantwoordelijkheid van de eigenaar om te borgen dat de eigen ogen zijn geregistreerd. Ook bij irisherkenning wordt de controle in het toestel uitgevoerd wat de privacyrisico's beperkt.

4.3 Gezichtsherkenning

Gezichtsherkenning ("selfie") werkt met de standaardcamera van de smartphone en is dus in principe breed beschikbaar. Er is een grote variatie in betrouwbaarheid, veel implementaties kunnen worden misleid door een foto of filmpje van de gebruiker te laten zien.

De "liveness check" bij gezichtsherkenning kan op verschillende manieren worden geïmplementeerd. Bekende voorbeelden zijn knipperen met de ogen of glimlachen. Ook bestaat een techniek waarbij met op het scherm wisselende kleuren worden geprojecteerd die op het gezicht weerkaatsen en centraal worden gecontroleerd.

Gezichtsherkenning wordt zowel uitgevoerd met centrale controle (zoals MasterCard Identity Check of "selfie pay") of met decentrale controle (zoals het unlocken van een Samsung S8).

Belangrijk is dat het voor de gebruiker duidelijk is of er gebruik wordt gemaakt van irisscanning of gezichtsherkenning als deze twee technieken door elkaar kunnen worden gebruikt.

4.4 Stemherkenning

Stemherkenning wordt zowel gebruikt om instructies in te voeren (zoals met Siri van Apple[3]) als om personen te authentiseren (zoals ING stem-bankieren). In principe zijn dit verschillende toepassingen. Zo kan via Siri een opdracht worden gegeven voor een betaling, die vervolgens in de bankieren app met een vingerafdruk of pincode wordt bevestigd. Maar bij stem-bankieren[4] kan juist een analyse van het stem-patroon worden gemaakt om te controleren of de juiste persoon de opdracht geeft.

4.5 Behavioral biometrics

Behavioral biometrics is een verzamelnaam voor het controleren op een aantal verschillende gedragskenmerken. Voorbeelden zijn het snelheidspatroon bij het typen van tekst, het gebruik van de muis of het touchscreen.
Al deze patronen zijn in zekere mate persoonsgebonden en kunnen als (aanvullende) controle voor het vaststellen van de juistheid van de gebruiker worden ingezet.

Het voordeel van deze technologie is dat doorlopend kan worden gecontroleerd of de juiste gebruiker aanwezig is, want het tempo van typen kan tijdens een hele sessie worden gemonitord. Deze techniek leent zich sterker voor gebruik op een PC of laptop. Behavioral biometrics kan daarbij een aanvulling zijn op het gebruik van klassieke of biometrische authenticatie om toegang tot een systeem te krijgen. De controle vindt centraal plaats, bijvoorbeeld in een systeem van de financiële instelling.

[3] https://www.ing.nl/nieuws/nieuws_en_persberichten/2017/01/ing_introduceert_siri_in_mobiel_bankieren_app.html

[4] https://www.ing.nl/nieuws/nieuws_en_persberichten/2015/07/ing_maakt_betalen_met_stem_en-vingerafdrukherkenning_mogelijk_in_mobiel_bankieren_app.html

5. Conclusies en aanbevelingen

De technologie voor biometrische authenticatie kent een snelle ontwikkeling. Hoewel vingerafdruklezers en andere technieken al lange tijd bestaan, werd de techniek pas echt populair met de introductie van Touch ID door Apple in 2015. Sinds die tijd wordt de techniek door financiële instellingen ingezet in mobiel bankieren en betalen apps. Dit is versterkt doordat ook in Android de techniek nu wordt ondersteund. Ook andere vormen van biometrie zijn in gebruik, zoals bijvoorbeeld stemherkenning.

