Universitetet i Oslo

IN2120 – Midtsemesteroppgave

T120: Security Comparison of Vipps and Apple Pay

Kandidatnummer deltaker 1:

Kandidatnummer deltaker 2:

Høst 2021

Innholdsfortegnelse

Innledning

Viktigheten av systemsikkerhet

I dagens digitaliserte samfunn, blir sikkerhet mer og mer viktig. Når det meste av vår kommunikasjon skjer digitalt, er det viktig at vi tar hensyn til at det foregår under sikre omstendigheter. Det er mye informasjon som strømmer gjennom internettet hele tiden: mennesker chatter og sender meldinger til hverandre, bedrifter kommuniserer gjennom e-post og andre digitale tjenester. Til og med de offentlige tjenestene har gått gjennom en digitaliseringsrevolusjon. Før måtte folk stå i lange køer for å betale regninger. Nå har banker utviklet nettløsninger, der brukere kan betale regninger og sende summebeløp til andre, kun ved å trykke på en knapp. Eksempler på det er Vipps og Apple Pay, som er to adskilte utviklede nettbaserte betalingsløsninger som skal gi mulighet til sine brukere å kunne betale til ulike aktører innen ulike bransjer ganske enkelt.

All denne informasjonen som strømmer over nettet, står i fare for å lekke og bli misbrukt, hvis utviklere, forvaltere, og brukere av tjenester med informasjonsoverføring, informasjonsprosessering og informasjonslagring i databaser og i plattformer, ikke passer godt på. Sensitive personopplysninger er spesielt viktig å ta vare på. Viktigheten av ivaretagelse for sikkerheten av personopplysninger er til og med spesifisert i lover og regler, som for eksempel GDPR (General Data Protection Regulation), personvernlovverket, som har som formål å beskytte individers sikkerhet av deres personopplysninger som er brukt, sendt, lagret og/eller overført i digitale tjenester.

Mulige konsekvenser ved dårlig ivaretatt personvern er, at informasjonen kan lekke. Som resultat kan den bli fanget opp av trusselaktører som kan misbruke den, enten ved tilsiktede eller utilsiktede skader. Eksempler på misbruk av personvern er identitetstyveri, bedrageri, økonomisk tyveri, trusler og manipulasjoner. Mer konkrete eksempler jan være, at noen framstille seg for deg for å få tak i annen informasjon, utføre betalinger fra din konto, sperrer din tilgang til dine brukerkontoer, bruker det for å manipulere deg gjennom direkte trusler, for eksempel ved å kreve et pengebeløp mot å gi deg tilbake tilgangen, osv.

Som vi skjønner, er det veldig viktig å kunne vite hvordan beskytte informasjon riktig. Derfor har “SC27”, en subkomite av «International Organization for Standardization» sammen med «International Electrotchnical Comission» utviklet en internasjonalt standartmodell ved navn ISO «Information technology – Security techniques – Information security management

systems – Overview and vocabulary» (*ISO/IEC 2700, Wikipedia*). Denne standardmodellen definerer informasjonssikkerhet slik:

"Informasjonssikkerhet er beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet. I tillegg kan andre egenskaper, for eksempel autentisitet, sporbarhet, uavviselighet og pålitelighet, omfattes» (*Jøsang, 2021, s.17*). Konfidensialitet, integritet og tilgjengelighet er samlet sammen under begrepet KIT-sikkerhetsmålene. Det er bestemt, at disse står sentralt i informasjonssikkerhet. Autentisitet, sporbarhet, uavviselighet og pålitelighet kommer i tillegg.

ISO 2700 definerer videre begrepene konfidensialitet, integritet og tilgjengelighet slik:

- «Konfidensialitet er egenskapen av at informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.» (Jøsang, 2021, s.22)
- «Integritet er egenskapen av å opprettholde korrekthet og kompletthet av dataressurser.» (Jøsang, 2021, s.23)
- «Tilgjengelighet er egenskapen av at data og tjenester er tilgjengelige og anvendbare ved forespørsel fra en autorisert entitet.» (Jøsang, 2021, s.24)

Autentisitet brukes som et adjektiv på det som er ekte, sann, oppriktig og troverdig (Det Norske Akademi for Språk og Litteratur, 2021). Sporbarhet vil si at eventuelle hendelser skal kunne spores tilbake, slik at det kan være klart hvem som skal stå til regnskap for bestemte handlinger og hendelser. Uavviselighet innebærer, at identiteter skal knyttes opp til et dokument, en transaksjon eller lignende, slik at det spiller rollen av en signatur som ikke kan benektes å ha blitt signert av den som har utført signeringen (Fornyings- og administrasjonsdepartementet/Kommunal- og moderniseringsdepartementet/Regjeringen, 2008). Pålitelighet er egenskapen av at systemer ikke inneholder mange, eller noen feil. Dersom feil forekommer i et system, så betyr pålitelighet, at de feilene kan bli tolerert av systemet uten at funksjonalitet faller ut. (*Jøsang, 2021, s.28*)

Brudd på konfidensialitet, integritet eller tilgjengelighet fører til skade av informasjonsverdiene.

Kravene om informasjonssikkerhet stammer fra tre kilder: 1. «Krav om adekvat sikkerhet i applikasjoner og forretningsprosesser i henhold til standard praksis og forvaltning», 2. «Krav om å begrense sikkerhetsrisiko til et akseptabelt nivå.» og 3. «Juridiske lovbestemmelser, regulatoriske og kontraktsmessige krav til informasjonssikkerhet» (Jøsang, 2021, s.18).

Det finnes en rekke tiltak som støtter KIT-sikkerhetsmålene. Tiltakene deles inn i forebyggende, oppdagende, og korrektive tiltak. Forebyggende tiltak handler om å kunne forhindre inntreffelsen av hendelser, og reduserer sannsynligheten for sikkerhetshendelser. Oppdagende tiltak, er de tiltak som iverksettes for å oppdage eventuelle hendelser som har inntruffet, og korrektive tiltak skal korrigere etter hendelser, ved å gjenopprette drift og reparere den skade som er mulig.

En annen type kategorisering for sikkerhetstiltak, er å sortere dataen dens nåværende tilstand. Det kan være under lagring, under overføring, eller under prosessering. Den tredje mulige inndelingen av sikkerhetstiltak, er om de er fysiske, som f.eks. låser, kameraovervåkning, alarm, om de er tekniske, for eks. brukerautentisering, kryptering, nettverkssikkerhet, eller er de organisatorisk, som f.eks. policyer, sikkerhetskultur, hendelseshåndtering osv (Jøsang, 2021, s.21).

Oppgavebeskrivelse

I denne oppgaven skal vi presentere de applikasjonsbaserte mobilbetalingsløsningene Vipps og Apple Pay. Vi skal se på deres funksjonalitet og sikkerhetstiltak. Vi kommer til å drøfte informasjonssikkerheten som blir forvaltet i nettbetalingsløsningene Vipps og Apple Pay for å støtte KIT-sikkerhetsmålene. Til slutt skal vi sammenligne metodene og de implementerte løsningene som de bruker for å støtte KIT og for å opprettholde en god sikkerhetsledelse og sikkerhetskultur.

Vipps

Hva er Vipps?

Vipps er en applikasjonsbasert mobilbetalingsløsning, som er utviklet av det norske selskapet Vipps AS. Løsningen ble utviklet med formålet å kunne bidra til et samfunn med ny teknologi i bruk. I utgangspunktet var tjenesten laget for DNB, og lansert av dem som en digital betalingsløsning for smarttelefoner i 2015. I 2018 fusjonerte tjenesten sammen med BankID og BankAxept, hvor av den store suksessnøkkelen forekommer. De tre fusjonerte sammen til det nye selskapet Vipps AS og ble til Nordens største aktør innen betaling og identifisering (Eika, 2021). Etter hvert ønsket også flere og flere banker samarbeid med Vipps AS, helt til at

tjenesten ble videreutviklet til å kunne brukes av alle uavhengig av hvilken bank de er kunder av, så lenge de har et fungerende kontonummer i en norsk bank, og et norsk telefonnummer. Selv om Vipps eies av flere selskaper i dag, har DNB behold sin posisjon som den største eieren med hele 52% eierandel (Nysveen/E24, 2017). Vipps samarbeider også med EMPSA, den europeiske mobilbetalingsassosiasjonen, der de samarbeider om å muliggjøre bruk av Vipps også i utlandet (Wikipedia, 2021).