- Biometrie kan **bijdragen** aan de veiligheid van betalingsverkeer doordat sterke klantauthenticatie eenvoudiger in het gebruik wordt. Daarmee is sterke klantauthenticatie met gelijkblijvend gebruiksgemak vaker toepasbaar, zoals bij het doen van een betaling.
- De mate van veiligheid is echter **sterk afhankelijk van de kwaliteit** van implementatie, zowel voor het proces (registratie) als de gebruikte techniek. Er is veel innovatie en internationale standaarden zijn nog in ontwikkeling. Onafhankelijke certificatie is nog niet beschikbaar.
- De **privacy regelgeving** is vanaf 2018 met de invoering van de General Data Protection Regulation verder aangescherpt voor opslag van persoonlijk identificeerbare informatie.
- **Juridisch** zijn er nog de nodige **onzekerheden** over regelgeving en mogelijke betwistingen.

5.1 Conclusies

Veiligheid

De veiligheid van biometrische authenticatie is sterk afhankelijk van de kwaliteit van implementatie. Hierin zijn grote verschillen mogelijk, waardoor financiële instellingen specifieke keuzes moeten maken welke technieken ondersteund worden, en welke verdere maatregelen voor risicobeperking worden genomen. Deze maatregelen worden door elk van de financiële instellingen apart bepaald en door de toezichthouder getoetst.

In de huidige apps zijn de mogelijkheden voor transacties met vingerafdruklezers gelijk aan die met mobiele pincodes zijn ingegeven. Transacties die zo worden toegestaan zijn bijvoorbeeld onder een bepaald maximum bedrag of betreffen overboekingen naar reeds bekende rekeningnummers.

Ook bij (toekomstige) verwerking van rekeninginformatie of transacties via betalingsdienstaanbieders (PSD2) houdt de bank de verantwoordelijkheid voor de veilige communicatie en afhandeling van de biometrische gegevens.

Goede communicatie van de veiligheidsmaatregelen door de financiële instelling naar de gebruikers is van groot belang voor veilig gebruik en maatschappelijke acceptatie.

Privacy

Opslag en gebruik van biometrische gegevens is aan sterke regelgeving onderworpen. Toepassingen dienen daarom zorgvuldig te worden getoetst aan Europese regelgeving zoals de General Data Protection Regulation (2018).

Robuustheid

Hoewel er sprake is van diverse internationale standaarden voor de werking van biometrische authenticatie, is er (nog) geen onafhankelijke toetsing of certificatie. Daardoor is er een grotere afhankelijkheid van de beoordeling kwaliteit van implementatie door de verschillende leveranciers.

DNB beschouwt het identificeren en authentiseren van klanten en betalingen als wezenlijke bedrijfsprocessen voor een financiële instelling. Dat betekent dan ook dat de biometrische oplossingen gezien worden als een mogelijke vorm van uitbesteding. Als gevolg daarvan dient een financiële instelling passende maatregelen te treffen voor de beheersing van de risico's en het monitoren daarvan.

Toegankelijkheid

Biometrie kan de toegankelijkheid van het betalingsverkeer vergroten. Vroegtijdige afstemming met specifieke doelgroepen bij het ontwerp van toepassingen is daarbij van belang.

Efficiency

Biometrie voor (mobiel) bankieren en betalen vergroot in de eerste plaats het gemak van sterke klant authenticatie.

Barrières

Het is belangrijk dat de gebruiker de keuze houdt voor het gebruik van een password of pincode naast het mogelijke gebruik van een biometrisch kenmerk zoals een vingerafdruk.
Voor meer juridische zekerheid is uitgebreidere jurisprudentie gewenst.

5.2 Aanbevelingen

5.2.1 Informeer de consument over de verschillende vormen van biometrische authenticatie

De gebruikte technieken voor biometrische authenticatie lopen sterk uiteen en het veiligheidsniveau is afhankelijk van de kwaliteit van de implementatie. Daarbij kan een toestel over meerdere authenticatievormen naast elkaar beschikken met onderling verschillende eigenschappen en veiligheid. Financiële instellingen die gebruik maken van biometrische authenticatie dienen hun klanten daarom op een effectieve manier in te lichten over het juiste gebruik en mogelijke alternatieven. Ook is het belangrijk om voor het ontwerp van de toepassingen vroegtijdig af te stemmen met de bij het MOB aangesloten belangengroepen zoals Ieder(in), Oogvereniging en ouderenorganisaties om de kansen voor betere toegankelijkheid van betalingsverkeer zo goed mogelijk uit te nutten.

5.2.2 Onderzoek de ontwikkelingen van biometrische authenticatie en standaarden

De technologie voor biometrische authenticatie is sterk in ontwikkeling. Fabrikanten van apparatuur innoveren doorlopend, daarnaast wordt in internationale standaarden door diverse partijen gewerkt aan classificering van de technologie en toepassingen. In de bijlage in bijlage 3 is een overzicht opgenomen van een aantal bekende initiatieven. Dit overzicht kan door het volgen van de markt in een werkgroep verder worden uitgewerkt waarbij de relevantie voor betalingsverkeer wordt geduid.

5.2.3 Onderzoek de mogelijkheid van onafhankelijke certificatie

De beoordeling van het veiligheidsniveau van specifieke implementaties wordt nu door verschillende bedrijven individueel gedaan omdat er geen onafhankelijke certificerende instantie aanwezig is. Dit vereist veel specifieke kennis en informatie. Indien een onafhankelijk (internationaal) certificatiestelsel aanwezig is, kunnen de verschillende partijen daarnaar verwijzen.

De ontwikkelingen op dit gebied vereisen een goed uitgewerkt normenstelsel, wat ook voldoende ruimte moet bieden voor verdere innovaties.
Als dergelijke normen zijn vastgesteld kan voor specifieke gebieden een certificatiestelsel ingericht worden als daarvoor voldoende draagvlak bestaat. Geadviseerd wordt om ook op het gebied van certificatie de marktontwikkelingen in de Werkgroep Veiligheid te volgen en de mogelijkheden voor toepassing aan te geven met behoud van innovatie mogelijkheden.

5.2.4 Inventariseer het juridische kader (wetgeving en jurisprudentie)

In deze nota zijn de juridische aspecten slechts beperkt geadresseerd. Verdere analyse is nodig om de impact van privacywetgeving voor de opslag en verwerking van biometrische gegevens door banken en betaaldienstverleners te bepalen. Ook de jurisprudentie voor betwiste transacties op basis van biometrische authenticatie en onrechtmatig gebruik zal meer duidelijk moeten worden.

Financiële instellingen, verwerkende bedrijven en winkeliers worden gewezen op het grote belang van veiligheid en privacy bij de opslag en verwerking van persoonskenmerken. Regelgeving zoals Payment Services Directive 2, de bijbehorende Regulatory Technical standards en de General Data Protection Regulation zijn daarbij maatgevend.

6. Bijlage 1: Verschillende implementaties

6.1 Vingerafdrukherkenning

Bij de meeste banken[5] is het mogelijk om met vingerafdruk in te loggen, te betalen en andere bankzaken te regelen. Deze functie werkt met Touch ID van Apple (gebruikt in iPhone of iPad) met iOS versie 9 of hoger, en op de meeste Android toestellen met vingerafdrukherkenning met versie 6 of hoger.

Sinds november 2016 is het mogelijk voor klanten bij bunq om hun vingers te scannen bij het bevestigen van betalingen. Deze 4 Fingers Touchless ID verificatietechniek is ontwikkeld door technologiebedrijf Veridium. Door het houden van vier vingers van één hand bij de camera kan worden vastgesteld of de hand behoort bij de rekeninghouder.

Mastercard kondigde in april 217 aan pilots afgerond te hebben in Zuid-Afrika voor een biometrische creditcard, een kaart met ingebouwde vingerprintscanner. In de chip van de kaart kunnen 2 vingerafdrukken bewaard worden. Meer tests volgen binnenkort in Europa en Azië[6].

Apple werkt momenteel aan een vervanger voor Touch ID,; de vingerafdrukscanner wordt in het scherm verwerkt en niet meer in een aparte knop. Deze Iphone8 versie zal in september uitgerold worden, al kan deze datum naar achteren schuiven door technische problemen waar het bedrijf tegenaan loopt[7].