Vipps tilbyr ulike transaksjonstjenester, som blant annet er betaling på internett, i applikasjoner, og i fysiske butikker. Appen er utformet til å passe både for privatpersoner, og bedrifter, organisasjoner, lag, foreninger og innsamlingsaksjoner, der man har mulighet til å sende og motta penger til og fra disse. I tillegg er det mulig å betale regninger ved hjelp av Vipps Regninger, eller betale eFaktura.

Hvordan fungerer tjenesten?

Overføringen av penger mellom private mennesker, skjer ved å kun oppgi mottakeren sitt telefonnummer, istedenfor kontonummer. Dette bidrar i seg selv til en bedre sikkerhet av kontoer, og økt konfidensialitet, ved at kontonumre kan forbli hemmelige selv under transaksjoner. Denne metoden fører også til økt effektivitet, i og med at penger overført gjennom Vipps havner øyeblikkelig i mottakeren sin konto, mens overføring ved bruk av kontonumre ved nettbank tar en viss tid til mottakeren får pengene. Vipps har også funksjoner som gjør det mulig å forespørre om pengebeløp fra bestemte personer. De fra sin tur kan velge å godta forespørselen og sende beløpet, eller avvise den, kun ved å trykke på forespørselen. I tillegg finnes det adskilte chatterom til hver eneste kontakt. Den kan man for eksempel bruke for å avklare pengebeløp og detaljer ved bruk av summen.

Vipps kan også brukes til å betale i terminaler i fysiske butikker. Denne funksjonen baserer seg på BankAxept. Derfor er det en forutsetning om en allerede etablert BankAxept-brukerkonto i utvalgte banker som støtter Vipps i betalingsterminaler, for å kunne bruke denne funksjonen (Vipps, 2021). Slike betalinger utføres ved at en QR-kode vises i betalingsterminalen og skannes av Vipps applikasjonen. Da vil det dukke opp en betalingsforespørsel i appen, som består av beløpet som forespørres og mottakernavnet. Når betalingsforespørselen bekreftes, vil betalingen bli akseptert av betalingssystemet, og brukeren vil få en bekreftelse på det i Vipps.

For å bruke Vipps må man først ha et norsk telefonnummer, personnummer, folkeregistrert adresse, e-post, bankkonto i en norsk bank, norsk bankkort, enten Visa eller Mastercard, og BankID (Vipps, 2021). Utviklerne av appen valgte å ha det slik for å kunne tilby en sikker mobilbetalingstjeneste i landet.

For å registrere seg i Vipps, må en allerede ha registrering i BankID. BankID er en personlig og enkel elektronisk legitimasjon for sikker identifisering og signering på nettet (BankID, 2021). BankID brukes både som en legitimasjon i den digitale verden i Norge, og til elektronisk signering av dokumenter. BankID er godkjent etter EU-standarden eIDAS nivå 3 «High», som tilsvarer nivå 4 «High» i det norske rammeverket for autentisering og uavviselighet RAU (Jøsang, 2021, s.131). Tjenesten er basert på to-faktor-autentisering, der den ene faktoren er en dynamisk engangskode du får generert gjennom kodebrikke, kodekort, SMS, app osv. Den andre faktoren er ditt personlige, statiske passord. Koden er noe du har, mens passordet er noe du kan. Bruker ID-en er personnummeret. Personnummer pleies å holdes ganske konfidensielt til vanlig, derfor kan også dette betraktes som en faktor til, under autentiseringen, ved visse argumenter, der dette argumentet er et av dem.

BankID-registeret, som tilhører eierselskapet Vipps, er en føderert identitetsdomene. Dette betyr, at de registrerte ID-ene og autentiseringsfunksjonene i BankID, benyttes som en felles ressurs av flere tjenestetilbydere. Tjenestetilbyderne som bruker BankID, må betale til Vipps hver gang de autentiserer en bruker (Jøsang, 2021, s.140).

Vipps har satt to typer beløpsgrenser for bruk av applikasjonen, for å beskytte sine brukere. Den ene grensen setter begrensning på hvor store beløp man kan sende ved ulike autentiseringsmetoder. Beløper inntil 5000 krever en autentisering med FaceID, TouchID, eller pin-kode. Høyere beløp krever en tofaktor-autentisering, med BankID i tillegg til FaceID eller TouchID. I tillegg betales det et gebyr for transaksjoner over 5000, mens transaksjoner under dette beløpet er kostnadsfrie. Den andre beløpsgrensen er en årlig grense, som består av mottaksgrensen på maksimalt 700 000kr på 1 år for private, og 650 000kr for bedrifter, mens avsendergrensen er 850 000 per år for private. Når de årlige grensene blir oppnådd vil ikke bruk av Vipps være mulig inntil grenseperioden er over (Vipps, 2021). Slik øker sikkerheten, mens risikoen for kriminalitet og misbruk reduseres.

Så hvordan klarer et så stort selskap med så avansert teknologi, og bruk av sensitive personopplysninger, klare å holde seg sikker, selv med over 3,9 millioner brukere?

Opplysninger som brukeren oppgir ved registrering lagres ikke på selve enheten, men er kun synlige i Vipps applikasjonen. Dette er nødvendig for identifisering og administrering av kundeforholdet. Brukerautentiseringen i Vipps krever fødselsnummer for å kunne opprettholde en sikker identifisering av brukerne. Informasjon som brukere oppgir ved autentisering, lagres heller ikke på enheten (Vipps, 2020). Når betalingstransaksjoner skal gjennomføres blir kontoopplysninger og kortinformasjon knyttet til pengekilden behandlet. Disse lagres heller ikke på enheten, men de er synlige i applikasjonen.

Beskyttelse av brukerprofil i Vipps er basert på bruker-PIN-koden som brukeren lager ved registrering. Vipps lagrer denne pinkoden som autentikator for den bestemte identiteten i sine databaser. Vipps lagrer i tillegg enheten, enhetens operativsystem, og mobilidentifikatoren, som tilhører selve mobilenheten og er unik (Vipps, 2020). Dette er Vipps sin sikkerhetstiltak for systemautentisering. Ved innlogging må brukeren oppgi pinkoden, slik at systemet kan sjekke om det stemmer med det som er lagret i deres databaser, og dermed godkjenne innloggingen hvis innloggingsinformasjonen er korrekt.

Sporbarhet i Vipps støttes gjennom sikkerhetstiltakene om aktivitetslogg. Alle transaksjoner lagres, i tillegg til alle beskjedene i tilknytning til dem.

IAM – Identitets- og tilgangshåndtering i Vipps

Nå skal vi se på hvordan Vipps gjennomfører fasene i IAM (identitets- og tilgangshåndtering). Identitetshåndteringen er det første som må utføres for at tilgangshåndteringen i det hele tatt skal kunne ta plass. Begge består av en konfigureringsfase og en bruksfase.

Identitetshåndteringen trengs for å håndtere identiteter ved å definere hvem som er autorisert, samtidig som det defineres hvilke regler det gjelder for de autoriserte. Dette setter grunnlaget for at tilgangshåndteringsfunksjonene skal kunne drives, nemlig fordi tilgang kan delegeres når det er klart (spesifisert) hvem som er autorisert til det, og hvem som ikke er det. (Jøsang, s.28)

Identitetshåndteringen forekommer i innloggings- og brukerregistreringssituasjoner. Ved registrering må brukeren oppgi informasjonen som Vipps setter krav til, se i avsnittet «Hvordan fungerer tjenesten» på side 6. Da sender Vipps et automatisk oppslag til skatteetatens Folkeregister, som har registrert personopplysningene i sine registre, slik at de

kan utføre identifisering av brukeren og verifisere identiteten. I tillegg blir den oppgitte informasjonen sendt til verifisering også til BankID. Når vedkommende er bekreftet autentisk både fra folkeregisteret og BankID, vil brukerens identitet og bruker-ID blir registreres og lagret hos ressurseieren Vipps. Under registreringsfasen blir det opprettet en kobling mellom brukerens telefonnummer og kontonummer, slik at det videre kan brukes kun mobilnummeret ved transaksjoner, mens kontonummeret kan forbli konfidensiell. Vipps og BankID klargjør autentikatorer for den bestemte identiteten, og overfører dem til tilhørende bruker (Vipps, 2021). Vipps autentikatorene gjelder for innlogging og transaksjoner med beløp opp til 5000kr, mens BankID klargjør autentikatorer for høyere beløp.

Da vil første trinnet fra identitetshåndtering gjennomføres. Det er at ressurseieren autoriserer brukeren ved å spesifisere tilgangsregler og tilgangspolicy for den bestemte brukeren i PAP (Policy Administration Point).

Når en bruker logger inn, er det igjen en del av identitetshåndtering, men under bruksfasen. Da må vedkommende aller først oppgi sine bruker-ID og autentikatore, som i dette tilfellet er f.eks. passord, FaceID eller TouchID. Autentiseringsfunksjonene sjekker om denne identiteten er registrert og autorisert i autentiseringstjeneren (IdP). Dersom informasjonen stemmer med det som er registrert i autentiseringstjeneren, blir brukeren slippet inn til systemet.

Tilgangskontroll utføres når brukeren allerede er logget inn på systemet, og kan sende forespørsler om tilgang til bestemte ressurser/tjenester som systemet tilbyr. Da setter systemet i gang med å sjekke om den bestemte identiteten er autorisert for tilgang til den forespurte ressursen. Systemet må gjennomføre en tilgangsautentisering gjennom prosessen kalt tilgangskontroll. Dette skjer ved at funksjonene for tilgangskontroll sjekker de etablerte policyene og reglene i PAP. Disse blir sett på av PDP (Policy Decision Point), som tar beslutningen om tilgang. Denne beslutningen blir håndhevet av PEP (Policy Enforcement Point) og tillater eller avviser den forespurte tilgangen til den bestemte ressursen.

Informasjonsdeling og -beskyttelse

Vipps kan i enkelte registrerings-, innloggings- og betalingssituasjoner dele noe informasjon om brukeren med brukerstedet. Dette skal gi brukerne mulighet til raskere registrering i de andre brukerstedene, samtidig som brukerstedene kan bruke informasjonen for å persontilpasse sine tjenester for den bestemte brukeren. I slike situasjoner deles informasjon

lagret i Vipps-brukerprofilen, som for eksempel fornavn og etternavn, adresse, e-postadresse, telefonnummer, fødselsdato og kontonummer. For at det skal kunne skje, må brukeren først oppgi sitt samtykke om informasjonsdeling til Vipps. Hvilke informasjon som deles avhenger av hva brukerstedet ber om, og hva som framkommer i samtykket (Vipps, 2020). Brukerstedet holdes ansvarlig for å behandle denne informasjonen i samsvar med beskyttelseskrav for personvern i fra GDPR (General Data Protection Regulering), den europeiske personvernfordringen. Brukere har muligheten til å sjekke i Vipps hvilke brukersteder informasjon deles med, og trekke sitt- samtykke om informasjonsdeling til ulike brukersteder. En slik beslutning vil stoppe videre datadeling med den bestemte brukerstedet. Likevel har disse brukerstedene mest sannsynlig lagret personopplysningene som de har fått tidligere i sin kundeadministrasjon.

Et eksempel på situasjoner hvor denne informasjonsdelingen finner sted er ved bruk av funksjonen «Vipps Logg inn». Den tillater brukere å kunne logge seg inn, eller registrere seg, på andre brukersteder gjennom Vipps. Dette brukes mye for eksempel i restauranter, utesteder, og andre steder som krever en registrering av sine besøkende. Steder som krever registrering av brukerne vil på denne måten ikke trenge å bruke tid og ressurser på registrering. Samtidig vil de være sikre på at informasjonen de får inn gjennom Vipps innlogging er riktig, siden Vipps er basert på BankID. Dermed gjør løsningen prosessene svært enkle for både brukere og brukersteder. (Vipps, 2021)

Informasjonsdelingen i Vipps Logg inn baserer seg på informasjonskapsler, også kalt cookies. Dette er små midlertidige filer som lagres på enheten ved besøk av nettsiden (Nettvett, 2021). Disse slettes automatisk etter en viss tidsperiode og kan administreres under innstillingene. Bruker må først godkjenne cookies for at Vipps skal få lov til å dele dem videre. Vipps Logg inn sjekker om informasjonskapslene ikke er kopiert eller endret, ved å hente informasjon om nettleseren ved bruk av en sikkerhetsløsning (Vipps, 2021). Denne sjekken sørger for integritet, fordi her skal man bekrefte at informasjonen ikke er blitt endret eller kopiert av uautentiserte parter. Vipps overfører ikke informasjonskapslene til tredjeparter, og bevarer slik konfidensialitet.

Vipps er den eneste aktøren som har tilknytning til din identitet. Informasjon relatert til identiteten er beskyttet med høyeste krav til datasikkerhet og datatilgang (Vipps, 2020). For å kjenne igjen enhetene knyttet til den samme identiteten, bruker Vipps en informasjonskapsel med en unik tallverdi som genereres tilfeldig, og det er heller ikke mulig å avlede

vedkommende sin identitet ut ifra denne tallverdien. Slik fungerer den unike tallverdien som en unik nøkkel.

For å støtte sporbarhet, har Vipps innført følgende tiltak. Data om ens «Vipps Logg inn»-bruk, blir registrert og lagret. Dataene omfatter blant annet brukeratferd og enhetens tilstand. De blir brukt kun for å oppdage uvanlig atferd og detektere avvik fra normale verdier. Bare når det oppdages kan det motvirkes. Dermed kan de benyttes for å motvirke og eventuelt følge opp straffbare handlinger rettet mot den bestemte identiteten og/eller brukerstedet. Her antar vi, at Vipps setter en rekke policyer og standarder i samsvar med organisatoriske tiltak for sporbarhet, slik at dersom det oppstår en hendelse, kan noen stå til regnskap for aktiviteten/handlingen. «sporbarhet er basert på logging av aktiviteter i systemer og nettverk, og kartlegger hvilken bruker eller annen entitet som står bak hver logget aktivitet». (Jøsang, 2020, s. 27)

Dersom mobilen der du bruker Vipps blir mistet eller frastjålet mens Vipps-kontoen er aktiv, skal det meldes fra til Vipps så snart som mulig. Da vil Vipps foreta sperring av brukerkontoen. Dersom Vipps Logg inn også er aktivt på enheten, anbefaler Vipps, at du fjerner den for enheten, gjennom Vipps under «Profil».

Trusler

Phishing-angrep er et tekno-sosialt angrep, der trusselaktører sender falske meldinger gjennom f.eks. e-post eller SMS. Phishing gjennom SMS, blir også kalt «Smishing». Slike meldinger inneholder typisk falske lenker, etterfulgt av fristende meldinger som skal spille på mottakerens følelser og få han/hun til å svare ved å åpne lenken. Slike angrep kan for eksempel være kombinert med et drive-by-angrep, der besøk av lenken vil følge til automatisk nedlastning av skadevare på enheten, uten at mottageren får vite det. Et annet mål, kan være å få mottageren til å oppgi sensitiv informasjon på lenken. Denne informasjonen, eller direkte observasjon av mottagerens aktivitet på lenken, kan utnyttes av angriperen til å utføre man-in-the-middle-angrep. Slik har phishing angrep klart å bli den vanligste og mest brukte angrepsvektoren. «Fra omtrent år 2020 er phishing den desidert vanligste angrepsvektoren for cyberangrep og datakriminalitet på internett, ifølge FBI» (Jøsang, 2021, s.74).

Svindlere kan bruke slike typer angrep, til å for eksempel fiske opp brukerID, passord og BankID.