6.2 Gezichtsherkenning

Selfiepay / Identity Check app
Samen met Mastercard heeft ABNAMRO onder de naam Selfiepay een proef gedaan van augustus 2016 t/m januari 2017 (na verlenging) met 750

[5] ABNAMRO, ING, RABOBANK, SNS, BUNQ

[6] http://www.nu.nl/internet/4633182/mastercard-test-betaalkaart-met-vingerafdrukscanner.html

[7] https://www.iphoned.nl/nieuws/iphone-8-vingerafdrukscanner-touch-id/

creditcardhouders om middels het maken van een selfie te betalen[8]. Het systeem werkt bij toestellen zonder vingerafdruklezer met een vorm van gezichtsherkenning, waarbij een video van de gebruiker gemaakt wordt. Om fraude te voorkomen moeten de gebruikers met de ogen knipperen.

Na de proef in Nederland zijn met de Mastercard Identity Check app ook proeven gedaan in Verenigde staten en Canada. Volgens Mastercard zal de app in de loop van 2017 in een groot aantal landen waaronder Nederland worden uitgerold.

Video identificatie

Bij sommige online banken zoals bunq en N26 kan men een bankrekening openen zónder geld over te maken vanaf een andere rekening door een videogesprek in het Engels aan te gaan waarbij men een identiteitsbewijs toont. Na registratie en controle van de gegevens wordt de bankrekening aangemaakt[9].

6.3 Stemherkenning

Particuliere klanten van ING kunnen gebruik maken van spraakassistent Siri in de ING Mobiel Bankieren App. Met Siri kunnen klanten met hun stem een opdracht geven om geld over te maken of om geld te ontvangen via een betaalverzoek.

ING klanten kunnen ook gebruik maken van stemherkenning (stem-bankieren) om in te loggen of betalingen goed te keuren. Door drie keer de zin “luister naar mijn stem en je weet wie ik ben” uit te spreken wordt de app getraind de stem te herkennen; bij inloggen wordt de stem vergeleken met het profiel. Deze stembediening is genaamd Nina (“Nuance Interactive Natural Assistant”).

[8] http://newsroom.mastercard.com/eu/nl/press-releases/netherlands-first-test-country-for-credit-card-payments-with-identity-recognition-2/

[9] https://nl.groovehq.com/knowledge_base/topics/hoe-gebruik-ik-video-calls-voor-verificatie

6.4 Diverse waarschuwingen bij instellen vingerafdruk

ING website[10]:

U heeft Mobiel bankieren zó in de vingers

Met uw vingerafdruk inloggen en betalingen bevestigen in de Mobiel Bankieren App. Dat kan op uw iPhone en iPad met Apple´s Touch ID. Het unieke patroon van uw vingerafdruk wordt gescand en geeft toegang tot de app. Lees hoe dat precies werkt. En hoe instellen gaat.

Hoe stelt u vingerafdruk in?

Ga op uw iPhone of iPad bij 'Instellingen' naar 'Touch ID en toegangscode'. Volg daar de aanwijzingen. Ga op uw iPhone of iPad bij 'Instellingen' naar 'Touch ID en toegangscode'. Volg daar de aanwijzingen. **Touch ID is beschikbaar vanaf iPhone 5s, iPad Air 2 en iPad 3 met iOS 8 of hoger**. Bekijk onderstaande video hoe u inloggen met vingerafdruk instelt in de Mobiel Bankieren App. Belangrijk: lees hoe u vingerafdruk in de app verstandig gebruikt.

Touch ID gebruikt een veilige chip

Volgens Apple geeft uw iPhone of iPad de gedetailleerde informatie over uw vingerafdruk nooit prijs. Niet in iCloud, niet bij Apple. Uw gescande vingerafdrukken staan alleen op een beveiligde chip op uw toestel. U vindt meer informatie op de site van Apple.