Vipps har vurdert dette trusselet og innført relevante tiltak. Gjennom sikkerhetslæring opplyser de folk om faren av at slike phishing-meldinger kan komme. Vipps velger derfor å aldri forespørre slik sensitiv informasjon, som f.eks. kortinformasjon, gjennom SMS eller e-post. Slik gjør de det klart og tydelig for sine brukere, at dersom de får slike meldinger, så bør de ikke svare. Hvis noen derimot vil sjekke profilstatusen sin må de gjøre det gjennom å logge seg inn på appen. Dersom en bruker likevel klarer å oppgi informasjon til en phishing-melding, må vedkommende varsle Vipps og banken sin umiddelbart.

Apple Pay

Hva er Apple Pay?

Apple Pay er en mobilbetalingsløsning utviklet av det amerikanske selskapet Apple i 2014. Tjenesten gjør betaling mulig gjennom Apple sine enheter: iPhone, iPad, Apple Watch og Apple Macintosh (Wikipedia, 2020). Tjenesten fungerer sammen med Apple Wallet, en iOS-applikasjon som gir opplevelsen av en digital lommebok, der du kan legge inn dine bankkort, gavekort, kuponger, bonuskort, billetter, boardingkort og lignende (Wikipedia, 2018). Apple Pay støttes av kun ni banker i Norge ((Monese, Monobank, Nordea, Revolut, Santander Consumer Finance, Sbanken, ST1, Komplett Bank og Storebrand).

Transaksjoner gjennom Apple Pay kan utføres både digitalt over internett til nettbutikker som støtter det, og i mobilapplikasjoner fra App Store, men også fysisk gjennom betalingsterminaler på butikker. Betalinger i betalingsterminaler utføres gjennom nærfeltskommunikasjon (NFC), kontaktløs betaling. Apple Pay kan også fungere sammen med kort fra MasterCard, Visa og American Express (Apple, 2021). Ved betaling gjennom Apple Pay, får brukerne belønninger som de kan bruke senere, som f.eks. bonus, kuponger eller rabatt.

Tjenesten, sammen med Apple Cash, gjør det mulig for brukere av Apple-enheter å kunne utføre sending og mottak av penger gjennom SMS. Denne funksjonaliteten fungerer for tiden kun i USA. (Apple, 2021)

Hvordan fungerer tjenesten?

Designet av Apple Pay skal beskytte personinformasjonen og sørge for dens sikkerhet. Det skjer ved at Apple Pay ikke tar vare på, eller har tilgang til, det originale kortet eller forhåndsbetalte kortnumre, som brukes med Apple Pay. Dessuten, blir det ikke beholdt noen transaksjonsinformasjon som kan kobles tilbake til brukeren (Apple, 2021). Slik forblir transaksjonen kun mellom vedkommende bruker, selger eller utvikler og utstederen av vedkommende sitt kart.

Pengeoverføringen gjennom Apple Cash, er en tjeneste som muliggjøres gjennom Apple partnerbanken Green Dot Bank. Green Dot Bank har ansvaret for beskyttelse av de personlige opplysningene mot uautoriserte. Dette kravet oppfyller de gjennom bruk av sikkerhetstiltak som er i samsvar med Federalloven i USA (AppleCash, 2017). Disse tiltakene inkluderer tekniske, fysiske og administrative sikkerhetstiltak for å opprettholde konfidensialitet, integritet og tilgjengelighet.

Hvis bruker ønsker å logge seg inn i Apple Pay på en ny enhet, vil det kreve en identifisering gjennom tofaktor-autentisering. Dette vil være krav også for konfigureringer. Tofaktor-autentiseringen baseres på en sekssifret verifiseringskode og passordet for Apple ID. Verifiseringskoden er en dynamisk autentiseringsenhet som blir generert av Apple gjennom SMS eller telefonanrop. Passordet er et selvvalgt statisk passord. Disse to faktorene i tofaktor-autentiseringen er helt uavhengige av hverandre og setter grunnlaget for det sterke autentiseringsmetoden som støtter KIT-sikkerhetsmålene (Jøsang, 2021, s.25 og s.129). Ifølge brukerhåndbok for iPhone bidrar tofaktor-autentiseringen til å hindre andre å få tilgang til AppleID-konto, selv om de kjenner til passordet (Apple, 2021).

IAM – Identitets- og tilgangshåndtering i Apple Pay

Aktivitetene rundt IAM, identitets- og tilgangshåndtering, er det mest sentrale i ethvert system. Derfor skal vi nå se på Apple Pay sin gjennomføring av disse IAM-aktivitetene, ved å starte først med identitetshåndtering, og deretter se på tilgangshåndteringen. Identitetshåndteringen i Apple Pay forekommer i innloggings- og brukerregistreringssituasjoner.

Som regel starter de fleste registreringsprosesser med at brukeren angir personlig informasjon, men slik er det ikke i Apple Pay. Grunnen til det er at alle Apple mobiltelefoner forespør

denne informasjonen og lager en Apple ID for den bestemte brukeren. Apple har den egenskapen, at det krever registrering og innlogging gjennom Apple ID for å kunne bruke enheten (Apple, 2021). Når du har laget en Apple ID en gang, for eksempel på mobilen, så kan du bruke den samme Apple ID-en til å logge deg på alle dine andre Apple enheter, som for eksempel Apple Watch, iPad, iMac. Slik lager og forvalter Apple sin egen register over sine brukeridentiteter, gjennom en silomodell for identitetshåndtering.

For å få tilgang til Apple Pay må du først være logget inn på enheten gjennom Apple ID. Derfor krever ikke Apple Pay registrering av en ny brukerkonto eller innlogging, fordi du er allerede identifisert og autentisert gjennom Apple ID. I dette tilfellet er Apple både ressurseier og autentiseringstjener. Slik kan Apple Pay hoppe over konfigureringsfasen for brukerregistrering.

Likevel trengs det å registrere betalingskort som brukeren ønsker å bruke i Apple Pay. Registreringen skjer ved at betalingskortet skannes. Sikkerhetsfunksjoner innebygde i maskinvaren og programvaren, krypterer den originale kortinformasjonen med en hemmelig symmetrisk, eller en offentlig asymmetrisk nøkkel på enheten. Den krypterte informasjonen blir sendt til Apple-tjeneren, gjennom nett (Apple, 2021). Krypteringen gjør det umulig for uautoriserte entiteter, som ikke har de riktige kryptografiske nøklene, å kunne lese informasjonsinnholdet. Slik brukes krypteringen her som et tiltak for å støtte konfidensialitet og integritet, og bevare systemsikkerheten.

Ressurseieren (Apple-tjeneren) sin autentisering av brukeren ved spesifisering av tilgangspolicy og -regler i PAP skjer på følgende måte. Apple-tjeneren, som har de riktige kryptografiske nøklene, dekrypterer kortinformasjonen med en hemmelig symmetrisk eller en privat asymmetrisk nøkkel. Deretter spesifiseres det et bestemt betalingsnettverk for det oppgitte kortet. Så blir informasjonen enkrypert igjen og de riktige kryptografiske nøklene blir levert til det spesifiserte betalingsnettverket, slik at kun den kan låse opp informasjonen for å bruke den ved betalinger (Apple, 2021). Krypteringen her skal sikre at dataen er korrekt og ikke endret av uatoriserte. Slik støttes datautentisering og dataintegritet. I denne fasen blir det både spesifisert policyer, og autentikatorene for betalingsaktiviteter (de riktige kryptografiske nøklene) blir levert til de riktige aktørene (betalingsnettverket). Denne spesifiseringen av betalingsnettverket er ressurseieren sin autorisering av brukeren ved å spesifisere tilgangspolicy og -regler i PAP, og med det er også første del av tilgangshåndteringens konfigureringsfase over.

Da kan Apple starte med det neste trinnet i identitetshåndteringens konfigureringsfase, som er å klargjøre autentikatorer og utlevere dem til brukeren. Før autentiseringstjeneren kan starte med å klargjøre autentikatorer for kortet, må Apple Pay aller først utføre identifisering av det oppgitte betalingskortet. Dette er nødvendig for å støtte konfidensialitet og integritet, og forhindre svindel. Derfor blir den krypterte betalingskortinformasjonen sendt som en datapakke fra Apple-tjeneren til kortutstederen, f.eks. banken (Apple, 2021). Kortutstenderen sjekker om dataene stemmer. Dersom alt er korrekt, blir de bekreftet autentiske. Da kan Apple Pay starte med den delen i konfigureringsfasen, som er å klargjøre autentikatorer for det bestemte kortet. Betalingsnettverket, kortutstederen, eller banken oppretter et spesifikt kontonummer, som skal brukes av den bestemte enheten. Det nye spesifikke kontonummeret blir kryptert og sendt av kortutsteder til Apple Pay. Det er dette spesifikke kontonummeret, og ikke det originale kortnummeret, som blir lagret i Apple Pay som en kortidentitet. Sammen med den krypterte dataen, blir det også sendt andre data, som f.eks. en genereringsnøkkel som blir brukt til å generere unike sikkerhetskoder (private asymmetrisk nøkler) for hver transaksjon (Apple, 2021). Det betyr at hver nøkkel skal brukes til kun en anvendelse. Dette er autentikatorene som har blitt utlevert til brukeren.

Det spesifikke kortnummeret, som ble laget av banken, kan ikke dekrypteres av Apple. Den blir lagret på enheten din i «Secure Element», som fungerer som en sertifisert, bransjestandardisert brikke for sikker lagring av betalingsinformasjon i Apple (Apple, 2021). Kontonummeret er isolert fra alle Apple tjenester, som iOS, Apple Watch, iCloud osv. Dette, for at andre nettverk og systemer i Apple ikke får tilgang til det isolerte kontonummeret. På denne måten vil ikke eventuelle sårbarheter i andre systemer kunne være potensielle trusler for enheten der Apple Pay er aktiv, og de vil ikke kunne misbrukes for uatentiserte aktiviteter i Apple Pay. Slik har Apple ikke tilgang eller lagring av de opprinnelige kortnumrene.

Tilgangshåndteringens andre trinn iverksettes når brukeren forespør en betaling, uansett om det gjelder for nettbutikker, applikasjoner, betalingsterminaler og NFC, eller overføring til en annen person. For alle disse forespørslene vil Apple Pay kreve en autentisering. Autentiseringen som kreves er Face ID og Touch ID. For Apple Watch skjer bekreftelsen for betalinger gjennom en dobbeltklikk på sideknappene, eller trykk på skjermen, avhengig av modell (Apple, 2021).

Informasjonsdeling og -beskyttelse

«Secure Element» kjører Java Card-plattformen og oppfyller finansbransjens krav til elektroniske betalinger. «Secure Element»-IC-en og Java-Card-plattformen er sertifisert i samsvar med EMVCos prosess for sikkerhetsevaluering (Apple, 2021). Etter utført sikkerhetsevaluering, utstedes en unik IC og et unikt plattformsertifikat av EMVCo.

Apple Pay bruker ulike metoder for de ulike betalingsfunksjonene sine. I fysiske butikker brukes det NFC-teknologi (Near Field Communication) mellom enheten og bankterminalen for betalinger. Overføringen av informasjon mellom enheten og bankterminalen krever at brukeren skal autentisere seg, enten ved sikkerhetskode, FaceID eller TouchID. Når det blir verifisert, vil «Secure Element» oppgi det spesifikke kontonummeret, og en unik dynamisk sikkerhetskode fra genereringsnøkkelen, i tillegg til annen nødvendig informasjon for gjennomføring av transaksjonen (Apple, 2021). Da vil kortutstederen eller betalingsnettverket måtte bekrefte betalingsinformasjonen, ved å sjekke den dynamiske sikkerhetskoden, for at betalingen skal kunne godkjennes. På denne måten vil verken Apple Pay eller enheten aldri trenge å oppgi den originale kortinformasjonen.

NFC-betalinger foretar en NFC-kontroll, som håndterer Near Field Communication-protokoller. På bakgrunn av disse protokollene, blir informasjon kommunisert mellom Secure Element og applikasjonsprosessoren, og mellom Secure Element og terminalen på utsalgsstedet (Apple, 2021).

Betaling med Apple Pay over internett eller i apper, starter med at Appel Pay mottar de krypterte transaksjonsopplysningene. Betalingen forespør brukeren om en godkjenning gjennom en melding på enheten. Brukeren må bekrefte kjøpet, gjennom å autentisere seg med FaceID eller TouchID. Dette gjøres for å sikre en trygg behandling av betalingsinformasjonen før den sendes videre til utvikleren eller betalingsbehandleren. Krypteringsnøkler sikrer at kun den bestemte appen eller nettsiden som du betaler til, får tilgang til den krypterte betalingsinformasjonen din. I tillegg må nettsteder som tilbyr Apple Pay som en betalingsalternativ verifisere domenene sine hver gang. Betalingsinformasjonen blir sendt til betalingsnettverket eller kortutstederen, som igjen må bekrefte informasjonens autentisitet, for at betalingen skal godkjennes (Apple, 2021). Slik blir den opprinnelige kortinformasjonen igjen beholdt hemmelig. Gjennom dette opprettholdes det både konfidensialitet og integritet. Dessuten krever Apple Pay av nettsteder og apper som bruker den, at de har bestemte retningslinjer for personvern som begrenser deres bruk av dataen.

Trusler

Dersom man mister enhet der Apple Pay er aktivert, har man flere valgmuligheter. Hvis «Finn iPhone» er aktivert, kan man bare sette enheten i «mistet modus», som gjør at kortene blir stoppet til mistet modus blir fjernet igjen (Apple, 2021). Da kan brukeren slippe arbeidet med å legge inn kortene på nytt, når vedkommende finner enheten sin. En annen løsning er å gå til sin Apple ID-konto fra en annen enhet, og derifra slette historikk for alle betalingene utført gjennom Apple Pay. Dette vil bli utført, selv om den mistede enheten ikke er koblet til internett for øyeblikket. I tillegg kan sperringen av kart og Apple Pay skje, ved at det ringes til kortutstederen eller banken og kreve sperring av Apple Pay sin tilgang til kortene som er lagt inn. Dette er preventive tiltak som skal hindre i at hendelser inntreffer når enheten ligger i feil hender og eieren ikke har direkte tilgang til sin enhet. Likevel kan eieren ha kontroll over den på denne måten, og hindre uautorisert bruk av enheten sin. Slik blir konfidensialitet og integritet bevart.

Sammenligning

Både Vipps og Apple Pay har utviklet tiltak for å støtte KIT-sikkerhetsmålene, slik at deres tjenester skal kunne sørge for konfidensialitet, integritet og tilgjengelighet for sine brukere og deres personopplysninger. Men er de implementerte tiltakene sikre nok? I denne delen skal vi drøfte det, og sammenligne sikkerhetstiltak-valget og -bruken til Vipps og Apple Pay. Vi skal se på fordeler og ulemper ved prosessene deres for identitetshåndtering og tilgangshåndtering, både for konfigureringsfasen og bruksfasen.

Registrering i både Apple Pay og Vipps krever en tofaktor-autentisering for en høyere sikkerhet. For Vipps gjelder dette ved brukerregistrering, mens for Apple Pay gjelder det kun ved kortregistrering, fordi Apple Pay trenger ikke å registrere nye brukere (som forklart i IAM – identitets- og tilgangshåndtering i Apple Pay på side 13). Siden registreringsprosessen er utført ved Apple ID, ved registreringen av en ny enhet, da er man allerede identifisert og autentisert gjennom Apple ID (Apple, 2021). I dette tilfellet er Apple både ressurseier og autentiseringstjener. Slik kan Apple Pay hoppe over konfigureringsfasen for brukerregistrering i Apple Pay, mens registreringsprosessen i Vipps utføres med BankID hver gang man skal registrere seg på Vipps.