ABNAMRO website[11]:

Belangrijk om te weten

- Zorg ervoor dat uitsluitend uw eigen vingerafdrukken zijn geregistreerd op uw toestel als u die wilt gebruiken in de Mobiel Bankieren app. Misschien realiseert u zich niet dat er vingerafdrukken van anderen op uw toestel zijn geregistreerd. Controleer dit bij de instellingen van uw toestel.
- Bent u er niet zeker van dat alleen uw vingerafdrukken zijn geregistreerd? Verwijder dan alle vingerafdrukken en registreer opnieuw uw vingerafdrukken.
- Deel uw toestel niet met anderen als u uw vingerafdruk wilt inschakelen voor de app zodat anderen niet die van hun kunnen toevoegen. Wanneer een vingerafdruk wordt verwijderd of toegevoegd, krijgt u een melding op uw scherm dat het gebruik van deze functie in de app is geblokkeerd. U moet Touch ID/Vingerafdruk dan opnieuw inschakelen.

Let op: Hebben anderen ook hun vingerafdruk op het toestel geregistreerd? Als u die niet verwijdert, kunnen zij ook inloggen en bankieren in de Mobiel Bankieren app, bijvoorbeeld een overboeking doen vanaf uw rekening.

[10] https://www.ing.nl/particulier/mobiel-en-internetbankieren/mobiel-bankieren/inloggen-met-uw-vingerafdruk/touch-id-raakt-uw-bankzaken/index.html

[11] https://www.abnamro.nl/nl/prive/internet-en-mobiel/mobiel-bankieren/vingerafdruk/index.html

Rabobank website[12]:

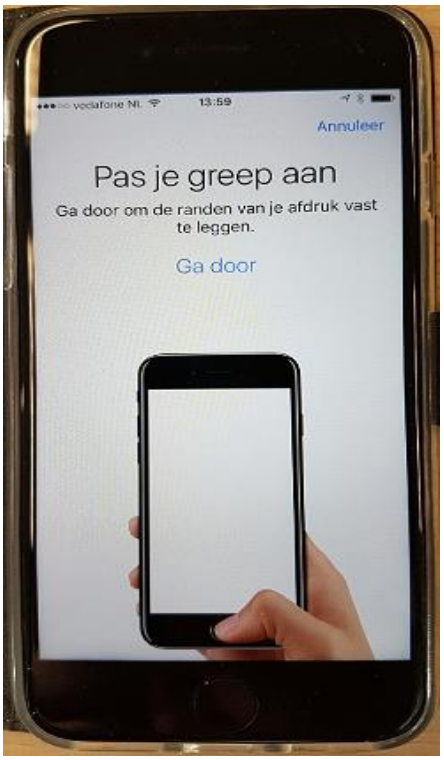
Hoe kan ik Touch ID veilig gebruiken?

Op een toestel kunnen meerdere vingerafdrukken geregistreerd zijn. Het kan zijn dat dit door meerdere gebruikers, zoals bijvoorbeeld gezinsleden, is gedaan. Het toestel van Apple beschouwt al deze afdrukken echter als afkomstig van dezelfde persoon.

Hierdoor zou iedereen met een geregistreerde vingerafdruk kunnen bankieren met de Rabobank Bankieren App op uw toestel.

Stel de vingerafdruk alleen in voor die personen die u ook toegang wilt geven tot uw telefoon. Wij raden u aan om dit alleen voor uzelf te doen als u Touch ID gebruikt voor de Rabo Bankieren App.

[12] https://www.rabobank.nl/particulieren/apps/rabo-bankieren-app/touch-id/?intcamp=pa-apps-nieuw.in.de.app&inttype=link-lees.meer&intsource=particulieren.apps.rabo-bankieren-app