Ved innlogging krever Vipps enkel autentisering gjennom kun en faktor, FaceID, TouchID eller PIN-kode, som nevnt lenger opp. Dette gjør tjenesten lettere tilgjengelig for brukerne, når de ønsker å bruke den på dagligbasis. Dette har de vurdert som sikkert, i og med, at det kreves en tofaktorautentisering ved registrering, som skal sikre en riktig brukerregistrering, og også fordi autentisering kreves ved overføringstransaksjoner, som forklart i neste avsnitt.

Når det kommer til det å utføre betalinger, har de likheten om at begge tjenestene krever kun enfaktorautentisering gjennom FaceID, TouchID eller PIN-kode. Likevel er det et skille, når det kommer til høyere beløper, fordi Vipps har vurdert, at høyere beløp enn 5000kr trenger en tofaktorautentisering gjennom en dynamisk generert kode fra BankID i tillegg til FaceID, TouchID eller PIN-kode. Gjennom dette sikkerhetstiltaket, oppnår Vipps en bedre beskyttelse av integriteten og konfidensialiteten for brukernes bankkontoer.

Beskyttelsen av personopplysningene skjer på to ulike måter i de to mobilbetalingsløsningene. Apple Pay har noe som heter Secure Element for å håndtere kort- og betalingsopplysningene. Secure Element har funksjonen av en sertifisert og bransjestandartisert brikke, der betalingsinformasjon kan lagres sikkert i Apple. (Dypere beskrivelse av Secure Element står i «informasjonsdeling og -beskyttelse» på side 15-16.)

Bruk av Secure Element i Apple Pay gir en veldig god beskyttelse for opplysningenes konfidensialitet og integritet, samtidig som den støtter tilgjengelighet. Alle opplysninger om kortinformasjonen lagres kun i Secure Element. Apple-tjeneren kommuniserer med kortutstederen, for at kortutstederen skal spesifisere et nytt kortnummer og sende den kryptert tilbake til Apple-tjeneren. Sammen med det spesifikke kortnummeret, sender kortutstederen også en unik genereringsnøkkel. Kommunikasjonen mellom Apple-tjeneren og kortutstederen skjer gjennom kryptering i TLS-protokoller. Det nye spesifikke nummeret lagres i Secure Element på enheten.

Som vi allerede forklarte, er Secure Element isolert av alle andre Apple tjenester, som for eksempel iOS, Apple Watch, iCloud, slik at ingen andre kan ha tilgang til informasjonen lagret i Secure Element. Secure Element har da ansvaret for å kommunisere den lagrede informasjonen til de autoriserte entitetene, f.eks. ved transaksjonsaktiviteter. Dette gjør den ved å følge de spesifiserte policyene og reglene, slik at informasjonen blir sendt kun til entiteter med riktige krypteringsnøkler.

Den sterke konfidensialiteten skyldes i hovedsaken tre faktorer: 1.kortnummeret er ikke lagret i sin originale tilstand, men som et nytt spesifisert kortnummer,

2. det spesifikke kortnummeret er lagret i Secure Element, som jo er isolert fra alle andre tjenester,

3. selv Appel-tjeneren klarer ikke å dekryptere dataen som kortutstederen sender for lagring i Secure Element

På denne måten bidrar Secure Element til å bevare en streng konfidensialitet for kort- og betalingsopplysningene i Apple Pay, noe som gjør tjenesten utrolig sikker. Uautoriserte kan ikke få tilgang til informasjonen og ressursene, verken ved tilsiktede eller utilsiktede trusler.

Vipps lagrer all informasjonen relatert til brukerprofilen i sin database. Det inkluderer kortinformasjonen, den statiske autentikatoren (PIN-koden), enhetens mobilidentifikator og operativsystem osv. Derfor kan vi si, at sikkerhetstiltakene som Apple Pay har innført for lagring av informasjon er sterkere enn de til Vipps.

Vipps sin lagring av alle disse dataene i sine databaser, kan utgjøre en sårbarhet for informasjonen. Da vil faren være større ved en eventuell hendelse, som for eksempel at en trusselaktør kommer seg inn i vipps sine databaser, da vil trusselaktøren ha tilgang til flere brukerkontoer og -opplysninger. Apple Pay har unngått denne sårbarheten, ved at sensitive data, som f.eks kortnummer og genereringsnummer, lagres i Secure Element. Siden Secure Element er selvstendig og isolert, vil ikke en trusselaktør som klarer å bryte seg inn i Secure Element klare å få innsyn i de sensitive dataene for andre brukere.

Dessuten, er det slik at de innebygde sikkerhetsfunksjonene (som vi forklarte tidligere i teksten), som f.eks kryptering, i Apple-tjeneren, gjør det nesten umulig for uautoriserte å komme seg inn til Secure Element. Dermed gir det en sterkere konfidensialitet.

Likevel har Vipps ivaretatt sikkerheten av personopplysningene og dataene gjennom sine tiltak, i samsvar med personopplysningsloven (BankAxept, 2018). Vipps har dokumentert rutiner og tiltak som skal sikre konfidensialiteten, integriteten og tilgjengeligheten av personopplysningene, i henhold til GDPR artikkel 32 (Vipps 2020). I tillegg er det slik, at Vipps lagrer kun informasjon du oppgir til appen, kun basert på samtykket som du som bruker gir. «All behandling av Vipps' behandling av brukernes personopplysninger må ha et rettslig behandlingsgrunnlag for å kunne være lovlig» (Vipps 2020).

Vipps' deling av personopplysninger med andre organisasjoner, er veldig interessant å se på. Vipps kan nemlig foreta en deling av informasjonen tilknyttet til brukeren med andre organisasjoner. Dette gjøres med formålet om, at andre tjenester skal kunne persontilpasse det

de tilbyr brukerne, for en bedre brukeropplevelse, og en mer effektiv markedsføring. Dette gjøres gjennom overføring av informasjonskapsler. Det foregår en sjekk av informasjonskapslenes integritet før de sendes, slik at det kan være sikkert at de ikke er endret uautorisert. Dessuten er det slik, at Vipps kan utføre denne typen informasjonsdeling, kun ved samtykke av brukeren. Informasjonsdelingen skjer akkurat på den måten som ble spesifisert i samtykket. Derfor er informasjonsdelingen ganske sikker. Brukeren har også lov til å trekke samtykket sitt når som helst. Da vil Vipps slutte å dele informasjonen med de bestemte organisasjonene, som forklart tidligere.

Samtidig finnes det noen sårbarheter. Et eksempel på det er når Vipps slutter å dele informasjon. Informasjon som tidligere ble delt av Vipps til andre organisasjoner, lagres som oftest i organisasjonenes databaser. Selv ved stopp av informasjonsdelingen, vil den allerede registrerte informasjonen bli beholdt hos den andre organisasjonen, som forklart tidligere i teksten. Dette gjelder også når Vipps applikasjonen blir slettet fra mobilenheten. Likevel er det slik at personopplysninger som er lagret hos andre organisasjoner er uten beskyttelse. Når en organisasjon mottar personopplysninger, er de selv ansvarlige for at bruk av disse skal være i samsvar med personopplysningsloven.

Videre, når det gjelder transaksjonene, skjer de på følgende måte.

I betalingsterminaler, fungerer Apple Pay gjennom mobiltelefon-enheter eller Apple Watch-enheter. Det skjer gjennom NFC-teknologi. Ved betalinger vil en betalingsforespørsel komme opp på enheten og kreve bekreftelse for å utføres. Brukeren bekrefter forespørselen ved å autentisere seg gjennom FaceID eller TouchID. Måten enheten og bankterminalen kommuniserer på er gjennom NFC-teknologien. Teknologien foretar en kontroll med Near Field Communication-protokoller. På bakgrunn av disse protokollene, blir informasjon kommunisert mellom Secure Element og applikasjonsprosessoren, og mellom Secure Element og terminalen på utsalgsstedet.

Vipps støtter ikke NFC. I stedet utføres betalinger ved betalingsterminaler gjennom skanning av en QR-kode i betalingsterminalen. Da får brukeren opp en push-melding på mobilenheten, som brukeren trenger å bekrefte for å fullføre betalingen. Også her blir bekreftelsen etterfulgt av autentisering gjennom FaceID, TouchID eller PIN-kode.

Til motsetning av Apple Pay, har Vipps valgt å lagre transaksjonene i appen, som et tiltak som støtter sporbarhet. «sporbarhet er basert på logging av aktiviteter i systemer og nettverk, og kartlegger hvilken bruker eller annen entitet som står bak hver logget aktivitet» (Jøsang,

2021, s.27). Dette tiltaket har de også innført som følge av krav fra regelverket for hvitvasking og krav til dokumentasjon ifølge bokføringsloven (BankAxept, 2018). Ved å ha transaksjonslogg, kan aktiviteter knyttes til entiteten som har utført dem. Slik er det alltid klart hvem som skal stå for regnskap til hver eneste aktivitet, og hendelser kan spores. Derfor vil det være nyttig både for privatbrukere og organisasjoner.

Dersom en bruker oppdager transaksjoner i transaksjonsloggen som ikke er utført av dem selv, vil brukeren kunne varsle dette til Vipps eller banken sin. Da kan de for eksempel sperre betalingskortet eller Vipps-brukerkontoen, og foreta en prosess for å finne ut trusselaktøren som står bak handlingen. Dette ville ikke ha vært mulig å oppdage uten en slik transaksjonslogg, fordi da ville verken Vipps eller brukeren ha hatt innsyn i aktivitetene.

Andre aktiviteter og data, som for eksempel «Vipps Logg inn»-bruk, blir også registrert og lagret. Hva disse dataene omfatter, hva slags krav som er satt for dem, og hvordan de behandlet, er forklart i «Informasjonsdeling og -beskyttelse» på side 11.

I og med at Appel Pay ikke har en slik logg av transaksjoner, som kan knyttes tilbake til identiteter som har utført dem, vil de ikke være i stand til å oppdage uvanlig atferd og detektere avvik. Dermed mangler Apple Pay dette tiltaket for sporbarhet.

Som nevnt lenger opp i teksten, har Vipps satt to typer grenser for bruk av applikasjonen deres. Den første er en beløpsgrense på 5000kr, der transaksjoner inntil dette beløpet krever en enkelfaktor-autentisering med kun FaceID, TouchID eller PIN-kode. Den andre grensen er for totale årlige transaksjoner. Privatpersoner har lov til å overføre beløp inntil 850 000kr og motta opp til 700 000kr årlig. Bedrifter kan kun motta opp til 650 000kr gjennom Vipps årlig. Dessuten betales det et transaksjonsgebyr for beløp over 5000kr.

Disse grensene øker sikkerheten, og reduserer risikoen for kriminalitet og misbruk, både for privatpersoner og for samfunnsmessige verdier. For privatpersoner er det fint, at det kreves en høyere autentiseringsfunksjon ved transaksjoner av høyere beløp. Slik vil faren for mulig svindel med høy skadepåføring, reduseres, fordi det vil være vanskeligere for uatoriserte entiteter å foreta en eventuell autentisering.

De årlige grensene setter fokus på samfunnssikkerheten. De er innført for å kunne forhindre hendelser som for eksempel hvitvasking, som er i strid med samfunnsordningene.

Håndtering av trusler, skjer på følgende måte. Vipps har tatt ansvar i forhold til den potensielle trusselen phishing-angrep, som beskrevet i avsnittet «Trusler» i Vipps-delen på

side 11. Vipps har tatt stilling til det, og innført et tiltak om sikkerhetslæring. De opplyser nemlig sine brukere i at de aldri vil forespørre om informasjon, og spesielt personopplysninger, gjennom medier som kan brukes i phishing-angrep, nemlig SMS og e-post. Dette sier de klart og tydelig, slik at deres brukere kan vite, at dersom de får slike meldinger, så er det definitivt en trusselaktør som står bak, og ikke Vipps.

Apple Pay mangler denne typen sikkerhetslæring angående phishing-angrep. Dermed er deres system mer sårbart for phishing-angrep. Derfor er brukere av Apple Pay, muligens mer utsatte for den type angrep enn brukere av Vipps.

Vipps driver med sikkerhetslæring, også når de opplyser brukerne sine om hva de skal gjøre dersom de mister sin enhet der Vipps er aktivert. Apple Pay foretar også sikkerhetslæring, når det gjelder i å opplyse brukerne sine om måter de bør gå frem på, dersom de mister en enhet der Apple Pay er aktivt.

Apple Pay er en kontaktløs betaling som fungerer i betalingsterminaler i en stor mengde av apper, butikker og nettbutikker. Det vil si at dette er en global løsning med en stor utbredelse som kan benyttes i utvalgte land og regioner, både i utlandet og innlandet (Apple, 2020). Dersom de fleste bankene i verden støtter mobilbetaling, kan denne betalingsløsningen bli et godt alternativ for de som reiser mye.

Apple Pay er kompatibelt med et bredere utvalg av enheter enn Vipps, som for eksempel betaling med iWatch. Mange konsumenter opterer for Apple Pay i stedet for Vipps fordi Apple Pay viser seg å fungere raskere og tilbyr en sikrere betaling. Dersom Apple Pay krever bare fingeravtrykks- eller ansiktsgjenkjenning for å godta betalingen, trenger man ikke å taste inn PIN-koden. I tillegg er kort- og kontoopplysningene skjult for mottakeren.

Både Vipps og Apple Pay har noen områder der de tar i bruk sterkere tiltak enn det den andre bedriften gjør. Samtidig har de noen tilleggstiltak som skal kompensere for mangler i andre tiltak. I og med, at begge selskapene forankrer sine valg i GDPR personlovverket, kan vi se på begge dem som selskap som bevarer KIT-sikkerhetsmålene for sine brukere og deres informasjon. Hvilken av selskapene som gjør det best mulig, kommer an på hva slags verdier brukeren har, og hvilke verdier brukeren ønsker å ivareta mest.

Sammendrag

Vipps og Apple Pay er to betalingsløsninger, utviklet av to ulike selskap i to ulike land. Vipps brukes foreløpig kun mellom norske innbyggere registrert i Folkeregisteret, mens Apple Pay har forutsetningen, at den kan brukes gjennom enheter med iOS-operativsystemer, og derfor kan Apple Pay brukes på tvers av landegrenser. Likevel kan ikke noen funksjonaliteter av Apple Pay, som for eksempel å pengeoverføring via Apple Cash og SMS, brukes utenfor USA.

For å kunne foreta en sammenligning av de to mobilbetalingstjenestene, avklarte vi aller først hva vi mener med ulike begreper relatert til informasjonssikkerhet, og definerte hvordan vi skal bruke dem videre i teksten.

Vi har sett på hvordan de to betalingsløsningene fungerer hver for seg. Det innebærer funksjonalitet av tjenester de tilbyr, identitets- og tilgangshåndtering, og bevaring og støtte av sikkerheten av informasjonsregistrene de forvalter. Begge selskapene har utviklet sine tiltak for å støtte sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet. Noen av tiltakene de har utviklet ligner på hverandre, mens andre skiller seg fra hverandre ved ulike trekk, forvaltningsmetoder og funksjonalitet. I tillegg tok vi for oss noen mulige sårbarheter og trusler for de ulike tjenestene, og forklarte hvordan selskapene var valgt å håndtere disse.

Til slutt sammenlignet vi bruken av de ulike tiltakene hos de to betalingstjenestene, ved å se på fordeler og ulemper, og sette dem mot hverandre. I denne delen delte vi også våre meninger, tanker, antakelser og konklusjoner.

Vi konkluderte med, at begge betalingsløsningene har sine fordeler og noen funksjonaliteter som muligens åpner for potensielle sårbarheter og trusler. Begge tjenestene er utviklet ved å ta hensyn til det å ivareta sikkerheten av personopplysningene de bruker etter lover og regler i personvernlovverket GDPR. Både Vipps og Apple Pay har noen tiltak som muligens er bedre enn samsvarende tiltak det andre selskapet bruker. Likevel kommer det an på hva organisasjonen har som verdier, hva de trenger å ta hensyn til, og hvordan de kompenserer med andre tiltak for noe et tiltak mangler. Derfor vil det ikke være helt riktig å fastsette, at den ene løsningen er nødvendigvis bedre enn den andre. Det er det hver eneste bruker som avgjør for seg selv, men da er det viktig å ta beslutningen ut ifra hva brukeren har som verdier.