Datum
11 mei 2017

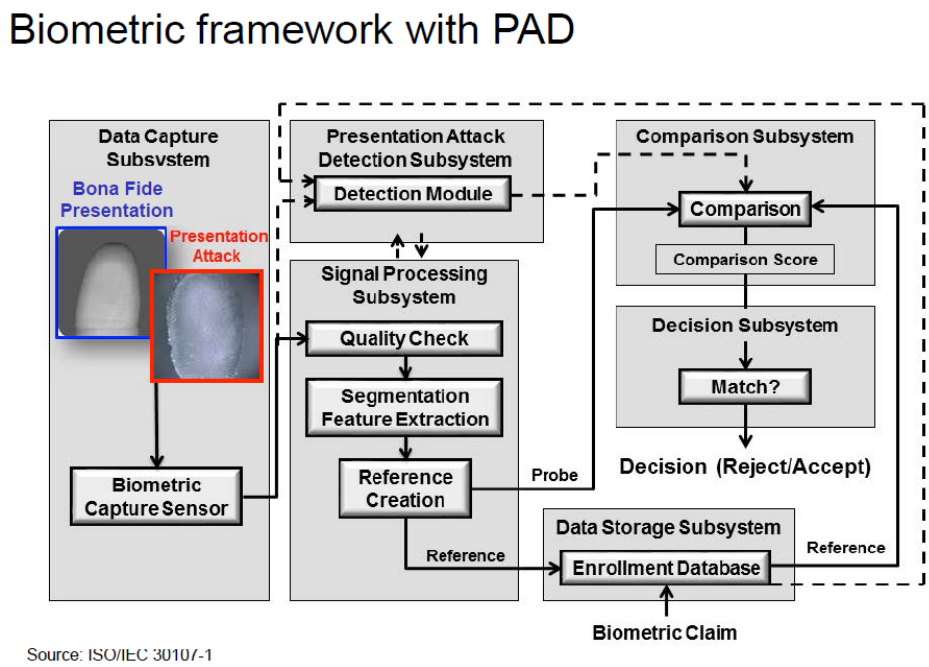
Kenmerk
MOB/ T018-1568171659-150

7. Bijlage 2: Technische aspecten

7.1 Opbouw van biometrische verificatiesystemen

De ISO standaard 30107 beschrijft hoe een biometrisch systeem met "presentation attack detection" is opgebouwd. Daarbij spelen de volgende onderdelen een rol:

- De sensor waarmee het biometrische kenmerk wordt afgelezen;
- Het subsysteem wat dit signaal verwerkt en in een referentieformaat ("template") vastlegt;
- De opslag van de referentiegegevens ("enrollment database");
- Het subsysteem wat bewaakt tegen valse kenmerken ("presentation attack detection");
- De vergelijking van het ingelezen kenmerk en het vastgelegde kenmerk;
- Het besluit over de juistheid van het ingelezen kenmerk;



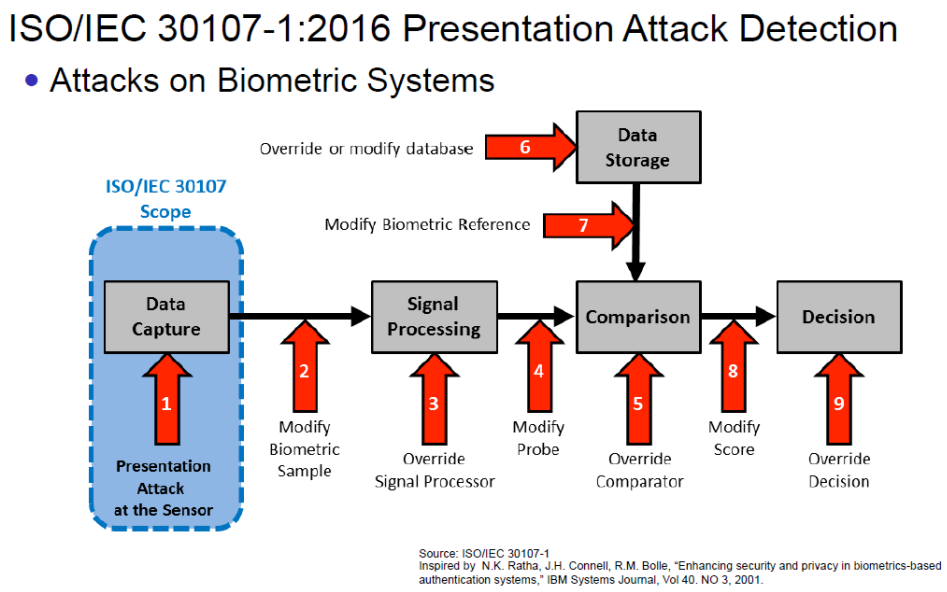
Source: ISO/IEC 30107-1

7.2 Aanvallen op biometrische systemen

Op basis van de gemodelleerde opbouw van het biometrische system is een classificatie van mogelijke aanvallen daarop gemaakt.