Referanser:

Wikipedia (2021) *ISO/IEC 2700*. Tilgjengelig fra: *https://en.wikipedia.org/wiki/ISO/IEC_27000* (Hentet: 12. oktober 2021).

Jøsang, A. (2021*), Informasjonssikkerhet.* Oslo: Universitetsforlaget

(Det Norske Akademi for Språk og Litteratur (2021) *Autentisitet*. Tilgjengelig fra: https://naob.no/ordbok/autentisitet (Hentet: 12. oktober 2021)

Fornyings- og administrasjonsdepartementet/Kommunal- og moderniseringsdepartementet/Regjeringen (2008) *Rammeverk for autentisering og uavviselighet i elektronisk kommuni8kasjon med og i offentlig sektor*. Tilgjengelig fra: https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/ , https://eid.difi.no/nb/esignering/ord-og-begrep (Hentet: 12. oktober 2021)

BankAxept (2018) *Personvernerklæring – BankAxept*. Tilgjengelig fra: https://bankaxept.no/om-oss/ (Hentet: 1. november 2021).

Eika (2021) *Vil etablere Nordens ledende betalings- og identifiseringsaktør.* Tilgjengelig fra: https://www2.eika.no/aktuelt/ny-betalings-og-identifiseringssamarbeid (Hentet: 2. november 2021).

Nysveen, E. og E24 (2017) *Over 100 banker går sammen om Vipps*. Tilgjengelig fra: https://e24.no/boers-og-finans/i/a2RoxA/over-100-banker-gaar-sammen-om-vipps (Hentet: 20. oktober 2021)

Wikipedia (2021) *Vipps*. Tilgjengelig fra: https://no.wikipedia.org/wiki/Vipps (Hentet: 20. oktober 2021)

BankID (2021). *HVA ER BANKID?* Tilgjengelig fra: https://www.bankid.no/privat/los-mitt-bankid-problem/ofte-stilte-sporsmal/generelt-om-bankid/hva-er-bankid/ (Hentet: 20. oktober 2021)

Vipps (2020) *Vilkår for Vipps privat versjon 1.21*. Tilgjengelig fra: https://vipps.no/vilkar/vilkar-privat/ (Hentet: 20. oktober 2021)

Vipps (2021) *Banker med Vipps i terminal*. Tilgjengelig fra: https://www.vipps.no/produkter-og-tjenester/privat/vipps-i-terminal/vipps-i-terminal/banker-med-vipps-i-terminal/ (Hentet: 20. oktober 2021).

Vipps (2020) *Vilkår for Vipps privat versjon 1.21/ 3.2 Registrering, identifisering og beløpsgrenser.* Tilgjengelig fra: https://vipps.no/vilkar/vilkar-privat/ (Hentet: 21. oktober 2021).

Vipps (2020) *Personvernerklæring Vipps/ Versjon 1.10/Hvilken informasjon lagrer vi.* Tilgjengelig fra: https://www.vipps.no/vilkar/cookie-og-personvern/ (Hentet: 21. oktober 2021).

Vipps (2020) *Personvernerklæring Vipps/ Versjon 1.10/2.4 Samtykke.* Tilgjengelig fra: https://www.vipps.no/vilkar/cookie-og-personvern/ (Hentet: 21. oktober 2021).

Vipps (2021) *Mange bruker Vipps for enkel og trygg innsjekk på serveringssteder.* Tilgjengelig fra: https://www.vipps.no/om-oss/nyheter/mange-bruker-vipps-for-enkel-og-trygg-innsjekk-pa-serveringsteder/ (Hentet: 30. oktober 2021).

Nettvett (2021) *Slik administrer du informasjonskapsler*. Tilgjengelig fra: https://nettvett.no/slik-administrer-du-informasjonskapsler/ (Hentet: 21. oktober 2021).

Vipps (2020) *Vilkår for Vipps privat versjon 1.21/3.4.3 Informasjonssikkerhet og gjenkjenningsteknologi i forbindelse med Vipps Logg inn.* Tilgjengelig fra: https://www.vipps.no/vilkar/vilkar-privat/ (Hentet: 23. oktober 2021).

Wikipedia (2020) *Apple Pay*. Tilgjengelig fra: https://no.wikipedia.org/wiki/Apple_Pay (Hentet: 25. oktober 2021).

Wikipedia (2018) *Apple Wallet*. Tilgjengelig fra: https://no.wikipedia.org/wiki/Apple_Wallet (Hentet: 25. oktober 2021).

Apple (2021) *Make purchases using Apple Pay*. Tilgjengelig fra: https://support.apple.com/en-us/HT201239#stores (Hentet: 25. oktober 2021).

Apple (2021) *Make purchases using Apple Pay/ How to pay using Apple Pay in stores and other places*. Tilgjengelig fra: https://support.apple.com/en-us/HT201239#stores (Hentet: 25. oktober 2021).

Apple (2021) *Apple Cash*. Tilgjengelig fra: https://www.apple.com/apple-cash/ (Hentet: 24. oktober 2021).

Apple (2021) *Oversikt over sikkerhet og personvern for Apple Pay/ Når du legger til kreditt- eller debetkort, forhåndsbetalte kort eller reisekort*. Tilgjengelig fra: https://support.apple.com/no-no/HT203027 (Hentet: 25. oktober 2021).

GreenDotBank/AppleCash (2017) *Green Dot Bank Privacy Policy.* Tilgjengelig fra: https://applecash.greendot.com/privacy/ (Hentet: 26. oktober 2021).

Apple (2021) *Administrer tofaktorautentisering for Apple-ID-en din på iPhone*. Tilgjengelig fra: https://support.apple.com/no-no/guide/iphone/iphd709a3c46/ios (Hentet: 25. oktober 2021).

Apple (2021) *Logg på med Apple-ID*. Tilgjengelig fra: https://support.apple.com/no-no/HT204053 (Hentet: 25. oktober 2021).

Apple (2021) *When you add credit, debit, prepaid, or transit cards*. Tilgjengelig fra: https://support.apple.com/en-us/HT203027 (Hentet: 25.oktober 2021).

Apple (2021) *Sikkerhet for Apple Pay-komponenter/Secure Element*. Tilgjengelig fra: https://support.apple.com/no-no/guide/security/sec2561eb018/web (Hentet: 25. oktober 2021).

Apple (2021) *Apple Pay-tjenere*. Tilgjengelig fra: https://support.apple.com/no-no/guide/security/sec2561eb018/web (Hentet: 25. oktober 2021).

Apple (2021) *NFC-kontroller*. Tilgjengelig fra: https://support.apple.com/no-no/guide/security/sec2561eb018/web (Hentet: 26. oktober 2021).

Apple (2021) *Kontaktløse kort i Apple Pay*. Tilgjengelig fra: https://support.apple.com/no-no/guide/security/secbd55491ad/1/web/1 (Hentet: 26. oktober 2021).

Apple (2021) *Sikring av kjøp med ApplePay*. Tilgjengelig fra: https://support.apple.com/no-no/guide/security/secc5227ff3c/1/web/1 (Hentet: 26. oktober 2021).

Apple (2021) *Hvis en iPhone, iPad eller iPod touch blir mistet eller stjålet.* Tilgjengelig fra: https://support.apple.com/no-no/HT201472 (Hentet: 24. oktober 2021).

Apple (2021) *Hvis du skal bytte til en ny enhet*. Tilgjengelig fra: https://support.apple.com/no-no/HT202033 (Hentet: 27. oktober 2021).

BankAxept (2018) *Personvernerklæring – BankAxept*. Tilgjengelig fra: https://bankaxept.no/om-oss/ (Hentet: 1. november 2021).

Apple (2021) *Land og regioner som støtter Apple Pay*. Tilgjengelig fra: https://support.apple.com/no-no/HT207957 (Hentet: 26. oktober 2021).