Daarbij wordt onderscheid gemaakt in de volgende aanvallen:

- Misleiden van de sensor (“presentation attack”)
- Wijzigen van het ingelezen kenmerk;
- Aanpassen van de signaalverwerking;
- Wijzigen van de opgeslagen referentiegegevens;
- Wijzigen van het controle mechanisme;
- Wijzigen van de besluitvorming.



8. Overzicht van standaardisatie

Standaardisatie op het gebied van biometrie is te verdelen in de volgende gebieden:

- Uitwisselbaarheid
- Kwaliteitsbeoordeling
- Toepassing
- Detectie van misbruik
- Best Practices (Technical Reports)

De betreffende standaards worden in ISO/IEC verband ontwikkeld (SC37).

Naast de ISO/IEC standaardisatie is de FIDO Alliance (Fast Identity Online) belangrijk. De FIDO Alliance houdt zich bezig met standaarden voor veilige authenticatie zoals “Universal Second Factor” en een “Universal Authentication Framework”. Dit biedt een breed geaccepteerd kader voor gebruik van onder meer biometrische kenmerken bij authenticatie. Er is echter nog een debat gaande hoe de FIDO standaard zich verhoudt tot de voorgestelde EBA regelgeving (RTS on Strong Customer Authentication).

8.1 ISO/IEC standaarden

ISO/IEC SC37 Biometrics
Established by JTC 1 in June 2002 to ensure a high-priority, focused and comprehensive approach worldwide for the rapid development of formal generic biometric standards

Scope of SC37
“Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects”

ISO/IEC 24713-1:2008(en)
Information technology — Biometric profiles for interoperability and data interchange — Part 1: Overview of biometric systems and biometric profiles
https://www.iso.org/obp/ui/#iso:std:iso-iec:24713:-1:ed-1:v1:en

ISO/IEC 19785-2:2006(en)
Information technology — Common Biometric Exchange Formats Framework
ISO/IEC 19785 consists of the following parts, under the general title Information technology — Common Biometric Exchange Formats Framework:
— Part 1: Data element specification
— Part 2: Procedures for the operation of the Biometric Registration Authority
The following part is under preparation:
— Part 3: Patron Format Specifications

ISO/IEC TR 29144:2014(en)
Information technology — Biometrics — The use of biometric technology in commercial Identity Management applications and processes

ISO/IEC 19784 consists of the following parts, under the general title Information technology — Biometric application programming interface:
— Part 1: BioAPI specification
— Part 2: Biometric archive function provider interface
— Part 4: Biometric sensor function provider interface

ISO/IEC 24709 consists of the following parts, under the general title Information technology - Conformance testing for the biometric application programming interface (BioAPI):
https://www.iso.org/obp/ui/#iso:std:iso-iec:24709:-2:ed-1:v1:en
— Part 1: Methods and procedures
— Part 2: Test assertions for biometric service providers
The following parts are under preparation:
— Part 3: Test assertions for BioAPI frameworks
— Part 4: Test assertions for biometric applications

ISO/IEC 30107 consists of the following parts, under the general title Information technology — Biometric presentation attack detection:

— Part 1: Framework

— Part 2: Data formats

— Part 3: Testing and reporting

ISO/IEC TR 30125:2016(en)

Information technology — Biometrics used with mobile devices

https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:30125:ed-1:v1:en

This Technical Report provides guidance for developing a consistent and secure method of biometric (either alone or supported by non-biometric) personalization and authentication in a mobile environment for systems procured on the open market.

Guidance is provided for

— 1:1 verification or 1:few positive identification;

— biometric sample capture in the mobile environment where conditions are not well controlled and not covered in ISO/IEC Biometric interchange format standards and the ISO/IEC Biometric sample quality Technical Reports;